Rigorous Security Proofs for Practical Quantum Key Distribution

by

Devashish Tupkary

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2026

© Devashish Tupkary 2026

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Marco Tomamichel Professor, Dept. of Electrical and Computer Engineering, National University of Singapore
Supervisor(s):	Norbert Lütkenhaus Professor, Dept. of Physics and Astronomy, University of Waterloo
Internal Member:	Kevin Resch Professor, Dept. of Physics and Astronomy, University of Waterloo
Internal-External Member:	Graeme Smith Associate Professor, Dept. of Applied Mathematics, University of Waterloo
Other Member(s):	Michele Mosca Professor, Deparment of Combinatorics & Optimization, University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

This thesis is based on the following works, of which I am first author:

- Ref. [1] (Chapter 4) : Devashish Tupkary, Ernest Y.-Z. Tan, and Norbert Lütkenhaus. *Security proof for variable-length quantum key distribution.* Phys. Rev. Research 6, 023002, April 2024.
- Ref. [2] (Chapter 6) : Devashish Tupkary, Shlok Nahar, Pulkit Sinha, and Norbert Lütkenhaus. *Phase error rate estimation in QKD with imperfect detectors.* Quantum 9, 1937, December 2025.
- Ref. [3] (Chapter 7) : Devashish Tupkary, Shlok Nahar, Amir Arqand, Ernest Y.-Z Tan, and Norbert Lütkenhaus. *A rigorous and complete security proof of decoy-state BB84 quantum key distribution.* arXiv, January 2026.
- Ref. [4] (Chapter 8) : Devashish Tupkary, Shlok Nahar, and Ernest Y.-Z. Tan. *Authentication in Security Proofs for Quantum Key Distribution.* arXiv, January 2026.

This thesis is also based on the following works, of which I am second author:

- Ref. [5] (Chapter 5) : Shlok Nahar, Devashish Tupkary, Yuming Zhao, Norbert Lütkenhaus, and Ernest Y.-Z. Tan. *Postselection Technique for Optical Quantum Key Distribution with Improved de Finetti Reductions.* PRX Quantum 5, 040315, October 2024. Shlok Nahar is primarily responsible for the de Finetti reductions, and incorporating optics in the postselection technique. I, along with Ernest Y.-Z. Tan, am responsible for the rigorous application of the postselection technique to QKD security analysis.
- Ref. [6] (Chapters 4 and 5) : Lars Kamin, Devashish Tupkary, and Norbert Lütkenhaus. *Improved finite-size effects in QKD protocols with applications to decoy-state QKD.* arXiv, February 2025. Lars Kamin is responsible for the finite-size analysis of decoy-state protocols. I am responsible for adapting those methods to variable-length protocols.

This thesis also adapts small portions of Ref. [7], of which I am first author.

This thesis uses code written as a part of the Open QKD Security software package [8]. It also uses additional code written by Lars Kamin, John Burniston, and Shlok Nahar

for specific publications. In particular, the code used for plots in Chapter 7 was entirely written by Lars Kamin and John Burniston as a part of the work Ref. [9], in which I was not involved. The code used for the decoy-state plots in Chapters 4 and 5 was mostly written by Lars Kamin as a part of Ref. [6]. The code used for plots in Chapter 6 was written collaboratively by the author and Shlok Nahar.

Abstract

This thesis is concerned with the rigorous security analysis of practical Quantum Key Distribution (QKD) protocols, using a variety of modern proof techniques. Throughout, the emphasis is on mathematical rigor across a wide range of security proof frameworks.

We begin by presenting a security proof for variable-length QKD protocols against IID collective attacks, which represents the first such result for generic QKD protocols. We then show that this analysis can be lifted to hold against coherent attacks by an adversary, using the postselection technique. In doing so, we extend the application of the postselection technique to practical QKD protocols, and resolve a long-standing flaw in the method, thereby placing its application to QKD on a rigorous mathematical footing.

We next study security proofs based on entropic uncertainty relations. These proofs proceed by bounding the so-called "phase error rate", using the observed statistics available in the actual protocol. All known methods of bounding the phase error rate require strong assumptions on hardware: namely, that all detectors have exactly equal probability of detection. This renders these security analysis inapplicable to practical QKD scenarios. We show that such phase error rates can be bounded even when detectors are imperfect and only approximately characterized. This resolves a long-standing well-known open problem of nearly two decades, and renders this proof technique applicable to realistic scenarios.

We then study security proofs using the recently obtained marginal-constrained entropy accumulation theorem, and obtain a highly rigorous and general result for the security analysis for practical QKD protocols. Most importantly, the proof is constructed in a transparent and self-contained manner, and is designed to be a key ingredient in certification efforts for QKD. Moreover, it can be easily modified to apply to other protocols of interest, and to device imperfections and side-channels.

We also revisit the assumptions on authentication traditionally made in QKD security analyses, which assume that all classical messages are delivered faithfully and on time, without any aborts. We show that these assumptions are generally unrealistic, and that adopting realistic authentication assumptions necessitates a modification of both the standard QKD security definition and the corresponding security analysis. However, under mild and easily satisfied protocol design conditions, security under realistic authentication can be reduced to the usual idealized setting. As a result, existing QKD security proofs can be lifted to the realistic authentication setting with only a minor protocol modification.

A distinctive feature of this thesis is its unified presentation of multiple major QKD security proof frameworks using consistent protocol descriptions and notation. This first-of-its-kind treatment enables direct comparison and contrast between different approaches,

a perspective that is often obscured when these techniques are developed in isolation. Consequently, this work is intended not only as a collection of new technical results, but also as a pedagogical reference for understanding rigorous security analysis in quantum key distribution.

Acknowledgements

It is difficult to find the right words to describe the contributions of my supervisor, Norbert Lütkenhaus, to this thesis. Throughout my time at IQC, he has been unfailingly supportive of my work, always generous with his time despite an exceptionally busy schedule, and an exemplary mentor in every sense. I invariably left his office in better spirits than when I entered. Perhaps the highest praise I can offer is that my years in graduate school have been among the most fulfilling and rewarding years of my life, and this is due in large part to his guidance and mentorship. If I am ever in the position to advise graduate students of my own, I will strive to emulate his approach as closely as I can.

This thesis owes an enormous debt to Ernest Y. Z. Tan. Ernest is not merely competent, but *scarily* so - the kind of competence that made one wonder how anyone gets there in the first place. A proof that passed Ernest's scrutiny had a genuinely negligible probability of being flawed. Almost everything I know about information theory, along with a substantial portion of the technical skills utilized in this thesis, I owe to him. Our discussions were always immensely valuable, and he had an uncanny ability to identify subtle issues long before they became apparent to others - a feature I exploited often in my work.

Another person who deserves special mention is Shlok Nahar, who has the distinction[1] of being my single biggest collaborator during my PhD. Shlok contributed to nearly all of the work I did throughout graduate school; more importantly, he and I contributed in complementary ways, and at times with wildly different intuitions and perspectives. We got into disagreements on a weekly basis, and their resolution typically left both of us slightly wiser. I am deeply grateful to have had him as a collaborator.

Overall, this thesis benefited greatly from being part of the OQCT group, which has a remarkably strong, vibrant, and intellectually generous community. I am especially grateful to Zhiyao Wang, Aodhán Corrigan, Jerome Wiesseman, John Burniston, Lars Kamin, Amir Arqand, and Florian Kanitschar, with whom I had numerous discussions that shaped my thinking in both direct and subtle ways. In particular, Lars Kamin and John Burniston wrote a substantial body of open source code that is utilized in this thesis. I am also very grateful to Guillermo Currás-Lorenzo, Margarida Pereira, and Victor Zapatero for valuable discussions and fruitful collaborations.

I would like to thank my PhD advisory committee members: Professor Thomas Jennewein, Professor Michele Mosca, Professor Graeme Smith and my supervisor for giving helpful feedback and time towards my research progress. I would also like to thank the

[1] It is perhaps debatable whether this truly counts as a distinction.

members of my PhD examination committee for their time and effort in reading this thesis and for serving on the examining committee.

I would also like to thank Michele Roche and Chin Lee for being exceptionally efficient organizers and for handling a a large variety of bureaucratic tasks. Once they told me they would take care of something, I felt genuinely free to delete that task from my brain.

Finally, I would like to thank my family, both back home and the larger one I found here in Waterloo. This family is far too big to name individually, but I would certainly not have had even half as much fun without the countless walks, chai sessions, dinners, trips, and movie nights we shared. I feel incredibly fortunate to have spent these years surrounded by such an amazing group of people.

Dedication

To Aai, Baba, and Tai.

Table of Contents

Examining Committee Membership ii

Author's Declaration iii

Statement of Contributions iv

Abstract vi

Acknowledgements viii

Dedication x

List of Figures xviii

List of Tables xxiii

1 Introduction 1

1.1 Traditional Classical Cryptography 3

1.2 Quantum Computers 4

1.3 Quantum Key Distribution 5

1.4 "PQC vs QKD" 5

1.5 Organization of this thesis 8

1.6 How to read this thesis 10

2 Background **12**
2.1 Quantum Information Theory . . . 12
2.1.1 Quantum States . . . 13
2.1.2 Measurements . . . 15
2.1.3 Quantum Channels . . . 16
2.1.4 Norms and Distances . . . 17
2.2 Entropies and their properties . . . 18
2.2.1 Von Neumann entropy . . . 19
2.2.2 Renyi Entropies . . . 20
2.2.3 Smoothed min Entropies . . . 22
2.3 Quantum Optics . . . 24
2.3.1 Optical modes . . . 25
2.3.2 Detectors . . . 28
2.4 Miscellaneous . . . 31
2.4.1 Numerics . . . 32

3 Basics of Quantum Key Distribution **33**
3.1 Security Definition . . . 35
3.1.1 Performance . . . 38
3.1.2 Secrecy and Correctness . . . 39
3.2 Protocol Description . . . 39
3.2.1 Protocol Variations . . . 43
3.3 BB84 signal states, measurements, announcements and sifting . . . 45
3.3.1 States Sent by Alice . . . 45
3.3.2 Measurements Performed by Bob . . . 47
3.3.3 Public Announcements and Sifting . . . 50
3.3.4 Motivation for decoy-state protocols . . . 51
3.4 Correctness via error-verification . . . 52

3.5 Leftover Hashing Lemma . . . 53
3.5.1 Bounding the entropy in Leftover Hashing Lemma . . . 54
3.6 Practical QKD Toolbox . . . 56
3.6.1 Source-Replacement Schemes . . . 56
3.6.2 Source Maps . . . 59
3.6.3 Squashing Maps . . . 63
3.7 QKD proof techniques . . . 66
3.7.1 Entropic Uncertainty Relations . . . 66
3.7.2 Postselection technique . . . 67
3.7.3 Entropy accumulation based proofs . . . 68
3.7.4 Phase error correction . . . 69

4 Variable-length Quantum Key Distribution 70
4.1 Proving Fixed-Length Security . . . 72
4.2 Proving Variable-length Security . . . 76
4.3 Constructing feasible sets confidence sets . . . 82
4.3.1 Binomial tail probabilities and confidence intervals . . . 83
4.3.2 From binomial distribution to Set constructions . . . 84
4.4 Application to Qubit BB84 . . . 87
4.4.1 Key Rate Plots . . . 89
4.5 Application to Decoy-State BB84 . . . 94
4.6 Variable-length input to privacy amplification . . . 94
4.6.1 Sifting in QKD . . . 95
4.6.2 The problem . . . 96
4.6.3 The solution . . . 97
4.7 Summary and Outlook . . . 99

5 Postselection technique lift to coherent attacks **101**
5.1 De Finetti Reductions . . . 103
5.1.1 A simple de Finetti reduction . . . 104
5.1.2 Improvements . . . 106
5.2 Correct application of De Finetti reductions in QKD . . . 108
5.2.1 Using de Finetti reductions for QKD . . . 108
5.2.2 Reducing Security of QKD protocols to the IID case . . . 112
5.2.3 Improvements from block-diagonal symmetry . . . 117
5.3 Postselection technique for optical protocols . . . 118
5.4 Application to BB84 protocols . . . 121
5.4.1 Recipe . . . 122
5.4.2 Qubit BB84 . . . 123
5.4.3 Decoy-state BB84 . . . 123
5.5 Summary and Outlook . . . 124

6 Entropic Uncertainty Relations and Phase Error Estimation **127**
6.1 Variable length security in EUR . . . 130
6.2 Protocol Description and phase error rates . . . 131
6.2.1 Requirements on phase error estimation . . . 134
6.3 Phase error estimation for BB84 with perfect detectors . . . 137
6.3.1 Protocol Measurements . . . 138
6.3.2 Constructing Equivalent Protocol . . . 139
6.3.3 Sampling . . . 140
6.4 Phase error estimation for BB84 with imperfect detectors . . . 142
6.4.1 Protocol Measurements . . . 143
6.4.2 Constructing an equivalent protocol . . . 146
6.4.3 Cost of removing the basis-independent loss assumption . . . 148
6.4.4 Sampling . . . 149

6.5 Application to decoy-state BB84 . . . 153
6.5.1 Protocol specification . . . 153
6.5.2 Required and actual phase error estimation bound . . . 155
6.5.3 Variable-length security statement for decoy-state . . . 156
6.6 Results . . . 157
6.6.1 Recipe for computing key rates in the presence of basis-efficiency mismatch . . . 158
6.6.2 Detector Model . . . 159
6.6.3 Computing bounds on δ_1, δ_2. . . . 161
6.6.4 Plots . . . 163
6.6.5 Extension to multi-mode case . . . 164
6.7 Summary and Outlook . . . 167

7 Security using Marginal-constrained Entropy Accumulation Theorem 175
7.1 Generic Protocol Specification . . . 178
7.2 Additional Background . . . 187
7.3 Proving security of QKD Protocol using MEAT . . . 189
7.3.1 Expressing the protocol as a sequence of channels . . . 189
7.3.2 Dimensions of Eve's systems . . . 199
7.3.3 Security proof for Generic QKD Protocol (finite-dimensional case) . . . 201
7.3.4 Security via application of MEAT . . . 205
7.3.5 Reformulating the minimization over attack channels . . . 208
7.3.6 Final security statement . . . 212
7.3.7 Discussion . . . 215
7.4 Extending Security to optical protocols . . . 220
7.5 Plots . . . 223
7.5.1 Qubit BB84 . . . 224
7.5.2 Decoy-state BB84 . . . 225
7.6 Summary and Outlook . . . 226

8 Classical Authentication in QKD security proofs **228**
8.1 Security Definition with asymmetric aborts . . . 231
8.2 Model and Reduction Statement . . . 234
8.2.1 Authenticated Classical Communication Model . . . 234
8.2.2 Implementing the authenticated communication model . . . 237
8.2.3 Authentication Post-Processing Protocol (APP) . . . 238
8.2.4 Reduction Statement . . . 241
8.3 Proof of the Reduction Theorem 8.2.1 . . . 242
8.3.1 Proving that `auth-abort` in the core QKD protocol results in both parties aborting . . . 242
8.3.2 Reducing to security before authentication post-processing . . . 243
8.3.3 Reducing to scenario where authentication satisfies honest behaviour 249
8.4 Delayed Authentication . . . 256
8.4.1 Delayed Authentication Post-Processing Protocol (del-APP) . . . 257
8.4.2 Reduction Statement . . . 259
8.5 Summary and Outlook . . . 260

9 Summary and Outlook **262**

References **266**

APPENDICES **285**

A Variable-length input to privacy amplification **286**

B Proofs of statements for the postselection technique **290**

C Proofs of statements for EUR analysis **294**
C.1 Variable-length security . . . 294
C.2 Technical Statements . . . 300

C.3 Sampling . . . 302
C.3.1 Random Sampling . . . 302
C.3.2 Sampling with imperfect detectors . . . 304
C.4 Combining bounds . . . 307
C.5 Decoy Analysis . . . 309
C.5.1 Bounds on zero and one photon statistics . . . 311
C.5.2 Rigorous use of Hoeffdings . . . 312

D Proofs of statements related to delayed Authentication **315**

E Miscellaneous **320**

E.1 Proof of the Correctness and Secrecy Decomposition of the Security Definition (Section 3.1.2) . . . 320
E.2 Explanation of Decoy-State Plots from Section 4.5 . . . 322

List of Figures

2.1 Schematic of a beam splitter with two input ports (left and bottom) and two output ports (right and top). 29

2.2 Idealized polarizing beam splitter (PBS) that routes the horizontal and vertical polarization components of the input mode into separate spatial output modes. 29

2.3 Schematic of a threshold (on/off) detector. In the imperfect model, η denotes the overall detection efficiency and p_{dc} the dark-count probability per detection window. 30

3.1 Schematic of a quantum key distribution (QKD) protocol. The task is to establish a shared secret key between two distant parties, Alice and Bob. The protocol relies on trusted quantum devices operated within secure perimeters, access to local true random number generators (TRNGs), an authenticated classical channel, and an insecure quantum channel that may be fully controlled by an adversary. Figure from [10]. 34

3.2 Schematic of an active detection setup using threshold detectors. 48

3.3 Schematic of the passive detection setup using theshold detectors. 49

3.4 Schematic illustrating the use of a source map. A virtual source prepares $(\xi_k)_{A''}$, which is mapped to the real emitted state $(\sigma_k)_{A'}$ by a source map Ψ. Then, one can "give" Eve control over the source map (meaning that she is allowed to perform any operation she wants in place of the source map). The security of the latter implies security of the former, as argued rigorously in Lemma 7.4.1. 60

3.5 An infinite-dimensional POVM can be modelled as a squashing map Λ followed by a finite-dimensional POVM. Giving the squashing map Λ to Eve allows us to restrict our analysis to the finite-dimensional POVM. 64

4.1 Expected key rate for fixed-length protocols $\widetilde{R}_{\text{fixed}}(t)$ for various values of t, key rate upon acceptance for fixed-length protocols $R_{\text{fixed}}(t)$ plotted for various values of t, and the expected key rate for variable-length protocol plotted $\widetilde{R}_{\text{variable}}$, plotted for a fixed honest behaviour of the channel. 91

4.2 Expected key rate for fixed-length protocols $\widetilde{R}_{\text{fixed}}(t)$ for various values of t, key rate upon acceptance for fixed-length protocols $R_{\text{fixed}}(t)$ plotted for various values of t, and the expected key rate for variable-length protocol plotted $\widetilde{R}_{\text{variable}}$, for an unpredictable honest behaviour. 93

4.3 Key rate for variable-length decoy-state BB84 protocol plotted against loss, for the typical observations of the protocol, against IID collective attacks. 95

5.1 Key rate for variable-length qubit BB84 protocol plotted against loss, with and without the postselection lift to coherent attacks. 124

5.2 Key rate for variable-length decoy-state BB84 protocol plotted against loss, with and without the postselection lift to coherent attacks. 125

6.1 Schematic for the two-step measurement procedure from Lemma 6.3.1. Note that the second step measurement $\{G_k\}_{k\in\mathcal{A}_i}$ depends on the outcome of the first step measurement. 139

6.2 Protocol flowchart for the equivalent protocol from Section 6.3, where basis-independent loss assumption (Eq. (6.7)) is satisfied. The dotted arrows and boxes represent virtual measurements that do not actually happen in the real protocol. Connections between different boxes are highlighted using curved arrows. We use the Serfling bound (Lemma 6.3.2) to obtain a bound on the phase error rate from observations. The phase error rate is then used to bound the smooth min entropy using the EUR statement. We use $\boldsymbol{N}_P$ to denote the number of P measurement outcomes, where P denotes a POVM element. For clarity, we have omitted the conditioning on events in the figure (but not in our proof). The basis used for measurements is indicated in each box, and refers to the basis used by *both* Alice and Bob. 170

6.3 Protocol flowchart for the equivalent protocol from Section 6.4, where basis-independent loss assumption (Eq. (6.7)) is not satisfied. For the POVMs, the reader may refer to Table 6.1 or Section 6.4.1. Compared to Fig. 6.3, the testing and key generation rounds go through an additional second step filtering measurement that depends on the basis used. The basis used in these measurements in indicated in each box, and indicates the basis used by *both* Alice and Bob. 171

6.4 Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol, against loss. We plot key rates for $n = 10^{12}$ number of total signals sent, for various values of $\Delta_\eta, \Delta_{\text{dc}}$. We find that random swapping of the 0 and 1 detectors drastically improves the key rates obtained. 172

6.5 Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against loss. We plot key rates for various values of total number of signals sent (n), for $\Delta_\eta = \Delta_{\text{dc}} = 0.05$. 173

6.6 Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against detector characterization parameters $\Delta_\eta, \Delta_{\text{dc}}$. We plot key rates for a channel with 25dB loss. 174

7.1 The evolution of the state through Eve's attack channels $\{\mathcal{A}_j\}$, and Alice and Bob's operations $\{\mathcal{G}_j\}$ for the Virtual entanglement-based protocol. The evolution of states is also described in Lemma 7.3.4. Note that the announcements $\widehat{C}_j$ are made available to Eve through an explicit copy $\widetilde{C}_j$, which gets merged with E'_j to form E_j. 197

7.2 (Same as Fig. 7.1). The evolution of the state through Eve's attack channels $\{\mathcal{A}_j\}$, and Alice and Bob's operations $\{\mathcal{G}_j\}$ for the Virtual entanglement-based protocol. The evolution of states is also described in Lemma 7.3.4. Note that the announcements $\widehat{C}_j$ are made available to Eve through an explicit copy $\widetilde{C}_j$, which gets merged with E'_j to form E_j. The MEAT [11, Theorem 4.1a] is applied for the sequence of channels $\{\mathcal{M}_j\}$. 206

7.3 Key rate for variable-length qubit BB84 protocol plotted against loss, using MEAT, computed using open source code from Ref. [9]. 224

7.4 Key rate for the variable-length decoy-state BB84 protocol plotted as a function of loss, computed using MEAT. While key rates can, in principle, be evaluated at higher loss values, this becomes numerically challenging due to the optimization over the Rényi parameter. The results shown here are obtained using open-source code from Ref. [9]; we refer the reader to that work for additional plots covering a broader range of loss values. 225

8.1 The practical authenticated classical communication model used in this chapter. Messages pass through Eve, who may delay, drop, or substitute them with `auth-abort`, subject to the constraints described in Section 8.2.1. Time flows from top to bottom in the figure, which illustrates an example scenario: in earlier parts of the protocol (not shown in the figure), 4 messages have been sent from Alice to Bob, and 13 messages from Bob to Alice. Eve does not interfere with Alice's 5th message to Bob. However, she chooses to delay Bob's 14th message. (Presumably, Alice does not send a new message during this period because she is waiting to receive one.) During the delay, Eve receives Bob's 15th message and also delivers the 6th message to Bob. According to our communication model, this implies that $C^{(6)}_{E\to B}$ must be `auth-abort`, since it was received before Alice sent her 6th message. 236

8.2 Schematic of AuthPP Protocol described in Section 8.2.3. Alice and Bob first update their key registers based on whether they received an `auth-abort` in any of the prior communication. They then communicate their tentatively `accept` / `abort` decisions. They then perform a final update operation on their key registers depending on their final `accept` / `abort` decision. 240

8.3 A diagram illustrating transformations between real and ideal states evolving through the AuthPP Protocol. The '?' indicates the transformations that must be shown to be true in Lemma 8.3.2. The states go through the map $\mathcal{E}^{\text{repl}}_{\text{auth}} \in \text{CPTP}(K_A K_B \boldsymbol{C}_{\mathbf{fin}}, K_A K_B \boldsymbol{C}_{\mathbf{fin}})$ that replaces the key registers depending on $\boldsymbol{C}_{\mathbf{fin}}$. They then go through some communication steps given by $\mathcal{E}_{\text{comm}} \in \text{CPTP}(K_A K_B \boldsymbol{E}_{\mathbf{fin}}, K_A K_B \boldsymbol{E}'_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}})$ (influenced by Eve). Finally, Alice and Bob perform the final updates to their key registers described by $\mathcal{E}_{\text{update}} \in \text{CPTP}(K_A K_B \boldsymbol{C}_{\mathbf{auth}}, K_A K_B \boldsymbol{C}_{\mathbf{auth}})$. 245

8.4 For every operation that Eve performs in the virtual authentication setting, one can construct an equivalent operation in the honest authentication setting, where Eve creates a copy of each sent message and performs her original operation on this copy. She does not forward the result of her attack on the copy to the receiver; instead, she forwards the original, unmodified message to the receiving party. 255

8.5 Schematic of del-AuthPP Protocol described in Section 8.4.1. Alice and Bob first communicate and verify transcripts. If transcripts matches, they accept the protocol. Else, they abort the protocol and replace their key registers with $\perp$s. 258

9.1 Key rate for the variable-length decoy-state BB84 protocol plotted as a function of loss, comparing the different proof techniques presented in this thesis. Note that the protocols are not strictly identical across techniques, due to differences inherent to the respective proof methods. For MEAT, the protocol is as described in Section 7.5. The PS protocol is identical to the MEAT protocol, except that it does not allow on-the-fly announcements. For EUR, the protocol follows Section 6.6. Such comparison plots, over a wider range of parameters, were first presented in Refs. [12, 9]; the present figure is generated using code based on Ref. [9] (MEAT), Ref. [2] (EUR) and Ref. [6] (PS), which we duly acknowledge. In particular, Refs. [12, 9] should be cited for all results pertaining to the numerical comparison of key rates between these proof techniques. 263

List of Tables

6.1 Different symbols used in our proof. Note that b_A, b_B refer to basis choice of Alice and Bob. However, b_1, b_2 refer to the basis used by *both* Alice and Bob, for the second and third step measurements. Whenever a basis is explicitly written as X/Z (or b_1, b_2) it represents *both* Alice and Bob's basis choices. 146

7.1 Parameters required to define an instance of Generic QKD Protocol. 180

Chapter 1

Introduction

> Where I try to explain to a layperson why their taxes should fund this thesis; where I lay bare some of the existential questions that have arisen along the way to this thesis; and where I explain the best way to read this thesis, and justify its length.

Human beings have an inherent need to communicate. From spoken language to writing, and from the telegraph to the internet, a large fraction of technological progress has been driven by the desire to transmit information reliably across distance and time. Writing allows ideas to persist across generations; telephones allow voices to travel across continents; and modern digital communication platforms enable instantaneous global interaction. Beyond communication itself lies a deeper and equally fundamental requirement: the need for *private* communication. Humans must be able to share information selectively, with the assurance that only intended recipients can access it. Throughout history, private communication has been essential for diplomacy, trade, personal relationships, and military strategy.

In a world with just simple face-to-face interactions, this private communication would be as simple as checking that nobody is hiding in the bushes. As communication technologies evolve beyond face-to-face interactions, so too does the need to protect messages from interception.

The art and science of enabling secure communication in the presence of adversaries is known as *cryptography*.[1] Evidence of cryptographic techniques appears across many ancient

[1]The word "secure" is often used to mean a variety of things in cryptography, depending on whether one is concerned with confidentiality, integrity, authenticity, or something else.

civilizations. One of the earliest known examples dates back to around 1900 BC, found in an inscription in the tomb of an Egyptian nobleman, where unusual hieroglyphic substitutions were used to conceal meaning [13]. In ancient India, the *Arthashastra*, written somewhere around 300BC attributed to Kautilya, describes espionage practices and explicitly mentions the use of "secret writing" for covert communication. In the Roman era, Julius Caesar famously employed what is now known as the Caesar cipher to transmit messages to his generals.

The Caesar cipher is a simple substitution cipher, in which each letter of the plain text (the message to be communicated) is shifted by a fixed number of positions in the alphabet, to yield the cipher text. While historically significant, such schemes rely on the secrecy of the encryption method itself. Once the method is known, the cipher can be broken easily, for example through frequency analysis of letters in the underlying language. In the case of the Caesar cipher, one can simply try shifting the letters in reverse, and checking which shifts lead to meaningful plain texts. This limitation illustrates an important principle, later formalized as Kerckhoffs' principle: security should not depend on keeping the system itself secret.

A major conceptual advance came during the Renaissance with the work of Blaise de Vigenère, who introduced ciphers that made explicit use of a secret *key*. A secret key is any piece of information which is known to the communicating parties, but unknown to the eavesdropper. In the Vigenère cipher, this key is combined with the plain text letters using modular arithmetic. The Vigenère cipher employs a short key that is repeated periodically, a feature that was later refined by the Vernam cipher (also known as the one-time pad), in which the key was required to be as long as the message itself. In both these cases, even if the encryption procedure is known, this does not necessarily suffice to break the cipher, since correct decryption additionally requires knowledge of the secret key.

The twentieth century, and in particular the Second World War, marked a turning point in cryptography. Mechanical and electromechanical cipher devices such as the German Enigma machine and the Japanese Purple cipher were deployed at unprecedented scale. Their cryptanalysis by Allied efforts demonstrated both the power and the limitations of classical cryptographic techniques, and helped establish cryptography as a scientific discipline rather than a collection of ad hoc methods.

This transition was completed by the work of Claude Shannon. In his seminal paper [14], Shannon placed proved *perfect secrecy* - that is, where the cipher text tells you nothing at all about the underlying plain text - is achievable if and only if the encryption key is at least as long as the message and is used only once. The resulting scheme, known as the one-time pad, is provably secure against any adversary, regardless of computational power

(as long as the key is perfectly secure).

Thus, secure communication can be reduced to the problem of *key distribution*. If two parties can somehow share a secret key securely, then they can use the one-time pad to protect their messages. Conversely, if key distribution is insecure, no encryption scheme can compensate for it, since the eavesdropper is assumed to know everything about the encryption process except the key. This observation lies at the heart of modern cryptography and directly motivates the subject of this thesis.

1.1 Traditional Classical Cryptography

Modern cryptography operates in a fundamentally digital setting. Information is represented as bits, processed by classical computers, and transmitted over classical communication networks such as the internet. Cryptographic algorithms are implemented as software or hardware procedures that manipulate bit strings, and adversaries are modeled as entities with access to the certain communication infrastructure and computational resources, subject to specified limitations.

In this setting, the central challenge is enabling two distant parties to communicate securely over a public channel that may be fully monitored by an adversary. Early symmetric-key cryptographic systems assumed that communicating parties already shared a secret key, established presumably by sending a trusted courier, or during a prior meeting. While effective in small or controlled environments, this assumption does not scale to large networks, where secure pre-distribution of keys becomes logistically infeasible.

A major breakthrough occurred in the 1970s with the invention of public-key cryptography. Protocols such as Diffie–Hellman key exchange [15] and RSA [16] allow two parties to establish a shared secret over an open, insecure but authenticated classical channel. By *authenticated*, we mean that an adversary may eavesdrop on all communicated messages but cannot impersonate either party or modify transmitted messages[2]. These schemes rely on mathematical problems believed to be computationally hard[3], such as the discrete logarithm problem or integer factorization. Crucially, this hardness is a *belief* rather than a proven fact. Moreover, this belief is known to be invalid in the presence of large-scale quantum computers, as we discuss below. Historically, such beliefs about

[2]While this is a standard assumption in cryptography, in practice, an adversary can always delay, block, or interrupt messages, and any concrete authentication scheme allows a nonzero probability of successful forgery. These subtleties are discussed briefly in the context of QKD in Chapter 8.

[3]That is, have runtime that is exponential in the size of the input.

computational hardness have repeatedly turned out to be optimistic. For example, when RSA was introduced in 1977, key sizes on the order of 512 bits were widely considered secure for the foreseeable future. However, advances in algorithms, hardware, and large-scale collaborative computation led to the successful factorization of a 512-bit RSA modulus in 1999—less than a quarter century after the scheme's proposal—rendering such key sizes insecure [17]. Similar episodes have occurred for other cryptographic assumptions, which shows that confidence in computational hardness is inherently provisional and subject to revision as techniques evolve.

In practice, modern secure communication systems use hybrid encryption architectures. Public-key cryptography is employed only to establish a short symmetric key, after which efficient symmetric-key algorithms such as AES [18] are used to encrypt bulk data. This approach combines the scalability of public-key cryptography with the efficiency of symmetric encryption.

Crucially, the security of all such classical cryptographic systems, especially public-key cryptography is *computational*. Their guarantees rely on assumptions about the limitations of adversaries' computational power, and their abilities to solve certain mathematical problems. If these assumptions fail, the security of the system collapses.

1.2 Quantum Computers

The conditional nature of computational security became particularly apparent with the emergence of quantum computing. In 1994, Peter Shor discovered a quantum algorithm capable of efficiently factoring large integers and computing discrete logarithms [19]. Shor's algorithm implies that a sufficiently large quantum computer would completely break widely deployed public-key cryptosystems, including RSA and elliptic-curve cryptography, which underpins the overwhelming majority of public-key deployments on today's Internet.

This discovery was both surprising and consequential. It demonstrated that cryptographic security based solely on classical computational hardness is vulnerable to advances in computing paradigms. In response, significant effort has been devoted to the development of post-quantum cryptography (PQC): classical cryptographic schemes designed to remain secure against quantum adversaries. These schemes are based on problems believed to be hard for both classical and quantum computers. The ongoing NIST post-quantum cryptography standardization process [20] reflects the global importance of this transition.

Despite these advances, post-quantum cryptography remains computational in nature. Its security continues to rely on unproven assumptions about algorithmic hardness.

1.3 Quantum Key Distribution

In parallel with the development of post-quantum cryptography, a fundamentally different approach to secure communication emerged. In 1984, Bennett and Brassard proposed a new protocol, which now bears their names [21] (and for which they were awarded the Turing Award); it uses the principles of quantum mechanics to establish[4] secret keys. This work gave birth to the field of quantum key distribution. The central idea is to encode information into quantum states of light in such a way, that any attempt at stealing this information results in a disturbance of those states. This can then be detected by the honest communicating parties, which can abort the protocol when necessary.

Quantum key distribution (QKD) enables two parties to establish a shared secret key with information-theoretic security, even in the presence of an adversary with unlimited computational power. Security follows from the properties of information implied by physical principles, such as the impossibility of perfectly copying unknown quantum states and the unavoidable disturbance caused by measurement (and by assumptions on the functioning of the hardware).

Over the past four decades, QKD has evolved from a theoretical proposal into a mature field with experimental demonstrations over optical fiber, free-space links, and satellite-based platforms. Commercial QKD systems exist today, and efforts are underway to standardize and certify QKD technologies. Chapter 7 in this thesis is a result of one such effort.

1.4 "PQC vs QKD"

There is an ongoing and at times contentious exchange regarding the respective roles of post-quantum cryptography (PQC) and quantum key distribution (QKD). This discussion raises fundamental questions about the long-term foundations of cryptographic security[5] and is therefore worth briefly addressing here. A comprehensive treatment is beyond the scope of this thesis, and the topic has been examined in considerably greater depth elsewhere; we refer the reader, for example, to Refs. [22, 23, 24, 25, 26, 27, 28]. Nevertheless, since this thesis is concerned with the security analysis of QKD protocols, it would be inappropriate to omit this discussion entirely.

[4] Note that the protocol, and QKD in general, *establishes* secret keys rather than distributing pre-existing ones. A more accurate name would therefore be quantum key establishment. Alas, it is now too late.

[5] and has raised many existential questions for this author.

Proponents of PQC emphasize that many real-world cryptographic failures are not caused by breakthroughs in the underlying mathematical assumptions, but rather by more mundane engineering issues, such as software vulnerabilities, side-channel leakage, poor operational security, and social engineering. In this context, it is argued that QKD introduces a new class of implementation challenges, including novel side-channel attacks and system-level vulnerabilities, for which there is comparatively less operational experience and confidence. They further note that QKD comes with practical constraints: it requires a dedicated quantum channel, and it addresses only the problem of key distribution. As a result, it must be combined with additional mechanisms for authentication and encryption, often relying on classical cryptographic components. From this perspective, QKD may be intellectually appealing, but it requires specialized hardware and (in practice) a pre-shared seed key to authenticate classical communication[6]. Moreover, present-day QKD deployments face distance limitations and can be vulnerable to implementation and side-channel attacks. These considerations are used to argue that QKD is too expensive and operationally cumbersome to be broadly useful. Finally, discussions around timelines for cryptographically relevant quantum computers remain highly uncertain, with expert assessments often extending well beyond a decade [31]. However, this consideration is not central to the role of QKD, which is not intended solely as a countermeasure to specific quantum algorithms such as Shor's algorithm, but rather as a means of providing cryptographic diversity and mitigating future risks, whether classical or quantum.

In contrast, proponents of QKD emphasize that it promises information-theoretically secure key establishment—something that purely classical approaches such as PQC cannot provide.[7] They further argue that, for long-term confidentiality, future breakthroughs in cryptanalysis cannot be ruled out, and that it is therefore valuable to have a key-establishment mechanism whose security does not rest on computational assumptions. This perspective is often formalized through the so-called Mosca inequality, which highlights the risk that the time until large-scale quantum attacks become feasible may be shorter than the combined data shelf-life and cryptographic migration time [27, 31]. Proponents additionally argue that although current QKD systems remain costly, these costs are expected to decrease as the technology matures and deployments scale. Furthermore, while present-day QKD systems are limited in transmission distance, the eventual development of quantum repeaters [32] has the potential to overcome this limitation. Until such technology

[6]Although authentication is required for classical cryptographic schemes as well. Even when using computationally secure authentication, QKD still provides strong "everlasting security" [29] guarantees under the assumption that the authentication remains secure during the execution of the protocol [28, 30].

[7]This information-theoretic security applies to the mathematical model of the protocol with modelling assumptions, and does not automatically extend to imperfect physical implementations. However, note that this is the case for the implementation of *any* cryptographic protocol, whether classical or quantum.

becomes available, long-distance QKD can be realized through trusted-node networks.

The author of this thesis adopts a deliberately agnostic position with respect to this ongoing debate. As will be seen throughout this work, QKD enables the establishment of information-theoretic security—at least at the level of a precisely specified protocol description under explicit modeling assumptions on the relevant hardware implementing the protocol. Such security guarantees are fundamentally unattainable using purely classical cryptographic methods, and this constitutes a distinctive scientific and engineering achievement that, in itself, justifies continued study of the field.

This perspective is further motivated by the historical difficulty of reliably forecasting the longevity of classical cryptographic assumptions. Experience has repeatedly shown that predictions about when particular cryptosystems will become insecure are highly uncertain and often optimistic. In this sense, information-theoretic security offers a qualitatively different form of assurance—one that is not contingent on assumptions about future computational capabilities—and provides a compelling rationale for investigating QKD alongside classical and post-quantum approaches.

At the same time, QKD systems typically entail higher costs, require dedicated hardware, and are susceptible to their own class of side-channel attacks that target imperfections in practical implementations. Consequently, substantial theoretical and experimental effort is required to obtain satisfactory security proofs for mathematical models of QKD systems that are both rigorous and realistic, in the sense that they accurately capture the relevant features of the underlying physical implementations. In fact, the primary goal of this thesis is to help advance the theoretical state of the art in this direction.

Whether the additional security guarantees offered by QKD justify its practical cost, operational complexity, and deployment constraints is ultimately not a scientific question, but one to be decided by economic, regulatory, and strategic considerations. In this thesis, we do not attempt to adjudicate this trade-off. Rather, the objective is to ensure that the security claims made by QKD protocols are stated as precisely, transparently, and rigorously as possible, and that the assumptions underlying these claims are clearly articulated and directly connected to realistic deployment scenarios. Arguments concerning whether the eventual market for QKD technologies will be large or small lie outside the scope of this thesis. In this sense, the value of the results presented here does not depend on market outcomes, but rather on their ability to sharpen our understanding of QKD and to provide a rigorous basis upon which future engineering, certification, or deployment decisions may be made.

1.5 Organization of this thesis

This thesis is focused on the *rigorous* security analysis of *practical* QKD protocols using a *variety* of proof techniques. Each emphasized word in this sentence is deliberate and reflects a central theme.

Rigorous. There exists a large body of academic literature on QKD security proofs; however, many existing works contain gaps, implicit assumptions, or unresolved technical issues. This thesis builds on substantial prior work while aiming to address these deficiencies by presenting a careful, explicit, and internally consistent analysis that avoids such omissions and errors. For instance, in Chapter 5 we fix a longstanding flaw in the postselection technique for QKD. Moreover, there is currently no single paper that fully specifies a practical QKD protocol in all of its operational detail and then provides a self-contained and rigorous security analysis of that protocol (see Refs. [7, 33] for recent attempts at filling this gap). Our own attempt to provide such an analysis is also very recent, and presented in Chapter 7.

Practical. It should be noted that a highly formal and fully rigorous security analysis of a QKD protocol does exist [34]. However, that analysis applies to an idealized protocol that is not designed for practical implementation and abstracts away many operational and physical details relevant to real-world systems.

In contrast, this thesis focuses explicitly on protocols - such as the decoy-state BB84 protocol - that are intended to be implementable in practices, and also makes contributions to the security analysis in the presence of hardware imperfections (Chapter 6). The analysis developed here, especially in Chapter 7 is sufficiently general to accommodate a wide range of protocol variants and implementation choices.

Variety. Finally, modern QKD security theory offers a wide range of proof techniques, most of which are often studied in isolation. A distinctive feature of this thesis is that it covers three of the four major proof techniques used in contemporary QKD security analysis [7].[8] As a result, this work is intended to be both comparative and pedagogical, and to serve as a reference for readers interested in rigorous security analyses of practical QKD protocols, across multiple proof techniques.

[8]The phase error correction approach, which is not covered here, is closely related to the entropic uncertainty relations approach studied in this thesis; see Ref. [35]. Both approaches rely on obtaining suitable bounding the same quantity, the so called phase error rate.

The thesis is organized as follows:

In Chapter 2, we introduce the notation and conventions from quantum information theory used throughout this thesis, review relevant entropic quantities and their basic properties, and provide a brief overview of the aspects of quantum optics needed to model practical QKD implementations.

In Chapter 3, we cover the basics of QKD. We present the generic protocol framework studied in this thesis, state the security definition, and review core tools used in security analyses of practical protocols. This includes, in particular, the use of the Leftover Hashing Lemma, and other tools such as source-replacement schemes, squashing maps, and source maps.

In Chapter 4 we start covering new results. We study variable-length security and the additional conceptual and technical issues that arise when the output key length is not a fixed value, but depends on the protocol observations. We present a generic security proof for variable-length QKD protocols and highlight the specific modifications relative to the standard fixed-length analysis. We also show that these modifications do not introduce a substantial performance penalty.

Chapter 5 studies the postselection technique and its application to practical QKD. The postselection technique [36, 5] is a generic tool that can be used to reduce the security analysis of protocols satisfying a certain "permutation-invariant" property, to security analysis against IID collective attacks. We resolve several issues that must be addressed before this technique can be rigorously applied to practical optical, prepare-and-measure implementations. In particular, this includes the role of infinite-dimensional Hilbert spaces (and the resulting dimension dependence of the reduction) as well as a patch to a critical gap in the original argument applying this technique to QKD.

Chapter 6 develops security proofs based on entropic uncertainty relations. A central object in this approach is the phase error rate and the challenge of bounding it using experimentally accessible data. All prior treatments relied on highly idealized detector models - for example, assuming perfectly identical detection probabilities - in order to obtain such bounds, and consequently fail to tolerate even infinitesimal deviations from this idealized setting. As a result, obtaining meaningful bounds on the phase error rate in the presence of realistic detector imperfections has remained a well-known open problem for nearly two decades. In this thesis, we provide a solution to this problem by introducing new results on sampling measurements from quantum states. These results render entropic uncertainty relation–based (and phase error correction-based) security proofs applicable to practical detector scenarios.

Chapter 7 presents security analyses based on the marginal-constrained entropy accumulation theorem. This chapter contains a rigorous and complete security proof for a well specified decoy-state BB84 protocol. Building on decades of prior work, we combine the relevant ingredients into a single coherent framework that yields tight key-rate bounds and provides a clear path toward incorporating realistic implementation imperfections. Beyond establishing the security of a specific protocol, this chapter develops a general and modular framework that can be readily adapted to a broad class of QKD protocols. The framework unifies all major ingredients required for the analysis of realistic QKD protocols, including the analysis of classical authentication and classical processing, source-replacement schemes, finite-size analysis, source maps, squashing maps, and decoy-state techniques. In doing so, this work consolidates a diverse range of techniques scattered across the QKD literature into a unified formalism, representing a general and rigorous treatment of QKD security, which can be reused for further analyses.

Chapter 8 discusses classical authentication and its role in QKD protocols. Standard QKD analyses often assume an ideal authenticated classical channel in which messages are always delivered correctly (albeit with arbitrary delay). In practice, practical authentication mechanisms instead guarantee that either a message is accepted as authentic or the receiver outputs a special failure symbol. We explain how this discrepancy necessitates a careful treatment of asymmetric abort events (where one party aborts while the other does not), and we show how (under appropriate conditions) the resulting security analysis in the realistic authentication setting can be reduced to the security analysis of the standard, idealized authentication setting.

Chapter 9 concludes the thesis with a summary of contributions, a discussion of open problems and future directions, and a comparative perspective on the proof techniques developed throughout the thesis.

1.6 How to read this thesis

This thesis is written using largely consistent notation throughout, and any changes to notation are explicitly highlighted when they are unavoidable, as is occasionally necessary given the breadth of topics covered. More importantly, it is written in a modular fashion. Each of Chapters 4 to 8 presents a distinct research contribution and may be read independently of the others. All necessary background material is consolidated in Chapters 2 and 3. Chapter 2 provides general mathematical background material; readers who are already well versed in quantum information theory may choose to skip or skim this chapter.

Chapter 3 introduces QKD-specific background and may similarly be skimmed by readers already familiar with QKD.

Readers interested in a particular proof technique may therefore focus on the corresponding chapter: Chapter 5 for the postselection technique, Chapter 6 for entropic uncertainty relations, and Chapter 7 for the entropy accumulation approach. Chapter 8 addresses classical authentication and its role in QKD, and can be read independently of the security proof techniques developed elsewhere in the thesis.

Furthermore, our notation closely follows that of the recent review on QKD security proofs in Ref. [7], which may make this thesis a useful technical companion to that work.

Chapter 2

Background

Where we set up basic background in quantum information theory; where we discuss a large number of statements about several different entropies; and where we introduce the quantum description of light and associated hardware required to understand QKD.

2.1 Quantum Information Theory

This section reviews essential concepts from quantum information theory [37] and establishes the notation and conventions used throughout this thesis. We use capital letters such as A, B, and C to denote *registers*, which represent physical systems capable of storing information. For a sequence of registers, A_j denotes the jth register, and we write A_i^j to denote the collection of registers $A_i, \ldots, A_j$. The register A is further associated with a complex Hilbert space $\mathcal{H}_A$, which provides the linear-algebraic structure used to represent states, measurements, and transformations of the system. Throughout this thesis, we will typically work with finite-dimensional registers; cases involving infinite-dimensional registers will be clear from the context.

For such spaces, we define the following sets of operators:

- $\mathrm{L}(A, B)$: the set of all linear operators acting on $\mathcal{H}_A$ to produce vectors in $\mathcal{H}_B$, that is,
$$\mathrm{L}(A, B) = \{X : \mathcal{H}_A \to \mathcal{H}_B \mid X \text{ is linear}\}.$$

This space is itself a finite-dimensional complex vector space of dimension $(\dim \mathcal{H}_A)(\dim \mathcal{H}_B)$. We use $\mathrm{L}(A)$ to denote $\mathrm{L}(A, A)$.

- $\mathrm{Pos}(A)$: the set of (hermitian) positive semidefinite operators on $\mathcal{H}_A$, i.e.,

$$\mathrm{Pos}(A) = \{X \in L(A) : X = X^\dagger,\ X \geq 0\}.$$

- $\mathrm{S}_\leq(A)$: the set of subnormalized states on A, i.e., positive semidefinite operators with trace at most one:

$$\mathrm{S}_\leq(A) = \{\rho_A \in \mathrm{Pos}(A) : \mathrm{Tr}[\rho_A] \leq 1\}.$$

- $\mathrm{S}_=(A)$: the set of normalized quantum states (density operators) on A, i.e.,

$$\mathrm{S}_=(A) = \{\rho_A \in \mathrm{Pos}(A) : \mathrm{Tr}[\rho_A] = 1\}.$$

- $\mathrm{U}(A)$: the set of unitary operators on $\mathcal{H}_A$, that is,

$$\mathrm{U}(A) = \{U \in \mathrm{L}(A) : U^\dagger U = UU^\dagger = \mathbb{I}_A\}.$$

  These represent reversible physical transformations acting on register A.

- $\mathrm{V}(A, B)$: the set of isometries from A to B, defined as

$$\mathrm{V}(A, B) = \{V : \mathcal{H}_A \to \mathcal{H}_B \text{ linear} \mid V^\dagger V = \mathbb{I}_A\}.$$

  Isometries preserve inner products but need not be surjective; they model quantum evolutions that embed system A into a larger system B.

If A is a register with associated Hilbert space $\mathcal{H}_A$, we will sometimes use $\mathrm{Pos}(\mathcal{H}_A)$ and $\mathrm{Pos}(A)$ interchangeably. This notational choice simplifies expressions in later chapters.

2.1.1 Quantum States

Definition 2.1.1. A (possibly subnormalized) **quantum state** on a register A is represented by a positive semidefinite operator $\rho_A \in \mathrm{Pos}(A)$ with $\mathrm{Tr}(\rho_A) \leq 1$, where subscripts specify the registers on which the state exists. When $\mathrm{Tr}(\rho_A) = 1$, the state is said to be normalized.

Definition 2.1.2. A state is **pure** if it can be written as $\rho_A = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}_A$. Otherwise, it is mixed.

Composite systems are described by tensor products: for registers A and B, the joint space is $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. A joint state ρ_{AB} on AB has marginals given by the partial trace, e.g., $\rho_A = \mathrm{Tr}_B(\rho_{AB})$. For a multipartite state $\rho_{ABC\cdots}$, we write ρ_A to denote its marginal on register A. Conversely, for a state ρ_A, we use ρ_{AB} to denote some extension of ρ_A to an additional register B.

Definition 2.1.3. A state $\rho \in \mathrm{S}_{\leq}(CQ)$ is said to be **classical on** C (with respect to a specified basis on C) if it is in the form[1]

$$\rho_{CQ} = \sum_c \lambda_c \, |c\rangle\langle c| \otimes \sigma_c, \tag{2.1}$$

for some normalized states $\sigma_c \in \mathrm{S}_{=}(Q)$ and weights $\lambda_c \geq 0$, with $|c\rangle$ being the specified basis states on C. In most circumstances, we will not explicitly specify this "classical basis" of C, leaving it to be implicitly defined by context. Throughout this thesis, all variants of the register C (including decorated versions such as $\hat{C}$, $\tilde{C}$, C_{EC} etc.) are taken to be classical registers.

In the protocols studied in this thesis, different operations are often performed depending on which events occur during the execution of the protocol. It is therefore necessary to condition on classical events in order to describe such conditional operations precisely. An event on a register C is simply a subset of the possible values that the register C can take. For any event Ω, we use Ω^{C} to denote its complement. We introduce the relevant definitions below.

Definition 2.1.4. (Conditioning on classical events) For a state $\rho \in \mathrm{S}_{\leq}(CQ)$ classical on C, written in the form $\rho_{CQ} = \sum_c \lambda_c \, |c\rangle\langle c| \otimes \sigma_c$ for some $\sigma_c \in \mathrm{S}_{=}(Q)$ and $\lambda_c \geq 0$, and an event Ω defined on the register C, we will define a corresponding **partial state** and **conditional state** as, respectively,

$$\rho_{\wedge\Omega} \coloneqq \lambda_c \sum_{c\in\Omega} |c\rangle\langle c| \otimes \sigma_c, \qquad\qquad \rho_{|\Omega} \coloneqq \frac{\mathrm{Tr}\{\rho\}}{\mathrm{Tr}\{\rho_{\wedge\Omega}\}}\rho_{\wedge\Omega} = \frac{\sum_c \lambda_c}{\sum_{c\in\Omega}\lambda_c}\rho_{\wedge\Omega}. \tag{2.2}$$

We refer to $\rho_{\wedge\Omega}$ as the state ρ being partial[2] on Ω. The process of taking partial states is commutative and "associative", in the sense that for any events Ω, Ω' we have $(\rho_{\wedge\Omega})_{\wedge\Omega'} = (\rho_{\wedge\Omega'})_{\wedge\Omega} = \rho_{\wedge(\Omega\wedge\Omega')}$. On the other hand, some disambiguating parentheses are needed when combined with taking conditional states (due to the normalization factors).

[1] Throughout this thesis, we adopt the convention that whenever a summation $\sum_c$ is written without an explicit specification of the summation range, it is understood to be taken over all admissible values of the variable c, with the corresponding domain being implicitly determined by the surrounding context.

[2] One could instead also think of it as being "subnormalized conditioned" on the event Ω.

Given these definitions, for a normalized state $\rho \in \mathrm{S}_=(CQ)$ that is classical on C, we can write it in the form

$$\rho_{CQ} = \sum_c \rho(c) \, |c\rangle\langle c| \otimes \rho_{Q|c}, \tag{2.3}$$

where $\rho(c)$ denotes the probability of register C storing c according to ρ, and $\rho_{Q|c}$ can indeed be interpreted as the corresponding conditional state on Q, i.e. $\rho_{Q|c} = \mathrm{tr}_C[\rho_{|\Omega_{C=c}}]$ where $\Omega_{C=c}$ is the event C stores c.

Definition 2.1.5. For registers Q, Q' with $\dim(Q) \leq \dim(Q')$, a **purifying function for Q onto Q'** is a function $\mathtt{Pur} : \mathrm{S}_\leq(Q) \to \mathrm{S}_\leq(QQ')$ such that for any state ρ_Q, the state $\mathtt{Pur}(\rho_Q)$ is a purification of ρ_Q onto the register Q', i.e. a (possibly subnormalized) rank-1 operator such that $\mathrm{tr}_{Q'}[\mathtt{Pur}(\rho_Q)] = \rho_Q$.

Note that a purifying function is *not* a channel (i.e. CPTP map), for instance, because it is necessarily nonlinear. Furthermore, all purifications of a given state ρ_Q are isometrically related [37, Proposition 2.29], in the sense that if $|\psi\rangle_{RQ}$ and $|\phi\rangle_{R'Q}$ are two purifications of ρ_Q, then there exists an isometry $V \in \mathrm{V}(R, R')$ such that

$$(\, \mathbb{I}_Q \otimes V \,) \, |\psi\rangle_{QR} = |\phi\rangle_{QR'} \, .$$

2.1.2 Measurements

In quantum mechanics, measurements are described mathematically by positive operator-valued measures (POVMs). Each POVM is specified by a collection of positive semidefinite operators that together represent the possible outcomes of the measurement.

Definition 2.1.6 (POVM)**.** A **positive operator-valued measure (POVM)** on the register A with outcome set $\mathcal{O}$ is a collection of operators

$$\{\Gamma_k : k \in \mathcal{O}\} \subseteq \mathrm{Pos}(A)$$

satisfying

$$\sum_{k \in \mathcal{O}} \Gamma_k = \mathbb{I}_A.$$

Each operator Γ_k is referred to as a POVM element and corresponds to a distinct measurement outcome $k \in \mathcal{O}$. The probability that outcome k occurs when the system in a state $\rho \in S_=(A)$ is measured using the above POVM, is given by:

$$p(k) = \mathrm{Tr}(\Gamma_k \rho).$$

In this general framework, projective measurements correspond to POVMs whose elements are orthogonal projections. In more general settings, such as when the measurement apparatus involves ancillary systems or coarse-graining of outcomes, POVMs provide the correct mathematical description of what is physically observed.

2.1.3 Quantum Channels

Definition 2.1.7. A **quantum channel** is a linear map $\Phi : L(A) \to L(B)$ that is completely positive and trace preserving. A linear map on the operator space is completely positive if, for every auxiliary register R, the extended map $\Phi \otimes \mathrm{id}_R$ maps positive operators to positive operators. A channel is trace-preserving if $\mathrm{Tr}[\Phi(X)] = \mathrm{Tr}[X]$ for all $X \in L(A)$.

We denote the set of CPTP maps from registers A to B via $\mathrm{CPTP}(A, B)$. By Stinespring's theorem [37, Proposition 2.20], every quantum channel can be represented as

$$\Phi(\rho_A) = \mathrm{Tr}_E \left(U_{AE}(\rho_A \otimes |0\rangle\langle 0|\, E) U_{AE}^\dagger \right),$$

for some environment system E and unitary operator U_{AE} acting jointly on A and E.

The following lemma is a standard result stating that any extension of a state ρ_A can be obtained by applying an appropriate quantum channel to the purifying subsystem of some purification of ρ_A.

Lemma 2.1.1. *Let $\rho_A \in \mathrm{S}_=(A)$ be a density operator. Furthermore, let $\rho_{AB} \in \mathrm{S}_=(AB)$ and $\rho_{AA'} \in \mathrm{S}_=(AA')$ be any extension and purification of ρ_A, respectively. Then*

$$\exists \mathcal{N} \in \mathrm{CPTP}(A', B) \text{ s. t. } \rho_{AB} = \mathcal{N}[\rho_{AA'}]. \tag{2.4}$$

Proof. Let ρ_{ABR} be any purification of ρ_{AB}, then by the isometric equivalence of purifications, there exists an isometry $V : A' \to BR$ such that

$$\rho_{ABR} = V \rho_{AA'} V^\dagger. \tag{2.5}$$

Therefore, $\rho_{AB} = \mathrm{Tr}_R \left[V \rho_{AA'} V^\dagger \right]$. The claim follows by setting $\mathcal{N}$ to be a channel which first applies the isometry V, and then traces out the R register. □

We will often work with channels that implement some measurement and stores the outcomes in a new register. These channels are defined below.

Definition 2.1.8 (Measurement channel)**.** Let $\{\Gamma_k\}_{k=1}^m \subset \mathrm{Pos}(A)$ be a POVM. Let X be a classical register of dimension m. We define the **measurement channel** $\mathcal{M}^{\mathrm{meas}}_{\{\Gamma_k\}} \in \mathrm{CPTP}(A, X)$ corresponding to the POVM $\{\Gamma_k\}_{k=1}^m$ to be the quantum channel which acts on any state as

$$\mathcal{M}^{\mathrm{meas}}_{\{\Gamma_k\}}[\rho] = \sum_{k=1}^{m} \mathrm{Tr}\left[\Gamma_k \rho\right] |k\rangle\langle k|_X \,. \tag{2.6}$$

2.1.4 Norms and Distances

We now define several norms and distance measures that are required for the mathematical machinery used in this thesis. In practice, we only make essential use of the Schatten 1-norm (Eq. (2.7)) and the associated trace distance or 1-norm. The remaining notions are included primarily for completeness, as they are needed to define the purified distance that appears in the definition of the smooth min-entropy. The detailed properties of these additional quantities are not directly utilized in this thesis. We refer to the reader to Ref. [38] for more details.

Definition 2.1.9. (Schatten p-norm) For every linear operator X, we define its **Schatten p-norm** as

$$\|X\|_p \coloneqq \left(\mathrm{Tr}\{|X|^p\}\right)^{1/p}, \tag{2.7}$$

where $p \in [1, \infty)$ and $|X| = \sqrt{X^\dagger X}$.

Definition 2.1.10. (Generalized Trace Distance [38, Eq.(3.23)]) Let $\rho_A, \sigma_A \in \mathrm{S}_{\leq}(A)$ be two (possibly subnormalized) quantum states on a register A. The **generalized trace distance** between ρ_A and σ_A is defined as

$$T(\rho_A, \sigma_A) \coloneqq \frac{1}{2}\big\|\rho_A - \sigma_A\big\|_1 + \frac{1}{2}\big|\mathrm{Tr}[\rho_A] - \mathrm{Tr}[\sigma_A]\big|, \tag{2.8}$$

where $\|X\|_1 = \mathrm{Tr}\left[\sqrt{X^\dagger X}\right]$ denotes the trace norm or Schatten 1-norm.

If $\rho_A, \sigma_A \in S_=(A)$ are normalized quantum states, then $\mathrm{Tr}[\rho_A] = \mathrm{Tr}[\sigma_A] = 1$, and the generalized trace distance reduces to the usual **trace distance**

$$T(\rho_A, \sigma_A) = \frac{1}{2}\|\rho_A - \sigma_A\|_1.$$

In this case, $T(\rho_A, \sigma_A)$ quantifies the statistical distinguishability between ρ_A and σ_A: if one is given a single copy of a quantum state that is either ρ_A or σ_A, each occurring with apriori probability $\frac{1}{2}$, then the optimal probability of correctly identifying the state by any quantum measurement is

$$p_{\text{guess}}(\rho_A, \sigma_A) = \frac{1}{2}\big(1 + T(\rho_A, \sigma_A)\big).$$

Thus, the trace distance quantifies the maximum distinguishing advantage between two quantum states.

Definition 2.1.11. (Generalized Fidelity and Purified Distance [38, Definition 3.7,3.8]) Let $\rho_A, \sigma_A \in \mathrm{S}_{\leq}(A)$ be two subnormalized quantum states. The **generalized fidelity** between them is defined as

$$F(\rho_A, \sigma_A) \coloneqq \left(\left\| \sqrt{\rho_A}\sqrt{\sigma_A} \right\|_1 + \sqrt{\big(1 - \mathrm{Tr}[\rho_A]\big)\big(1 - \mathrm{Tr}[\sigma_A]\big)} \right)^2. \tag{2.9}$$

The corresponding **purified distance** is given by

$$P(\rho_A, \sigma_A) \coloneqq \sqrt{1 - F(\rho_A, \sigma_A)}\,. \tag{2.10}$$

For normalized states, the second term in $F(\rho_A, \sigma_A)$ vanishes, and these definitions coincide with the standard fidelity and purified distance.

The generalized trace distance and generalized fidelity are related by the Fuchs-van de Graff inequalities, in exactly the same manner as the usual trace distance and fideltiy.

Lemma 2.1.2. *(Fuchs–van de Graaf Inequalities [38, Lemma 3.5], [39]) For all subnormalized states $\rho_A, \sigma_A \in S_{\leq}(A)$,*

$$T(\rho_A, \sigma_A) \leq P(\rho_A, \sigma_A) \leq \sqrt{2T(\rho_A, \sigma_A)}. \tag{2.11}$$

2.2 Entropies and their properties

Entropy measures quantify uncertainty, randomness, and correlations in quantum systems, and they play a central role in modern security proofs for QKD. In this thesis, we will primarily work with three kinds of entropies [38]: the von Neumann entropy, the family Rényi entropies, and smooth min- and max-entropies.

Operationally, these entropies admit interpretations in terms of fundamental information-processing tasks. For our purposes, we rely on the fact that Rényi entropies and smooth min-entropies quantify the amount of near-uniform randomness that can be extracted in the presence of quantum side information, which is precisely the quantity that enters QKD security proofs (see Lemma 3.5.1). Furthermore, under suitable conditions, both of these entropies can be related to the von Neumann entropy. The latter not only characterizes the asymptotic performance of QKD protocols, but is also the quantity that is often computed in our numerical key rate evaluations, for instance in Chapters 4 and 5.

We will now state the definitions and properties of these entropies which are required later in the thesis. We stress that the definitions are included for completeness, our analysis relies only on structural properties such as relations between conditioned and unconditioned entropies, chain rules, data-processing inequalities, and similar identities. Throughout this thesis, all logarithms (i.e, $\log(x)$) are taken to base 2.

2.2.1 Von Neumann entropy

Definition 2.2.1 (Von Neumann entropy)**.** Let $\rho_A \in \mathrm{S}_=(A)$ be a density operator. The **von Neumann entropy** of ρ_A is defined as

$$H(A)_\rho \;:=\; -\operatorname{Tr}[\rho_A \log \rho_A]\,. \tag{2.12}$$

For a bipartite state $\rho_{AB} \in \mathrm{S}_=(AB)$, we define the **conditional von Neumann entropy** by

$$H(A|B)_\rho \;:=\; H(AB)_\rho - H(B)_\rho. \tag{2.13}$$

The conditional entropy can be negative, but is non-negative if A is classical.

Lemma 2.2.1 (Averaging over conditioning on events)**.** *Let ρ_{ABCY} be a state that is classical on Y, C:*

$$\rho_{ABCY} = \sum_{y\in\Lambda} p(y)\, \rho_{ABC|y} \otimes |y\rangle\langle y|_Y\,, \tag{2.14}$$

where $p(y)$ is a probability distribution over Λ, and Y can be generated from C (more precisely: $Y \leftrightarrow C \leftrightarrow AB$ forms a Markov chain), where $\{|y\rangle\}_{y\in\Lambda}$ is an orthonormal basis for Y and each $\rho_{ABC|y} \in \mathrm{S}_=(ABC)$. Then the von Neumann conditional entropy satisfies

$$H(A|BC) = H(A|BCY)_\rho = \sum_{y\in\Lambda} p(y)\, H(A|BC)_{\rho_{|y}}. \tag{2.15}$$

Proof. The proof follows from the definition of the entropies and simple algebraic manipulations □

.

2.2.2 Renyi Entropies

Definition 2.2.2 (Rényi entropy)**.** For $\rho \in \mathrm{S}_{=}(AB)$, and $\alpha \in (0,1) \cup (1,\infty)$, the **sandwiched Rényi entropy** of A given B for a state ρ_{AB} is given by

$$\widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho} \coloneqq \max_{\sigma_B \in S_{\circ}(B)} \widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho|\sigma}, \tag{2.16}$$

where

$$\widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho|\sigma} \coloneqq \begin{cases} \frac{1}{1-\alpha} \log \mathrm{Tr}\left[\left(\sigma_B^{\frac{1-\alpha}{2\alpha}} \rho_{AB} \sigma_B^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha}\right] & \text{if } \rho \in A \otimes \mathrm{supp}(\sigma)\ , \\ -\infty & \text{otherwise.} \end{cases} \tag{2.17}$$

Note that the sandwiched Rényi Entropy may be notated differently in different works: for instance, it is denoted as $H_{\alpha}(A|B)$ in Ref. [40] (Definition 1), and $\widetilde{H}^{\uparrow}_{A|B}$ in Ref. [38] (Definition 5.2), and $H^{\uparrow}_{\alpha}(A|B)$ in Ref. [41] (Definition B.1). We will now state several results regarding the Rényi entropy that we utilize in this thesis. We start with results on data processing inequalities.

Lemma 2.2.2. *(Data-processing [42, Theorem 1]) Let $\rho \in \mathrm{S}_{=}(QQ')$, take any $\alpha \in [\frac{1}{2}, 1) \cup (1,\infty]$. Then for any channel $\mathcal{E} \in \mathrm{CPTP}(Q', Q'')$,*

$$\widetilde{H}^{\uparrow}_{\alpha}(Q|Q'')_{\mathcal{E}[\rho]} \geq \widetilde{H}^{\uparrow}_{\alpha}(Q|Q')_{\rho}. \tag{2.18}$$

If $\mathcal{E}$ is an isometry, then we have equality in the above bound.

The following lemma relates the entropy on a state conditioned on an event, to the entropy of the state without any conditioning.

Lemma 2.2.3. *([41, Lemma B.5]) Let $\rho_{ABC} \in \mathrm{S}_{=}(ABC)$ be classical on C, such that $\rho_{ABC} = \sum_c p_c \left|c\right\rangle\!\left\langle c\right| \otimes \rho_{AB|c}$ for some probability distribution $\{p_c\}$ and normalized conditional states $\rho_{AB_{|c}}$. Then, for each c and any $\alpha \in (1,\infty)$, we have:*

$$\widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho_{|c}} \geq \widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho} - \frac{\alpha}{\alpha - 1} \log\left(\frac{1}{p_c}\right) \tag{2.19}$$

The following lemma allows us to split off classical registers by subtracting the number of bits of those registers.

Lemma 2.2.4. *([43, Proposition 2.9]) Let $\rho_{ABC} \in \mathrm{S}_=(ABC)$ be classical on C. Then, for any $\alpha \in (0, \infty)$, we have:*

$$\widetilde{H}^{\uparrow}_{\alpha}(A|BC)_{\rho} \geq \widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho} - \log|C| \tag{2.20}$$

The following lemma states that Rényi entropy is additive across tensor products.

Lemma 2.2.5. *(Additivity of Rényi Entropy, [38, Corollary 5.2]) For any two states $\rho_{AB} \in \mathrm{S}_=(AB), \sigma_{CD} \in \mathrm{S}_=(CD)$, and $\alpha \geq \frac{1}{2}$, we have*

$$\widetilde{H}^{\uparrow}_{\alpha}(AC|BD)_{\rho\otimes\sigma} = \widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho} + \widetilde{H}^{\uparrow}_{\alpha}(C|D)_{\sigma}. \tag{2.21}$$

The next lemma relates the Rényi entropy to the von Neumann entropy. It is used along with the previous lemma in Chapter 4 to reduce the n-round Rényi entropy to n times the single-round von Neumann entropy.

Lemma 2.2.6. *([41, Lemma B.9]) For any $\rho_{AB} \in \mathrm{S}_=(AB)$, and $1 < \alpha < 1 + 1/\log(1 + 2d_A)$, we have*

$$\widetilde{H}^{\uparrow}_{\alpha}(A|B)_{\rho} > H(A|B)_{\rho} - (\alpha - 1)\log^2(1 + 2d_A). \tag{2.22}$$

The following lemma is analogous to Lemma 2.2.1, where we average over conditional entropies of states conditioned on events.

Lemma 2.2.7. *Let $\rho_{ABCY} = \sum_{y\in\Lambda} p(y)\rho_{ABC|y} \otimes |y\rangle\langle y| \in \mathrm{S}_=(ABCY)$ be classical in Y, C, where $p(y)$ is a probability distribution over Λ, and Y can be generated from C (more precisely: $Y \leftrightarrow C \leftrightarrow AB$ forms a Markov chain). Let $\Lambda' \subseteq \Lambda$. Then,*

$$\sum_{y\in\Lambda'} p(y) 2^{-\frac{(\alpha-1)}{\alpha}\widetilde{H}^{\uparrow}_{\alpha}(A|BC)_{\rho_{|y}}} \leq 2^{-\frac{(\alpha-1)}{\alpha}\widetilde{H}^{\uparrow}_{\alpha}(A|BC)_{\rho}}. \tag{2.23}$$

Proof. We have

$$\sum_{y\in\Lambda'} p(y) 2^{-\frac{(\alpha-1)}{\alpha}\widetilde{H}^{\uparrow}_{\alpha}(A|BC)_{\rho_{|y}}} \leq \sum_{y\in\Lambda} p(y) 2^{-\frac{(\alpha-1)}{\alpha}\widetilde{H}^{\uparrow}_{\alpha}(A|BC)_{\rho_{|y}}}, \tag{2.24}$$

since we only add positive terms to the expression to go from the LHS to the RHS. Now, on the RHS, $p(y)$ is a normalized probability distribution function over Λ. Therefore, we can directly use [38, Proposition 5.1], and we obtain

$$\sum_{y\in\Lambda} p(y) 2^{-\frac{(\alpha-1)}{\alpha}\widetilde{H}^{\uparrow}_{\alpha}(A|BC)_{\rho_{|y}}} = 2^{-\frac{(\alpha-1)}{\alpha}\widetilde{H}^{\uparrow}_{\alpha}(A|BCY)_{\rho}}. \tag{2.25}$$

Since Y can be generated from C, the fact that $\widetilde{H}^{\uparrow}_{\alpha}(A|BCY) = \widetilde{H}^{\uparrow}_{\alpha}(A|BC)$ follows by applying the data-processing inequality for Rényi entropy (Lemma 2.2.2) in both directions $YC \to C$ and $C \to YC$. Therefore, the claim follows. □

2.2.3 Smoothed min Entropies

Definition 2.2.3 (Conditional Min-Entropy)**.** Let $\rho_{AB} \in \mathrm{S}_{\leq}(AB)$ be a (possible subnormalized) bipartite quantum state. The **conditional min-entropy** of A given B is defined as

$$H_{\min}(A|B)_{\rho} := -\inf_{\sigma_B \in \mathrm{S}_{\leq}(B)} \inf\{\lambda \in \mathbb{R} : \rho \leq 2^{\lambda}\sigma\}. \tag{2.26}$$

Equivalently, $H_{\min}(A|B)_{\rho}$ is the largest real number λ such that

$$\rho_{AB} \leq 2^{-\lambda}\, \mathbb{I}_A \otimes \sigma_B$$

for some $\sigma_B \in \mathrm{S}_{\leq}(B)$.

Intuitively, the conditional min-entropy quantifies how unpredictable A is to an observer holding the quantum system B. In the special case where A is classical, it characterizes the optimal probability of correctly guessing the value of A given access to B:

$$p_{\text{opt-guess}}(A|B)_{\rho} = 2^{-H_{\min}(A|B)_{\rho}}.$$

Hence, a larger min-entropy corresponds to a smaller guessing probability and thus to greater secrecy of A conditioned on B.

Definition 2.2.4 (Smooth Entropies)**.** For $\varepsilon \geq 0$, the **ε-smoothed conditional min-entropy** of A given B is defined as

$$H^{\varepsilon}_{\min}(A|B)_{\rho} := \sup_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}, \tag{2.27}$$

where $\mathcal{B}^{\varepsilon}(\rho_{AB})$ denotes the set of all subnormalized states $\tilde{\rho}_{AB} \in \mathrm{S}_{\leq}(AB)$ that are ε-close to ρ_{AB} in purified distance:

$$\mathcal{B}^{\varepsilon}(\rho_{AB}) = \{\, \tilde{\rho}_{AB} \in \mathrm{S}_{\leq}(AB) : P(\tilde{\rho}_{AB}, \rho_{AB}) \leq \varepsilon \,\}. \tag{2.28}$$

Similarly, the ε-**smoothed conditional max-entropy** of A given B is defined as

$$H_{\max}^{\varepsilon}(A|B)_{\rho} \coloneqq \inf_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}, \tag{2.29}$$

The smoothing parameter ε allows for small perturbations of the state ρ_{AB} and captures a notion of approximate secrecy: $H_{\min}^{\varepsilon}(A|B)_{\rho}$ quantifies the number of nearly uniform and independent bits that can be extracted from A given access to B, up to an error ε. We will work with smooth entropies in Chapter 6 where we will utilize the following statement known as entropic uncertainty relations:

Theorem 2.2.1 (Entropic uncertainty relation with quantum side information [44])**.** *Let $\rho_{ABE} \in \mathrm{S}_{=}(ABE)$[3] be a tripartite state. Consider two POVMs on A, given by $\{M_x\}_{x\in\mathcal{X}}$, and $\{N_z\}_{z\in\mathcal{Z}}$, and refer to them as X and Z respectively. Let X and Z be the classical registers that store the classical outcomes obtained by measuring register A with these these POVMs respectively (while leaving the other registers unchanged), so that the corresponding post-measurement classical–quantum states are*

$$\rho_{XBE} = \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A \left[(M_x \otimes \mathbb{I}_{BE})\rho_{ABE}\right], \tag{2.30}$$

and

$$\rho_{ZBE} = \sum_{z\in\mathcal{Z}} |z\rangle\langle z|_Z \otimes \mathrm{Tr}_A \left[(N_z \otimes \mathbb{I}_{BE})\rho_{ABE})\right]. \tag{2.31}$$

Then, for any $\varepsilon \in (0,1)$,

$$H_{\min}^{\varepsilon}(Z|E)_{\rho} + H_{\max}^{\varepsilon}(X|B)_{\rho} \;\geq\; \log\left(\frac{1}{c_q}\right), \tag{2.32}$$

where the ***measurement incompatibility constant*** *c_q is defined by*

$$c_q \;\coloneqq\; \max_{x\in\mathcal{X},\, z\in\mathcal{Z}} \left\| \sqrt{M_x}\,\sqrt{N_z} \right\|_{\infty}^{2}. \tag{2.33}$$

[3]We can also extend this statement to subnormalized states, but we do not require it in this thesis.

The quantity c_q quantifies the overlap (or compatibility) of the two POVMs. If the two POVMs are nearly compatible (large overlap), then c_q is close to 1 and the bound in Eq. (2.32) becomes weak. Conversely, if the measurements are highly incompatible (small overlap), then c_q is small and the right-hand side $\log(1/c_q)$ is large, forcing a strong tradeoff: high predictability of the X outcome given E implies low predictability of the Z outcome given B, and vice versa. We will see how this is utilized in the QKD security analysis in Section 3.7.1 and Chapter 6. We will now state some lemmas that we need to work with these entropies.

The following lemma can be used to remove classical registers from the smooth min-entropy, as long as one subtracts the number of bits of those registers, analogous to Lemma 2.2.4.

Lemma 2.2.8. *([38, Lemma 6.8]) Let $\rho_{AEC} \in \mathrm{S}_{\leq}(AEC)$ be a (possibly subnormalized) state classical on C. Then, for every $\varepsilon \in (0,1)$,*

$$H_{\min}^{\varepsilon}(A|EC)_{\rho} \geq H_{\min}^{\varepsilon}(A|E)_{\rho} \; - \; \log|C|. \tag{2.34}$$

The following lemma is used to relate the entropy conditioned on an event to the entropy without conditioning on the event. Notice that it concerns states that are *partial* on an event (not *conditioned*), i.e, the states that include the events are not normalized.

Lemma 2.2.9 ([34, Lemma 10])**.** *Let $\rho_{AEC} \in \mathrm{S}_{\leq}(AEC)$ be a (possibly subnormalized) state classical on C, and let Ω be any event on C. Then, for every $\varepsilon \in (0, \sqrt{\Pr(\Omega)_{\rho}})$, we have:*

$$H_{\min}^{\varepsilon}(A|EC)_{\rho\wedge\Omega} \geq H_{\min}^{\varepsilon}(A|EC)_{\rho} \tag{2.35}$$

Lemma 2.2.10 (Data processing inequality for the smooth min-entropy [38, Theorem 6.2]))**.** *Let $\rho_{AQ} \in \mathrm{S}_{\leq}(AQ)$ be a (possibly subnormalized) quantum state, and let $\mathcal{E} \in \mathrm{CPTP}(Q, Q')$. Then, for every $\varepsilon \in [0, \sqrt{\mathrm{Tr}[\rho]}))$,*

$$\begin{aligned} H_{\min}^{\varepsilon}(A \mid Q)_{(\rho_{AQ})} \; &\leq \; H_{\min}^{\varepsilon}(A \mid Q')_{(\mathbb{I}_A\otimes\mathcal{E})[\rho_{AQ}]}, \\ H_{\max}^{\varepsilon}(A \mid Q)_{(\rho_{AQ})} \; &\leq \; H_{\max}^{\varepsilon}(A \mid Q')_{(\mathbb{I}_A\otimes\mathcal{E})[\rho_{AQ}]}. \end{aligned} \tag{2.36}$$

2.3 Quantum Optics

QKD protocols are implemented using quantum optics, with information encoded in photons of light. As a result, it is necessary to understand the basic principles of quantum optics in

order to construct accurate mathematical models of the quantum operations performed by the honest parties. In particular, we must understand the mathematical descriptions of states prepared by Alice and the measurements performed by Bob. For an introductory treatment of quantum optics, see Ref. [45].

2.3.1 Optical modes

In classical electrodynamics, an optical mode refers to an element of a chosen orthonormal basis of solutions to Maxwell's equations for the electromagnetic field (or equivalently, for the vector potential) in vacuum, subject to appropriate boundary conditions. A general classical field configuration can be expressed as a linear combination of such modes.

Upon quantization, the electromagnetic field is promoted to an operator-valued field. In the canonical quantization procedure, the complex amplitudes associated with each classical mode are replaced by annihilation and creation operators. Each optical mode is then mathematically equivalent to an independent quantum harmonic oscillator.

It is important to emphasize that an optical mode is simply a choice of basis used to describe the quantum optical system. In principle, one may choose any complete orthonormal mode basis (for example, plane-wave modes, cavity modes, or wavepacket modes). Each choice comes equipped with mode functions that determine how physical quantities of interest such as the electric and magnetic field operators vary in space and time. For the purposes of this thesis, we do not need to work explicitly with the spatial structure of the mode functions, and we therefore focus only on the associated mode operators.

Let $\hat{a}$ and $\hat{a}^\dagger$ denote the annihilation and creation operators of a given optical mode, and let $|\text{vac}\rangle$ denote the vacuum state, corresponding to the absence of photons in that mode. These operators satisfy the canonical commutation relation

$$[\hat{a}, \hat{a}^\dagger] = 1. \tag{2.37}$$

In this thesis, we consider state-preparation procedures that produce either (i) ideal single-photon qubit states[4] or (ii) phase-randomized weak coherent states. Ideal single-photon states are useful as a conceptual model and as a benchmark for security analyses, while weak coherent states provide an accurate description of practical optical sources (lasers) used in quantum key distribution. To describe both cases, we first introduce Fock states.

[4] A single photon state over two modes is exactly identical to qubit.

Fock states

Fock states, also known as photon-number states, are eigenstates of the number operator $\hat{a}^\dagger\hat{a}$. We denote these states by $|n\rangle$, where $N \in \mathbb{N}$ denotes the eigenvalue of the state. That is, they satisfy

$$\hat{a}^\dagger\hat{a}\,|N\rangle = N\,|N\rangle\,. \tag{2.38}$$

The vacuum state is given by $|\text{vac}\rangle$, where we reserve the use of $|0\rangle$ to describe one of the basis states of a qubit, and use $|\text{vac}\rangle$ to denote the zero photon vacuum state instead. Higher-number states can be generated by repeated application of the creation operator,

$$|N\rangle = \frac{(\hat{a}^\dagger)^N}{\sqrt{N!}}\,|\text{vac}\rangle\,. \tag{2.39}$$

The set $\{|N\rangle : N \in \mathbb{N}\}$ forms a complete orthonormal basis for the Hilbert space of a single optical mode.

The action of the annihilation and creation operators on Fock states is given by

$$\hat{a}\,|N\rangle = \sqrt{N}\;|N-1\rangle\,, \tag{2.40}$$

$$\hat{a}^\dagger\,|N\rangle = \sqrt{N+1}\;|N+1\rangle\,, \tag{2.41}$$

for all $n \in \mathbb{N}$, with the convention that $\hat{a}\,|\text{vac}\rangle = 0$.

Single-photon states

A single-photon state corresponds to the Fock state $|1\rangle$. In practice, photons possess additional degrees of freedom, such as polarization, temporal mode, or spatial mode. When restricting attention to a fixed optical mode, the single-photon subspace is one-dimensional. However, when additional degrees of freedom are considered—most notably polarization—the single-photon subspace can be used to encode a qubit.

For example, fixing all degrees of freedom except polarization, one may define two orthogonal single-photon states $|1\rangle_H = \hat{a}_H^\dagger\,|\text{vac}\rangle$ and $|1\rangle_V = \hat{a}_V^\dagger\,|\text{vac}\rangle$ corresponding to horizontal and vertical polarization, respectively. An arbitrary single-photon qubit state can then be written as a superposition

$$\alpha\,|1\rangle_H + \beta\,|1\rangle_V\,,$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

Coherent states

Coherent states are defined as eigenstates of the annihilation operator. For a complex amplitude $\alpha \in \mathbb{C}$, the coherent state $|\alpha\rangle$ satisfies

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.42}$$

Coherent states can be expressed in the Fock basis as

$$|\alpha\rangle := e^{-|\alpha|^2/2} \sum_{N=0}^{\infty} \frac{\alpha^N}{\sqrt{N!}}\,|N\rangle\,. \tag{2.43}$$

The mean photon number of the coherent state is given by

$$\mu := \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = |\alpha|^2. \tag{2.44}$$

One can write α as $\alpha = \sqrt{\mu}\,e^{i\theta}$ where $\theta \in [0, 2\pi]$ corresponds to the phase and $\mu \in \mathbb{R}$ corresponds to the intensity of the coherent state.

In many practical settings the optical phase is not fixed but is instead uniformly randomized. We refer to the resulting state as a *phase-randomized* coherent state. It is defined as the mixture

$$\rho_\mu^{\mathrm{PR}} := \frac{1}{2\pi}\int_0^{2\pi} d\theta\ \left|\sqrt{\mu}e^{i\theta}\right\rangle\!\left\langle\sqrt{\mu}e^{i\theta}\right|. \tag{2.45}$$

Using the Fock-basis expansion of coherent states (Eq. (2.43)), one finds that phase randomization removes the off-diagonal coherences in the photon-number basis, yielding a state that is diagonal in the Fock basis:

$$\rho_\mu^{\mathrm{PR}} = \sum_{N=0}^{\infty} p_\mu^{\mathrm{poiss}}(N)\ |N\rangle\langle N|\,, \tag{2.46}$$

where $p_\mu^{\mathrm{poiss}}(N)$ is the Poisson distribution with mean μ,

$$p_\mu^{\mathrm{poiss}}(N) = e^{-\mu}\frac{\mu^N}{N!}, \qquad N \in \mathbb{N}. \tag{2.47}$$

In particular, ρ_μ^{PR} may be interpreted as a classical mixture of N-photon Fock states, where the photon number N is distributed according to $p_\mu^{\mathrm{poiss}}(N)$.

2.3.2 Detectors

In QKD, Bob's measurement apparatus is implemented using standard linear-optical elements such as beam splitters (BS) and polarizing beam splitters (PBS) followed by (single-photon) threshold detectors. In this thesis we model these components at a level sufficient to describe the POVMs induced on the relevant optical modes, as is standard for QKD security analysis.

Beam splitters

A (lossless) beam splitter is a two-mode linear optical element that mixes two input modes into two output modes via a unitary transformation (see Fig. 2.1). Let $\hat{a}$ and $\hat{b}$ denote annihilation operators for two input spatial modes. A beam splitter with amplitude transmissivity t and reflectivity r (satisfying $|t|^2 + |r|^2 = 1$) induces the following mode transformation

$$\begin{pmatrix} \hat{a}_{\text{out}} \\ \hat{b}_{\text{out}} \end{pmatrix} = \begin{pmatrix} t & r \\ -r^* & t^* \end{pmatrix} \begin{pmatrix} \hat{a}_{\text{in}} \\ \hat{b}_{\text{in}} \end{pmatrix}. \tag{2.48}$$

A common convention for a symmetric 50:50 beam splitter is $t = 1/\sqrt{2}$ and $r = i/\sqrt{2}$, for which

$$\hat{a}_{\text{out}} = \frac{\hat{a}_{\text{in}} + i\hat{b}_{\text{in}}}{\sqrt{2}}, \qquad \hat{b}_{\text{out}} = \frac{i\hat{a}_{\text{in}} + \hat{b}_{\text{in}}}{\sqrt{2}}.$$

Beam splitters are used throughout polarization-based BB84 receivers, to select a measurement basis passively or to route light between different interferometric paths.

Polarizing beam splitters

A polarizing beam splitter (PBS) separates two orthogonal polarizations (e.g., horizontal H and vertical V) into different spatial output modes (see Fig. 2.2). At an idealized level, a PBS acts as a polarization-dependent router: it transmits one polarization and reflects the orthogonal polarization. In a polarization-encoded BB84 receiver, a PBS is typically used to map the two orthogonal polarization outcomes to two separate detectors.

Threshold detectors

A threshold detector is a binary (on/off) photodetector: it does not measure the photon number, but only reports whether at least one photon was detected (see Fig. 2.3). In the

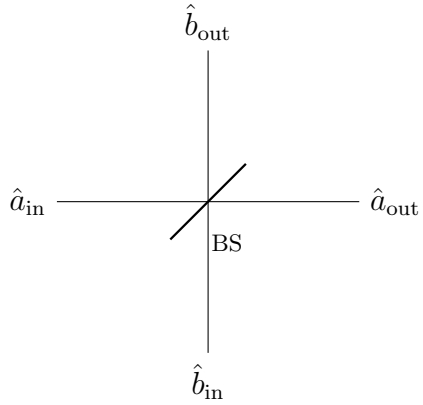


Figure 2.1: Schematic of a beam splitter with two input ports (left and bottom) and two output ports (right and top).

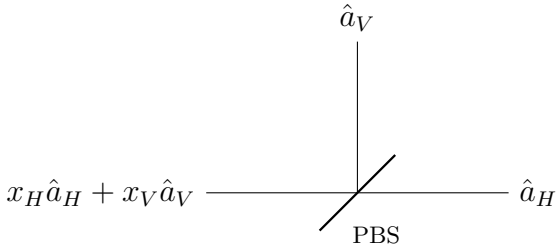


Figure 2.2: Idealized polarizing beam splitter (PBS) that routes the horizontal and vertical polarization components of the input mode into separate spatial output modes.

idealized perfect case (unit efficiency, no dark counts), the measurement has outcomes *no click* and *click*, described by the POVM

$$\Gamma_{\text{noclick}} \coloneqq |\text{vac}\rangle\langle\text{vac}|\,, \qquad \Gamma_{\text{click}} \coloneqq \mathbb{I} - |\text{vac}\rangle\langle\text{vac}| = \sum_{n=1}^{\infty} |n\rangle\langle n|\,, \tag{2.49}$$

where the operators act on the Hilbert space of the measured optical mode, that is, the mode going into the detector.

Realistic threshold detectors are imperfect. Two dominant non-idealities are:

- **Finite detection efficiency:** the probability that an incoming single photon produces a detection event is typically less than 1. This effect is modeled by a parameter $\eta \in [0, 1]$, referred to as the (overall) detection efficiency.

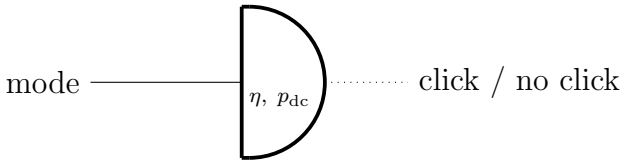


Figure 2.3: Schematic of a threshold (on/off) detector. In the imperfect model, η denotes the overall detection efficiency and p_{dc} the dark-count probability per detection window.

- **Dark counts:** the detector may produce a click even in the absence of incident photons. Experimentally, dark counts are often reported as a rate (e.g., counts per second). For theoretical analysis, however, it is convenient to work with the probability of a dark count occurring within a given detection time window. We denote this probability by $p_{\mathrm{dc}} \in [0, 1]$.

These effects are commonly modeled as follows. Loss is treated as an effective beam splitter of transmissivity η placed in front of an otherwise ideal threshold detector, so that each photon is independently transmitted to the detector with probability η. Dark counts are modeled as classical post-processing: independently of the incoming optical state, the detector produces a click with probability p_{dc} during the detection time window.

Taken together, this model implies that, when the detector is illuminated by an n-photon Fock state $|n\rangle$, the probability of obtaining no click is

$$\Pr(\text{noclick} \mid n) = (1 - p_{\mathrm{dc}})\,(1 - \eta)^n, \tag{2.50}$$

i.e., no dark count occurs and all n photons fail to be detected. Equivalently, the corresponding POVM elements describing the imperfect threshold detector are

$$\Gamma^{\mathrm{noisy}}_{\mathrm{noclick}} = (1 - p_{\mathrm{dc}}) \sum_{n=0}^{\infty} (1 - \eta)^n \,|n\rangle\langle n|\,, \qquad \Gamma^{\mathrm{noisy}}_{\mathrm{click}} = \mathbb{I} - \Gamma^{\mathrm{noisy}}_{\mathrm{noclick}}. \tag{2.51}$$

This simple model is widely used in QKD security analyses, as it accurately captures the statistics of threshold detection while avoiding the introduction of additional internal detector degrees of freedom.

Having covered the basics of quantum optics, we will specify the relevant details of state preparation and measurement in QKD protocols in Section 3.2.1.

2.4 Miscellaneous

In this section we collect some remaining miscellaneous concepts. We start with the definition of universal$_2$ hashing, which is a critical ingredient of QKD protocols.

Definition 2.4.1. (δ-almost-universal$_2$ and universal$_2$ hash families) Given a domain D and a finite codomain D', a **δ-almost-universal$_2$** (δ-AU$_2$) hash family consists of a set $\mathcal{F}$ of functions $f : D \to D'$, together with a probability distribution P_{HASH} over $\mathcal{F}$. The defining property is that, if h is sampled according to P_{HASH}, then for all distinct $x, y \in D$, the probability of a collision is bounded as,

$$\Pr[h(x) = h(y)] \leq \delta, \tag{2.52}$$

where the probability is taken over the choice of h. A special case is **universal$_2$ hashing**, which corresponds to

$$\delta = \frac{1}{|D'|}. \tag{2.53}$$

A further special case is **ideal universal$_2$ hashing**, which corresponds to $\delta = \frac{1}{|D'|}$ and equality holding in Eq. (2.52), i.e. for all distinct $x, y \in D$,

$$\Pr[h(x) = h(y)] = \frac{1}{|D'|}. \tag{2.54}$$

It is straightforward to show that the family of maps from m bits to n bits defined by matrix multiplication, after choosing an $n \times m$ binary matrix uniformly at random, is an ideal universal$_2$ family of hash functions. However, this construction is not typically used in QKD applications, as it requires a seed of length mn bits to specify the matrix. Instead, structured families of universal hash functions with much smaller seed requirements are employed. In particular, Toeplitz hashing is known to be ideal universal$_2$ [46], while requiring only $(m + n - 1)$ bits of seed randomness.[5]

We will also work with frequency distributions and probability distributions, which are defined below.

[5] A Toeplitz matrix is a matrix whose entries are constant along each diagonal. That is, an $n \times m$ binary Toeplitz matrix T satisfies $T_{i,j} = t_{i-j}$ for some binary sequence $\{t_k\}$, so the entire matrix is fully specified by its first row and first column, requiring $m + n - 1$ bits in total.

Definition 2.4.2. (Frequency distributions) For a string $z_1^n \in \mathcal{Z}^n$ on some alphabet $\mathcal{Z}$, $\text{freq}_{z_1^n}$ denotes the following probability distribution on $\mathcal{Z}$:

$$\text{freq}_{z_1^n}(z) \coloneqq \frac{\text{number of occurrences of } z \text{ in } z_1^n}{n}. \tag{2.55}$$

We denote the set of probability distributions over an alphabet $\mathcal{Z}$, via $\mathbb{P}(\mathcal{Z})$. Note that we have, by definition, $\text{freq}_{z_1^n} \in \mathbb{P}(\mathcal{Z})$.

2.4.1 Numerics

We will often be tasked with solving optimization problems of the form

$$\begin{aligned} &\inf_{\rho} && f(\rho) \\ &\text{subject to:} && \text{linear constraints on } \rho, \\ &&& \rho > 0 \end{aligned} \tag{2.56}$$

where $f(\rho)$ is a convex function. Loosely speaking, this can be interpreted as optimizing over the worst-case attack by an adversary that is compatible with the observed statistics. The objective function $f(\rho)$ is typically some single-round entropic quantity of interest, $\rho > 0$ ensures that we get a valid quantum state, and compatibility with observations is enforced via linear constraints on ρ.

The main challenge in performing these computations is that we require a value that is guaranteed to be a *lower bound* on the true infimum. Consequently, some common optimization approaches, such as gradient descent, are not immediately suitable, as they do not provide guarantees of global optimality. Fortunately, several works have developed numerical methods that aim to produce values below the true QKD infimum [9, 47, 48, 49, 50, 51, 52, 53, 54] for a variety of relevant optimization problems.

In this thesis, we will *not* go into the details or nuances of performing these computations, and instead rely on established work that addresses these tasks. Nevertheless, we note that this topic can be subtle and technically involved. Practical constraints such as numerical precision and solver tolerances often complicate attempts to obtain reliable lower bounds. Moreover, various modifications (with appropriate justification) are frequently applied to reduce the complexity of the problem before it is passed to a numerical routine. We do not discuss these details in this thesis, and instead refer to the specific papers that develop these techniques for more details. In particular, we primarily rely on Ref. [47] for the computations in Chapters 4 and 5, and its extension to Rényi entropies [9] in Chapter 7.

Chapter 3

Basics of Quantum Key Distribution

> Where we explain what QKD is and why it works; where we introduce the central tools used in practical QKD security analysis; and where we outline the range of proof techniques available for QKD security analysis.

In this chapter, we cover the basic concepts and tools of QKD security analysis that are used throughout this thesis. We restrict our attention to prepare-and-measure QKD protocols, as these are the primary focus of this thesis. Nevertheless, many of the tools presented here also apply to entanglement-based protocols, and in some cases can be extended to measurement-device-independent (MDI) QKD [55].

Quantum key distribution (QKD) enables two distant parties, Alice and Bob, to establish a shared secret key by exchanging quantum states and authenticated classical messages (see Fig. 3.1). Both Alice and Bob are assumed to have access to local randomness if needed[1], which they utilize in making random choices. This randomness is assumed to be perfect, and uncorrelated to the adversary. Alice uses this randomness to prepare quantum states and send them to Bob, who performs measurements (potentially using his local randomness) on the received systems. The quantum channel connecting Alice and Bob is assumed to be completely insecure: the adversary Eve is allowed to perform arbitrary operations on the quantum systems leaving Alice's laboratory before they enter Bob's laboratory. The intuitive reason why QKD is possible is that Alice sends quantum states that are not all mutually orthogonal. Consequently, no party (including Eve) can perfectly distinguish all possible signal states sent by Alice.

[1] Atleast one party is required to utilize local randomness to create the initial raw data in QKD.

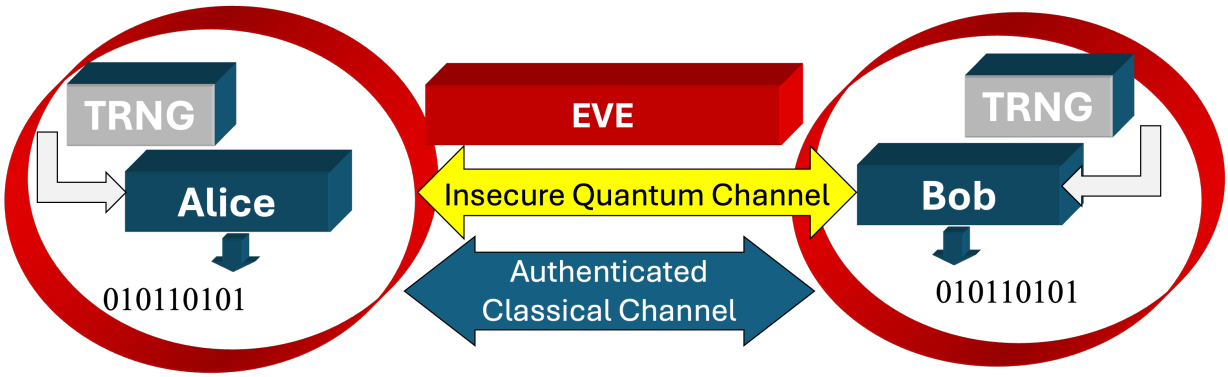


Figure 3.1: Schematic of a quantum key distribution (QKD) protocol. The task is to establish a shared secret key between two distant parties, Alice and Bob. The protocol relies on trusted quantum devices operated within secure perimeters, access to local true random number generators (TRNGs), an authenticated classical channel, and an insecure quantum channel that may be fully controlled by an adversary. Figure from [10].

However, secrecy alone is not sufficient: Alice and Bob must also end up with *identical* keys. At first glance, this appears contradictory, since Bob must be able to correctly infer Alice's data, while we have just argued that no measurement can perfectly distinguish all of Alice's states. This tension is resolved as follows. After Alice has sent the quantum states and Bob has performed his measurements, Alice announces (over a classical channel) which *subset* each signal state belongs to. These subsets are typically chosen so that the states within each subset are perfectly distinguishable. In some rounds, Bob's measurement is compatible with the announced subset, allowing him to infer Alice's data with high accuracy; in other rounds, it is not, and those rounds are discarded. This procedure necessarily requires classical communication between Alice and Bob.

Classical communication is also required for several other steps of the protocol. Alice and Bob must inspect parts of their data to decide whether to accept or abort the protocol, and to determine the length of the final key they aim to generate. Moreover, in any practical implementation, noise and imperfections lead to discrepancies between Alice's and Bob's data, making it necessary to perform classical post-processing steps such as error correction, error verification, and privacy amplification. These procedures are discussed in detail in Section 3.2.

Throughout this thesis, Alice and Bob are assumed to have access to an authenticated classical channel. Except in Chapter 8, this assumption is taken to mean that all classical messages sent by one honest party are eventually received correctly by the other party,

without modification. The adversary is allowed to read all classical messages, but is assumed not to tamper with them. This is a standard assumption in QKD security proof literature. In Chapter 8, we examine this assumption in detail, and show that while it is unrealistic, the security analysis undertaken with this unrealistic assumption can then be subsequently lifted to hold under weaker and more realistic assumptions (see Remark 3.1.1 in the next section).

This chapter is organized as follows. In Section 3.1, we introduce the security definition of QKD, and define the two requirements of *secrecy* and *correctness*. In Section 3.2, we present a generic description for prepare-and-measure QKD protocols, which we analyze in subsequent chapters. In Section 3.3, we describe the states prepared, measurements performed, announcements made, and sifting procedures for the protocols studied in this thesis. In Section 3.4 we show that correctness is satisfied for the protocol we study, and thus for the rest of this thesis, we focus on proving secrecy. In Section 3.5, we state the Leftover Hashing Lemma and explain its central role in proving the secrecy of QKD protocols. In Section 3.5.1, we explain the various kinds of entropic bounds that are needed to use the Leftover Hashing Lemma, and briefly discuss how such bounds can be obtained. In Section 3.6, we present some tools that are widespread in QKD security analysis, such as source-replacement schemes [56, 57], source maps [58], squashing maps [59, 60, 61, 62, 63]. Finally, in Section 3.7 we briefly discuss the various QKD proof techniques, which are expanded upon in later chapters.

3.1 Security Definition

Let us focus on the output state of a generic QKD protocol, defined on the registers $K_A K_B \boldsymbol{E}$. Alice and Bob possess classical registers K_A and K_B, which encode keys of arbitrary length. This is formalized by modelling K_A as a direct sum

$$K_A = \bigoplus_{l_A} K_A^{l_A},$$

where $K_A^{l_A}$ is a classical register holding a key of length l_A. An analogous decomposition is used for K_B. We treat any party aborting as outputting a key of length 0, represented by a special symbol $\perp$. The register $\boldsymbol{E}$ denotes all of Eve's information at the end of the protocol, and may include a copy of all classical communication.

For the entirety of this thesis, except in Chapter 8, we consider a setting in which the QKD protocol always terminates with Alice and Bob outputting keys of the *same* length.

In the communication model we adopt (where all messages are transmitted faithfully, and delivered some time after they are sent), such a requirement can be enforced by appropriate protocol design, for instance by having Alice and Bob exchange their respective output key length values, ensuring that the lengths match.

Remark 3.1.1. *Realistic channels do not provide such strong guarantees, since Eve can always block, reorder, or delay classical messages. Nevertheless, in Chapter 8 we show that any security analysis carried out under the assumption of honest authentication (i.e., all messages are delivered faithfully at some point after being sent, with no adversarial interference) can be* lifted *to the more realistic setting where Eve may attack the classical authentication mechanism. This lifting procedure is entirely generic, and does not depend on the details of the QKD protocol. For simplicity, we therefore adopt the standard honest authentication assumption throughout the initial parts of this thesis, and later show in Chapter 8 how this assumption can be removed.*

In this case, the output state can be written as

$$\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \coloneqq \bigoplus_l \Pr(\Omega_{\text{len}=l}) \rho^{\text{real}}_{K_A^l K_B^l \boldsymbol{E} | \Omega_{\text{len}=l}} \tag{3.1}$$

where $\Omega_{\text{len}=l}$ denotes the event that Alice and Bob produce a key of length l. The ideal output state $\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}}$ is defined to be the one obtained by acting a map $\mathcal{R}_{\text{ideal}} \in \text{CPTP}(K_A K_B, K_A K_B)$ acting on the real output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}$ as

$$\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} \coloneqq \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \right]. \tag{3.2}$$

The map $\mathcal{R}_{\text{ideal}}$ looks at the length of the keys stored in registers K_A, K_B to compute l, and replaces the K_A, K_B registers with the ideal state[2]

$$\tau^{l,l}_{K_A K_B} = \frac{1}{2^l} \sum_{k \in \{0,1\}^l} |kk\rangle\langle kk|_{K_A K_B} \tag{3.3}$$

Thus intuitively, any key obtained from the ideal state is safe to use, since it is "secret" against any side-information registers. We can now state the security definition of QKD.

Definition 3.1.1. (QKD Security with symmetric aborts [64, 65]) Let $\mathcal{P}_{\text{QKD}}$ be a QKD protocol, and let $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}$ be the output state of the QKD protocol, and let $\mathcal{W}(\mathcal{P}_{\text{QKD}})$ denote the set of possible output states of the QKD protocol. Suppose that the output

[2] If $l = 0$, then $\tau^{l,l}_{K_A K_B} = |\perp\perp\rangle\langle\perp\perp|_{K_A K_B}$.

key lengths for all output states in $\mathcal{W}(\mathcal{P}_{\text{QKD}})$ are always equal. Let $\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}}$ be the ideal output state, obtained by acting the map $\mathcal{R}_{\text{ideal}}$ on the actual output state. That is

$$\begin{aligned}\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} &\coloneqq \bigoplus_l \Pr(\Omega_{\text{len}=l}) \rho^{\text{real}}_{K_A^l K_B^l \boldsymbol{E}|\Omega_{\text{len}=l}}, \\ \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} &\coloneqq \mathcal{R}_{\text{ideal}}\left[\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}\right].\end{aligned} \tag{3.4}$$

Then, the (variable-length) QKD protocol is $\varepsilon^{\text{secure}}$-secure if, for all output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$[3], the following inequality is satisfied[4]:

$$\frac{1}{2}\left\|\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}}\right\|_1 \leq \varepsilon^{\text{secure}}. \tag{3.5}$$

If one specializes to a case where the QKD protocol outputs a key of some *fixed* length l_{fixed} conditioned on a particular acceptance event Ω_{acc}, and aborts otherwise (i.e. produces a key of zero bits upon the event $\Omega^{\text{C}}_{\text{acc}}$), then we refer to it as a fixed-length protocol. In this case, the states in Eq. (3.4) simplify further to the special form

$$\begin{aligned}\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} &\coloneqq \Pr(\Omega_{\text{acc}}) \rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{acc}}} + \Pr\left(\Omega^{\text{C}}_{\text{acc}}\right) \rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega^{\text{C}}_{\text{acc}}}, \\ \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} &\coloneqq \mathcal{R}_{\text{ideal}}\left[\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}\right],\end{aligned} \tag{3.6}$$

and thus the above $\varepsilon^{\text{secure}}$-security condition (for a fixed-length QKD protocol) simplifies to the condition that all output states $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$ satisfy

$$\frac{1}{2}\left\|\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}}\right\|_1 = \Pr(\Omega_{\text{acc}}) \frac{1}{2}\left\|\rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{acc}}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{acc}}}\right\|_1 \leq \varepsilon^{\text{secure}}, \tag{3.7}$$

since the distance between the real and ideal states is zero when the protocol aborts ($\Omega^{\text{C}}_{\text{acc}}$ occurs).

Thus, a QKD protocol is said to be secure if it always outputs a state that is close to an ideal state. In fact, the above definition can be shown to be universally composable [65, 64, 67], meaning that the generated key can be safely used as a subroutine in arbitrary

[3]Throughout this thesis, we will often work with equivalent descriptions of the QKD protocol and of the security definition. These descriptions are equivalent due to the fact that they all characterize the same correct set of possible output states.

[4]Note that in Ref. [66], the trace norm appearing in the security definition is not divided by 2. In contrast, the typical security definition [64, 65] includes the explicit factor of 1/2. The definition used in Ref. [66] is deliberate and well motivated within that work; we stress that the difference amounts only to an overall factor of 2 in the security parameter.

cryptographic applications without compromising security, even when composed with other protocols and executed concurrently. While composability is a subtle concept which we do not discuss here, one can already see its essential content directly from the trace-distance criterion. In particular, it is easy to show that replacing the ideal QKD output state with the real output state at any point within a larger cryptographic protocol can only change the probability of an event (in the larger cryptographic protocol) by at most $\varepsilon^{\text{secure}}$. Thus, for the purposes of the security analysis of the larger protocol, one can assume that one has access to the ideal QKD state.

3.1.1 Performance

Notice that the security definition itself says nothing how often a key is produced. In particular, the probability that the protocol accepts or aborts depends on the attack strategy employed by Eve, and no restrictions are imposed on this behaviour. From a purely security-theoretic perspective, a protocol that aborts all the time is therefore perfectly secure.

> "A plane that doesn't fly usually doesn't crash."
>
> Renato Renner [68].

For this reason, security alone is not a sufficient criterion for judging the usefulness of a QKD protocol. One must additionally consider its performance.

This requires specifying an honest behaviour of the protocol, which specifies the realistic behaviour of the protocol when no adversary is present. A common performance criterion is *robustness*, which guarentees that the protocol does not abort too often for the specified honest behaviour. In this case, one shows that, under a specified honest model, the protocol accepts with high probability at least $1 - \varepsilon_{\text{robust}}$.

An alternative, and often more informative, figure of merit is the *expected key rate*. This is the average performance of the protocol over multiple runs, under the assumed honest behaviour. The expected key rate captures both the probability of acceptance and the amount of key generated upon acceptance.[5]

[5]Note that the expected key rate comes with its own subtleties. Consider any QKD protocol that is ε-secure, with some expected key length. Now, modify this protocol so that Alice first tosses a coin with probability $\varepsilon_{\text{coin}}$ of landing tails. If the coin lands heads, she implements the original QKD protocol; if it lands tails, she simply tells Bob, and they insert an arbitrarily long string of zeros into the key register.

3.1.2 Secrecy and Correctness

The security requirement for QKD is typically broken down into two simpler requirements of secrecy and correctness, which we define below. We state the definitions for variable-length protocols, since fixed-length protocols can simply be treated as a special case of variable-length protocols where there are only two possible output lengths, ℓ_{fixed} and 0.

Definition 3.1.2 (Correctness and Secrecy)**.** Let $\mathcal{P}_{\text{QKD}}$ be a QKD protocol, and let $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}$ be the output state of the QKD protocol, and let $\mathcal{W}(\mathcal{P}_{\text{QKD}})$ denote the set of possible output states of the QKD protocol, i.e, consider the same setting as in Definition 3.1.1. The QKD protocol is $\varepsilon^{\text{secret}}$-secret if, for all output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$, the following inequality is satisfied:

$$\frac{1}{2}\left\|\rho^{\text{real}}_{K_A \boldsymbol{E}} - \rho^{\text{ideal}}_{K_A \boldsymbol{E}}\right\|_1 \leq \varepsilon^{\text{secret}}. \tag{3.8}$$

The QKD protocol is $\varepsilon^{\text{correct}}$-correct, if, for all output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$, the following inequality is satisfied:

$$\Pr(K_A \neq K_B)_{\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}} \leq \varepsilon^{\text{correct}}. \tag{3.9}$$

The secrecy requirement ensures that Alice's key is secret and unknown to Eve. The correctness requirement ensures that Alice and Bob have the same key. Both requirements can be combined to obtain the required security property for QKD protocols via the following lemma, proved in Appendix. E.

Lemma 3.1.1. *(Correctness and Secrecy imply Security) A QKD protocol that is $\varepsilon^{\text{secret}}$-secret, and $\varepsilon^{\text{correct}}$-correct, is $(\varepsilon^{\text{secret}} + \varepsilon^{\text{correct}})$-secure.*

3.2 Protocol Description

In this section, we describe a generic QKD protocol that will serve as the basis for our security analysis throughout this thesis. A more general and formal version of this protocol will be introduced in Chapter 7, where it will be analyzed in detail. We deliberately begin

This modified protocol can be easily shown to be $(\varepsilon + \varepsilon_{\text{coin}})$-secure. However, the expected key rate can now be made arbitrarily large. Clearly, one would not want to use such a protocol, because in the special case where the coin lands tails, Alice and Bob would generate an extremely long but essentially meaningless key, and in fact would never need to run a new QKD protocol again.

with a simpler formulation here for two reasons. First, the analyses in Chapters 4 to 6 is unable to handle the general version of this protocol which can be tackled using the full generality of the MEAT [11], and thus introducing all of its components at this stage would only obscure the key ideas. Second, the level of formality and precision in Chapter 7 is substantially higher than in the other chapters, since Chapter 7 is intended to provide a complete and rigorous security analysis. Thus, we omit some technical details that are included in that complete analysis which are not needed in Chapters 4 to 6. Importantly, the simpler protocol presented here, and its security analysis in Chapters 4 to 6 is fully rigorous and mathematically sound; it merely omits some additional formal machinery. We nevertheless maintain notation that is consistent with the general formulation in Chapter 7.

We assume that the protocol begins with Alice and Bob having access to local randomness stored in classical registers, which they use to implement the steps of the QKD protocol. The adversary is uncorrelated to this randomness, which is only accessible to the honest parties, and is never leaked to the adversary (even after the termination of the QKD protocol).[6] In this thesis, we do not explicitly describe the generation and use of these local random numbers in the QKD protocol execution; they are implicitly utilized in choosing the signal states sent, basis choices, and choosing seeds for hashing. We note that the assumption of perfect random numbers can be relaxed by utilizing random number generators that are ε_{rng}-close to perfect, in the composable security framework.

Protocol 1 (QKD Protocol)**.**

1. For rounds j from 1 to n, Alice and Bob perform the following operations:

   (a) **State Preparation:** At time t_j^{A}, Alice prepares a state $\sigma_k \in \text{S}_{=}(A'_j)$ out of $\bar{d}_A$ possible states, with probability p_k, and sends them to Bob through an insecure quantum channel. She stores the label k for her choice of the signal state in a classical register X_j. This step requires the use of local randomness. Alice sends these states in sequence, and we therefore have $t_j^{\text{A}} < t_{j+1}^{\text{A}}$.

   (b) **Measurement:** At time t_j^{B}, Bob performs a measurement using a POVM $\{\Gamma_k^{(B_j)}\}_{k=1\ldots\bar{d}_B}$, obtains one of $\bar{d}_B$ possible outcomes, and stores his results in a classical register Y_j . Depending on the exact detection setup used, this step may require the use of local randomness. Bob performs these measurements in sequence, and we therefore have $t_j^{\text{B}} < t_{j+1}^{\text{B}}$.

[6] While this randomness is sometimes used to generate states or classical messages that are publicly released at some point (when explicitly specified in the protocol), what we mean by this requirement is that the "raw" values of the randomness are never made accessible to the adversary.

Remark 3.2.1. ***Optional permutation step:*** *Alice (or Bob) picks a random permutation and announces it. Both parties then apply this permutation to their classical data. This step is required only for protocols analyzed using the postselection technique in Chapter 5 to satisfy certain permutation invariance requirements (Lemma 5.2.1), and therefore appears exclusively in that chapter; it also entails an additional public announcement. However, since the postselection technique ultimately reduces the security analysis to that of IID collective attacks, it suffices to analyze security against IID collective attacks alone. In that setting, this permutation step plays no role, as argued in Lemma 5.2.2, and can be ignored*[7]*. Consequently, we do need to explicitly introduce notation or registers for this step.*

(c) **Public announcement:** At some time after all states have been sent and measured, Alice and Bob engage in interactive public announcements, using authenticated classical channel. These public announcements result in a classical register $\widehat{C}_j$.

(d) **Sifting and key map:** Alice maps her local data stored in X_j, along with the public annoucements $\widehat{C}_j$, to her private register S_j. She then applies a deterministic rule, based solely on $\widehat{C}_j$, to discard certain rounds from S_j. This produces the (potentially shortened) pre-amplification string, which is stored in the register $\mathbf{S}$.[8] In this thesis, we consider protocols where Alice's remapping and discarding are defined so that whenever a value of S_j will be discarded (based on $\widehat{C}_j$), S_j is set to a fixed placeholder symbol $\perp$. Since Alice determines the mapping to S_j, she can directly encode discard rounds in this way.[9]

After all the announcements and sifting and key map operations are completed, the state of the protocol is given by

$$\rho_{\mathbf{S}S_1^n X_1^n Y_1^n \widehat{C}_1^n \hat{\boldsymbol{E}}}. \tag{3.10}$$

where $\hat{\boldsymbol{E}}$ denotes Eve's quantum side information at the end of her attack on the n rounds. Alice and Bob move on to the next step in the protocol only after all public

[7]However, it still needs to be implemented in the protocol, in order to justify the usage of the postselection technique.

[8]Thus, the register $\mathbf{S}$ takes values from the set of all possible strings of length less than or equal to n, and composed of symbols from the alphabet of the register S_j that are *not* discarded. In most common scenarios, S_j takes values in $\{0, 1, \perp\}$ (based on $\widehat{C}_j$,X_j), and the last outcome denotes that the round is going to be discarded. Thus, $\mathbf{S}$ stores a binary string of length up to n bits.

[9]In principle, this means that Alice could implement the discarding step by inspecting the sequence S_1^n alone, without separately referring to the announcements $\widehat{C}_1^n$.

announcements are completed (which also implies that all signal preparation and measurements are completed). Eve is assumed to have access to public announcements $\widehat{C}_1^n$.

2. **Variable length decision:** Alice and Bob use predetermined functions of the public announcements $\widehat{C}_1^n$ to determine parameters for error correction and key generation. Often these functions only depend on the frequency distribution $\mathbf{F}^{\text{obs}} := \text{freq}(\hat{c}_1^n)$ of the public announcements, where we use $\hat{c}_1^n$ to denote the value stored in the classical register $\widehat{C}_1^n$.

   (a) Alice computes the value $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) \in \mathbb{N}$ which determines the number of possible transcripts possible in the error-correction protocol.

   (b) Alice computes the length of the output key to be produced, given by $\ell(\mathbf{F}^{\text{obs}}) \in \mathbb{N}$, using a predetermined function $\ell(\cdot)$. The functions $\ell(\mathbf{F}^{\text{obs}})$ and $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})$ are closely related through the security proof.

   (c) These values may be computed by both parties, or computed by one party and then sent to the other. Since Eve knows $\mathbf{F}^{\text{obs}}$, revealing these values via public announcements to Eve does not give her any new information.

   The state in the protocol, conditioned on observing a specific value in the $\widehat{C}_1^n$ registers, is given by

$$\rho_{\mathbf{S}S_1^n X_1^n Y_1^n \widehat{C}_1^n \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n)}, \tag{3.11}$$

   where $\Omega(\hat{c}_1^n)$ denotes the event that the value $\hat{c}_1^n$ is observed in the $\widehat{C}_1^n$ registers. Note that Bob can also discard the same rounds as Alice to obtain a string $\boldsymbol{Y}$ of the same length as $\mathbf{S}$..

3. **Error correction:** Alice and Bob perform an error-correction protocol that results in Bob outputting a guess for Alice's pre-amplification string. This error-correction protocol is such that the number of possible transcripts is the protocol is upper bounded by $2^{\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})}$.[10] The protocol results in Bob outputting a guess $\mathbf{S}_B$ for Alice's pre-amplification string. Note that since the location of the discarded rounds are known to both Bob and Alice, this protocol is designed such that $\mathbf{S}_B$ and $\mathbf{S}$ have exactly the same length (typically by having Bob start with the string $\boldsymbol{Y}$).

[10] For the simplest protocols, where Alice sends an error syndrome of exactly $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})$ bits to Bob, the value $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})$ coincides with the number of bits leaked. For protocols where Alice may send up to some maximum number of bits, one instead sets the maximum number of bits to $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) - 1$, so that the total number of possible transcripts is at most $2 + 2^2 + \cdots + 2^{\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})-1} = 2^{\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})} - 2 \leq 2^{\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})}$.

The state in the protocol, conditioned on observing a specific value in the $\widehat{C}_1^n$ registers, is given by

$$\rho_{\mathbf{SS}_B\widehat{C}_1^n C_{\mathrm{EC}} F_{\mathrm{K}} F_{\mathrm{EC}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n)}. \tag{3.12}$$

where $\Omega(\hat{c}_1^n)$ denotes the event that $\widehat{C}_1^n$ registers take the value $\hat{c}_1^n$. Note that here we omit the registers Y_1^n, since they are no longer needed for the rest of the protocol. This is tantamount to either deleting them, or ensuring that this register is not leaked to the adversary at any point (even after the completion of the protocol).

4. **Error verification:** Alice and Bob perform error-verification by computing universal$_2$ hashes on their respective pre-amplification strings $(\mathbf{S}, \mathbf{S}_B)$. The hash families map the input strings to $\lceil \log(1/\varepsilon_{\mathrm{EV}}) \rceil$ output bits. They do so by sharing the hash seed in register H_{EV}, and having one party share the computed hash value with the other party in the register C_{EV}. We use Ω_{EV} to refer to the event where the hash values match. Alice and Bob abort the protocol if Ω_{EV} does not occur.

   The state in the protocol, conditioned on $\Omega(\hat{c}_1^n)$ and error-verification passing, is given by

$$\rho_{\mathbf{SS}_B\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}}. \tag{3.13}$$

   where $\wedge$ denotes the logical 'and' operator and Ω_{EV} denotes the event that error-verification passes, i.e hash values matched.

5. **Privacy amplification:** Alice and Bob perform *ideal* universal$_2$[11] hashing on their their pre-amplification strings to generate the output key. That is, they first compute the length $l_{\text{pre-PA}}$ of strings stored in $\mathbf{S}, \mathbf{S}_B$, and then choose a hash function from an ideal universal$_2$ family mapping $l_{\text{pre-PA}}$ bits to $\ell(\hat{c}_1^n)$ bits. The hash choice is publicly communicated in the register H_{PA}, and the chosen hash function is applied to $\mathbf{S}, \mathbf{S}_B$ to obtain the final output registers K_A, K_B.

   The state in the protocol, conditioned on $\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}$, is given by

$$\rho_{K_A K_B \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} H_{\mathrm{PA}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}}. \tag{3.14}$$

3.2.1 Protocol Variations

We now comment on several protocol variations that will be studied throughout this thesis.

[11] Recall that ideal universal$_2$ (see Definition 2.4.1) corresponds to the case where the collision probability of the hash is *equal* to $1/|D'|$, where D' is the codomain of the hash family. Note that this requirement can be relaxed to universal$_2$ by sacrificing one additional bit of output key, see Remark 3.5.1 for a discussion.

On-the-fly announcements: First, observe that the protocol described above assumes that all public announcements occur *after* all quantum signals have been transmitted and measured. If these public announcements before the all quantum signals have been sent and measured, then it allows Eve to potentially adapt her attack based on these announcements. Such announcements are referred to as "on-the-fly" announcements (see [7, Section 5.1.2] for a discussion). This restriction, forbidding on-the-fly announcements, greatly simplifies the security analysis and is, in fact, essential for the postselection-based proof in Chapter 5. Although such a restriction is not inherently required by the EUR or phase-error approaches, our analyses in Chapter 6 likewise assume it for technical convenience. In contrast, the MEAT framework places no such limitation, and therefore Chapter 7 allows on-the-fly announcements.

Fixed-length protocols: Second, the protocol above is formulated as a variable-length protocol. A simpler special case, which is easier to analyze, is the fixed-length version. This is obtained by imposing the following restrictions on the QKD Protocol from Section 3.2:

- The variable-length decision step in the protocol is restricted to a simple **acceptance test** form, in which Alice computes the observed frequency distribution $\mathbf{F}^{\mathrm{obs}} = \mathrm{freq}(\hat{c}_1^n)$ on the classical string $\hat{c}_1^n$, and checks whether this frequency distribution lies inside some predetermined set ($\mathcal{S}_{\mathrm{acc}}$) of frequency vectors often called an **acceptance set**. If it does, we refer to this as the acceptance test "passing", and the protocol produces an output key of length ℓ_{fixed} (assuming error-verification also passes). Else, the protocol aborts.

- We require that there exists a *fixed* constant value $\lambda_{\mathrm{EC}}^{\mathrm{fixed}} \in \mathbb{N}$, such that the number of possible transcripts in the error correction step (conditioned on the acceptance test passing) is at most $2^{\lambda_{\mathrm{EC}}^{\mathrm{fixed}}}$.

- At the privacy amplification step, Alice and Bob instead check only whether the acceptance test passed, and the error-verification passed. If both these events hold, Alice and Bob accept the protocol overall, and hash to final keys of length ℓ_{fixed}; otherwise they abort the protocol. Note that this means the event Ω_{acc} of the protocol accepting overall is exactly the joint event

$$\Omega_{\mathrm{acc}} = \Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}, \tag{3.15}$$

  and thus we may instead denote it as $\Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}$ in contexts where that is more convenient.

Having explained the high-level structure of the protocol that we analyze in later chapters above, we now consider some additional details that needed to obtain a concrete realization of the QKD protocol. This includes

- the precise set of signal states sent and the measurements performed, which we specify in the next section;
- the exact form of the public announcements, and how they are computed from the underlying data generated by state preparation and measurement;
- the parameters governing state preparation (e.g., probabilities, intensities, and related settings), which are only specified on a per-chapter basis;
- the specific error-correction and privacy-amplification choices such as the exact error-correction protocol, hash families, etc. Beyond the aspects already stated above, further implementation details of these classical subroutines do not affect the security analysis, and we therefore do not specify them.

The following section can also be skipped on the first reading: readers can return to this section when they encounter security analysis that required those details.

3.3 BB84 signal states, measurements, announcements and sifting

We consider two families of protocols: qubit-based BB84 [21] and decoy-state BB84 [69, 70, 71]. In both cases, Alice prepares quantum states that encode classical information in one of two mutually unbiased bases, conventionally denoted by X and Z. If Bob uses an active measurement setup, he chooses to make a measurement in either X or Z. If he uses a passive detection setup, a beam splitter is used instead of an active basis choice. We consider polarization as the encoding degree of freedom.

3.3.1 States Sent by Alice

We now specify the signal states $\{\sigma_k\}_k$ and preparation probabilities $\{p_k\}_k$ appearing in Step 1a of the QKD Protocol. It is convenient to decompose the state preparation label k as

$$k = (a, z),$$

for the qubit BB84 setting or, in the decoy-state setting,

$$k = (a, \mu, z),$$

where a denotes the polarization choice, μ the intensity setting, and $z \in \{\texttt{test}, \texttt{gen}\}$ indicates whether the round is designated as a "test" round or " generation" round. In test rounds, Alice and Bob announce their exact state sent, and measurement outcome obtained, and thus no key is generated from these rounds. In the generation rounds, Alice and Bob only announce their basis choice, and Bob announces whether he obtained he obtained a no-click outcome (no detectors clicked), or a click outcome (some detectors clicked).

The choice of k proceeds as follows. First, Alice selects z, determining whether the round is a test (with probability γ) or key-generation (with probability $(1-\gamma)$) round. Conditioned on this choice, she samples the remaining components of k according to a probability distribution that may depend on z. This is denoted via $p_{a|z}$ or $p_{a,\mu|z}$.

Qubit BB84. For qubit BB84, the polarization alphabet is

$$a \in \{0, 1, +, -\},$$

corresponding to the computational (Z) and Hadamard (X) bases. The signal states are given by

$$\sigma_{(a,z)} = |a\rangle\langle a| \,,$$

where $|0\rangle, |1\rangle$ corresponds to Z basis and $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ corresponds to X basis. The prepared quantum state depends only on the polarization choice a and is independent of z; the latter is recorded purely as classical side information in Alice's register.

Decoy-state BB84. For decoy-state BB84, the polarization alphabet is

$$a \in \{H, V, A, D\},$$

partitioned into the rectilinear basis $\{H, V\}$ and the diagonal basis $\{A, D\}$. Alice additionally chooses an intensity setting μ from a finite set of possible intensities. We assume that Alice prepares fully phase-randomized coherent states with perfect polarization encoding. The corresponding signal states are

$$\sigma_{(a,\mu,z)} = \sum_{N=0}^{\infty} e^{-\mu} \frac{\mu^N}{N!} |N\rangle\langle N|_a \,, \tag{3.16}$$

where $|N\rangle\langle N|_a$ denotes an N-photon Fock state in which all photons have polarization a. As in the qubit case, the prepared quantum state depends only on (a, μ) and is independent of whether the round is a test or key-generation round.

In both protocols, Alice records the full label k in her classical register X_j for round j. Consequently, the alphabet of X_j coincides with the set of all possible signal-state labels k. Note that Alice preparing a single qubit can be equivalently thought of as Alice producing a single photon, of the appropriate polarization.

3.3.2 Measurements Performed by Bob

We now specify Bob's measurement in Step 1b of the QKD Protocol. As the same measurement is performed in every round, we suppress the round index j throughout. Bob stores the exact measurement outcome in his classical register Y_j.

Qubit Measurements. In the qubit BB84 protocol with loss, Bob's measurement acts on a three-dimensional Hilbert space $\widetilde{\mathcal{H}}_B \cong \mathbb{C}^3$, where the subspace spanned by $|0\rangle, |1\rangle$ corresponds to the logical qubit, and an additional orthogonal basis state $|\text{vac}\rangle$ represents a no-detection (loss) event.

Upon choosing a basis $b_B \in \{\mathsf{Z}, \mathsf{X}\}$, Bob performs a three-outcome projective measurement. If $b_B = \mathsf{Z}$, the POVM is given by

$$\{|0\rangle\langle 0|, \ |1\rangle\langle 1|, \ |\text{vac}\rangle\langle\text{vac}|\},$$

and if $b_B = \mathsf{X}$, the POVM is

$$\{|+\rangle\langle +|, \ |-\rangle\langle -|, \ |\text{vac}\rangle\langle\text{vac}|\}.$$

Active detection setup with threshold detectors We model an active detection setup (see Fig. 3.2) as follows. Bob receives an optical signal described by annihilation operators $\hat{a}_H$ and $\hat{a}_V$ corresponding to horizontal and vertical polarization modes. Bob actively chooses a basis $b_B \in \{\mathsf{Z}, \mathsf{X}\}$ and applies a basis-dependent linear-optical transformation that maps the input modes to a pair of output modes $\hat{b}_0^{(b_B)}$ and $\hat{b}_1^{(b_B)}$, which are then measured using threshold detectors.

For $b_B = \mathsf{Z}$, we take the output modes to be

$$\hat{b}_0^{(\mathsf{Z})} = \hat{a}_H, \qquad \hat{b}_1^{(\mathsf{Z})} = \hat{a}_V. \tag{3.17}$$

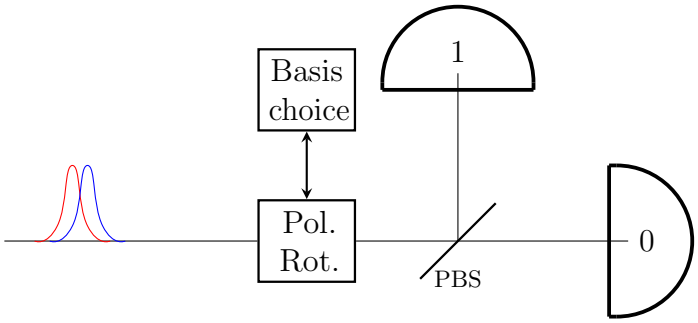


Figure 3.2: Schematic of an active detection setup using threshold detectors.

For the diagonal basis $b_B = \mathsf{X}$, Bob applies a 45° polarization rotation, yielding the output modes

$$\hat{b}_0^{(\mathsf{X})} = \frac{1}{\sqrt{2}}(\hat{a}_H + \hat{a}_V), \qquad \hat{b}_1^{(\mathsf{X})} = \frac{1}{\sqrt{2}}(\hat{a}_H - \hat{a}_V). \tag{3.18}$$

Each output mode is monitored by a threshold detector. For any subset $S_{\text{click}} \subseteq \{0, 1\}$, the POVM element corresponding to exactly the detectors in S_{click} clicking is

$$M_{S_{\text{click}}}^{(B,b_B)} = \sum_{\{N_j \geq 1\}_{j \in S_{\text{click}}}} \frac{1}{\prod_{j \in S_{\text{click}}} N_j!} \left(\prod_{j \in S_{\text{click}}} (\hat{b}_j^{(b_B)\dagger})^{N_j} \right) |\text{vac}\rangle\langle\text{vac}| \left(\prod_{j \in S_{\text{click}}} (\hat{b}_j^{(b_B)})^{N_j} \right), \tag{3.19}$$

and the no-click outcome is

$$M_{\emptyset}^{(B,b_B)} = |\text{vac}\rangle\langle\text{vac}|\,.$$

Bob records the complete outcome (including the chosen basis) in his classical register Y_j.

In this thesis, we plot key rates for the active basis-choice scenario of the decoy-state BB84 protocol. To do so, we consider a scenario in which Bob maps his double-click outcomes in each basis to single-click outcomes at random. This classical post-processing step is required for the appropriate use of squashing maps, as explained in Section 3.6.3. As a result, in each basis Bob effectively has three outcomes, rather than four. The corresponding POVM elements can be obtained by straightforward linear combinations of POVM elements defined above.

For the passive BB84 setup, we do not explicitly plot key rates. Where possible, however, we explain how our results can be applied to passive implementations as well. In particular, all analyses in this thesis except for the entropic uncertainty relation (EUR) analysis in Chapter 6 can be straightforwardly extended to passive setups.

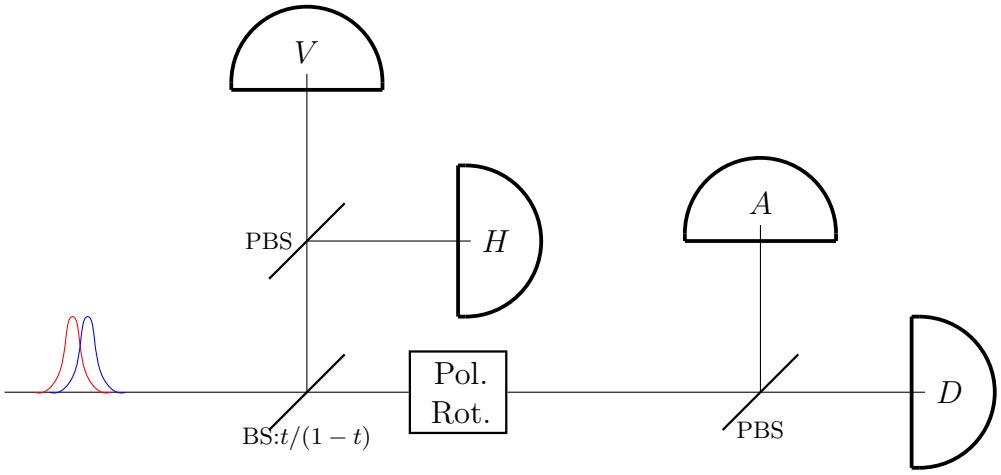


Figure 3.3: Schematic of the passive detection setup using theshold detectors.

Passive setup with Threshold detectors. In the passive detection setup (see Fig. 3.3), Bob implements a passive basis choice using a beam splitter with splitting ratio $t \in [0, 1]$. One output arm is sent directly to a polarizing beam splitter followed by two detectors. The other arm is sent through a polarization rotator, and is then measured using a polarizing beam splitter followed by two detectors. The first arm can be viewed as implementing a Z-basis measurement, while the second can be viewed as implementing a 45°-rotated X-basis measurement. The output modes can be written in terms of the input modes via

$$\begin{aligned} \hat{b}_H &= \sqrt{t}\,\hat{a}_H, \\ \hat{b}_V &= \sqrt{t}\,\hat{a}_V, \\ \hat{b}_D &= \sqrt{\tfrac{1-t}{2}}\,(\hat{a}_H + \hat{a}_V), \\ \hat{b}_A &= \sqrt{\tfrac{1-t}{2}}\,(\hat{a}_H - \hat{a}_V). \end{aligned} \tag{3.20}$$

There are 16 possible click patterns in total. Among these, there are four possible single-click events. These single-clicks can be used to assign a basis b_B to Bob's outcome, noting that this basis assignment is not an active choice by Bob, but is instead inferred from the measurement data. In addition, there are two possible double-click patterns, one associated with each basis. All remaining outcomes correspond to cross-click events, in which more than one detector clicks across different bases.

Remark 3.3.1. *The exact operator-level form of these POVM elements is not always directly relevant for the QKD security analysis. The main property we will rely on is that*

they are jointly block-diagonal with respect to the total photon number. This structure is used in the construction of squashing maps (see Section 3.6.3). Such maps allow us to restrict attention to effective POVMs supported only on a finite photon-number subspace—sometimes even the single-photon (qubit) subspace—without affecting security.

3.3.3 Public Announcements and Sifting

Our protocols involve the following procedure for public announcements and sifting. For the active BB84 case, we assume that double-clicks are being randomly mapped to single-clicks.

- **Test rounds.** On all test rounds, Alice and Bob both publicly announce their exact state preparation and measurement outcomes. They set $S_j = \perp$, and these rounds are discarded and not used for key generation.
- **Key-generation rounds.** On all key generation rounds, Bob publicly announces whether he obtained a detection event outcome or not.
  - If Bob does not obtain a detection event, he makes no further announcement. Alice sets $S_j = \perp$, and the round is discarded.
  - If Bob obtains a detection event, he publicly announces his measurement basis. Alice announces her basis. If these bases match, Alice then assigns a bit value to S_j based on her state preparation, and Bob assigns a corresponding bit value to his local data. If they do not match, Alice sets S_j to $\perp$, and the round is discarded.

For passive protocols, Alice and Bob announce all relevant information in test rounds. In key generation rounds, they follow the above procedure when Bob obtains either a single-click outcome or a no-click outcome. If Bob instead obtains a multi-click outcome, he announces this fact and the corresponding round is discarded.

The remainder of the protocol proceeds exactly as in QKD Protocol. We have now specified enough details of the protocol to provide a clear overall picture of its operation. Note that in Chapter 7 we will specify the protocol in considerably more detail. We now turn to the security analysis of the protocol, beginning with correctness, which is addressed in the next section.

3.3.4 Motivation for decoy-state protocols

Here, we briefly motivate why decoy-state protocols are important for practical QKD implementations. The qubit BB84 protocol is conceptually natural: it relies on sending qubit states that are not perfectly distinguishable. A single photon constitutes a qubit because its polarization degree of freedom spans a two-dimensional Hilbert space. However, the qubit BB84 protocol is highly impractical to implement directly, as it would require preparing exactly one photon on demand with a precise polarization. It is also very difficult to ensure that Bob measures a qubit state, since Eve is free to send any number of photons into Bob's lab. Instead, practical systems rely on phase-randomized weak coherent pulse (WCP) sources for technological feasibility, which emit states with a Poissonian photon number distribution (Eq. (3.16)). Moreover, Bob uses threshold detectors, which do not resolve photon number.

In such implementations, any pulse for which Alice's source emits a multiphoton state is fundamentally insecure. This is because an adversary can perform a photon-number-splitting (PNS) attack [72, 73, 74, 75]. In this attack, Eve deterministically splits off one photon from a multiphoton pulse and stores it in a quantum memory, while forwarding the remaining photons to Bob. Since Bob uses threshold detectors and cannot resolve photon number, he cannot detect that the pulse has been modified, nor that the total photon number has been reduced. After Alice and Bob publicly announce their basis choices, Eve measures her stored photon in the correct basis, thereby learning the encoded bit without changing Alice's and Bob's observations.

Moreover, by exploiting channel loss, Eve can selectively suppress single-photon signals (which are immune to the PNS attack) while preferentially transmitting compromised multiphoton pulses, all while reproducing the expected detection statistics at Bob's side. As a result, the Poissonian photon number statistics of WCP sources severely degrade the achievable key rate unless explicitly addressed. Decoy-state protocols [70, 69, 71] are employed to mitigate this vulnerability.

To build intuition, consider a hypothetical source that emits a *definite* photon number and also announces it to Alice. Alice and Bob could then group their observed data based on the photon number and directly extract the single-photon contribution, while pessimistically discarding all multiphoton rounds. This prevents Eve from concealing a PNS attack by mixing single- and multiphoton behavior.

In practice, the photon number is not announced. The decoy-state method provides a statistical substitute by varying the intensity of the WCP source, thereby producing different photon-number distributions. Crucially, Eve cannot distinguish an m-photon pulse

originating from different intensity settings, as her interaction can depend only on the photon number and not on Alice's choice of intensity, which is unknown at the time of the attack. Thus, the observations on rounds with different intensities can be used to infer something about Eve's attack on rounds with specific photon number (typically zero-photon or one-photon rounds). This is the essence of the decoy-state idea.

Overall, the task remains fundamentally the same: to infer properties of Eve's attack, and hence the amount of information she may have gained, using the observed statistics. Decoy-state protocols simply provide a richer set of states, measurements, and observed data with which to perform this inference. As we will see in Sections 3.5 and 3.5.1, these observations are ultimately used to bound an appropriate entropic quantity that quantifies secrecy.

3.4 Correctness via error-verification

It is straightforward to prove that correctness is satisfied in our protocol description, which we will do now. In fact, this argument relies solely on the properties of the error-verification step in our QKD Protocol, and is largely independent of the rest of the protocol.

Lemma 3.4.1 (Correctness is satisfied)**.** *The QKD Protocol is $\varepsilon_{\mathrm{EV}}$-correct.*

Proof. This proof is a simple consequence of the error-verification step from QKD Protocol, and the proof of correctness can be found in many works. For any output state of the QKD protocol, we have

$$\begin{aligned}
\Pr(K_A \neq K_B) &= \Pr(K_A \neq K_B \wedge \Omega_{\mathrm{EV}}) + \Pr\left(K_A \neq K_B \wedge \Omega_{\mathrm{EV}}^{\mathrm{C}}\right) \\
&= \Pr(K_A \neq K_B \wedge \Omega_{\mathrm{EV}}) \\
&\leq \Pr(\mathbf{S} \neq \mathbf{S}_B \wedge \Omega_{\mathrm{EV}}) \\
&= \Pr(\Omega_{\mathrm{EV}} | \mathbf{S} \neq \mathbf{S}_B) \Pr(\mathbf{S} \neq \mathbf{S}_B) \\
&\leq \Pr(\Omega_{\mathrm{EV}} | \mathbf{S} \neq \mathbf{S}_B) \\
&\leq 2^{-(\lceil \log(1/\varepsilon_{\mathrm{EV}}) \rceil)} \\
&\leq \varepsilon_{\mathrm{EV}},
\end{aligned} \tag{3.21}$$

where the first line follows from the properties of probability, and the second line follows from the fact that $\Omega_{\mathrm{EV}}^{\mathrm{C}} \implies K_A = K_B$, since the protocol aborts. The third line follows from that fact that $K_A \neq K_B \implies \mathbf{S} \neq \mathbf{S}_B$; in other words, the output keys being unequal necessarily implies that the pre-amplification strings are unequal. The fourth and fifth

lines follow from the properties of probability. The sixth line follows from the fact that error-verification involves checking universal$_2$ hashes, and the final line follows from simple algebra. □

Thus, to complete the security analysis of QKD Protocol, it remains only to establish the secrecy requirement. This is the technically challenging part of the proof. We therefore turn next to the Leftover Hashing Lemma, which serves as a key tool in this analysis.

3.5 Leftover Hashing Lemma

The Leftover Hashing Lemma is a central tool in QKD security analysis. It provides a method for converting classical data that is not perfectly secret into data that is *close* to perfectly secret, by applying a hash function chosen from a universal$_2$ hash family. The quality of this extraction is determined by an appropriate entropic measure of the underlying state, typically expressed in terms of either Rényi entropies or smooth min-entropies. Note that there are many variants of the Leftover Hashing Lemma, and when we refer to the LHL, we mean the broader family of such results.

Lemma 3.5.1. *(Leftover-hashing Lemma (LHL). [40, Theorem 8] and [34, Proposition 8].) Let $\rho_{AE} \in \mathrm{S}_=(AE)$ be a classical-quantum state, and $(\mathcal{H}_{\mathcal{A}\to\mathcal{Z}}, p_h)$ be a family of* ideal *universal$_2$ hash functions with $\mathcal{K} = \{0,1\}^l$. Consider the state ρ_{KEH} that is obtained when h is a function drawn from that family with probability p_h, and applied to the register A to obtain the register K, and the choice of the function is stored in H. Then, we have*

$$\frac{1}{2}\left\|\rho_{KEH} - \frac{1}{|\mathcal{K}|}\mathbb{I}_K \otimes \rho_{EH}\right\|_1 \leq 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}^{\uparrow}_{\alpha}(A|E)_\rho - l + 2\right)}, \tag{3.22}$$

for $\alpha \in (1,2)$[12] If $\rho_{AE} \in \mathrm{S}_{\leq}(AE)$ is a subnormalized state, and $\bar{\varepsilon} \in [0, \sqrt{\mathrm{Tr}[\rho_{AE}]})$, we also have,

$$\frac{1}{2}\left\|\rho_{KEH} - \frac{1}{|\mathcal{K}|}\mathbb{I}_K \otimes \rho_{EH}\right\|_1 \leq 2^{-\frac{1}{2}(H^{\varepsilon}_{\min}\bar{\varepsilon}(A|E)_\rho - l + 2)} + 2\bar{\varepsilon}, \tag{3.23}$$

In the QKD Protocol, let us consider the state just before privacy amplification, denoted

$$\rho_{\mathbf{SS}_B\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}},$$

[12]For the entirety of this thesis, unless otherwise specified, the Rényi parameter $\alpha \in (1,2)$, since that is the regime relevant for QKD.

where, for the moment, we omit the conditioning on the events. The Leftover Hashing Lemma asserts that once we obtain a lower bound on the relevant entropy of this state, the extractable key length l can be chosen to be approximately equal to this entropy.

Of course, in a cryptographic protocol, Eve is not kind enough to reveal the attack she has performed, and we would not trust her even if she did. Therefore the state for which the entropy must be evaluated is not known to Alice and Bob. Instead, one performs some kind of worst-case analysis over all states compatible with the observed data, which we describe in the next section. This analysis addresses how the associated entropies can be bounded, and which types of bounds are fundamentally impossible to obtain. Indeed, the bulk of QKD security analysis consists of appropriately bounding the relevant entropic quantity which is then utilized in the LHL.

Finally, note that Alice and Bob must communicate classically to ensure that they apply the same hash function to $\mathbf{S}$ and $\mathbf{S}_B$. This choice of hash function is assumed to be revealed to the adversary, both in the protocol and in the statement of the Leftover Hashing Lemma, but only after Alice announces it and not beforehand.

Remark 3.5.1. *When considering hash families that output l-bits, one must be careful to distinguish between* universal$_2$ *hashing (defined by requiring the collision probability to be $\leq 2^{-l}$) and* ideal universal$_2$ *hashing (where the collision probability is exactly 2^{-l}), a subtle difference that is often missed in the literature. In particular, the Rényi leftover hashing lemma stated in Ref. [40], as well as the smooth min-entropy version in Ref. [34], require* ideal *universal$_2$ hashing. This ideal requirement can in fact be relaxed: one may use ordinary universal$_2$ hashing instead, obtaining essentially the same bound at the cost of losing only one or two bits of key, as shown in Ref. [12]. For this thesis, we restrict our analysis and statements to protocols that utilize ideal universal$_2$ hashing in the privacy amplification step. Note that Toeplitz hashing is ideal universal$_2$ [46, 76].*

3.5.1 Bounding the entropy in Leftover Hashing Lemma

We now consider the various kinds of entropic bounds one may attempt to obtain for use in the LHL. In particular, we also discuss which of them are possible and which of them are fundamentally impossible. For simplicity, we restrict attention to fixed-length attacks, where a ℓ_{fixed}-bit key is produced upon the event Ω_{acc}, and key of length 0 is produced otherwise ($\Omega_{\text{acc}}^{\text{C}}$). A useful tool for building intuition is the **intercept–resend attack**, in which Eve stores everything leaving Alice's lab and forwards only arbitrary "garbage" signals to Bob. (Note that more involved versions of this attack exist, but this simpler version suffices for the point we wish to make here). In this case, once the public announcements $\widehat{C}_1^n$ are

revealed, Eve typically knows Alice's raw key S_1^n exactly, and therefore also knows the pre-amplification string $\mathbf{S}$.

Remark 3.5.2. *Recall that in our protocol description the universal$_2$ hashing is applied to the register* $\mathbf{S}$*. In many of the examples below, however, we will instead bound the entropy of the register* S_1^n*, because it is typically more convenient to analyze that register. However, notice that these registers are equivalent from Eve's perspective: she has access to the public announcements* $\widehat{C}_1^n$*, she can freely transform* $\mathbf{S}$ *to* S_1^n *and vice versa. Thus, it is natural to expect the relevant entropy quantities to also be exactly equal. We show this formally in Chapters 4 and 7, and use these registers interchangeably for the sake of pedagogy here.*

- We may attempt to obtain bounds of the form
$$H_{\min}^{\bar{\varepsilon}}\big(S_1^n \mid \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}\big)_{\rho} \geq \textbf{constant}$$
However, a moment of thought shows that, due to the possibility of an intercept–resend attack (where Eve gets full information on the S_1^n), any such bound must be essentially trivial, and the constant must be close to 0.[13]

- Instead, one may attempt to bound the entropy of the state conditioned on acceptance, that is:
$$H_{\min}^{\bar{\varepsilon}}\big(S_1^n \mid \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}\big)_{\rho|\Omega_{\mathrm{acc}}} \geq \textbf{constant}.$$
However, again, the intercept–resend attack renders the above bound trivial: Eve gets a perfect copy of S_1^n, *regardless of any event* that is conditioned on. Note that this problem can be avoided by having the smoothing parameter itself depend on $\Pr(\Omega_{\mathrm{acc}})$.[14] We will see an example of such an approach in our proof of variable-lengths security using the EUR approach in Chapter 6.

- One could try subnormalized conditioning, that is
$$H_{\min}^{\bar{\varepsilon}}\big(S_1^n \mid \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}\big)_{\rho\wedge\Omega_{\mathrm{acc}}} \geq \textbf{constant}.$$
Non-trivial bounds of the above form are indeed possible, and are obtained when considering fixed-length protocols using the postselection technique (Chapter 5), and the EUR technique (Chapter 6). Furthermore, it turns out that such bounds actually suffice for proving the security of QKD protocols, precisely because the security requirement also includes a $\Pr(\Omega_{\mathrm{acc}})$ prefactor in the trace distance term (see Definition 3.1.1).

[13] It is typically not exactly zero, due to the smoothing.

[14] Typically via $\bar{\varepsilon} \approx \sqrt{\cdot/\Pr(\Omega_{\mathrm{acc}})}$, so the smoothing parameter grows larger as acceptance probability grows smaller.

- Another possibility is to consider a bound of the form

$$H_{\min}^{\bar{\varepsilon}}\big(S_1^n \mid \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}\big)_{\rho|\Omega_{\mathrm{acc}}} \geq \textbf{constant} - \textbf{pre-factor} \times \log\left(\frac{1}{\Pr(\Omega_{\mathrm{acc}})}\right).$$

  Here the right-hand side explicitly depends on the probability of the conditioning event. Such bounds are possible, precisely because the logarithmic penalty term. Bounds of this type typically arise in proofs relying on the EAT [77, 41].[15]

The key point is that one must condition on appropriate events, and do so in the correct way, in order to obtain meaningful lower bounds on the entropy that can be used in a rigorous security proof. We will see concrete examples of this principle throughout this thesis. These are different ways of formalizing the intuition that, while the entropy is not be large for all possible states that can arise, the set of all states can be divided into two categories: those for which the entropy bound is high, and those for which the protocol aborts with high probability. In both cases, security is obtained.

3.6 Practical QKD Toolbox

We will now cover some standard tools that are utilized in QKD security analysis, such as the source-replacement schemes [56, 57], source maps [58], squashing maps [59, 60, 61, 62, 63]. Note that apart from the source-replacement scheme, the remaining tools are only required when dealing with optical implementations of QKD, and are utilized in reducing infinite-dimensional state preparation and measurement operations to finite dimensions. Accordingly, the reader may safely defer a detailed study of these tools until they are encountered later in the thesis. They can also be used more generally to incorporate imperfections [58, 78, 79, 80].

3.6.1 Source-Replacement Schemes

The source-replacement scheme is a technique that can be used to describe Alice's preparation of states in $\mathrm{S}_{=}(A')$ equivalently as her creating a pure, entangled state across $\mathrm{S}_{=}(\bar{A}\hat{A}A')$, and then performing measurements on $\bar{A}$. The A' system then behaves as required, whereas the $\hat{A}$ system is referred to as the *shield* system, and is required to correctly describe the preparation of mixed states. This is a system that is not measured by Alice, Bob, or

[15] Although our analysis using MEAT [11] in Chapter 7 will follow a somewhat different path.

Eve. Note that this is a purely theoretical device, and the actual protocol does not need to change in any way. It is useful because it allows us to think of prepare-and-measure protocols as entanglement-based protocols. The proof proceeds by explicit construction. The formal lemma describing the use of the source-replacement scheme is stated below.

Lemma 3.6.1 (Source-Replacement and Shield Systems)**.** *Consider a procedure that prepares one out of $\bar{d}_A$ possible states $\sigma_k \in \mathrm{S}_=(A')$ with probability p_k and records the outcome choice k in the register X. Let $|\sigma_k\rangle_{\hat{A}A'}$ be a purification of σ_k, and let $\{|k\rangle_{\bar{A}}\}_i$ be an orthonormal basis on the register $\bar{A}$ of dimension $\bar{d}_A$. Then, the same procedure can be equivalently described by the preparation of the pure state*

$$\sigma_{\bar{A}\hat{A}A'} = \sum_{i,k=1}^{\bar{d}_A} \sqrt{p_i p_k}\, |i\rangle\langle k|_{\bar{A}} \otimes |\sigma_i\rangle\langle\sigma_k|_{\hat{A}A'}\,, \tag{3.24}$$

followed by projectively measuring the $\bar{A}$ system with $\{|k\rangle\langle k|\}_k$ and storing the outcome in the X system, and tracing out the $\hat{A}$ system. That is, the state obtained on the XA' registers for both procedures is identical.

Proof. The proof follows from explicit computation. Measuring the $\sigma_{\bar{A}\hat{A}A'}$ with the given POVM gives us

$$\sigma_{X\hat{A}A'} = \sum_{k=1}^{\bar{d}_A} p_k\, |k\rangle\langle k|_X \otimes |\sigma_k\rangle\langle\sigma_k|_{\hat{A}A'}\,. \tag{3.25}$$

Tracing out $\hat{A}$ gives us the state describing the original state preparation

$$\sigma_{XA'} = \sum_{k=1}^{\bar{d}_A} p_k\, |k\rangle\langle k|_X \otimes (\sigma_k)_{A'}. \tag{3.26}$$

□

Thus, we can equivalently describe the signal-preparation phase of the QKD Protocol as Alice preparing a global source-replaced state $\sigma_{A_1^n(A')_1^n} = \otimes_1^n \sigma_{AA'}$ (where we identify $A = \bar{A}\hat{A}$). After Eve's attack, this state becomes $\sigma_{A_1^n B_1^n \hat{\boldsymbol{E}}}$, which is then followed by measurements by Alice and Bob, along with subsequent protocol steps. This is exactly the structure one would expect in a typical entanglement-based protocol, in that both Alice and Bob perform measurements on a received state. Consequently, we may instead prove

security for the protocol in which Alice and Bob simply perform their measurements, and imagine that the state $\sigma_{A_1^n B_1^n \hat{\boldsymbol{E}}}$ is supplied directly by Eve.[16]

Notice that in the construction above, we have

$$\sigma_{A_1^n} = \bigotimes_{j=1}^{n} \sigma_A, \tag{3.27}$$

where

$$\sigma_A = \sum_{i,k} \sqrt{p_i p_k}\ \langle \sigma_i | \sigma_k \rangle_{\hat{A}A'} \, |i\rangle\langle k|_{\bar{A}} \tag{3.28}$$

is a fixed operator. Thus, Eve is not allowed to supply *any* arbitrary state of her choosing; she must supply a state whose marginal on A_1^n is an IID state that matches Eqs. (3.27) and (3.28). This reflects the fact that, in the original protocol, the state preparation is a trusted operation performed by Alice. We refer to this requirement as the *fixed-marginal promise* or the *fixed-marginal constraint*. This will play an important role in our analysis of the postselection technique in Chapter 5.

Security Definition Revisited

It is convenient to now view the QKD Protocol in terms of the source-replaced state, together with a CPTP map $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ that performs all operations involved in the QKD protocol. That is, $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ measures the $A_1^n B_1^n$ systems, performs all classical processing and public announcements in the registers $\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}}$, and finally produces the output key in the registers $K_A K_B$. In this picture, the ideal QKD map is given by $\mathcal{R}_{\mathrm{ideal}} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}}$; that is, it runs the original QKD protocol and then replaces the key registers with ideal ones, as described in Section 3.1. Note that the superscript ℓ denotes the *function* that determines the output key length from the public announcements. If one is interested in fixed-length protocols, we tolerate a slight abuse of notation and replace ℓ with the constant value ℓ_{fixed}.

Definition 3.6.1 (Equivalent formulation of QKD protocol)**.** At this stage, it is convenient to describe an instance of the QKD Protocol by the pair $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \sigma_A\}$, where

[16] Note that when computing key rates using numerical methods, to reduce complexity, the source-replacement scheme is often implemented only for the actual states sent without any `test` or `gen` label, with these labels instead being assigned by Alice after state preparation according to some probability distribution. For example, if $k = (a, z)$, then Alice can prepare states corresponding to a first, and *then* assign z according to $\Pr(z|a)$. The two pictures are equivalent.

$\mathcal{E}_{\mathrm{QKD}}^{(\ell)} \in \mathrm{CPTP}(A_1^n B_1^n, \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ implements the QKD protocol described in QKD Protocol (after replacing Alice's state-preparation operations with measurements). The ideal QKD protocol is then given by the pair $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}}, \sigma_A\}$, where $\mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}} = \mathcal{R}_{\mathrm{ideal}} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell)}$. Furthermore, we use $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})}, \sigma_A\}$ to describe a fixed-length variant of QKD Protocol (with the ideal protocol defined analogously).

Note that the fact that the above constitutes an equivalent definition comes from the fact that the set of possible output states for the above scenario is exactly identical to the original QKD protocol. This allows us to state the following equivalent definition of secrecy for a prepare-and-measure QKD protocol. We only require the secrecy definition here, although the full security definition can be reformulated in the same manner. These equivalent formulations will then be used in Chapters 4, 5 and 7.

Definition 3.6.2 ($\varepsilon^{\mathrm{secret}}$-secret PMQKD protocol with fixed marginal σ_A)**.** Consider the QKD Protocol represented as $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \sigma_A\}$.[17] The protocol is $\varepsilon^{\mathrm{secret}}$*-secret with fixed marginal* σ_A if

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell)} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}} \right) \otimes \mathrm{id}_{\hat{\boldsymbol{E}}} \right) \left[\rho_{A_1^n B_1^n \hat{\boldsymbol{E}}} \right] \right\|_1 \leq \varepsilon^{\mathrm{secret}}, \\ &\forall\, \rho_{A_1^n B_1^n \hat{\boldsymbol{E}}} \in \mathrm{S}_{=}(A_1^n B_1^n \hat{\boldsymbol{E}}) \text{ such that } \rho_{A_1^n} = (\sigma_A)^{\otimes n}. \end{aligned} \tag{3.29}$$

If one further specializes to IID collective attacks, where Eve is required to perform the same operations on each round, as we will in Chapters 4 and 5, then we obtain the following secrecy definition.

Definition 3.6.3 ($\varepsilon^{\mathrm{secret}}$-secret PMQKD protocol with fixed marginal σ_A against IID collective attacks)**.** Consider the QKD Protocol represented as $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \sigma_A\}$.[18] The protocol is $\varepsilon^{\mathrm{secret}}$*-secret with fixed marginal* σ_A against IID collective attacks if

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell)} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 \leq \varepsilon^{\mathrm{secret}}, \\ &\forall\, \rho_{ABE} \in \mathrm{S}_{=}(ABE) \text{ such that } \mathrm{Tr}_{BE}[\rho_{ABE}] = \sigma_A. \end{aligned} \tag{3.30}$$

3.6.2 Source Maps

The main idea behind source maps is fairly intuitive, as described in Fig. 3.4. The real source is first modelled as a virtual source followed by a quantum channel called the "source

[17] One can replace $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ with $\mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})}$ if one is interested in fixed-length protocols.

[18] One can replace $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ with $\mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})}$ if one is interested in fixed-length protocols.

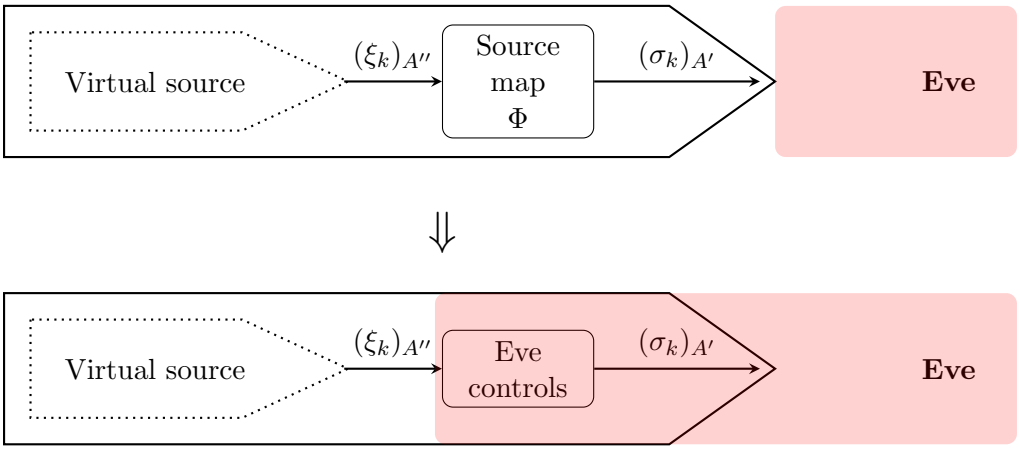


Figure 3.4: Schematic illustrating the use of a source map. A virtual source prepares $(\xi_k)_{A''}$, which is mapped to the real emitted state $(\sigma_k)_{A'}$ by a source map Ψ. Then, one can "give" Eve control over the source map (meaning that she is allowed to perform any operation she wants in place of the source map). The security of the latter implies security of the former, as argued rigorously in Lemma 7.4.1.

map". The source map is then "given" to Eve: a step that only gives her more power. In particular, Eve is allowed to replace the source map with any CPTP map of her choice. Consequently, any security statement proved under the assumption that Alice prepares $\{(\xi_k)_{A''}\}_k$ remains valid for the actual protocol in which Alice prepares $\{(\sigma_k)_{A'}\}_k$, since one of Eve's attacks in the virtual source setting involves her applying the source map Ψ as the first step of her attack. The security analysis can then be restricted to the more convenient virtual source. We rigorously apply source maps to QKD in Chapters 5 and 7, and defer to those chapters for a detailed and rigorous treatment. Here, we instead focus on providing intuition.

Definition 3.6.4 (Source map)**.** Let $\{(\sigma_k)_{A'}\}_k$ be the (possibly infinite-dimensional) family of states that Alice prepares in the actual protocol. Let A'' be a (typically finite-dimensional) register, and let $\{(\xi_k)_{A''}\}_k$ be a family of states on A''. A **source map** from the virtual source $\{(\xi_k)_{A''}\}_k$ to the actual source $\{(\sigma_k)_{A'}\}_k$ is a quantum channel $\Psi \in \mathrm{CPTP}(A'', A')$ such that

$$\sigma_k = \Psi[\xi_k] \qquad \text{for all } k. \tag{3.31}$$

We note that the registers A' and A'' are treated interchangeably throughout this thesis. In particular, any statement involving the register A' describing the real state preparation can also be applied to A'' (describing virtual state preparation).

Tagging map

An important class of source maps that is frequently used in the security analysis of decoy-state protocols is *tagging* [58]. Tagging applies when the real source emits states that are block-diagonal in a suitable decomposition, such as photon number. In this case, the real source can be replaced by a virtual source that operates as follows: with some probability, it emits a state supported on a finite photon-number subspace (corresponding to photon numbers below a fixed threshold), and with the remaining probability, it emits a classical *tag* that is readable by Eve and reveals the exact state that was prepared.

The purpose of the finite cut-off is to isolate a finite-dimensional subspace that can be handled explicitly in the security proof, while treating all higher photon-number components pessimistically by assuming that they are fully known to Eve. For example, in polarization-encoded decoy-state QKD, the source prepares fully phase-randomized coherent states, which are block-diagonal in the total photon number across all polarizations. Such a source can therefore be replaced by a virtual source that probabilistically emits a vacuum or low-photon-number state within a fixed cut-off, or otherwise emits a tagged signal that is assumed to be completely compromised.

Lemma 3.6.2 (Tagged laser source)**.** *Let $\sigma_{(a,\mu,z)} = \sum_{N=0}^{\infty} e^{-\mu} \frac{\mu^N}{N!} |N\rangle\langle N|_a$ be the real state prepared by Alice corresponding to setting choice a, μ, where $|N\rangle_a$ denotes a N-photon Fock state in the polarization a. Let the virtual state prepared by Alice be*

$$\xi_{(a,\mu,z)} = \sum_{N=0}^{N_{\text{ph}}} e^{-\mu} \frac{\mu^N}{N!} |N\rangle\langle N|_a + \left(1 - \sum_{N=0}^{N_{\text{ph}}} e^{-\mu} \frac{\mu^N}{N!}\right) |a,\mu\rangle\langle a,\mu| \,, \tag{3.32}$$

where $\{|a,\mu\rangle\}_{a,\mu}$ form an orthonormal basis for a space orthogonal to the span of $\{|N\rangle\}_{N=0}^{N_{\text{ph}}}$. Then there exists a source map Ψ_{tag} (see Definition 3.6.4) such that $\Psi_{\text{tag}}[\xi_{(a,\mu,z)}] = \sigma_{(a,\mu,z)}$ for all setting choices a, μ, z.

Proof. Define Ψ_{tag} to be the channel that projects onto $|a,\mu\rangle\langle a,\mu|$ and prepares

$$\frac{1}{\left(1 - \sum_{N=0}^{N_{\text{ph}}} e^{-\mu} \frac{\mu^N}{N!}\right)} \sum_{N=N_{\text{ph}}+1}^{\infty} e^{-\mu} \frac{\mu^N}{N!} |N\rangle\langle N|_a$$

for all a, μ; and that acts as the identity on the space spanned by $\{|N\rangle\}_{N=0}^{N_{\text{ph}}}$. It is then straightforward to verify that $\Psi_{\text{tag}}[\xi_{a,\mu}] = \sigma_{a,\mu}$. □

Security Definition Revisited (yet again)

We present yet another equivalent way to view and reason with QKD Protocol and its security definition, that focuses on the state preparation aspect. Recall that a prepare-and-measure protocol involves Alice preparing states $\sigma_k \in \mathrm{S}_=(A')$ with probability p_k in each round. That is, such protocols can be described as follows:

1. Alice first prepares the state $\sigma_{X_1^n (A')_1^n} = \left(\sum_k p_k \left|k\right\rangle\!\left\langle k\right|_X \otimes (\sigma_k)_{A'}\right)^{\otimes n}$.
2. This state is then subjected to Eve's attack $\mathcal{A} \in \mathrm{CPTP}((A')_1^n, B_1^n \hat{\boldsymbol{E}})$, resulting in the post attack state $\rho_{X_1^n B_1^n \hat{\boldsymbol{E}}}$.
3. This is followed by Bob's measurement and the remaining steps of the QKD Protocol, which can be described by a map $\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \in \mathrm{CPTP}(X_1^n B_1^n, \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$.

Equivalently, if we decide to replace Alice's state preparation procedure according to the source-replacement scheme, then we obtain the following equivalent description:

1. Alice first prepares the state $\rho_{\bar{A}_1^n \hat{A}_1^n (A')_1^n}$ as described in Lemma 7.3.3. We identify A with the systems $\bar{A}, \hat{A}$ that do not leave Alice's lab.
2. This state is then subjected to Eve's attack $\mathcal{A} \in \mathrm{CPTP}((A')_1^n, B_1^n \hat{\boldsymbol{E}})$, resulting in the post attack state $\rho_{A_1^n B_1^n \hat{\boldsymbol{E}}}$.
3. This is followed by both Alice's and Bob's measurement and the remaining steps of the QKD Protocol, which can be described by a map

$$\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \in \mathrm{CPTP}(X_1^n B_1^n, \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}}). \tag{3.33}$$

Note that the only difference between $\mathcal{E}^{(\ell)}_{\mathrm{QKD}}$ and $\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}$ (defined here) is that the former implements the QKD protocol with Alice's state preparation being described with the source-replacement scheme, and therefore involves an additional measurement on Alice's $\bar{A}$ system to create her local register X. In particular, we have

$$\mathcal{E}^{(\ell)}_{\mathrm{QKD}} = \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \circ \left(\mathcal{M}^{\mathrm{meas}}_{\{\left|k\right\rangle\!\left\langle k\right|\}}\right)^{\otimes n}, \tag{3.34}$$

where $\mathcal{M}^{\mathrm{meas}}_{\{\left|k\right\rangle\!\left\langle k\right|\}} \in \mathrm{CPTP}(A, X)$ is a channel that measures the A systems of the source-replaced state and stores the measurement outcome in the X register. Putting all of this together, we obtain the following equivalent definition.

Definition 3.6.5 (Equivalent formulation of QKD protocol)**.** At this stage, it is convenient to describe an instance of the QKD Protocol by the pair $\{\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}, \sigma_{XA'}\}$, where $\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \in \mathrm{CPTP}(X_1^n B_1^n, \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ implements the QKD protocol described in QKD Protocol. The *ideal* QKD protocol is then given by the pair $\{\widetilde{\mathcal{E}}^{(\ell),\mathrm{ideal}}_{\mathrm{QKD}}, \sigma_{XA'}\}$, where $\widetilde{\mathcal{E}}^{(\ell),\mathrm{ideal}}_{\mathrm{QKD}} = \mathcal{R}_{\mathrm{ideal}} \circ \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}$. The definition here is related to Definition 3.6.1 via

$$\sigma_{XA'} = \sum_k p_k \left|k\right\rangle\!\left\langle k\right|_X \otimes (\sigma_k)_{A'} \tag{3.35}$$

which represents Alice's state preparation, and

$$\mathcal{E}^{(\ell)}_{\mathrm{QKD}} = \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \circ \mathcal{M}^{\mathrm{meas}}_{\{|k\rangle\langle k|\}} \tag{3.36}$$

where $\mathcal{M}^{\mathrm{meas}}_{\{|k\rangle\langle k|\}}$ is the channel that performs Alice's measurements on the source-replaced state. The ideal QKD protocol is then given by the pair $\{\widetilde{\mathcal{E}}^{(\ell),\mathrm{ideal}}_{\mathrm{QKD}}, \sigma_{XA'}\}$, where $\widetilde{\mathcal{E}}^{(\ell),\mathrm{ideal}}_{\mathrm{QKD}} = \mathcal{R}_{\mathrm{ideal}} \circ \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}$.

This allows us to state the following equivalent definition of secrecy for a prepare-and-measure QKD protocol. We only require the secrecy definition here, although the full security definition can be reformulated in the same manner.

Definition 3.6.6 ($\varepsilon^{\mathrm{secret}}$-secret PMQKD protocol)**.** Consider the QKD Protocol represented as $\{\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}, \sigma_{XA'}\}$, where $\sigma_{XA'}$ represents Alice's signal preparation in each round. The protocol is $\varepsilon^{\mathrm{secret}}$**-secret** if

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\mathrm{Tr}_{K_B} \circ \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} - \mathrm{Tr}_{K_B} \circ \widetilde{\mathcal{E}}^{(\ell),\mathrm{ideal}}_{\mathrm{QKD}} \right) \otimes \mathcal{A} \right) \left[\sigma_{X_1^n (A')_1^n}\right] \right\|_1 \leq \varepsilon^{\mathrm{secret}}, \\ &\forall\, \mathcal{A} \in \mathrm{CPTP}((A')_1^n, B_1^n \hat{\boldsymbol{E}}) \end{aligned} \tag{3.37}$$

3.6.3 Squashing Maps

Squashing maps are used to modify detection setups to more convenient ones for theoretical analysis [60, 59, 61, 81, 62, 63, 82, 5] . As with source maps, we defer the formal statements regarding the use of squashing maps to Chapters 5 and 7, and describe them intuitively here (see Fig. 3.5). The main idea behind squashing maps is that the measurement statistics of a (possibly infinite-dimensional) system can be reproduced by a two-step procedure. First, a squashing map Λ is applied to the incoming state, mapping it to a potentially lower-dimensional register. This is then followed by a measurement on that register.

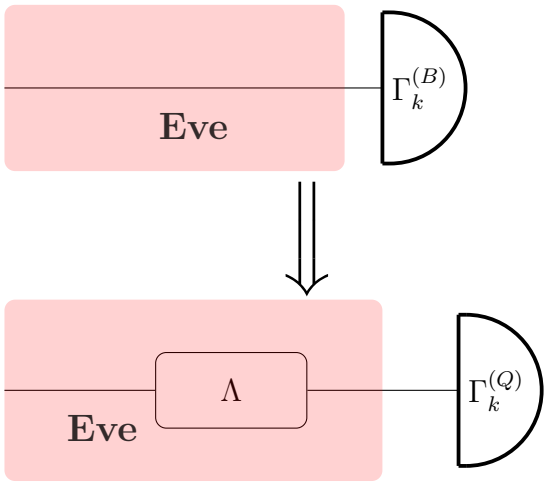


Figure 3.5: An infinite-dimensional POVM can be modelled as a squashing map Λ followed by a finite-dimensional POVM. Giving the squashing map Λ to Eve allows us to restrict our analysis to the finite-dimensional POVM.

Definition 3.6.7 (Squashing map)**.** Let $\{\Gamma_k^{(B)}\}_{k=1}^{\bar{d}_B}$ be a POVM acting on a (possibly infinite-dimensional) register B. Let Q be a (typically finite-dimensional) register, together with a POVM $\{\Gamma_k^{(Q)}\}_{k=1}^{\bar{d}_B}$ acting on Q. Then, a **squashing map** from the former POVM to the latter POVM is a quantum channel $\Lambda \in \mathrm{CPTP}(B, Q)$, such that

$$\mathrm{Tr}\left[\Gamma_k^{(B)}\rho\right] = \mathrm{Tr}\left[\Gamma_k^{(Q)}\,\Lambda[\rho]\right] \qquad \forall\, \rho \in \mathrm{S}_{=}(B),\ \forall\, k = 1, \ldots, \bar{d}_B. \tag{3.38}$$

Thus, instead of performing measurements with $\{\Gamma_k^{(B)}\}_k$, one can instead equivalently perform the squashing map and perform measurements using $\{\Gamma_k^{(Q)}\}_k$. The argument then proceeds by "giving" the squashing map to Eve, and allowing her to perform any operation she wants (see Fig. 3.5). We discuss a variety of squashing maps below:

- **Simple Squasher:** The first squashing map proposed in [60, 62] was the *simple squasher*, which reduced an active-basis–choice, polarization-encoded detection setup with perfect detectors to an effective qubit measurement (with double-click events randomly assigned to 0 or 1). We will use this squasher in Chapters 4, 5 and 7 for key rate calculations. In particular, this allows us to reduce the active-choice threshold detection setup to the one with qubit measurements (with an additional dimension for loss). Both these measurements are described in Section 3.3.1. Its main drawback

is that it requires detection efficiencies and dark count rates of all detectors to be identical.

- **The flag-state squasher:** The most versatile squashing construction currently used is the *flag-state squasher* [63], which applies to POVMs that are block-diagonal. It does not require all detectors to be identical, and in fact can be used even with imperfectly characterized detectors [78]. Importantly, it covers detection setups based on threshold detectors, which are block-diagonal in the photon-number basis, as described in Sections 2.3 and 3.3.

  We do not go into the technical details here, but briefly note that the flag-state squasher operates by splitting the Hilbert space into two subspaces. In the preserved subspaces (typically corresponding to low photon numbers), the incoming state is left unchanged and passed through. For higher photon numbers, the state is measured and the output consists of a classical flag encoding the measurement outcome.

  The main nuance to note is that if Eve's attack were completely unrestricted, then a protocol formulated directly in terms of the squashed POVM elements could not guarantee security. This is due to the existence of classical flags. Eve could simply measure the incoming state herself and then send Bob a flag encoding the outcome she obtained. Eve would then have full knowledge of Bob's measurement results, and no secrecy could be established. Consequently, this naive approach cannot yield meaningful security statements. Instead, one must impose suitable restrictions to prevent all information from being leaked through the flag registers.[19]

  There are several complementary ways of formalizing such restrictions [63, 6, 83], all of which rely on the fact that high photon-number components have a non-negligible probability of producing multi-click events. While we do not perform explicit computations in this thesis, we indicate how various results can nevertheless be applied in conjunction with the flag-state squasher.

- **The weight-preserving flag-state squasher:** The weight-preserving flag-state squasher is a modification of the flag-state squasher proposed in Ref. [5]. Its main motivation is to sidestep the difficulties that arise when combining the postselection technique with the standard flag-state squasher, in particular the challenge of enforcing the required flag-state squasher restrictions on the flag space. We defer a detailed discussion of this issue to Chapter 5.

[19] In Fig. 3.5, this can be interpreted as not giving Eve complete control over the squashing map, but rather only restricted control.

Having discussed the main tools of QKD security analysis, we give a brief explanation of the various proof technique approaches in the next section.

Remark 3.6.1. *We emphasize that, when using these tools, the precise nature of the reduction statements is important. The most useful reductions are those established directly at the level of protocol security; that is, security of the original QKD protocol follows from the security of a modified QKD protocol that is more convenient to analyze (because it replaces infinite-dimensional signal states with finite-dimensional ones, say). In this thesis, we will only carry out such reductions. This approach is particularly appealing because it allows one to perform the reduction first, and then apply* any *proof technique of choice to complete the remaining QKD security analysis.*

In contrast, many works only establish the relevant reduction at a later stage of the analysis, for instance at the level of the single-round optimization in the final key rate expression. Such reductions often interact in subtle ways with the chosen proof technique (see Remark 7.3.3), and are less general.

3.7 QKD proof techniques

In this section, we give a brief pedagogical overview of various proof techniques for QKD which are utilized at length throughout this thesis. This section is based on Ref. [7].

3.7.1 Entropic Uncertainty Relations

Proofs that rely on the entropic uncertainty relations [44] utilize the following statement to obtain a bound on the smooth min-entropy of the pre-amplification string, which is then used in the Leftover Hashing Lemma (see Section 3.5): that for any state $\rho_{A^m B^m \hat{\boldsymbol{E}}}$,

$$H_{\min}^{\bar{\epsilon}}(S_1^m|\hat{\boldsymbol{E}})_{\mathcal{E}_{\mathsf{Z}}(\rho)} + H_{\max}^{\bar{\epsilon}}(\widetilde{S}_1^m|B_1^m)_{\mathcal{E}_{\mathsf{X}}(\rho)} \geq mc_q \tag{3.39}$$

where $\mathcal{E}_{\mathsf{Z}}(\rho)$ is a channel that measures the A^m system in the Z basis, and $\mathcal{E}_{\mathsf{X}}(\rho)$ is a channel that measures the A^m system in the X basis, and c_q is a parameter that depends on these measurements POVMs [20]. Here, Alice's measurement POVMs and her reduced state are obtained from the source-replacement scheme (see also Section 3.6.1).

[20]The Z and X basis here need not be taken literally. One can use the EUR statement for *any* two POVMs, one corresponding to Z and X. (To obtain a useful statement, one must ensure that $c_q > 0$ for the two POVMs considered). For the BB84 protocol with ideal source, these correspond to the canonical Z and X basis measurements.

In the actual protocol, the Z measurements are performed, which determines (a part of) the pre-amplification string whose min-entropy we wish to bound. The max entropy term is then suitably bounded by obtaining an estimate (upper bound) on the number of "phase errors". This refers to the number of errors corresponding to (fictitious) measurements, where Alice and Bob measure these rounds in the complementary basis X instead of Z. Note that only one measurement (Z) is performed in the actual protocol. Thus, the central task in this approach is to properly define the phase error rate via fictitious measurements, and then bound it via suitable statistics arguments. We will study this technique in Chapter 6

Note that one typically only applies the EUR analysis on a part of the pre-amplification string $\mathbf{S}$[21]. Thus, one must also relate the smooth min-entropy obtained via the EUR analysis to the smooth min-entropy of the actual pre-amplification string. This is done with the use of suitable chain rules.

3.7.2 Postselection technique

The postselection technique [36, 5] is a proof technique that reduces the analysis of coherent attacks to the analysis of IID collective attacks, which we will cover in Chapter 5. It is composed primarily of three parts:

1. First, given a permutation invariant protocol, the permutation invariance property is used to reduce the analysis from all possible states $\rho_{A^nB^n}$ that could be shared by Alice and Bob to permutationally invariant states $\bar{\rho}_{A^nB^n}$ (with Eve holding a purification in the $\hat{\boldsymbol{E}}$ register).

2. Then, one applies a de Finetti theorem for permutationally invariant states, of the form

$$\bar{\rho}_{A^nB^n} \leq g_{n,x}\tau_{A^nB^n} = g_{n,x}\int d\sigma\sigma_{AB}^{\otimes n}. \tag{3.40}$$

   In the above formula, $\tau_{A^nB^n}$ is a particular mixture of IID states, while the $g_{n,x}$ term is defined by the formula $g_{n,x} = \binom{n+x-1}{x-1}$ (where x is a value that depends on the dimensions of Alice and Bob's subsystems), and affects the final security parameters and key length in the security analysis against coherent attacks. The above statement is used to reduce the security of the permutational invariant state $\bar{\rho}_{A^nB^n}$ to the security

[21] That is, the part that comes from rounds where Alice prepares single-photons. Rounds where Alice sends a multi-photon pulses cannot lead to secrecy due to the photon number splitting attack [72, 73, 74, 75], which manifests here as the c_q term becoming zero.

of a *purification* of $\tau_{A^nB^n}$, with some costs to the security parameter and key length that depend on $g_{n,x}$.

3. Finally, a finite-size security proof is obtained against *all* IID states in the mixture $\tau_{A^nB^n}$. Note that *any* proof method can be used for the IID security proof: we will see one such method in Chapter 4. This is then used to prove the security of the purification of $\tau_{A^nB^n}$.

Essentially, the proof can be viewed as "lifting" the security proof against IID collective attacks to one against coherent attacks, at the price of some penalties to the key length and security parameter. It is important to note that this lift is independent of the details of the proof technique used for the security analysis against IID collective attacks.

3.7.3 Entropy accumulation based proofs

There are a variety of accumulation theorems, such as the entropy accumulation theorem (EAT) [41, 84], generalized entropy accumulation theorem (GEAT) [77, 85] generalized Rényi entropy accumulation theorem [86], and marginal-constrained entropy accumulation theorems (MEAT) [87, 88, 11]. We will utilize the MEAT in Chapter 7, since that variant is the most suitable for the analysis of prepare-and-measure QKD protocols. In contrast, the EAT cannot be directly applied to prepare-and-measure protocols, and the GEAT and GREAT suffer from having to impose severe restrictions on the rate at which Alice can prepare and transmit the signal states.

Abstractly, entropy accumulation theorems obtain a lower bound on the n-round entropy (smooth-min and/or Rényi) of a sequential process in terms of a single-round quantity of the form[22]

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{S}|\widehat{C}_1^n\hat{\boldsymbol{E}})_{\rho|\Omega_{\mathrm{AT}}} \geq nh_{\mathrm{single-round}} - \text{corrections}, \tag{3.41}$$

where $\mathbf{S}$ are the secret registers containing the pre-amplification string, and $\hat{\boldsymbol{E}}$ denotes all of Eve's quantum side information registers. Here n is the total number of rounds in the QKD protocol, and $h_{\mathrm{single-round}}$ is a value that can be computed in terms of a minimization problem only involving single rounds of the protocol.

Thus, the security analysis within these proof techniques typically consists of justifying that the QKD protocol being implemented can be analyzed as a sequence of channels, and

[22]The correction term here depends on the probability of the event Ω_{acc}. Technically, the sequential process outputs a string different from $\mathbf{S}$, which goes through a discarding procedure, before resulting in the pre-amplification string $\mathbf{S}$. However, this discrepancy can be resolved as discussed earlier in Remark 3.5.2.

showing that these channels satisfy the conditions required to apply the relevant EAT theorem of interest. The task then reduces to the proper evaluation of the single-round quantity.

3.7.4 Phase error correction

This last proof technique is notable in that it does *not* go through the approach of bounding entropic quantities and using the Leftover hashing Lemma. It will not be discussed in this thesis, except via its connection to the EUR method, that is described below.

The phase error correction based proof technique [89, 90], sometimes referred to as a proof based on complementarity, is a proof technique based on the original Shor-Preskill [91] and the GLLP [92] proofs. In this technique, the security statement is related to the probability of a particular (virtual) phase error correction protocol succeeding. This, in turn is related to an upper bound on the number of "phase errors", which are define similarly as in the EUR approach. Thus, there is a immense degree of structural similarities between the EUR-based security proof approaches and the phase error correction-based security proof approaches. We do not discuss this exhaustively here, and refer the reader Ref. [7, Section 6.2.2] and Ref. [35] instead. However, we note that our results in Chapter 6 can be applied using phase error correction based proof technique as well.

Chapter 4

Variable-length Quantum Key Distribution

> Where we let QKD protocols decide their output key length; show that such protocols are necessary for practical implementations; investigate the various issues that arise when we let the lengths of strings appearing in the protocol vary; and make our lives easier by sticking to IID collective attacks.

Security proofs for QKD protocols are typically proven in the "fixed-length" scenario (see Section 3.2.1), where Alice and Bob either produce a key of a fixed length, or abort the protocol [34, 93, 94, 95, 96, 97, 98]. Such protocols accept and produce a key of fixed length if and only if their observed statistics belong to some predetermined "acceptance set". Otherwise, the protocol aborts. Such protocols have two main disadvantages.

First, in order to ensure that the protocol accepts with high probability for honest behaviour, the acceptance set $\mathcal{S}_{\text{acc}}$ (see Section 3.2.1) needs to be chosen carefully. Typically, the acceptance set is chosen to be the set of statistics that are close to what is expected from honest behaviour [93, 94, 95]. This requires Alice and Bob to know the honest behaviour of the channel connecting Alice and Bob, *before* a run of the QKD protocol. In many practical scenarios, such as ground-to-satellite QKD [99, 100, 101, 102, 103], it is difficult to know the behaviour of the channel in advance, since the behaviour depends on weather. In fact, this can be a problem even in fibre-based setups [104, 105, 106].

Second, even if the honest behaviour is known, the *size* of the acceptance set affects the length of the final key that can be produced. This reflects the fact that the key has

to be secure for the *worst-case* event that accepts. Larger acceptance sets have a higher probability of accepting on any given run of the QKD protocol, but lead to a shorter length of the final key, since they include worse accept events. We will see this shortly in Section 4.1. In particular, if users choose a large acceptance set, and then find that their observed statistics are much better than expected, they are *not* allowed to produce a larger key. Thus, there is a trade-off between fixed-length protocols that accept with high probability, and which produce a large key on accepting.

A variable-length QKD protocol is one that allows users to adjust the length of the key generated based upon the observed statistics during the protocol [64, 65]. This eliminates the trade-off described above. It also does not require the expected behaviour of the channel to be known in advance, simplifying implementations. In fact, variable-length protocols are almost invariably the ones implemented in the laboratory. Nevertheless, it is only relatively recently that rigorous security analyses for such protocols have been developed. The disconnect between practical implementations and the theoretical literature is perhaps best summarized by the following remark (produced with permission):

> "Norbert, I am shocked. I've always thought that one can decide on the final key length as a function of the observed error rate in any given QKD run."
>
> Giles Brassard, of BB84 fame.

In this chapter, we present a security proof for variable-length QKD protocols against IID collective attacks. This proof can then be lifted to hold against coherent attacks using the postselection technique [36], specifically [5, Corollary 4.1]. This lift is discussed in Chapter 5.

We will begin by first looking at security proofs for fixed-length protocols in Section 4.1. In Section 4.2 we will modify this analysis, and obtain a security proof for variable-length protocols. In Section 4.3 we explain the application of these results to the QKD Protocol. In Sections 4.4 and 4.5 we will apply our results to compute key rates for the qubit BB84 and decoy-state BB84 protocols, and compare the performance of fixed-length and variable-length protocols. We will see that the variable-length protocols offer significant advantages. Finally, in Section 4.6 we will present a subtle but important gap in the analysis of privacy amplification on variable-length input strings, and resolve it. This chapter is primarily based on Ref. [1], along with certain elements from Ref. [6].

Discussion on Variable-length proofs across proof techniques

Variable-length security proofs have been obtained in several prior proof techniques. Ref. [107] is an early work in the phase-error–correction framework that presents a security proof for qubit BB84, but it relies on several unsatisfactory assumptions (for instance, it assumes that Alice's pre-amplification string is perfectly uniform). A proof without such assumptions within the phase error correction framework can be found in [108, Chapter 3]. In the EUR framework, a proof was given in [109, Supplementary Note A]. We will present a and slightly more general proof for the EUR method in Chapter 6, essentially following the same steps as these prior works. For EAT-based methods, the MEAT framework [11] naturally accommodates variable-length protocols, and variable-length proofs can therefore be found in Refs. [9, 3].

4.1 Proving Fixed-Length Security

Recall our description of the fixed-length variant of QKD Protocol from Sections 3.2 and 3.2.1. After signal transmission and measurements, Alice and Bob compute the frequency distribution $\mathbf{F}^{\text{obs}} = \text{freq}(\hat{c}_1^n)$. If they find that $\mathbf{F}^{\text{obs}} \in \mathcal{S}_{\text{acc}}$, the acceptance test passes, and we refer to this event as Ω_{AT}. Otherwise, they abort. Alice and Bob may also abort during the error-verification steps, so the overall acceptance event is $\Omega_{\text{AT}} \wedge \Omega_{\text{EV}}$. Furthermore, using source replacement, the signal-preparation phase of QKD Protocol can be viewed as Alice performing measurements on the source-replaced state. The entire fixed-length protocol is represented by $\{\mathcal{E}_{\text{QKD}}^{(\ell_{\text{fixed}})}, \sigma_A\}$ (see Definition 3.6.1), where we recall that σ_A denotes the marginal on A, and $\mathcal{E}_{\text{QKD}}^{(\ell_{\text{fixed}})}$ is the QKD protocol map that implements measurements, public announcements, and classical postprocessing, and outputs the key registers K_A, K_B. Recalling the equivalent secrecy definition from Definition 3.6.3, we are required to show that

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\text{Tr}_{K_B} \circ \mathcal{E}_{\text{QKD}}^{(\ell_{\text{fixed}})} - \text{Tr}_{K_B} \circ \mathcal{E}_{\text{QKD}}^{(\ell_{\text{fixed}}),\text{ideal}} \right) \otimes \text{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 \leq \varepsilon^{\text{secret}}, \\ &\forall\, \rho_{ABE} \in \text{S}_{=}(ABE) \text{ such that } \text{Tr}_{BE}(\rho_{ABE}) = \sigma_A. \end{aligned} \tag{4.1}$$

For our analysis, we require the following structural property of the QKD maps $\mathcal{E}_{\text{QKD}}^{(\ell)}$.

Lemma 4.1.1 (Evolution of states in $\{\mathcal{E}_{\text{QKD}}^{(\ell)}, \sigma_A\}$)**.** *The evolution of states in the protocol* $\{\mathcal{E}_{\text{QKD}}^{(\ell)}, \sigma_A\}$ *can be written as*

$$\mathcal{E}_{\text{QKD}}^{(\ell)} = \mathcal{M}_{\text{CPP}} \circ \left(\mathcal{G}^{\otimes n} \right),$$

where $\mathcal{G} \in \mathrm{CPTP}(AB, SY\widehat{C})$ *performs the measurements and classical announcements in each round, and* $\mathcal{M}_{\mathrm{CPP}} \in \mathrm{CPTP}(S_1^n Y_1^n \widehat{C}_1^n, K_A K_B \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ *performs the subsequent post-processing.*

Proof. Follows from tje QKD Protocol, and the source-replacement scheme from Section 3.6.1. □

A fixed-length security proof [95, 93] proceeds by dividing all possible input states into two categories (see also [7, Section 4]: those that cause the protocol to abort with high probability, and those that do not. States that abort with high probability require no further analysis. For the remaining states, one proves that the required entropic bounds hold.

In particular, we first construct the *feasible set* $\mathcal{S}_{\mathrm{feas}} \subseteq \mathrm{S}_{=}(AB)$ with the following properties:

- If the initial state ρ_{AB} (with Eve holding the purifying system E) is not in the feasible set, then the probability of obtaining observations lying in the acceptance set (i.e, $\mathbf{F}^{\mathrm{obs}} \in \mathcal{S}_{\mathrm{acc}}$) is at most $\varepsilon_{\mathrm{AT}}$:

$$\rho \notin \mathcal{S}_{\mathrm{feas}} \implies \Pr(\Omega_{\mathrm{AT}}) = \Pr\left(\mathbf{F}^{\mathrm{obs}} \in \mathcal{S}_{\mathrm{acc}}\right)_{\rho} \leq \varepsilon_{\mathrm{AT}}. \tag{4.2}$$

  For all such states, we will show that security holds because the protocol will abort with high probability.

- For all remaining states, we compute a lower bound on the relevant entropic quantity, which then determines the output length ℓ_{fixed} to be

$$\begin{aligned}
\ell_{\mathrm{fixed}} \leq \max\Bigg\{ & 0, \\
& \left\lfloor n \inf_{\nu \in \Sigma(\mathcal{S}_{\mathrm{feas}})} \widetilde{H}_{\alpha}^{\uparrow}(S|\widehat{C}E)_{\nu} - \lambda_{\mathrm{EC}}^{\mathrm{fixed}} - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right) \right\rceil - \frac{\alpha}{\alpha - 1} \log\left(\frac{1}{\varepsilon_{\mathrm{PA}}}\right) + 2 \right\rfloor \Bigg\}, \\
\Sigma(\mathcal{S}_{\mathrm{feas}}) \coloneqq & \left\{ \mathcal{G}[\omega_{ABE}] \;\middle|\; \omega_A = \sigma_A, \omega_{AB} \in \mathcal{S}_{\mathrm{feas}} \right\},
\end{aligned} \tag{4.3}$$

  where E is purifying register. The set $\Sigma(\mathcal{S}_{\mathrm{feas}})$ corresponds to the set of possible states that can be obtained after signal transmission, measurements, public announcements, and sifting, for a single round of the QKD protocol, when the the starting state ω_{AB} belongs to the feasible set.

We will explicitly construct this feasible set for a QKD protocol in Section 4.4, using simple concentration inequalities. We can now write down the security statement for fixed-length protocols [93, 95].

Theorem 4.1.1 (Fixed-length security statement of $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})}, \sigma_A\}$ for IID collective attacks)**.** *Consider the (fixed-length) QKD Protocol given by* $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})}, \sigma_A\}$*, where* ℓ_{fixed} *is given by Eq. (4.3). Then, the protocol is* $\max\{\varepsilon_{\mathrm{PA}}, \varepsilon_{\mathrm{AT}}\}$*-secret against IID collective attacks,* $(\max\{\varepsilon_{\mathrm{PA}}, \varepsilon_{\mathrm{AT}}\} + \varepsilon_{\mathrm{EV}})$*-secure against IID collective attacks (see Definition 3.6.3).*

Proof. We have already shown that the protocol $\varepsilon_{\mathrm{EV}}$-correct in Lemma 3.4.1, and that correctness and secrecy imply security in Lemma 3.1.1. Thus, we only need to show that secrecy holds against IID collective attacks, i.e, Definition 3.6.3 is satisfied. We proceed by a case analysis on the state ρ_{AB}, which is the state shared by Alice and Bob after Eve's attack. Eve can without loss of generality be assumed to hold some purification of this state, denoted by ρ_{ABE}.[1] Thus, the QKD protocol starts with the state $\rho_{ABE}^{\otimes n}$, which is run through the channels $\mathcal{G}^{\otimes n}$ and $\mathcal{M}_{\mathrm{CPP}}$, to produce the final output state.

Note that it suffices to consider only those states that satisfy the marginal constraint, namely $\rho_A = \sigma_A$.

States not in the feasible set: For all states $\rho_{AB} \notin \mathcal{S}_{\mathrm{feas}}$, the secrecy requirement is satisfied, since the protocol aborts with high probability. We have

$$\begin{aligned}
\Delta &= \frac{1}{2}\left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}}),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n}\right] \right\|_1 \\
&= \Pr(\Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}) \frac{1}{2} \left\| \rho^{(\ell_{\mathrm{fixed}})}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}} - \rho^{(\ell_{\mathrm{fixed}}),\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}} \right\|_1 \\
&\leq \Pr(\Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}) \\
&\leq \Pr(\Omega_{\mathrm{AT}}) \\
&\leq \varepsilon_{\mathrm{AT}}
\end{aligned} \tag{4.4}$$

where the first two lines follow simply by rewriting the expression, the third line follows from the fact that the trace distance is upper bounded by 1, the fourth line follows from the properties of probability, and the final line follows from the fact that $\rho_{AB} \notin \mathcal{S}_{\mathrm{feas}}$.

[1] If Eve wishes to hold an extension rather than a purification, we may always consider a scenario in which she instead holds a purification of that extension and simply ignores the additional purifying system. This can also be formalized using suitable data-processing inequalities for the relevant entropies, since there always exists a quantum channel mapping the purifying system to the extension system (Lemma 2.1.1).

States in the feasible set: For all states $\rho_{AB} \in \mathcal{S}_{\text{feas}}$, we use the Leftover Hashing Lemma, and various manipulations of the entropic quantities, to show that the value of ℓ_{fixed} specified in Eq. (4.3) ensures secrecy. This can be seen by the following chain of inequalities:

$$\Delta = \frac{1}{2}\left\| \left(\left(\text{Tr}_{K_B} \circ \mathcal{E}_{\text{QKD}}^{(\ell_{\text{fixed}})} - \text{Tr}_{K_B} \circ \mathcal{E}_{\text{QKD}}^{(\ell_{\text{fixed}}),\text{ideal}} \right) \otimes \text{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 \tag{4.5}$$

$$= \Pr(\Omega_{\text{AT}} \wedge \Omega_{\text{EV}}) \, \frac{1}{2} \left\| \rho^{(\ell_{\text{fixed}})}_{K_A \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_1^n | \Omega_{\text{AT}} \wedge \Omega_{\text{EV}}} - \rho^{(\ell_{\text{fixed}}),\text{ideal}}_{K_A \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_1^n | \Omega_{\text{AT}} \wedge \Omega_{\text{EV}}} \right\|_1 \tag{4.6}$$

$$\leq \Pr(\Omega_{\text{AT}} \wedge \Omega_{\text{EV}}) \, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow (S_1^n | \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{EV}} E_1^n)_{\rho | \Omega_{\text{AT}} \wedge \Omega_{\text{EV}}} - \ell_{\text{fixed}} + 2 \right)} \tag{4.7}$$

$$\leq \Pr(\Omega_{\text{AT}} \wedge \Omega_{\text{EV}}) \, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow (S_1^n | \widehat{C}_1^n H_{\text{EV}} E_1^n)_{\rho | \Omega_{\text{AT}} \wedge \Omega_{\text{EV}}} - \lambda_{\text{EC}}^{\text{fixed}} - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}} \right) \right\rceil - \ell_{\text{fixed}} + 2 \right)} \tag{4.8}$$

$$\leq 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow (S_1^n | \widehat{C}_1^n H_{\text{EV}} E_1^n)_{\rho} - \lambda_{\text{EC}}^{\text{fixed}} - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}} \right) \right\rceil - \ell_{\text{fixed}} + 2 \right)} \tag{4.9}$$

$$= 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow (S_1^n | \widehat{C}_1^n E_1^n)_{\rho} - \lambda_{\text{EC}}^{\text{fixed}} - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}} \right) \right\rceil - \ell_{\text{fixed}} + 2 \right)} \tag{4.10}$$

$$= 2^{\frac{1-\alpha}{\alpha}\left(n \widetilde{H}_\alpha^\uparrow (S | \widehat{C} E)_{\mathcal{G}[\rho_{AB}]} - \lambda_{\text{EC}}^{\text{fixed}} - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}} \right) \right\rceil - \ell_{\text{fixed}} + 2 \right)} \tag{4.11}$$

$$\leq \varepsilon_{\text{PA}}. \tag{4.12}$$

Here $\widetilde{H}_\alpha^\uparrow$ denotes the Rényi entropy (see Definition 2.2.2), with α the Rényi parameter. In Eq. (4.7), we apply the Leftover Hashing Lemma for Rényi entropy[2] [40, Theorem 8] (restated in Lemma 3.5.1). In Eq. (4.8), we split off the contributions from the error-correction and error-verification registers using Lemma 2.2.4.[3] In Eq. (4.9), we remove the conditioning on the events $\Omega_{\text{AT}} \wedge \Omega_{\text{EV}}$ using Lemma 2.2.6. In Eq. (4.10), we remove the H_{EV} register without penalty, since it is completely uncorrelated with the remaining registers; this follows by applying data processing inequalities (Lemma 2.2.2) in both directions. In Eq. (4.11), we use the additivity of Rényi entropy for IID states, together with the fact that

$$\rho_{S_1^n \widehat{C}_1^n E_1^n} = \mathcal{G}^{\otimes n}[\rho_{ABE}^{\otimes n}].$$

[2]Note that in this proof, we pretend as though the S_1^n is the pre-amplification string, instead of $\mathbf{S}$: the latter is obtained from the former via sifting. This discrepancy is address in Section 4.6 (see also Remark 3.5.2).

[3]Technically, Bob also sends one additional bit indicating whether the hash values match. However, since the state is conditioned on Ω_{EV}, this bit takes a deterministic value and can therefore be removed at no cost. This is argued formally in Chapter 7.

Finally, Eq. (4.12) follows from the definition of ℓ_{fixed} in Eq. (4.3): since ℓ_{fixed} is obtained by minimizing over all possible states ρ_{ABE} where $\rho_{AB} \in \mathcal{S}_{\text{feas}}$.

Thus $\max\{\varepsilon_{\text{AT}}, \varepsilon_{\text{PA}}\}$-secrecy holds. This concludes our proof. □

A similar proof can be obtained using smoothed-min entropies, although in that case one has to consider states that are partial on $\Omega_{\text{AT}} \wedge \Omega_{\text{EV}}$ instead of states conditioned on that event, as we do here. However, the Rényi version typically gives tighter key rates. Moreover, we require the Rényi version for handling the variable-length case, as we point out in Remark 4.2.2 later.

Remark 4.1.1. *We strongly emphasize that at no point in the above argument did we make any assumption about the probability that Eve performs a particular attack. We do not know these probabilities, and Eve is free to behave adversarially in any manner she chooses. The statements we make are always of the form: "*if *Eve performs this attack, then the protocol aborts," or "*if *Eve performs some other attack, then the chosen hash length ensures secrecy." Thus, security holds* regardless *of Eve's behaviour, and without requiring any prior probability distribution over Eve's attacks.*

4.2 Proving Variable-length Security

When we consider the variable-length security requirement (Eq. (3.4)), we encounter a proliferation of events corresponding to various output key lengths and, consequently, many more terms in the final trace-distance quantity that we seek to bound. A naive extension of the fixed-length analysis would look something like this. We could first enumerate all possible acceptance sets, each of which corresponds to producing a key of a different length. Then, for each acceptance set, we could define a corresponding feasible set and repeat the steps of the fixed-length proof. Such an approach would yield a correct proof, but it suffers from a significant drawback: the final security parameter becomes the sum of the individual ε-terms obtained across the different cases. If the number of possible hash lengths is large (for instance, on the order of n), then the overall secrecy parameter degrades by a multiplicative factor of n. This is clearly undesirable.[4]

[4]Under certain conditions—specifically, when the acceptance sets form a "nested" sequence of increasing size—this penalty can be avoided; see Ref. [1, Section III] for such an approach. However, this nesting condition is quite restrictive, as it does not allow the protocol to be designed to handle unpredictable channel conditions. In this thesis, we directly obtain the more general setting, and therefore do not discuss the specialized result here.

We will now prove a general result that avoids this problem. We consider the QKD Protocol, which directly uses the observed frequency of outcomes in $\widehat{C}_1^n$ (denoted via $\mathbf{F}^{\text{obs}}$), to determine the length of the secret key to be produced and the number of bits to be used for error-correction. Crucially, our method involves the construction of a statistical estimator $b_{\text{stat}}(\mathbf{F}^{\text{obs}})$, that with high probability is a lower bound on the Rényi entropy $\widetilde{H}_\alpha^\uparrow(S_1^n|\widehat{C}_1^n E_1^n)_\rho$ of the state $\rho_{S_1^n \widehat{C}_1^n E_1^n}$ obtained in the QKD protocol. That is, we will require an estimator b_{stat} such that for any state ρ_{ABE}, it is the case that

$$\Pr_{\mathbf{F}^{\text{obs}}} \left(b_{\text{stat}}(\mathbf{F}^{\text{obs}}) \leq \widetilde{H}_\alpha^\uparrow(S_1^n|\widehat{C}_1^n E_1^n)_\rho \right) \geq 1 - \varepsilon_{\text{AT}}. \tag{4.13}$$

We will construct this estimator for a QKD protocol later in Section 4.4, using simple concentration inequalities. A lemma that helps in this construction is obtained below.

Remark 4.2.1. *Note that in a QKD protocol, we deal with a fixed yet unknown ρ_{ABE}, which is determined by Eve's attack, and which is* not *a random variable. This ρ_{ABE} then gives rise to a random variable $\mathbf{F}^{\text{obs}}$. Given that Alice and Bob observe $\mathbf{F}^{\text{obs}}$, obtained by performing measurements on $\rho_{ABE}^{\otimes n}$, we would like to construct the function $b_{\text{stat}}(\mathbf{F}^{\text{obs}})$ which acts as an estimator of Rényi entropy. To do so, we will need to construct a set $\mathcal{V}(\mathbf{F}^{\text{obs}})$ with the required properties, as described in the following Lemma.*

Lemma 4.2.1. *For any state ρ_{ABE}, let $\mathbf{F}^{\text{obs}} \in \mathbb{P}(\widehat{\mathbb{C}})$ denote the frequency distribution of outcomes in the register $\widehat{C}$, obtained by measuring the state $\rho_{ABE}^{\otimes n}$ in the QKD Protocol. That is, we have*

$$\rho_{S_1^n Y_1^n \widehat{C}_1^n E_1^n} = \rho_{SY\widehat{C}E}^{\otimes n} = \mathcal{G}^{\otimes n}[\rho_{ABE}^{\otimes n}], \tag{4.14}$$

and $\mathbf{F}^{\text{obs}}$ is the frequency distribution of outcomes in $\rho_{\widehat{C}_1^n}$. Suppose that we have a "confidence set" $V(\mathbf{F}^{\text{obs}})$[5] such that, for all states ρ_{AB}, it holds that[6]

$$\Pr_{\mathbf{F}^{\text{obs}}} \left(\rho_{AB} \in \mathcal{V}(\mathbf{F}^{\text{obs}}) \right) \geq 1 - \varepsilon_{\text{AT}}. \tag{4.15}$$

Then any $b_{\text{stat}}(\mathbf{F}^{\text{obs}})$ satisfying

$$\begin{aligned} b_{\text{stat}}(\mathbf{F}^{\text{obs}}) &\leq n \inf_{\nu \in \Sigma(\mathbf{F}^{\text{obs}})} \widetilde{H}_\alpha^\uparrow(S|\widehat{C}E)_\nu, \\ \Sigma(\mathbf{F}^{\text{obs}}) &:= \left\{ \mathcal{G}[\omega_{ABE}] \;\middle|\; \omega_A = \sigma_A \,, \omega_{AB} \in \mathcal{V}(\mathbf{F}^{\text{obs}}) \right\}, \end{aligned} \tag{4.16}$$

where E denotes purifying register, satisfies the required property from Eq. (4.13).

[5] Technically, $\mathcal{V}$ is a function that takes a frequency distribution as input and outputs a set of states.

[6] It is crucial to note that this lemma is making statements about a *fixed but unknown* state ρ_{AB}, which gives rise to random variables $\mathbf{F}^{\text{obs}}$ and $\mathcal{V}(\mathbf{F}^{\text{obs}})$.

Proof. From the additivity of Rényi entropy across tensor products (see Lemma 2.2.5), and the fact that $\rho_{S_1^n \widehat{C}_1^n E_1^n}$ is an IID state, we have that $\widetilde{H}_\alpha^\uparrow(S_1^n|\widehat{C}_1^n E_1^n)_{\mathcal{G}^{\otimes n}[\rho_{ABE}^{\otimes n}]} = n\widetilde{H}_\alpha^\uparrow(S|\widehat{C}E)_{\mathcal{G}[\rho_{ABE}]}$. Thus the required statement follows from:

$$\begin{aligned}\Pr\Big(b_{\text{stat}}(\mathbf{F}^{\text{obs}}) \leq \widetilde{H}_\alpha^\uparrow(S_1^n|\widehat{C}_1^n E_1^n)_\rho\Big) &= \Pr\Big(b_{\text{stat}}(\mathbf{F}^{\text{obs}}) \leq n\widetilde{H}_\alpha^\uparrow(S|\widehat{C}E)_{\mathcal{G}[\rho_{ABE}]}\Big) \\ &\geq \Pr\big(\rho_{AB} \in \mathcal{V}(\mathbf{F}^{\text{obs}})\big) \\ &\geq 1 - \varepsilon_{\text{AT}}\end{aligned} \tag{4.17}$$

where the probability is taken over $\mathbf{F}^{\text{obs}}$, where we used the fact that

$$\rho_{AB} \in \mathcal{V}(\mathbf{F}^{\text{obs}}) \implies b_{\text{stat}}(\mathbf{F}^{\text{obs}}) \leq n\widetilde{H}_\alpha^\uparrow(S|\widehat{C}E)_{\mathcal{G}[\rho_{ABE}]} \tag{4.18}$$

for the second line, and the property of $\mathcal{V}$ (Eq. (4.15)) for the final line. □

Thus, in order to construct the required $b_{\text{stat}}(\mathbf{F}^{\text{obs}})$, we only need to construct $\mathcal{V}(\mathbf{F}^{\text{obs}})$, which can be done using standard concentration inequalities. This then determines the length of the output key as follows:

- The function $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) : \mathbb{P}(\widehat{\mathcal{C}}) \to \mathbb{N}$, which determines the number of possible transcripts of the error-correction protocol that is used, can be chosen arbitrarily.
- Then, the output key length $\ell(\mathbf{F}^{\text{obs}})$ is given by

$$\ell(\mathbf{F}^{\text{obs}}) \coloneqq \max\left\{\left\lfloor b_{\text{stat}}(\mathbf{F}^{\text{obs}}) - \lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) - \theta(\varepsilon_{\text{EV}}, \varepsilon_{\text{PA}})\right\rfloor, 0\right\} \tag{4.19}$$

  where for brevity, we use

$$\theta(\varepsilon_{\text{EV}}, \varepsilon_{\text{PA}}) \coloneqq \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}}\right)\right\rceil + \frac{\alpha}{\alpha - 1}\log\left(\frac{1}{\varepsilon_{\text{PA}}}\right) - 2. \tag{4.20}$$

We can now write down the security statement for variable-length protocols.

Theorem 4.2.1 (Variable-length security statement of $\{\mathcal{E}_{\text{QKD}}^{(\ell)}, \sigma_A\}$ for IID collective attacks)**.** *Consider the variable-length QKD Protocol given by $\{\mathcal{E}_{\text{QKD}}^{(\ell)}, \sigma_A\}$, where $\ell(\mathbf{F}^{\text{obs}})$ is given by Eq. (4.19), and $b_{\text{stat}}(\mathbf{F}^{\text{obs}})$ satisfies Eq. (4.13). Then, the protocol is $(\varepsilon_{\text{PA}} + \varepsilon_{\text{AT}})$-secret against IID collective attacks, and $(\varepsilon_{\text{PA}} + \varepsilon_{\text{AT}} + \varepsilon_{\text{EV}})$-secure against IID collective attacks (see Definition 3.6.3).*

Proof. Again, as in the proof of Theorem 4.1.1, we only need to show that secrecy holds against IID collective attacks. Let us fix the attack Eve performs, i.e, we fix the state ρ_{AB} shared between Alice and Bob, and assume that Eve holds some purification ρ_{ABE}. As this protocol proceeds, we obtain the state $\rho_{S_1^n \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} E_1^n}$, where

$$\rho_{S_1^n Y_1^n \widehat{C}_1^n E_1^n} = \rho_{SY\widehat{C}E}^{\otimes n} = \mathcal{G}^{\otimes n}[\rho_{ABE}^{\otimes n}].$$

A critical step in our proof is the division of all possible observations into two sets: one that corresponds to observations leading to a key length that is sufficiently small to guarantee secrecy (denoted by $\mathcal{T}_{\leq}$), and another that does not (denoted by $\mathcal{T}_{>}$). Security for observations in the former set follows essentially from the fact that the key length is small enough. Security for observations in the latter set follows from the fact that such cases occur only with small probability, since the key length is chosen as a suitable function of $b_{\mathrm{stat}}(\mathbf{F}^{\mathrm{obs}})$, which itself acts as a statistical estimator of the Rényi entropy.

We define the sets $\mathcal{T}_{\leq}$ as

$$\mathcal{T}_{\leq} := \left\{ \mathbf{F}^{\mathrm{obs}} | \ell(\mathbf{F}^{\mathrm{obs}}) + \lambda_{\mathrm{EC}}(\mathbf{F}^{\mathrm{obs}}) + \theta(\varepsilon_{\mathrm{EV}}, \varepsilon_{\mathrm{PA}}) \leq \widetilde{H}_{\alpha}^{\uparrow}(S_1^n | \widehat{C}_1^n E_1^n)_{\rho} \ \wedge \ \ell(\mathbf{F}^{\mathrm{obs}}) > 0 \right\}, \quad (4.21)$$

$$\mathcal{T}_{>} := \left\{ \mathbf{F}^{\mathrm{obs}} | \ell(\mathbf{F}^{\mathrm{obs}}) + \lambda_{\mathrm{EC}}(\mathbf{F}^{\mathrm{obs}}) + \theta(\varepsilon_{\mathrm{EV}}, \varepsilon_{\mathrm{PA}}) > \widetilde{H}_{\alpha}^{\uparrow}(S_1^n | \widehat{C}_1^n E_1^n)_{\rho} \ \wedge \ \ell(\mathbf{F}^{\mathrm{obs}}) > 0 \right\}. \quad (4.22)$$

The analysis now proceeds by writing out the sum over all possible observations $\mathbf{F}^{\mathrm{obs}}$, and then grouping them according to the sums above.[7] Let $\Omega(\mathbf{F}^{\mathrm{obs}})$ be the event that $\widehat{C}_1^n$ holds a value $\hat{c}_1^n$ such that $\mathrm{freq}(\hat{c}_1^n) = \mathbf{F}^{\mathrm{obs}}$.

Let us consider the secrecy definition for variable-length protocols (Definition 3.6.3). The definition groups together terms with the same output length of the key, and the different events $\Omega(\mathbf{F}^{\mathrm{obs}})$ may correspond to the same output length of the key. Nevertheless, the events $\Omega(\mathbf{F}^{\mathrm{obs}})$ are deterministic functions of public announcements $\widehat{C}_1^n$. Thus, the states $\rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}}$ have orthogonal supports. Therefore, we have

$$\begin{aligned} \Delta &= \frac{1}{2} \left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}})} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell_{\mathrm{fixed}}),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 \\ &\leq \sum_{\substack{\mathbf{F}^{\mathrm{obs}} \\ \ell(\mathbf{F}^{\mathrm{obs}})>0}} \Pr\left(\Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}} \right) \times \\ &\quad \frac{1}{2} \left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}} \right\|_1 \end{aligned} \quad (4.23)$$

[7] Note that the main idea of the proof here is identical to that of published work [1]; however, the presentation here is cleaner and simpler.

where we can omit events which lead to aborts, which do not contribute to the trace distance. We can now split the sum over $\mathbf{F}^{\text{obs}}$ into two parts, one corresponding to $\mathbf{F}^{\text{obs}} \in \mathcal{T}_{>}$, and other correspoding to $\mathbf{F}^{\text{obs}} \in \mathcal{T}_{\leq}$. The first part of the above expression can be bounded as

$$
\begin{aligned}
\Delta_{>} \coloneqq & \sum_{\mathbf{F}^{\text{obs}} \in \mathcal{T}_{>}} \Pr\big(\Omega(\mathbf{F}^{\text{obs}}) \wedge \Omega_{\text{EV}}\big) \times \\
& \frac{1}{2} \left\| \rho_{K_A \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_1^n | \Omega(\mathbf{F}^{\text{obs}}) \wedge \Omega_{\text{EV}}} - \rho^{\text{ideal}}_{K_A \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_1^n | \Omega(\mathbf{F}^{\text{obs}}) \wedge \Omega_{\text{EV}}} \right\|_1 && (4.24) \\
& \leq \sum_{\mathbf{F}^{\text{obs}} \in \mathcal{T}_{>}} \Pr\big(\Omega(\mathbf{F}^{\text{obs}}) \wedge \Omega_{\text{EV}}\big) && (4.25) \\
& \leq \sum_{\mathbf{F}^{\text{obs}} \in \mathcal{T}_{>}} \Pr\big(\Omega(\mathbf{F}^{\text{obs}})\big) && (4.26) \\
& = \Pr_{\mathbf{F}^{\text{obs}}} \Big(\ell(\mathbf{F}^{\text{obs}}) + \lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) + \theta(\varepsilon_{\text{EV}}, \varepsilon_{\text{PA}}) > \widetilde{H}_{\alpha}^{\uparrow}(S_1^n \mid \widehat{C}_1^n E_1^n) \ \wedge \ \ell(\mathbf{F}^{\text{obs}}) > 0 \Big) && (4.27) \\
& \leq \Pr_{\mathbf{F}^{\text{obs}}} \Big(b_{\text{stat}}(\mathbf{F}^{\text{obs}}) > \widetilde{H}_{\alpha}^{\uparrow}(S_1^n \mid \widehat{C}_1^n E_1^n)_{\rho} \Big) && (4.28) \\
& \leq \varepsilon_{\text{AT}}. && (4.29)
\end{aligned}
$$

In Eq. (4.25), we use the fact that the trace distance is upper bounded by 1. In Eq. (4.26), we use basic properties of probability. Eq. (4.27) is a reformulation of Eq. (4.26), expressing the probability in terms of the defining property of the set $\mathcal{T}_{>}$. The inequality in Eq. (4.28) follows from the fact that the statements inside the probability in Eq. (4.27) imply $b_{\text{stat}}(\mathbf{F}^{\text{obs}}) \geq \widetilde{H}_{\alpha}^{\uparrow}(S_1^n \mid \widehat{C}_1^n E_1^n)_{\rho}$ (using Eq. (4.19)). Finally, Eq. (4.29) follows from the defining properties of the estimator b_{stat}, which guarantees that the probability of overestimating the Rényi entropy is bounded by ε_{AT}.

The remaining part of Δ can be bounded via the Leftover Hashing Lemmas, via

$$\Delta_{\leq} = \sum_{\mathbf{F}^{\mathrm{obs}} \in \mathcal{T}_{\leq}} \Pr\big(\Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}\big) \times$$

$$\frac{1}{2} \left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}} \right\|_1 \tag{4.30}$$

$$\leq \sum_{\mathbf{F}^{\mathrm{obs}} \in \mathcal{T}_{\leq}} \Pr\big(\Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}\big)\, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} E_1^n)_{\rho | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}} - \ell(\mathbf{F}^{\mathrm{obs}}) + 2\right)} \tag{4.31}$$

$$\leq \sum_{\mathbf{F}^{\mathrm{obs}} \in \mathcal{T}_{\leq}} \Pr\big(\Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}\big)\, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n H_{\mathrm{EV}} E_1^n)_{\rho | \Omega(\mathbf{F}^{\mathrm{obs}}) \wedge \Omega_{\mathrm{EV}}} - \lambda_{\mathrm{EC}}(\mathbf{F}^{\mathrm{obs}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \ell(\mathbf{F}^{\mathrm{obs}}) + 2\right)} \tag{4.32}$$

$$\leq \sum_{\mathbf{F}^{\mathrm{obs}} \in \mathcal{T}_{\leq}} \Pr\big(\Omega(\mathbf{F}^{\mathrm{obs}})\big)\, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n H_{\mathrm{EV}} E_1^n)_{\rho | \Omega(\mathbf{F}^{\mathrm{obs}})} - \lambda_{\mathrm{EC}}(\mathbf{F}^{\mathrm{obs}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \ell(\mathbf{F}^{\mathrm{obs}}) + 2\right)} \tag{4.33}$$

$$= \sum_{\mathbf{F}^{\mathrm{obs}} \in \mathcal{T}_{\leq}} \Pr\big(\Omega(\mathbf{F}^{\mathrm{obs}})\big)\, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n E_1^n)_{\rho | \Omega(\mathbf{F}^{\mathrm{obs}})} - \lambda_{\mathrm{EC}}(\mathbf{F}^{\mathrm{obs}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \ell(\mathbf{F}^{\mathrm{obs}}) + 2\right)} \tag{4.34}$$

$$\leq \sum_{\mathbf{F}^{\mathrm{obs}} \in \mathcal{T}_{\leq}} \Pr\big(\Omega(\mathbf{F}^{\mathrm{obs}})\big)\, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n E_1^n)_{\rho | \Omega(\mathbf{F}^{\mathrm{obs}})} - \widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n E_1^n)_\rho + \theta(\varepsilon_{\mathrm{EV}}, \varepsilon_{\mathrm{PA}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil + 2\right)} \tag{4.35}$$

$$\leq 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n E_1^n)_\rho - \widetilde{H}_\alpha^\uparrow(S_1^n | \widehat{C}_1^n E_1^n)_\rho + \theta(\varepsilon_{\mathrm{EV}}, \varepsilon_{\mathrm{PA}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil + 2\right)} \tag{4.36}$$

$$\leq \varepsilon_{\mathrm{PA}}. \tag{4.37}$$

In Eq. (4.31), we apply the Leftover Hashing Lemma (Lemma 3.5.1).[8] In Eq. (4.32), we split off the error correction and error verification registers using Lemma 2.2.4.[9] In Eq. (4.33), we remove the conditioning on the event Ω_{EV} using Lemma 2.2.3. In Eq. (4.34), we remove the H_{EV} register without penalty, since it is uncorrelated with the remaining registers; this follows formally from data processing (Lemma 2.2.2). In Eq. (4.35), we use the defining

[8] Note that in this proof, we pretend as though the S_1^n is the pre-amplification string, instead of $\mathbf{S}$: the latter is obtained from the former via sifting. This discrepancy is address in Section 4.6 (see also Remark 3.5.2).

[9] As before, since we condition on Ω_{EV}, the single bit sent by Bob indicating whether the hash values match takes a deterministic value and can therefore be ignored.

property of the set $\mathcal{T}_{\leq}$, namely that

$$\ell(\mathbf{F}^{\text{obs}}) + \lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) + \theta(\varepsilon_{\text{EV}}, \varepsilon_{\text{PA}}) \leq \widetilde{H}_{\alpha}^{\uparrow}(S_1^n \mid \widehat{C}_1^n E_1^n)_{\rho},$$

to replace the $\mathbf{F}^{\text{obs}}$-dependent terms by a global bound. This step is crucial, as it reduces the number of terms that depend on $\mathbf{F}^{\text{obs}}$. After this replacement, the expression appears to be a weighted average of Rényi entropies, and one can use Lemma 2.2.7 to combine all the terms to obtain Eq. (4.36). Finally, Eq. (4.37) follows from straightforward algebra.

The required statement then follows from

$$\Delta = \Delta_{>} + \Delta_{\leq} \leq \varepsilon_{\text{AT}} + \varepsilon_{\text{PA}}. \tag{4.38}$$

This concludes the proof. □

Remark 4.2.2. *We highlight two critical steps in the proof of Theorem 4.2.1. The first ingredient is the appropriate construction of sets $\mathcal{T}_{\leq}, \mathcal{T}_{>}$ and the relationship between these sets, $b_{\text{stat}}(\mathbf{F}^{\text{obs}})$ and $\ell(\mathbf{F}^{\text{obs}})$. These sets depend on Eve's attack, and our argument allows us to construct them appropriately for every possible attack, and then to bound the two contributions to Δ that arise from it. The second key step is the use of Lemma 2.2.7, which allows us to get rid of terms involving Rényi entropies of states conditioned on events. In particular, smooth min-entropy does not straightforwardly allow a statement analogous to Lemma 2.2.7: thus, the above proof requires the use of Rényi entropy.*

Having proved both fixed-length and variable-length security, we will now turn to the construction of the required sets needed for key rate calculations.

4.3 Constructing feasible sets confidence sets

In this section, we explain the construction of the sets required for using the results in this chapter ($\mathcal{S}_{\text{feas}}$ and $\mathcal{V}(\mathbf{F}^{\text{obs}})$). Recall that the QKD Protocol we consider produces a public announcement in each round, recorded in the register $\widehat{C}$, which has alphabet $\widehat{\mathcal{C}}$. We partition this alphabet of possible announcements into two disjoint subsets: one used for key generation, denoted $\widehat{\mathcal{C}}_{\text{gen}}$, and one used for testing, denoted $\widehat{\mathcal{C}}_{\text{test}}$[10]. Thus,

$$\widehat{\mathcal{C}} = \widehat{\mathcal{C}}_{\text{test}} \cup \widehat{\mathcal{C}}_{\text{gen}}.$$

[10]These labels reflect the structure of the concrete protocols considered later, where Alice designates each round as a `test` or `gen` round with probabilities γ and $1-\gamma$, respectively. For the purpose of the security analysis, however, this partition is simply a generic division of the announcement alphabet.

Roughly speaking, the announcements corresponding to test rounds are used to infer properties of the underlying quantum state, whereas the announcements corresponding to key-generation rounds are used to extract secret key bits.

Let $\{\Gamma_i^{(AB)}\}_{i\in\widehat{\mathcal{C}}}$ denote the POVM associated with the public announcements, where each POVM element is indexed by the corresponding announcement. In each round of the protocol, this POVM is applied and a single outcome is obtained. Since we assume IID collective attacks, the outcomes across rounds are independent and identically distributed. In particular, for any fixed announcement $i \in \widehat{\mathcal{C}}$, the number of times outcome i is observed over n rounds follows a binomial distribution, with an unknown success probability determined by the underlying state.

This observation was first made and utilized in Ref. [6], which motivates the use of statistical concentration results for binomial random variables, which we will employ below to construct confidence regions for the relevant parameters. Note that our analysis here very closely mirrors the one from Ref. [6], but is not identical to it. In particular, Ref. [6] obtains a slightly tighter result for fixed-length scenarios.

4.3.1 Binomial tail probabilities and confidence intervals

Let X be a binomial random variable with parameters (n, p), that is, $X \sim \text{Binomial}(n, p)$, where $p \in [0, 1]$ is an unknown success probability. Suppose that x successes are observed in n independent trials, and define the empirical frequency $f_{\text{obs}} := \frac{x}{n}$. For fixed integers n and x, the binomial tail probabilities

$$\Pr(X \leq x) = \sum_{k=0}^{x} \binom{n}{k} p^k (1-p)^{n-k} \quad \text{and} \quad \Pr(X \geq x) = \sum_{k=x}^{N} \binom{n}{k} p^k (1-p)^{n-k}$$

are monotone functions of the parameter p. Consequently, for any $\varepsilon \in (0, 1)$, there exist unique values of p for which these tail probabilities equal ε, which can be expressed in terms of quantiles of the beta distribution. Specifically, the equation

$$\Pr_{X\sim\text{Binomial}(n,p)}(X \geq x) = \varepsilon \tag{4.39}$$

is solved by

$$p = \mathcal{B}_{\text{beta}}\left(\varepsilon;\, x,\, n - x + 1\right), \tag{4.40}$$

where $\mathcal{B}_{\text{beta}}$ denotes the qth quantile of the beta distribution with shape parameters (a, b)[11]. Similarly, the equation

$$\Pr_{X\sim\text{Binomial}(n,p)}(X \leq x) = \varepsilon \tag{4.41}$$

is solved by

$$p = \mathcal{B}_{\text{beta}}\left(1-\varepsilon;\, x+1,\, n-x\right). \tag{4.42}$$

Equivalently, we have that [110, 111]

$$\begin{aligned} p \leq \mathcal{B}_{\text{beta}}\left(\varepsilon;\, x,\, n-x+1\right) &\implies \Pr(X \geq x) \leq \varepsilon \\ p \geq \mathcal{B}_{\text{beta}}\left(1-\varepsilon;\, x+1,\, n-x\right) &\implies \Pr(X \leq x) \leq \varepsilon \end{aligned} \tag{4.43}$$

We will now use Eq. (4.43) for constructing $\mathcal{S}_{\text{feas}}$ and $\mathcal{V}(\mathbf{F}^{\text{obs}})$ with the desired properties.

4.3.2 From binomial distribution to Set constructions

The following lemma constructs the feasible set $\mathcal{S}_{\text{feas}}$ from the acceptance set $\mathcal{S}_{\text{acc}}$ and the parameter ε_{AT}, in a way that satisfies the requirements of Section 4.1. The acceptance set (which we recall is the set of observations for which the acceptance test passes) is defined as the set of frequency vectors that lie close to a predetermined reference value $\bar{\mathbf{F}}$. This reference value is typically set to be the honest behaviour of the protocol. Our construction relies on the fact that, for each outcome $i \in \widehat{\mathcal{C}}$, the number of times outcome i is observed follows a binomial distribution, and corresponds to a measurement with POVM element $\Gamma_i^{(AB)}$.

Lemma 4.3.1 (Constructing the feasible set from Section 4.1)**.** *Let $\bar{\mathbf{F}} \in \mathbb{P}(\widehat{\mathcal{C}})$ be a frequency distribution such that the acceptance set $\mathcal{S}_{\text{acc}}$ is defined via*[12]

$$\mathcal{S}_{\text{acc}} \coloneqq \left\{\mathbf{F}^{\text{obs}} \mid |\mathbf{F}_i^{\text{obs}} - \bar{\mathbf{F}}_i| \leq t_i \;\forall i \in \widehat{\mathcal{C}}_{\text{test}}\right\} \tag{4.44}$$

Let $\Gamma_i^{(AB)}$ be the POVM element corresponding to $i \in \widehat{\mathcal{C}}$. Then, consider the feasible set $\mathcal{S}_{\text{feas}}$ defined as

$$\mathcal{S}_{\text{feas}} \coloneqq \left\{\rho \in \text{S}_{=}(AB) \mid \bar{\mathbf{F}}_i - t_i - \kappa_i^{\text{fixed,L}} \leq \text{Tr}\left[\Gamma_i^{(AB)}\rho\right] \leq \bar{\mathbf{F}}_i + t_i + \kappa_i^{\text{fixed,U}},\;\; \forall i \in \widehat{\mathcal{C}}_{\text{test}}\right\}, \tag{4.45}$$

[11] Note that the exact form of the beta distribution is unimportant: there exist standard libraries in standard numerical packages that can evaluate these expressions.

[12] One could also have $i \in \widehat{\mathcal{C}}$ in the set, instead of $i \in \widehat{\mathcal{C}}_{\text{test}}$ if one so desired.

where $\kappa_i^{\text{fixed,L}}$ *and* $\kappa_i^{\text{fixed,U}}$ *are given by*[13]

$$\begin{aligned}\kappa_i^{\text{fixed,L}} &= \bar{\mathbf{F}}_i - t_i - \mathcal{B}_{\text{beta}}\left(\varepsilon_{\text{AT}};\ n(\bar{\mathbf{F}}_i - t_i),\ n - n(\bar{\mathbf{F}}_i - t_i) + 1\right) \\ \kappa_i^{\text{fixed,U}} &= \mathcal{B}_{\text{beta}}\left(1 - \varepsilon_{\text{AT}};\ n(\bar{\mathbf{F}}_i + t_i) + 1, n - n(\bar{\mathbf{F}}_i - t_i)\right) - \bar{\mathbf{F}}_i - t_i.\end{aligned} \tag{4.46}$$

This feasible set satisfies the required property from Section 4.1, that is:

$$\rho_{AB} \notin \mathcal{S}_{\text{feas}} \implies \Pr(\Omega_{\text{AT}})_\rho \leq \varepsilon_{\text{AT}} \tag{4.47}$$

Note that in the lemma above, we make a specific choice of the acceptance set. In general, other choices are possible. For instance, see Refs. [93, 95], where the authors use the ℓ_1-norm between $\mathbf{F}^{\text{obs}}$ and $\bar{\mathbf{F}}$ to define the acceptance criterion.

Proof. The proof follows from a straightforward application of the bounds on the cumulative binomial distribution from Eq. (4.43). If $\rho \notin \mathcal{S}_{\text{feas}}$, there exists at least one i such that either

$$\begin{aligned}\text{Tr}\left[\Gamma_i^{(AB)}\rho\right] &\leq \bar{\mathbf{F}}_i - t_i - \kappa_i^{\text{fixed,L}} \\ &= \mathcal{B}_{\text{beta}}\left(\varepsilon_{\text{AT}};\ n(\bar{\mathbf{F}}_i - t_i),\ n - n(\bar{\mathbf{F}}_i - t_i) + 1\right)\end{aligned} \tag{4.48}$$

or

$$\begin{aligned}\text{Tr}\left[\Gamma_i^{(AB)}\rho\right] &\geq \bar{\mathbf{F}}_i + t_i + \kappa_i^{\text{fixed,U}} \\ &= \mathcal{B}_{\text{beta}}\left(1 - \varepsilon_{\text{AT}};\ n(\bar{\mathbf{F}}_i + t_i) + 1, n - n(\bar{\mathbf{F}}_i - t_i)\right)\end{aligned} \tag{4.49}$$

is satisfied.

Suppose it is the former. In that case, since $\Omega_{\text{AT}} \implies \mathbf{F}_i^{\text{obs}} \geq \bar{\mathbf{F}}_i - t_i$, we obtain

$$\Pr(\Omega_{\text{AT}}) \leq \Pr\left(\mathbf{F}_i^{\text{obs}} \geq \bar{\mathbf{F}}_i - t_i\right) \leq \varepsilon_{\text{AT}}, \tag{4.50}$$

where the final inequality follows from Eq. (4.43).

[13] Note that, strictly speaking, in Eq. (4.46) (which we obtain using the cumulative binomial distribution in Eq. (4.43)) the second and third arguments are required to be natural numbers. This issue can be easily addressed either by introducing appropriate floor and ceiling functions, or by choosing $\bar{\mathbf{F}}_i$ and t_i such that $n\bar{\mathbf{F}}_i$ and nt_i are natural numbers. In this thesis we take the latter approach for simplicity in our expressions.

Moreover, the second and third arguments also need to satisfy obvious bounds, such as positivity and being less than n. These constraints can likewise be enforced either via suitable use of minimum and maximum functions, or via suitable choice of $\bar{\mathbf{F}}_i$ and t_i. Again, we we take the latter approach for simplicity in our expressions.

Similarly, for the latter case, we have $\Omega_{\mathrm{AT}} \implies \mathbf{F}_i^{\mathrm{obs}} \leq \bar{\mathbf{F}}_i + t_i$, and hence

$$\Pr(\Omega_{\mathrm{AT}}) \leq \Pr\left(\mathbf{F}_i^{\mathrm{obs}} \leq \bar{\mathbf{F}}_i + t_i\right) \leq \varepsilon_{\mathrm{AT}}, \tag{4.51}$$

again by Eq. (4.43). This concludes the proof. □

Using the same approach, we have the following lemma that constructs the confidence set $\mathcal{V}(\mathbf{F}^{\mathrm{obs}})$ satisfying the requirements of Section 4.2.

Lemma 4.3.2 (Constructing the confidence set from Section 4.2)**.** *Let $\mathbf{F}^{\mathrm{obs}} \in \mathbb{P}(\widehat{\mathcal{C}})$ be a observed frequency distribution in the public announcement registers $\widehat{C}_1^n$. Let $\Gamma_i^{(AB)}$ be the POVM element corresponding to $i \in \widehat{\mathcal{C}}$. Then, consider the $\mathcal{V}(\mathbf{F}^{\mathrm{obs}})$ defined as*[14]

$$\mathcal{V}(\mathbf{F}^{\mathrm{obs}}) \coloneqq \left\{\rho \in \mathrm{S}_{=}(AB) \mid \mathbf{F}_i^{\mathrm{obs}} - \kappa_i^{\mathrm{var,L}} \leq \mathrm{Tr}\left[\Gamma_i^{(AB)}\rho\right] \leq \mathbf{F}_i^{\mathrm{obs}} + \kappa_i^{\mathrm{var,U}} \ \forall i \in \widehat{\mathcal{C}}_{\mathrm{test}}\right\}, \tag{4.52}$$

where $\kappa_i^{\mathrm{var,L}}$ and $\kappa_i^{\mathrm{fixed,U}}$ are given by

$$\begin{aligned}
\kappa_i^{\mathrm{var,L}} &= \mathbf{F}_i^{\mathrm{obs}} - \mathcal{B}_{\mathrm{beta}}\left(\frac{\varepsilon_{\mathrm{AT}}}{2\left|\widehat{\mathcal{C}}_{\mathrm{test}}\right|};\ n(\bar{\mathbf{F}}_i - t_i),\ n - n(\bar{\mathbf{F}}_i - t_i) + 1\right) \\
\kappa_i^{\mathrm{var,U}} &= \mathcal{B}_{\mathrm{beta}}\left(1 - \frac{\varepsilon_{\mathrm{AT}}}{2\left|\widehat{\mathcal{C}}_{\mathrm{test}}\right|};\ n(\bar{\mathbf{F}}_i + t_i) + 1, n - n(\bar{\mathbf{F}}_i - t_i)\right) - \bar{\mathbf{F}}_i - t_i.
\end{aligned} \tag{4.53}$$

This confidence set satisfies the required property from Section 4.2, that is, for all possible ρ_{AB}, we have:

$$\Pr_{\mathbf{F}^{\mathrm{obs}}}\left(\rho_{AB} \in \mathcal{V}(\mathbf{F}^{\mathrm{obs}})\right) > 1 - \varepsilon_{\mathrm{AT}} \tag{4.54}$$

Proof. Consider any $i \in \widehat{\mathcal{C}}_{\mathrm{test}}$, and recall that $n\mathbf{F}_i^{\mathrm{obs}}$ is a binomial random variable with probability of success given by $\mathrm{Tr}\left[\Gamma_i^{(AB)}\rho\right]$. Thus, using Eq. (4.43), we obtain the following Clopper-Pearson confidence [111] interval for binomial random variables, and obtain

$$\Pr_{\mathbf{F}^{\mathrm{obs}}}\left(\mathbf{F}_i^{\mathrm{obs}} - \kappa_i^{\mathrm{var,L}} \leq \mathrm{Tr}\left[\Gamma_i^{(AB)}\rho\right] \leq \mathbf{F}_i^{\mathrm{obs}} + \kappa_i^{\mathrm{var,U}}\right) \geq 1 - \frac{\varepsilon_{\mathrm{AT}}}{\left|\widehat{\mathcal{C}}_{\mathrm{test}}\right|} \tag{4.55}$$

[14] The range of probabilities in the expression below is simply the Clopper-Pearson confidence interval for binomial random variables [111].

where $\kappa_i^{\mathrm{var,U}}, \kappa_i^{\mathrm{var,L}}$ are defined in Eq. (4.53). Taking the negation of this event, and taking the union bound, we obtain

$$\begin{aligned}
&\Pr_{\mathbf{F}^{\mathrm{obs}}}\left(\mathrm{Tr}\left[\Gamma_i^{(AB)}\rho\right] \notin \left[\mathbf{F}_i^{\mathrm{obs}} + \kappa_i^{\mathrm{var,U}}, \mathbf{F}_i^{\mathrm{obs}} + \kappa_i^{\mathrm{var,U}}\right]\right) \leq \frac{\varepsilon_{\mathrm{AT}}}{\left|\widehat{\mathcal{C}}_{\mathrm{test}}\right|} \\
&\Pr_{\mathbf{F}^{\mathrm{obs}}}\left(\bigcup_{i\in\widehat{\mathcal{C}}_{\mathrm{test}}} \mathrm{Tr}\left[\Gamma_i^{(AB)}\rho\right] \notin \left[\mathbf{F}_i^{\mathrm{obs}} + \kappa_i^{\mathrm{var,U}}, \mathbf{F}_i^{\mathrm{obs}} + \kappa_i^{\mathrm{var,U}}\right]\right) \leq \varepsilon_{\mathrm{AT}} \\
&Pr_{\mathbf{F}^{\mathrm{obs}}}\left(\rho \in \mathcal{V}\mathbf{F}^{\mathrm{obs}}\right) \geq 1 - \varepsilon_{\mathrm{AT}}.
\end{aligned} \tag{4.56}$$

This concludes the proof.

□

Remark 4.3.1. *It is instructive to compare the sets $\mathcal{S}_{\mathrm{feas}}$ and $\mathcal{V}(\mathbf{F}^{\mathrm{obs}})$, since they appear in the key rate formulas as the domains of optimization of the same objective function. The first notable difference is that the feasible set $\mathcal{S}_{\mathrm{feas}}$ does not depend on the observed frequency vector $\mathbf{F}^{\mathrm{obs}}$: in a fixed-length protocol, a predetermined key length is produced whenever $\mathbf{F}^{\mathrm{obs}} \in \mathcal{S}_{\mathrm{acc}}$, and the protocol aborts otherwise.*

Consider now a situation in which honest behavior is realized, so that $\mathbf{F}^{\mathrm{obs}} \approx \bar{\mathbf{F}}$. In this case, there are two further notable differences. First, the set $\mathcal{S}_{\mathrm{feas}}$ is larger due to the parameters t_i. This reflects the fact that any realistic protocol must choose the acceptance set to have a large enough size in order to avoid aborting with overwhelming probability. We investigate this effect further when computing expected key rates in the next section.

Second, the parameters $\kappa_i^{\mathrm{var,L}}$ and $\kappa_i^{\mathrm{var,U}}$ are generally larger than their fixed-length counterparts $\kappa_i^{\mathrm{fixed,L}}$ and $\kappa_i^{\mathrm{fixed,U}}$. This difference arises because the variable-length analysis places a stronger requirement on the sampling estimates: we must ensure that all *true probabilities lie within their respective confidence intervals simultaneously. Achieving this requires the use of a union bound in the proof. In contrast, in the construction of the feasible set, it suffices that at least one value falls outside the relevant range, and no union bound is utilized.*

4.4 Application to Qubit BB84

We will now apply our results to Qubit BB84 protocol, specified in Section 3.2.1. At this stage, it may be useful to refer back to Section 3.3 to recall details about the states

sent, measurements performed, announcements undertaken and sifting procedure for the protocol. We first state the following corollaries concerning the security of fixed-length and variable-length Qubit BB84 protocols.

Corollary 4.4.1. *(Fixed-length Qubit BB84) Consider the fixed-length qubit BB84 variant of the QKD Protocol as specified in Section 3.3, with the acceptance set and feasible set $\mathcal{S}_{\text{feas}}$ (which depends on ε_{AT}) as constructed in Lemma 4.3.1. Then this fixed-length Qubit BB84 protocol is $(\max(\varepsilon_{\text{AT}}, \varepsilon_{\text{PA}}) + \varepsilon_{\text{EV}})$-secure against IID collective attacks, as long as the ℓ_{fixed} satisfies*

$$\begin{aligned}\ell_{\text{fixed}} \leq \max\Bigg\{\Bigg\lfloor & n \inf_{\nu \in \Sigma(\mathcal{S}_{\text{feas}})} H(S|\widehat{C}E)_\nu - n(\alpha-1)\log^2(1+2\dim(S)) - \lambda_{\text{EC}}^{\text{fixed}} \\ & - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}}\right)\right\rceil - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\text{PA}}}\right) + 2\Bigg\rfloor, 0\Bigg\} \\ \Sigma(\mathcal{S}_{\text{feas}}) \coloneqq \{\, & \mathcal{G}[\omega_{ABE}] \;\mid \omega_A = \sigma_A, \omega_{AB} \in \mathcal{S}_{\text{feas}}\}\,,\end{aligned} \tag{4.57}$$

where $\alpha \in (1, 1 + 1/\log(1+2\dim(S)))$, and E is a purifying register.

Proof. The result follows directly from the fixed-length IID security statement in Theorem 4.1.1, together with the specification of the feasible set given in Lemma 4.3.1. In addition, we use Lemma 2.2.6, which states that

$$\widetilde{H}_\alpha^\uparrow(S|\widehat{C}E) \geq H(S|\widehat{C}E) - (\alpha-1)\log^2\big(1+2\dim(S)\big).$$

□

Some comments are in order. Note that we replace the Rényi entropy $\widetilde{H}_\alpha^\uparrow(S|\widehat{C}E)$ with the von Neumann entropy $H(S|\widehat{C}E)$, since this substitution allows us to use established methods for the reliable numerical evaluation of the resulting optimization problem [47, 8] (which is convex in ω_{AB}). Directly evaluating the Rényi entropy would lead to larger key lengths, see Ref. [52] for methods to do so. The range of Rényi parameter $\alpha \in \big(1,\, 1 + 1/\log(1+2\dim(S))\big)$ is to ensure the validity of all intermediate statements used in the proof. The key rate can be optimized over the choice of alpha α, and it is straightforward to verify (by differentiating the key length expression with respect to α) that the choice

$$\alpha = 1 + \frac{\log(1/\varepsilon_{\text{PA}})}{\sqrt{n}\,\log(2\dim(S)+1)}$$

is optimal. This is the choice taken in the entirety of this chapter.

We now state the corresponding statement for variable-length Qubit BB84 protocols.

Corollary 4.4.2. *(Variable-length Qubit BB84) Consider the variable-length Qubit BB84 variant of the QKD Protocol as specified in Section 3.3, with the confidence set $\mathcal{V}(\mathbf{F}^{\text{obs}})$ (which depends on ε_{AT}) as constructed in Lemma 4.3.2. Then this variable-length Qubit BB84 protocol is $(\varepsilon_{\text{AT}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure against IID collective attacks, as long as the $\ell(\mathbf{F}^{\text{obs}})$ satisfies*

$$\begin{aligned} \ell(\mathbf{F}^{\text{obs}}) \leq \Bigg\lfloor & n \inf_{\nu \in \Sigma(\mathbf{F}^{\text{obs}})} H(S|\widehat{C}E)_\nu - n(\alpha-1)\log^2(1+2\dim(S)) - \lambda_{\text{EC}}^{\text{fixed}} \\ & - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}}\right) \right\rceil - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\text{PA}}}\right) + 2 \Bigg\rfloor, \\ \Sigma(\mathbf{F}^{\text{obs}}) \coloneqq & \left\{ \mathcal{G}[\omega_{ABE}] \;\middle|\; \omega_A = \sigma_A, \omega_{AB} \in \mathcal{V}(\mathbf{F}^{\text{obs}}) \right\}, \end{aligned} \tag{4.58}$$

where $\alpha \in (1, 1 + 1/\log(1+2\dim(S)))$

Proof. The proof follows from Theorem 4.2.1 and Lemmas 2.2.6 and 4.3.2, analogous to the proof of Corollary 4.4.1. □

4.4.1 Key Rate Plots

We will now apply Corollaries 4.4.1 and 4.4.2 to compute key rates for fixed-length and variable-length qubit BB84 protocols, and to compare their performance. In addition to the usual key rates, we also compute *expected key rates*. To motivate this notion, recall that a security proof specifies which key length the protocol produces *if* certain events occur. By itself, this does not quantify how much key is produced *on average* when the protocol is executed in practice.[15]

To define the expected key rate, we first specify an *honest behavior* of the channel, and hence of the protocol. That is, we assume that in the absence of an adversary the channel behaves according to a fixed model. This assumption induces an IID state $\rho_{\text{honest}}^{\otimes n}$ shared between Alice and Bob.

[15] In fact, a protocol that always produces a key of zero length is perfectly secure.

We then define

$$\begin{aligned}
R_{\text{fixed}} &:= \frac{\ell_{\text{fixed}}}{n} \qquad \text{(fixed-length key rate } \textit{if} \text{ the protocol accepts)},\\
R_{\text{variable}}(\mathbf{F}^{\text{obs}}) &:= \frac{\ell(\mathbf{F}^{\text{obs}})}{n} \qquad \text{(variable-length key rate } \textit{if}\ \mathbf{F}^{\text{obs}} \text{ is observed)},\\
\widetilde{R}_{\text{fixed}} &:= \Pr(\Omega_{\text{AT}} \wedge \Omega_{\text{EV}})_{\rho_{\text{honest}}^{\otimes n}} \cdot \frac{\ell_{\text{fixed}}}{n} \qquad \text{(expected fixed-length key rate)},\\
\widetilde{R}_{\text{variable}} &:= \sum_{\mathbf{F}^{\text{obs}}} \Pr\big(\Omega(\mathbf{F}^{\text{obs}}) \wedge \Omega_{\text{EV}}\big)_{\rho_{\text{honest}}^{\otimes n}} \cdot \frac{\ell(\mathbf{F}^{\text{obs}})}{n} \qquad \text{(expected variable-length key rate)}.
\end{aligned} \tag{4.59}$$

We will compute these quantities for two different scenarios of honest behavior. Note that in our numerical evaluations, we assume that the event Ω_{EV} occurs with probability close to one and focus instead on the impact of variations in the observed statistics.[16] For the qubit BB84 plots, we set $n = 10^8$, and the probability of testing to $\gamma = 0.1$. In both test and key generation rounds, each basis is chosen with probability 0.5, and therefore each state is sent with probability 0.25.

For fixed-length protocols, we set $\varepsilon^{\text{secret}} = \varepsilon_{\text{EV}} = \varepsilon_{\text{AT}} = \varepsilon_{\text{PA}} = 10^{-10}$, resulting in an overall security parameter of $\varepsilon^{\text{secure}} = 2 \times 10^{-10}$. We set $\lambda_{\text{EC}}^{\text{fixed}} = f_{\text{EC}} n H(S|Y\widehat{C})_{\rho_{\text{honest}}}$, where $f_{\text{EC}} = 1.16$ denotes the efficiency of the error-correction protocol. For variable-length protocols, we set $\varepsilon^{\text{secret}} = \varepsilon_{\text{EV}} = 10^{-10}$, $\varepsilon_{\text{AT}} = \varepsilon_{\text{PA}} = 10^{-10}/2$, again obtaining an overall security parameter of $\varepsilon^{\text{secure}} = 2 \times 10^{-10}$. We set $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) = f_{\text{EC}} n H(S|Y\widehat{C})_{\mathbf{F}^{\text{obs}}}$.[17] Note that many of these parameters should, in principle, be optimized to obtain the best possible key rates. However, we do not perform this optimization here, as our goal is simply to compare fixed-length and variable-length protocols.

Fixed honest behaviour

We first fix the honest behaviour of the channel to have 0dB loss, no depolarization, and no misalignment. This determines $\bar{\mathbf{F}}$ from the honest behaviour. We then vary the size of the acceptance test, which we constructed in Lemma 4.3.1. To do so, we define a single parameter t, and set $t_i = t$ for all i (recall that t_i controlled the size of deviation from $\bar{\mathbf{F}}_i$ that is allowed for the protocol to accept). As stated earlier, one may choose other

[16] This assumption can be justified, for example, by using sufficiently strong error correction.

[17] By this, we mean that $\mathbf{F}^{\text{obs}}$ induces a corresponding distribution on key generation rounds with respect to which the entropy is evaluated.

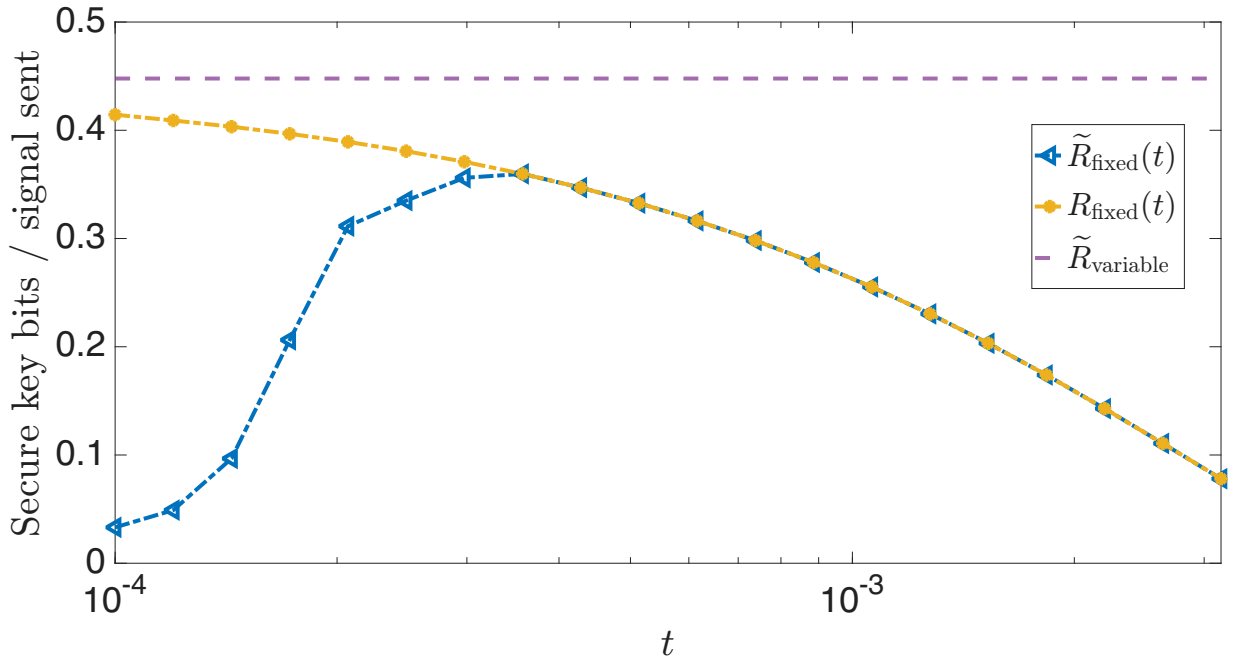


Figure 4.1: Expected key rate for fixed-length protocols $\widetilde{R}_{\text{fixed}}(t)$ for various values of t, key rate upon acceptance for fixed-length protocols $R_{\text{fixed}}(t)$ plotted for various values of t, and the expected key rate for variable-length protocol plotted $\widetilde{R}_{\text{variable}}$, plotted for a fixed honest behaviour of the channel.

acceptance criterion. The resulting key rates are plotted in Fig. 4.1 and discussed below. Note that that since the expected key rates include the probability over various observations, the value of t (which controls the size of the acceptance set) is not important.

1. The fixed-length key rate conditioned on acceptance is given by R_{fixed} and is a monotonically decreasing function of t. (As the size of the acceptance set increases, the worst-case observation within the acceptance set becomes more pessimistic, leading to a smaller key rate upon acceptance.)

2. The expected fixed-length key rate is given by $\widetilde{R}_{\text{fixed}}$. (This quantity is computed as follows.)

   (a) We first compute the expected honest behaviour of the channel, namely $\bar{\mathbf{F}}$, where

$$\bar{\mathbf{F}}_i = \text{Tr}\left[\Gamma_i^{(AB)} \rho_{\text{honest}}\right].$$

(b) We then sample n times from $\bar{\mathbf{F}}$, to obtain the observed frequency vector $\mathbf{F}^{\text{obs}}$, and check whether $\mathbf{F}^{\text{obs}} \in \mathcal{S}_{\text{acc}}$.

(c) This procedure is repeated 25 times, and $\Pr(\Omega_{\text{AT}})_{\rho_{\text{honest}}}$ is estimated by the empirical fraction of samples for which $\mathbf{F}^{\text{obs}} \in \mathcal{S}_{\text{acc}}$.

We observe that this expected key rate is small for very small values of t, since the protocol almost never accepts. It is also small for very large values of t, reflecting the fact that the key rate upon acceptance becomes small. The expected key rate therefore captures the trade-off between accepting with high probability and producing a large key upon acceptance.

3. We also plot the expected variable-length key rate $\widetilde{R}_{\text{variable}}$, which is computed analogously to item (2) by sampling n times from $\bar{\mathbf{F}}$ to obtain $\mathbf{F}^{\text{obs}}$, computing $\ell(\mathbf{F}^{\text{obs}})$, repeating this procedure 25 times, and averaging the resulting key rate.

Crucially, we find that the variable-length protocol achieves a higher expected key rate than the best fixed-length protocol. Since the variable-length protocol consists of exactly the same steps as the fixed-length protocol, and differs only in the parameters of the classical post-processing, its implementation does not impose any additional experimental or operational difficulties. This improvement therefore comes at no additional cost, while yielding a strictly higher expected key rate.

Unpredictable Honest Behaviour

In this section, we compute key rates for a scenario in which the honest behaviour of the channel is unpredictable. For simplicity, we consider a channel model that takes values from a discrete set of depolarization probabilities and misalignment angles. For a given run, the depolarization probability is chosen from the set $\{0, 0.02, 0.04\}$, and the misalignment angle is chosen uniformly from the set $\{0°, 4°, 8°\}$, with the loss fixed to 0dB. The channel therefore has $n_{\text{channel}} = 9$ possible realizations, each occurring with equal probability. We denote by $\rho^{(j)}_{\text{honest}}$ the state corresponding to the jth honest channel behaviour. The resulting key rates are plotted in Fig. 4.2.

1. The fixed-length key rate conditioned on acceptance is given by R_{fixed} and is a monotonically decreasing function of t, with $\bar{\mathbf{F}}$ determined by zero misalignment and no depolarization. This is exactly the same as the key rate plotted in Fig. 4.1.

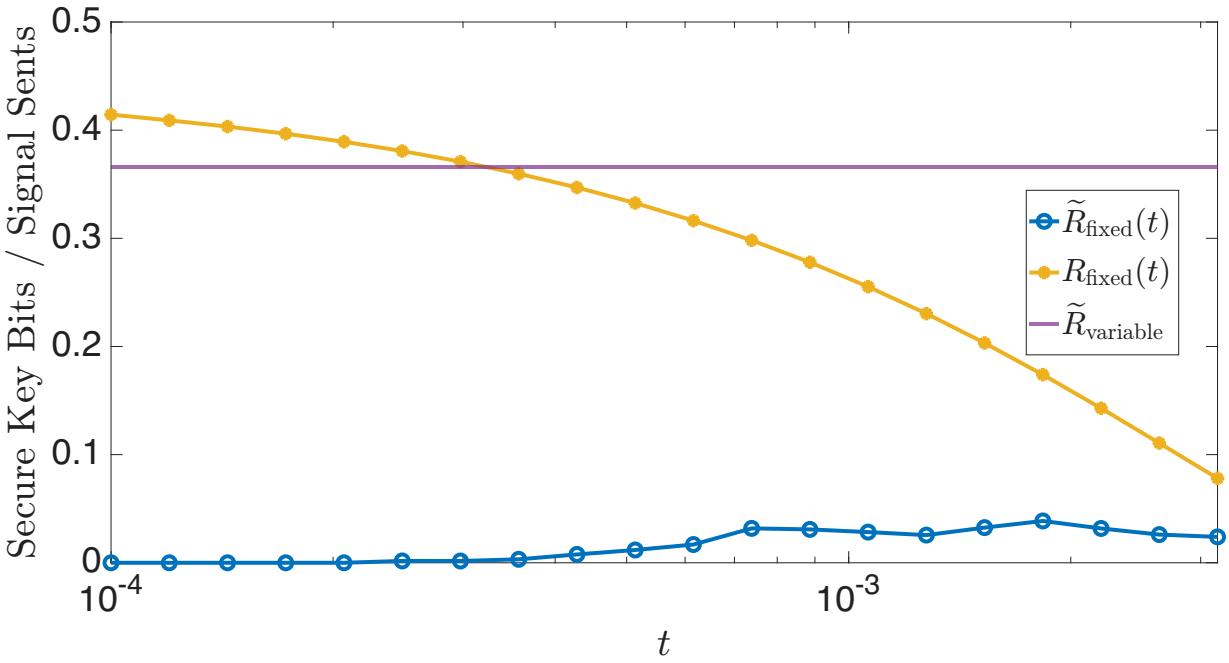


Figure 4.2: Expected key rate for fixed-length protocols $\widetilde{R}_{\text{fixed}}(t)$ for various values of t, key rate upon acceptance for fixed-length protocols $R_{\text{fixed}}(t)$ plotted for various values of t, and the expected key rate for variable-length protocol plotted $\widetilde{R}_{\text{variable}}$, for an unpredictable honest behaviour.

2. The expected fixed-length key rate is given by $\widetilde{R}_{\text{fixed}}$. Since there are different realizations of the channel, we first fix the channel realization to be one out of the n_{channel} values, and compute the expected key rate for that realization by following the procedure from earlier section, repeating the sampling 25 times. Since each channel is equally likely, we simply take the average of these computed key rates as the expected key rates.

   Here, the expected key rate is much smaller than the key rate upon acceptance, since the protocol accepts only on a small number of channel behaviours. As t grows larger, the size of the acceptance test increases, and the protocol starts acccepting on multiple possible channel realizations. However, the size of the acceptance test is already large, and key rate upon acceptance rapidly goes to zero, causing the expected key rate to also go to zero.

3. We also plot the expected variable-length key rate $\widetilde{R}_{\text{variable}}$, which is computed

analogously to item (2) by averaging the resulting key rate over the 9 possible channel realizations. Crucially, we find the expected key rate for variable-length protocols is much higher than the expected key rate for the fixed-length protocols.

Note that the degree of improvement shown by the variable-length protocol in Fig. 4.2 depends the variability in the honest behaviour. Larger variation in the honest behaviour will lead to a bigger difference in performance between fixed-length and varibale-length protocols.

4.5 Application to Decoy-State BB84

We now apply our variable-length security analysis to decoy-state protocols. We note that the components related to the decoy-state analysis were developed as part of Ref. [6], to which I did not contribute. Accordingly, these aspects are only reviewed briefly in thesis, and we refer the reader to Ref. [6] for further details. As already emphasized in Section 3.3.4, the central task remains unchanged: namely, to bound the relevant entropic quantity by exploiting the richer set of observed statistics available in decoy-state protocols. We give a brief explanation of how to go about performing decoy-state analysis in Appendix E.

We plot key rates for a protocol in which both Alice and Bob choose the Z basis with probability 0.9. The decoy intensities are given by $\mu_1 = 1$, $\mu_2 = 0.01$, and $\mu_3 = 0.001$. Each round is a `test` round with probability 0.1, and the decoy intensities are chosen uniformly at random. In `gen` rounds, only the signal intensity μ_1 is chosen, with probability 1. Double clicks on Bob's side are randomly assigned to single clicks, which allows us to use the qubit squasher (see Section 3.6.3). We plot variable key rates for the honest behaviour of the channel as a function of loss; that is, we assume that the observed frequency vector $\mathbf{F}^{\text{obs}}$ corresponds to the honest behaviour of the channel. we set $\varepsilon^{\text{secret}} = \varepsilon_{\text{EV}} = 10^{-10}$, $\varepsilon_{\text{AT}} = \varepsilon_{\text{PA}} = 10^{-10}/2$, again obtaining an overall security parameter of $\varepsilon^{\text{secure}} = 2 \times 10^{-10}$. We set $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}}) = f_{\text{EC}} n H(S \mid Y\widehat{C})_{\mathbf{F}^{\text{obs}}}$, and $f_{\text{EC}} = 1$. As before, many of these parameters can be optimized over for the best results, which we do not do here.

4.6 Variable-length input to privacy amplification

So far we have studied the variable-length aspects of the *final key* that is generated after privacy amplification in QKD protocols. In this section, we will turn our attention to

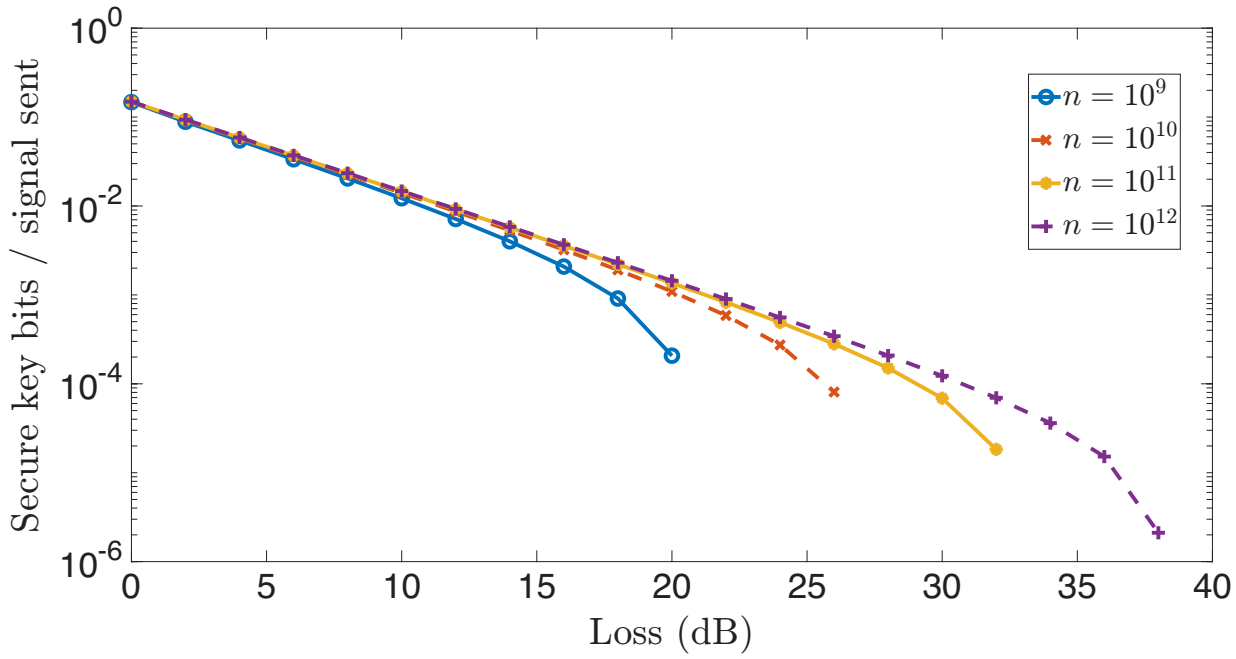


Figure 4.3: Key rate for variable-length decoy-state BB84 protocol plotted against loss, for the typical observations of the protocol, against IID collective attacks.

the variable-length aspect of the *pre-amplification string* in QKD implementations, before privacy amplification. In particular, we will point out and remedy a gap (pointed out briefly in Remark 3.5.2) between the theoretical analysis of privacy amplification and its experimental implementation. For simplicity, we only consider fixed-length QKD protocols. However, our result takes the form of a modified Leftover Hashing Lemma, and can be trivially generalized to variable-length protocols. We also do make any IID attack assumption in this section, and our results hold for arbitrary attacks.

4.6.1 Sifting in QKD

Consider the following three ways of implementing the sifting step in QKD protocols, where Alice and Bob wish to throw away certain rounds based on public announcements. Note that the QKD Protocol implements the procedure from Case 3 below, but the procedure analyzed in this chapter corresponds to Case 1.

1. **Map the discard outcomes to $\perp$, but don't discard them:** In this case, the state prior to privacy amplification is given by $\rho_{S_1^n \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}}$[18], where S is a register that takes values in $\{0, 1, \perp\}$. In this case, we can perform privacy amplification on S_1^n using universal$_2$ hashing from S_1^n to l bits. In particular, binary Toeplitz hashing, a widely used choice, is not possible.

2. **Map the discard outcomes to 0, but don't discard them:** In this case, the state prior to privacy amplification is given by $\rho_{\hat{S}_1^N \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}}$, where $\hat{S}$ is a register that takes values in $\{0, 1\}$. In this case, we can implement privacy amplification using universal$_2$ hashing from n bits to l bits. In particular, binary Toeplitz hashing, a widely used choice, is possible; however, the hash matrices must always be for input strings of a *fixed* length n.

3. **Actually discard the discard outcomes:** In this case, the state prior to privacy amplification is given by $\rho_{\mathbf{S} \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} \hat{\boldsymbol{E}}}$, where $\mathbf{S}$ is a register that takes values in the set of bitstrings of length less than or equal to n, which we shall denote as $\{0, 1\}^{\leq n}$. In this case, one first looks at the number of bits in the register $\mathbf{S}$, denoted by $\mathrm{len}(\mathbf{S})$, and chooses a universal$_2$ hashing procedure from $\mathrm{len}(\mathbf{S})$ bits to ℓ_{fixed}[19] bits. This is what is commonly done in QKD experiments, and is what is specified in QKD Protocol. Practically, one would like to use binary Toeplitz hashing in this procedure. However, we will see below that this is *not a valid universal$_2$ hashing procedure* from $\{0, 1\}^{\leq n}$ to ℓ_{fixed} bits.

The theoretical analysis of Case 1 and Case 2 is straightforward, since they constitute valid universal$_2$ hashing procedures from $\{0, 1, \perp\}^n$ to ℓ_{fixed} bits, and n bits to l bits, respectively. Thus, Leftover Hashing Lemmas can be directly applied. However, Case 3 is *not* necessarily a universal$_2$ hashing procedure from $\{0, 1\}^{\leq n}$ to ℓ_{fixed} bits, as we now explain. Thus we cannot directly apply the Leftover Hashing Lemma[20] in this case.

4.6.2 The problem

For every $l_{\mathrm{input}} \in \mathbb{N}$, let $\mathcal{F}_{\mathrm{hash}}(l_{\mathrm{input}}, \ell_{\mathrm{fixed}})$ denote a universal$_2$ hash family from l_{input} bits to ℓ_{fixed} bits. Then, the procedure described in Case 3 above is equivalent to *first* randomly

[18] Here we ignore Bob's registers, since we are only concerned with secrecy

[19] Here we use $\hat{c}_1^n$ rather than $\mathbf{F}^{\mathrm{obs}}$, since the additional generality comes with no cost. Recall that $\mathbf{F}^{\mathrm{obs}} = \mathrm{freq}(\hat{c}_1^n)$.

[20] Note that we ignore the nuance between ideal universal$_2$ hashing and universal$_2$ hashing (see Remark 3.5.1) in this section, since our analysis can be equally applied to both variants.

sampling $f_l \in \mathcal{F}_{\text{hash}}(l, \ell_{\text{fixed}})$ for every l, followed by computing $f_{\text{len}(\mathbf{S})}(\mathbf{S})$. Note that in this case, only one of the sampled f_ls is ever applied. In order for this procedure to be a valid universal$_2$ hashing procedure from $\{0,1\}^{\leq n}$ to ℓ_{fixed} bits, by definition it must be the case that for any two inputs $\vec{s}_1 \neq \vec{s}_2$, we have

$$\Pr_{f_1, f_2, \ldots, f_n}[f_{\text{len}(\vec{s}_1)}(\vec{s}_1) = f_{\text{len}(\vec{s}_2)}(\vec{s}_2)] \leq \frac{1}{2^{\ell_{\text{fixed}}}}. \tag{4.60}$$

When $\vec{s}_1$ and $\vec{s}_2$ are of the same length, then Eq. (4.60) follows from the universal$_2$ property of $\mathcal{F}_{\text{hash}}(l, \ell_{\text{fixed}})$. When $\vec{s}_1$ and $\vec{s}_2$ are of different length, an explicit counter example can be obtained by considering $\vec{s}_1$ and $\vec{s}_2$ to be all-zero strings of different lengths. In this case, if $\mathcal{F}_{\text{hash}}(l, \ell_{\text{fixed}})$ is a universal$_2$ *linear* hash family, then $f_{\text{len}(\vec{s}_1)}(\vec{s}_1) = f_{\text{len}(\vec{s}_2)}(\vec{s}_2) = \mathbf{0}$ with probability 1. This contradicts the required Eq. (4.60). Thus for binary Toeplitz hashing, Case 3 is *not* a valid universal$_2$ hashing procedure. Thus we cannot directly apply the leftover hashing lemma.

Remark 4.6.1. *We note that if every $\mathcal{F}_{\text{hash}}(l, \ell_{\text{fixed}})$ is chosen such that it is universal$_2$ and has the following "uniform output" property:*

$$\Pr_{f_l \in \mathcal{F}_{\text{hash}}(l, \ell_{\text{fixed}})}[f_l(\mathbf{z}) = k] \leq 1/2^l \quad \forall \quad \mathbf{z} \in \{0,1\}^i, k \in \{0,1\}^{\ell_{\text{fixed}}}, \tag{4.61}$$

then it is straightforward to prove that Eq. (4.60) holds and hence the described procedure is a valid universal$_2$ hashing. Furthermore, in principle any universal$_2$ hashing procedure can be modified into one that satisfies Eq. (4.61) by increasing the amount of random seed bits required and XORing the output of the hash function with this seed. This construction is utilized in the proof of the Lemma 4.6.1. However, physically implementing this conversion in an actual QKD protocol would be an undesirable additional cost, hence we instead provide a proof that shows that this is not necessary.

4.6.3 The solution

We address this issue with Lemmas 4.6.1 and 4.6.2 below. We start by proving the following modified Leftover Hashing Lemma that is applicable to Case 3, as long as the protocol satisfies the property that the positions and values of the discarded outcomes can be determined from the public announcements $\widehat{C}_1^n$ (we return to this point after presenting the lemmas and their proofs). Our approach is to first use Remark 4.6.1 to construct a virtual hashing procedure that is a valid universal$_2$ hashing procedure from $\{0,1\}^{\leq n}$ to ℓ_{fixed} bits. We will then show that the actual output states can be obtained by performing a CPTP map on the virtual output states. The required result then follows from data-processing inequalities.

Lemma 4.6.1. *Let $\rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}$ be a state classical in $\mathbf{SC}$ (where the $\mathbf{S}$ register takes values in $\{0,1\}^{\leq n}$), with the property that conditioned on each possible value $\bar{c}$ on the $\mathbf{C}$ register, the resulting distribution on $\mathbf{S}$ is only supported on values in $\{0,1\}^{k_{\bar{c}}}$ for some constant $k_{\bar{c}} \in \mathbb{N}$. Note that $\mathbf{C}$ is a classical register which can be store arbitrary values for the purposes of this lemma. Let $\rho_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}}$ be the state obtained from $\rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}$ by first computing the number of bits $\mathrm{len}(\mathbf{S})$ in the $\mathbf{S}$ register, then implementing a universal$_2$ hashing procedure from $\mathrm{len}(\mathbf{S})$ bits to ℓ_{fixed} bits (in other words, the procedure described in Case 3 of Section 4.6.1). Then for any event Ω on the classical register $\mathbf{C}$, we have (for $\rho^{(\mathrm{ideal})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}} \coloneqq \frac{\mathbb{I}_{K_A}}{|K_A|} \otimes \rho_{\mathbf{C}\hat{\boldsymbol{E}}}$):*

$$\begin{aligned}
&\Pr(\Omega)\frac{1}{2}\left\|\rho_{K_A\mathbf{C}\hat{\boldsymbol{E}}|\Omega} - \rho^{(\mathrm{ideal})}_{K_A\mathbf{C}\hat{\boldsymbol{E}}|\Omega}\right\|_1 \\
&\leq \Pr(\Omega)2^{-\left(\frac{\alpha-1}{\alpha}\right)\left(\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho|\Omega}-\ell_{\mathrm{fixed}}+2\right)} \\
&\leq 2^{-\left(\frac{\alpha-1}{\alpha}\right)\left(\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}-\ell_{\mathrm{fixed}}+2\right)}
\end{aligned} \tag{4.62}$$

The proof can be found in Appendix A.

While here we have focused on proving an analogue of the Leftover Hashing Lemma for Rényi entropy, a similar result for the smooth min-entropy version can be obtained by exactly the same proof, except that when conditioning on the event Ω, one should use the the subnormalized partial states.

In order to use Lemma 4.6.1, which justifies the use of the LHL, we have to compute bounds on the Rényi entropy $\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}$, which is computed on the state just prior to privacy amplification in Case 3. However, we expect that if the registers that were discarded to produce $\mathbf{S}$ from S_1^n are completely determined by the register $\mathbf{C}$, then this entropy should be the same as the value before the discarding process, since the conditioning register $\mathbf{C}$ could be used to isometrically convert between the values before and after discarding some registers. We formalize this claim in the following Lemma and subsequent discussion.

Lemma 4.6.2. *Suppose $\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}, \rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}$ are states that are classical in $\mathbf{C}$, and related to each other as follows: letting $R_{\bar{c}}$ be a register containing the support of the conditional state $\rho_{R|\mathbf{C}=\bar{c}}$, there exist isometries $V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}}$ such that*[21]

$$\begin{aligned}
&V\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}V^{\dagger} = \rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}, \text{ where} \\
&V \coloneqq \sum_{\bar{c}} V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}} \otimes |\bar{c}\rangle\langle\bar{c}|_{\mathbf{C}}\,.
\end{aligned} \tag{4.63}$$

[21] Eq. (4.63) is a well-defined expression despite the fact that V is not defined on all of $R\mathbf{C}$, because $\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}$ is only supported on the subspace on which V is defined.

Then we have

$$\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho} = \widetilde{H}^{\uparrow}_{\alpha}(R|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}. \tag{4.64}$$

The proof can be found in Chapter A.

To apply Lemma 4.6.2 in comparing Cases 1, 2 and 3 described previously, we can begin by viewing R as being S_1^n in Case 1 or $\hat{S}_1^n$ in Case 2. If the protocol satisfies the condition that the positions and values of discarded outcomes are fixed by the public announcements $\mathbf{C}$, we can define operations $V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}}$ that simply drop the discarded outcomes specified by $\bar{c}$, and it is not difficult to show the state $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$ in Case 3 has the following properties:

1. These $V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}}$ operations are indeed isometries, and $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$ is related to $\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}$ in the sense expressed in Eq. (4.63).
2. $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$ satisfies the conditions of Lemma 4.6.1, and hence Eq. (4.62) is valid.
3. $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$ satisfies the conditions of Lemma 4.6.2, and hence $H_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}$ in Eq. (4.62) can be replaced with $H_{\alpha}(R|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}$.

(Basically, the above statements hold because under that protocol condition, for each value $\bar{c}$, the output length of $V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}}$ is fixed, and all the discarded positions have fixed values so there are no "collisions".)

With this, we see that for Case 3 the bound in Eq. (4.62) holds with $\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}$ replaced by $\widetilde{H}^{\uparrow}_{\alpha}(S_1^n|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}$ from Case 1 or $\widetilde{H}^{\uparrow}_{\alpha}(\hat{S}_1^n|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}$ from Case 2; in particular, for the purposes of this thesis this means the proofs of Theorems 4.1.1 and 4.2.1 are valid[22] even if we apply the procedure in Case 3 rather than Case 2. To qualitatively summarize, under that protocol condition, the bounds obtained on the privacy amplification procedure in QKD are unaffected if the actual protocol implements Case 3 in place of Case 1 or Case 2.

4.7 Summary and Outlook

In this chapter we presented a security proof for variable-length QKD protocols against IID collective attacks. These protocols are highly relevant for implementations since they do not require users to characterize their channel before running the QKD protocol.

[22]Note that when we further simply these expressions to von Neumann entropies using Lemma 2.2.6, then that simplification depends and these the bound on $\widetilde{H}^{\uparrow}_{\alpha}(S_1^n|\mathbf{C}\hat{\boldsymbol{E}})$ on the dimension of S versus $\hat{S}$.

Instead, they include instructions for adjusting the length of the final key, and the amount of error-correction information, for every possible observation during the protocol. The key ingredient in this analysis was the construction of a statistical estimator that lower bounds the relevant entropic quantity, and the use the Rényi entropies in the proof (see Remark 4.2.2). In fact, we will see that the MEAT framework in Chapter 7 also uses similar ideas: however it notably makes do with a *weaker* statistical estimator than the one we demanded in this chapter (see Theorem 7.3.1).

These results eliminate the typical trade-off between probability of the protocol accepting and the output key length it produces when it accepts that is imposed by fixed-length protocols. They also remove the need for explicit channel characterization prior to the QKD protocol run. We exemplified our results by studying the performance of the qubit BB84 protocol implemented in this fashion. We showed that the variable-length implementation leads to a significant improvement in the expected key rate compared to fixed-length implementations, especially for scenarios where the channel is chaotic and unpredictable. We also applied our variable-length framework towards the decoy-state BB84 protocol, using the analysis from Ref. [6].

We highlight that our proof approach relies on a Leftover Hashing Lemma for Rényi entropies that was only recently developed in Ref. [40]. It does not seem entirely straightforward to construct a similar analysis using Leftover Hashing Lemma versions based on smooth min-entropy.

Finally, we identified and addressed a subtle gap in the analysis of sifting and privacy amplification arising from the variable length of the pre-amplification string $\mathbf{S}$. Our fix acts as retroactively, since it does not require any changes to the protocol implementation or the output key lengths.

Our analysis so far has the significant limitation that it applies only to IID collective attacks. This is not a reasonable assumption to make in QKD, since Eve can always implement an attack that violates it (for instance by attacking odd and even round signals differently). We therefore turn to the postselection technique in the next chapter, which allows our security analysis in this chapter to be lifted to hold against coherent attacks.

Chapter 5

Postselection technique lift to coherent attacks

> Where we break free from the shackles of IID collective attacks; where we obtain a reduction to IID collective attacks using permutation symmetries; and where we begin to incessantly count the dimensions of Alice's and Bob's systems (and agonize when they grow).

Proving the security of QKD protocols against coherent attacks is a challenging task, since the security proof must hold for any arbitrary strategy employed by the adversary. This stands in contrast to the IID collective attack setting, where Eve interacts with each round in an identical and independent manner. A powerful approach to bridge these two regimes is the postselection technique [36, 5], which provides conditions under which a security proof against IID collective attacks can be "lifted" to a proof that holds against general coherent attacks. In this chapter, we give a complete and self-contained treatment of the postselection technique as it applies to practical QKD protocols, which is based on Ref. [5]. The technique itself was originally proposed in Ref. [36].

We begin with an overview of the underlying mathematical tools in Section 5.1, focusing on the de Finetti reductions that lie at the heart of this method. We then explain how these reductions are used in QKD security proofs in Section 5.2. In Section 5.3, we investigate how to apply the postselection technique to optical implementations of QKD, which requires additional care due to the infinite-dimensional nature of photonic systems. In Section 5.4, we combine all these ingredients to obtain explicit key rates for the Qubit BB84 and

Decoy-state BB84 protocol against coherent attacks. In Section 5.5 we summarize the results in this chapter.

While the postselection technique is well established in principle, the existing literature did not provide a fully correct and operational proof suitable for realistic prepare-and-measure QKD protocols until Ref. [5], on which this chapter is based. In particular, several obstacles had to be resolved before a complete security proof could be obtained. The main issues addressed in this chapter are:

1. **Infinite-dimensional optical systems:** Bob's detection apparatus is inherently infinite-dimensional, and realistic models of his measurement process must reflect this. Although several tools exist to handle infinite-dimensional detectors [81, 62, 63, 82], many of them are not directly compatible with the postselection technique. We show how, and under what conditions, these tools can be utilized with the postselection technique. Moreover, in decoy-state protocols, Alice's emitted optical states also inhabit an infinite-dimensional Hilbert space. We rigorously apply the source maps [79] to reduce this to the standard finite-dimensional setting of tagged states [58], allowing the postselection technique to be applied without compromising correctness.

2. **A technical flaw in prior formulations of the postselection technique:** The original proof in Ref. [36] contained a step that is not valid as stated [112, Note added after publication]. An attempted correction in [113, Section 3.3.2] also introduced an error. In this chapter, we present the first correct and complete version of this step.

3. **Incorporating the fixed marginal constraint required for prepare-and-measure QKD:** Standard formulations of the postselection technique assume that the marginal on Alice's system is unconstrained. However, in generic prepare-and-measure protocols, Alice's marginal after the source-replacement scheme (see Section 3.6.1) is fixed by design, and the security proof must operate under this constraint. Prior versions of the postselection technique could not accommodate this, and therefore were inapplicable to prepare-and-measure protocols.[1] We extend the framework so that it naturally handles fixed-marginal conditions, thereby enabling its use in realistic QKD analyses.

Beyond establishing the first fully rigorous version of the postselection technique tailored to QKD, we also obtain significant performance improvements, leading to much tighter

[1] More precisely, these methods could still be applied, but would result in a reduction to an IID collective attack analysis that was required to hold for *all* IID states - including those that do not satisfy the required marginal property. This would typically yield zero key rates for generic QKD protocols.

key rates than previously achievable with postselection-based proofs (these results are primarily due to Shlok Nahar). Finally, we show how the entire analysis can be adapted to variable-length protocols from Chapter 4, which is essential for achieving optimal expected key rates in many practical settings.

5.1 De Finetti Reductions

Quantum de Finetti theorems [95, 36, 114, 115] are useful in reducing the analysis of various quantum information processing tasks to the IID case. In this work, we focus on quantum de Finetti reductions of following form used in Refs. [36, 114, 115], where a permutation invariant state $\bar{\rho}_{A_1^n B_1^n}$ (see Definition 5.1.2) satisfies:

$$\bar{\rho}_{A_1^n B_1^n} \leq g_{n,x}\ \tau_{A_1^n B_1^n}, \tag{5.1}$$

where $\tau_{A_1^n B_1^n} = \int \sigma_{AB}^{\otimes n} \mathrm{d}\sigma_{AB}$ is a normalized density matrix, and $g_{n,x} = \dim\left(\mathrm{Sym}^n\left(\mathbb{C}^x\right)\right) = \binom{n+x-1}{n}$ is the dimension of the symmetric subspace $Symx$, which we define in Definition 5.1.1. Although we will not require many detailed properties of this subspace to understand the present chapter, its dimension plays an important role. An easily computable upper bound on the dimension of the symmetric subspace is given in Section 5.4. We refer to a state of the form $\tau_{A_1^n B_1^n} = \int \sigma_{AB}^{\otimes n} \mathrm{d}\sigma_{AB}$ as a "de Finetti state". Typically, in reducing the analysis of quantum information processing tasks to the IID case, the following factors come into play:

1. The value of $g_{n,x}$: This should be as small as possible, as it appears as a penalty in the reduction to IID states.

2. The integral over IID states in $\tau_{A^n B^n}$: This should be such that the integral is only over states for which the task has been "analyzed", in the sense that some security property has been proven for all such IID states.

In this section we will present several improvements to the value of $g_{n,x}$ from Ref. [5]. These improvements are of two types. The first improves the dimensional scaling ($g_{n,x}$) in [115, Lemma 3.1] for generic states. The second improvement shows that the dimensions can be reduced for states that are invariant under certain symmetries, as an extension of Ref. [114] to the quantum case. Proofs of these improved statements are deferred to Ref [5].

5.1.1 A simple de Finetti reduction

We will now prove a simple de Finetti reduction [36], which provides intuition for why statements of this form can be expected to be true. The proof strategy below mirrors that of all the de Finetti reductions considered in this chapter, although later refinements are significantly more technically involved. We begin by defining the symmetric subspace, and a notion of permutation invariance for operators acting on tensor-product spaces. We use S_n^{perm} to denote the set of all possible permutations on n objects.

Definition 5.1.1. (Symmetric subspace [37, Chapter 7]) Let $\mathcal{H}$ be a finite-dimensional Hilbert space with dimension d_H, that is $\mathcal{H} \cong \mathbb{C}^{d_H}$. For each permutation $\pi \in S_n^{\text{perm}}$, let $P_\pi^{d_H,n}$ denote the standard unitary representation of π acting on $\mathcal{H}^{\otimes n}$. The **symmetric subspace** of $\mathcal{H}^{\otimes n}$ is defined as

$$\text{Sym}^n(\mathcal{H}) \coloneqq \left\{ |\psi\rangle \in \mathcal{H}^{\otimes n} : P_\pi^{d_H,n} |\psi\rangle = |\psi\rangle \text{ for all } \pi \in S_n^{\text{perm}} \right\}.$$

The dimension of the n-fold symmetric subspace is given by

$$\dim\left(\text{Sym}^n\left(\mathbb{C}^{d_H}\right)\right) = \binom{n + d_H - 1}{n}.$$

Definition 5.1.2. (Permutation-invariance of matrices [37, Chapter 7]) Given a matrix $\bar{\rho}_{H_1^n} \in \text{L}(H_1^n)$ and a permutation $\pi \in S_n^{\text{perm}}$ of its subsystems, we denote the action of π on $\bar{\rho}_{H_1^n}$ as

$$\bar{\rho}_{H_1^n} \mapsto P_\pi^{d_H,n} \, \bar{\rho}_{H_1^n} \, P_\pi^{d_H,n\dagger},$$

where $\mathcal{H} \cong \mathbb{C}^{d_H}$ and $P_\pi^{d_H,n}$ is the standard unitary representation of π on $\mathcal{H}^{\otimes n}$. We say that $\bar{\rho}_{H_1^n}$ is **permutation invariant** if it is invariant under the action of all permutations $\pi \in S_n^{\text{perm}}$.

Note that permutation invariant states are *not* necessarily supported on the symmetric subspace. For example, the maximally mixed state is permutation invariant but has full support on the entire Hilbert space. Nevertheless, the following result holds.

Lemma 5.1.1 (Permutation-invariant states admit symmetric purifications [95, Lemma 4.2.2])**.** *Let $\bar{\rho}_{H_1^n}$ be a permutation-invariant state*[2] *on $\text{S}_=(H_1^n)$, and let $\mathcal{H}$ be the finite-dimensional Hilbert space associated with H. Then there exists a purification of $\bar{\rho}_{H_1^n}$ supported on the symmetric subspace $\text{Sym}^n(\mathcal{H} \otimes \mathcal{H})$.*

[2]This can be straightforwardly generalized to hold for matrices on $\text{Pos}(H_1^n)$.

Moreover, the the symmetric subspace itself can be characterized using a mixture of IID states using the following lemma.

Lemma 5.1.2 (Symmetric projector as a Haar mixture of IID states)**.** *Let $\mathcal{H} \cong \mathbb{C}^{d_H}$ be a finite-dimensional Hilbert space, and let $\Pi_{\mathrm{Sym}^n(\mathcal{H})}$ denote the projector onto the symmetric subspace $\mathrm{Sym}^n(\mathcal{H}) \subset \mathcal{H}^{\otimes n}$. Then $\Pi_{\mathrm{Sym}^n(\mathcal{H})}$ admits the representation*

$$\Pi_{\mathrm{Sym}^n(\mathcal{H})} = \dim\left(\mathrm{Sym}^n\left(\mathbb{C}^{d_H}\right)\right) \int \sigma_H^{\otimes n} \, \mathrm{d}\sigma_H, \tag{5.2}$$

where the integral is taken over pure states $\sigma_H = |\psi\rangle\langle\psi|$ on $\mathcal{H}$ with respect to the unitarily invariant (Haar) probability measure.

Proof. Define

$$M \coloneqq \int \sigma_H^{\otimes n} \, \mathrm{d}\sigma_H, \tag{5.3}$$

where the integral ranges over pure states $\sigma_H = |\psi\rangle\langle\psi|$ on $\mathcal{H}$ with respect to the unitarily invariant (Haar) probability measure. First, note that for every pure state $|\psi\rangle \in \mathcal{H}$, we have $|\psi\rangle^{\otimes n} \in \mathrm{Sym}^n(\mathcal{H})$. Thus, we have

$$\Pi_{\mathrm{Sym}^n(\mathcal{H})} \, M \, \Pi_{\mathrm{Sym}^n(\mathcal{H})} = M, \tag{5.4}$$

so M has support contained in $\mathrm{Sym}^n(\mathcal{H})$.

Let U be any unitary on $\mathcal{H}$. Using Haar invariance of the measure,

$$U^{\otimes n} M (U^\dagger)^{\otimes n} = \int (U \sigma_H U^\dagger)^{\otimes n} \, \mathrm{d}\sigma_H = \int \sigma_H^{\otimes n} \, \mathrm{d}\sigma_H = M. \tag{5.5}$$

Now, consider the restriction of M to the symmetric subspace. Since M is supported on $\mathrm{Sym}^n(\mathcal{H})$ and commutes with $U^{\otimes n}$ for every unitary U, Schur's lemma [37] implies that M acts as a scalar multiple of the identity on $\mathrm{Sym}^n(\mathcal{H})$. This step relies on the fact that the action of $U^{\otimes n}$ on the symmetric subspace $\mathrm{Sym}^n(\mathcal{H})$ is irreducible, so that any operator supported on $\mathrm{Sym}^n(\mathcal{H})$ and commuting with $U^{\otimes n}$ must be proportional to the identity on $\mathrm{Sym}^n(\mathcal{H})$.

Thus, there exists a constant $c \geq 0$ such that

$$M = c \, \Pi_{\mathrm{Sym}^n(\mathcal{H})}.$$

Taking the trace of both sides,

$$\mathrm{Tr}(M) = \int \mathrm{Tr}\left(\sigma_H^{\otimes n}\right) \mathrm{d}\sigma_H = \int 1 \, \mathrm{d}\sigma_H = 1,$$

since $\sigma_H^{\otimes n}$ is a rank-one density operator and the Haar measure is normalized. Thus, $c = 1/\dim\left(\mathrm{Sym}^n\left(\mathbb{C}^{d_H}\right)\right)$, since $\mathrm{Tr}\left(\Pi_{\mathrm{Sym}^n(\mathcal{H})}\right) = \dim\left(\mathrm{Sym}^n\left(\mathbb{C}^{d_H}\right)\right)$ □

Combining these statements, we obtain the following de Finetti reduction.

Corollary 5.1.1. *(Simple de Finetti reduction without fixed marginal [36, Lemma 2]) Let $\rho_{H_1^n} \in \mathrm{S}_=(H_1^n)$ be a permutation invariant state. Then, there exist a probability measure $\mathrm{d}\sigma_H$ on the set of states $\sigma_H \in \mathrm{S}_=(H)$ on H such that*

$$\rho_{H^n} \;\leq\; g_{n,d_H^2} \int \sigma_H^{\otimes n} \, \mathrm{d}\sigma_H, \tag{5.6}$$

where $g_{n,x} = \dim\left(\mathrm{Sym}^n\left(\mathbb{C}^x\right)\right)$.

Proof. By Lemma 5.1.1, there exists a purification $\rho_{H_1^n K_1^n}$ of $\rho_{H_1^n}$, where $K \cong H$, which is supported on the symmetric subspace $\mathrm{Sym}^n(H \otimes K)$. Using Lemma 5.1.2, we obtain

$$\rho_{H_1^n K_1^n} \leq \Pi_{\mathrm{Sym}^n(H\otimes K)} = \dim\left(\mathrm{Sym}^n\left(\mathbb{C}^{d_H d_K}\right)\right) \int \sigma_{HK}^{\otimes n} d\sigma_{HK} \tag{5.7}$$

where the integral is with respect to the unitarily invariant measure. The required statement then follows from simply taking the partial trace over K_1^n in the above expression. □

Notice that the dimension that shows up in $g_{n,x}$ is d_H^2, which is due to the fact that we consider the symmetric subspace on $H_1^n \otimes K_1^n$, where the purification lives.

5.1.2 Improvements

Notice that Corollary 5.1.1 involves an integral over *all* IID states. In many applications, however, we would like a de Finetti reduction that preserves a fixed marginal on A. A statement of this form, along with a variety of improvements, is obtained below. For the purposes of this thesis, we simply state the improved de Finetti reductions below and apply them in Section 5.4 (since the author was not a primary contributor to those results). We refer the reader to Ref. [5] for a detailed discussion of the proof ideas, relevant techniques, extensions to group symmetries, and related works.

Corollary 5.1.2. *([5, Corollary 1]) Let $\sigma_A \in \mathrm{Pos}(\mathbb{C}^{d_A})$ and $\rho_{A_1^n B_1^n}$ be any permutation-invariant extension of $(\sigma_A)^{\otimes n}$. Then there exists a probability measure $d\sigma_{AB}$ on the set of non-negative extensions σ_{AB} of σ_A, such that*

$$\rho_{A_1^n B_1^n} \leq g_{n,x} \int \sigma_{AB}^{\otimes n} d\sigma_{AB} \tag{5.8}$$

holds for $x = d_A^2 d_B^2$.

Note that there is a dramatic improvement[3] over Corollary 3.2 from Ref. [115], since we go from $x = d_A^2 d_B^4$. Additionally, with this improvement we obtain the earlier de Finetti reduction without a fixed marginal [36, Lemma 2] (see Corollary 5.1.1) by considering A to be a trivial system, thus unifying both results.

A further improvements is available in settings where the underlying state can be assumed to be block diagonal; these are stated below. For pedagogical reasons, when applying de Finetti reductions to QKD in Section 5.2, we present results based on the de Finetti reduction with fixed marginal (Corollary 5.1.2), rather than the strengthened bounds discussed below. Since these improvements can be incorporated in a straightforward manner, the remainder of this section may be skipped without affecting the understanding of the rest of this chapter. Nevertheless, the results presented here are useful for improving finite-size bounds in practical key rate computations. We start with the definition of IID-block-diagonal states.

Definition 5.1.3 (IID-block-diagonal states)**.** Given a matrix $\rho_{A_1^n B_1^n} \in \mathrm{L}((\mathbb{C}^{d_A d_B})^{\otimes n})$, and a set of orthogonal projections $\{\Pi_i\}_{i=1}^k \subset \mathrm{L}(\mathbb{C}^{d_A d_B})$, we say that the matrix is *IID-block-diagonal* if

$$\rho_{A_1^n B_1^n} = \sum_{\vec{j} \in [k]^n} \Pi_{\vec{j}} \rho_{A_1^n B_1^n} \Pi_{\vec{j}}$$

where $\Pi_{\vec{j}} \coloneqq \Pi_{j_1} \otimes \ldots \otimes \Pi_{j_n}$. We denote the rank of projector Π_i as d_i; it corresponds to the dimension of the i^{th} block.

With this definition, we state the Corollary below, which will be the main result we use in later analysis.

[3] For the purposes of QKD key rates, this is indeed dramatic, as we shall soon see in Section 5.4

Corollary 5.1.3. *(de Finetti with IID block-diagonal symmetry and marginal constraint [5, Corollary 2]) Let $\sigma_A \in \mathrm{Pos}(\mathbb{C}^{d_A})$ and $\rho_{A_1^n B_1^n}$ be any permutation-invariant and IID-block-diagonal extension of $(\sigma_A)^{\otimes n}$ with respect to projections $\{\Pi_i^A \otimes \Pi_j^B\}_{i,j=1}^{k_A,k_B}$ of dimension $\{d_i^A d_j^B\}_{i,j=1}^{k_A,k_B}$, where d_i^A and d_j^B are the ranks of $\Pi_i^A \in \mathrm{L}(\mathbb{C}^{d_A})$ and $\Pi_j^B \in \mathrm{L}(\mathbb{C}^{d_B})$ respectively. Then there exists some probability measure $d\sigma_{AB}$ over the set of block-diagonal extensions σ_{AB} of σ_A such that*

$$\rho_{A_1^n B_1^n} \leq g_{n,x} \int \sigma_{AB}^{\otimes n} \, d\sigma_{AB}, \tag{5.9}$$

where $x = \sum_{i,j=1}^{k_A,k_B} {d_i^A}^2 {d_j^B}^2$.

Although the IID-block-diagonal condition might seem restrictive, we show in Section 5.4 that optical implementations often naturally result in such IID-block-diagonal structure. Thus, this would greatly tighten the analysis of optical implementations of quantum information protocols.

5.2 Correct application of De Finetti reductions in QKD

In this section, we fill in a missing gap in Ref. [36], in the reduction of QKD security proofs from arbitrary attacks to IID collective attacks, first noticed in [113]. We also explain how the postselection technique can be applied to prepare-and-measure protocols. The approach from Ref. [36] reduces the security proof of QKD protocols for arbitrary states to that of IID states in two steps. The first step is a reduction from the security of arbitrary states to the security of the state de Finetti state $\tau_{A_1^n B_1^n}$ (with Eve holding a purification). The second is a reduction from the security for $\tau_{A_1^n B_1^n}$ (with Eve holding a purification) to that of IID states. The second step in their analysis is argued intuitively and is not on sound mathematical grounds. Here, we present a rigorous proof of this step. For the sake of completeness, we explain the first step as well.

5.2.1 Using de Finetti reductions for QKD

We first recall some of our notation for QKD protocols. Following Definition 3.6.2, after performing source-replacement, the QKD Protocol can be equivalently identified with

$\{\mathcal{E}^{(\ell)}_{\mathrm{QKD}}, \sigma_A\}$, where $\mathcal{E}^{(\ell)}_{\mathrm{QKD}} \in \mathrm{CPTP}(A_1^n B_1^n, K_A K_B \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ and $\ell(\hat{c}_1^n)$ is the length of the output key the protocol produced, upon observing $\hat{c}_1^n$ in the public announcements registers $\widehat{C}_1^n$, and error-verification passing. Moreover, since $\varepsilon^{\mathrm{correct}}$-correctness is already satisfied, we only need to concern ourselves with the satisfying the secrecy requirements (see Lemma 3.1.1). The ideal QKD protocol $\mathcal{E}^{(\ell),\mathrm{ideal}}_{\mathrm{QKD}} \in \mathrm{CPTP}(A_1^n B_1^n, K_A K_B \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ is one which implements the actual QKD protocol $\mathcal{E}^{(\ell)}_{\mathrm{QKD}}$, and then applies the $\mathcal{R}_{\mathrm{ideal}}$ map (see Section 3.1), which replaces Alice and Bob's key registers with the perfect key of length of appropriate length. The overall secrecy requirement of a QKD protocol can be described in terms of the maps $\mathrm{Tr}_{K_B} \circ \mathcal{E}^{(\ell)}_{\mathrm{QKD}}$ and $\mathrm{Tr}_{K_B} \circ \mathcal{E}^{(\ell)}_{\mathrm{QKD}}$ (see Definition 3.6.2).

We now define what it means for a map to be permutation-invariant. Note that in this definition we also correct a technical error in Ref. [36] regarding the order in which the maps are applied.

Definition 5.2.1 (Permutation-invariance of maps)**.** A linear map $\Delta \in \mathrm{T}(A_1^n, B)$ is **permutation-invariant**, if for every $\pi \in S_n^{\mathrm{perm}}$, there exists a $G_\pi \in \mathrm{CPTP}(B, B)$ such that

$$G_\pi \circ \Delta \circ \mathcal{W}_\pi = \Delta \tag{5.10}$$

where $\mathcal{W}_\pi(\cdot) = P_\pi^{d_A,n} (\cdot) P_\pi^{d_A,n\dagger}$.

Arguably, the above property might be better described as "covariance" rather than "invariance", since for instance it does not require that the map is literally "invariant" in the sense $\Delta \circ \mathcal{W}_\pi = \Delta$. However, for this work we shall follow the existing terminology in the field.

Satisfying permutation invariance

Note that typical QKD protocols are not permutation invariant. Instead, permutation invariance must be enforced explicitly, and requires the optimal random permutation step of QKD Protocol to be implemented. This idea is formalized in Lemma 5.2.1 below and in Ref. [36]. A proof is provided in Appendix. B.

The idea is simple: if a channel $\mathcal{F} \in \mathrm{CPTP}(A^n, B)$ begins by applying a uniformly random permutation to its input registers, followed by operations that do not depend on the chosen permutation, and if the applied permutation is recorded in a classical output register, then $\mathcal{F}$ is permutation invariant in the sense of the above definition (since we can undo the effect of the permutation by modifying the register in which its value is announced). This holds even though $\mathcal{F}$ need not satisfy $\mathcal{F} \circ \mathcal{W}_\pi = \mathcal{F}$. Such a random permutation can

be implemented using approximately $n\log(n)$ uniformly random bits. In the QKD setting, these bits may be generated locally by one party and publicly announced, and therefore do not require any pre-shared secret key [5, Appendix B].

Lemma 5.2.1 (Satisfying permutation invariance)**.** *Consider the QKD protocol* $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \sigma_A\}$ *where* $\mathcal{E}_{\mathrm{QKD}}^{(\ell)} \in \mathrm{CPTP}(A_1^n B_1^n, K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ *is the QKD protocol map describing QKD Protocol. Define a new protocol map* $\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}$ *by first applying a uniformly random permutation to the systems* $A_1^n B_1^n$*, announcing the permutation in a classical register* C_{perm}*, and then applying* $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$*. Explicitly,*

$$\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}(\cdot) = \mathcal{E}_{\mathrm{QKD}}^{(\ell)} \circ \left(\sum_{\pi \in S_n^{\mathrm{perm}}} \frac{1}{n!} P_\pi^{n,d_A d_B}(\cdot) P_\pi^{n,d_A d_B\,\dagger} \otimes |\pi\rangle\langle\pi|_{C_{\mathrm{perm}}} \right). \tag{5.11}$$

Then the following statements hold:

1. *The protocol* $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}, \sigma_A\}$ *describes QKD Protocol with the optional permutation step applied to the* X_1^n, Y_1^n *registers, where the applied permutation is announced in the (additional) register* C_{perm}*, which is made available to Eve.*

2. *The difference between the real and ideal protocols,*

$$\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})} - \mathrm{Tr}_{K_B} \circ \mathcal{R}_{\mathrm{ideal}} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})},$$

   is permutation invariant according to Definition 5.1.2.

The following lemma (see Appendix. B for the proof) formalizes the intuitive statement that, if one is only concerned with proving secrecy against IID collective attacks, then the explicit permutation step does not affect the security analysis. We stress, however, that this permutation step *must still be implemented* in practice in order for the analysis developed in this work to be applicable. Throughout this chapter, we refer to $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ as QKD Protocol without the permutation step, and to $\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}$ as QKD Protocol with the permutation step.

Lemma 5.2.2. *Let* $\{\sigma_A, \mathcal{E}_{\mathrm{QKD}}^{(\ell)}\}$ *be a QKD protocol, and let* $\{\sigma_A, \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}\}$ *be a related QKD protocol in which the maps are related by a random permutation (Eq. (5.11)). Then,*

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm}),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n}\right] \right\|_1 \\ &= \frac{1}{2}\left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell)} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n}\right] \right\|_1. \end{aligned} \tag{5.12}$$

That is, security against IID collective attacks for $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ *implies security against IID collective attacks for* $\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}$*.*

Using the permutation invariance of protocols.

We proceed in a manner similar to Ref. [36], and prove Lemma 5.2.5, which can be used to relate $\varepsilon^{\text{secret}}$-secrecy of arbitrary states to the $\varepsilon^{\text{secret}}$-secrecy of a state that is a purification of a de Finetti state. To do so, we prove Lemmas 5.2.3 and 5.2.4. Note that Lemma 5.2.3 is also proved in the proof of [36, Theorem 2]. All proofs can be found in Appendix. B

Lemma 5.2.3. *Let $\mathcal{F}, \mathcal{F}' \in \mathrm{T}(A_1^n B_1^n, K)$ be linear maps such that $\mathcal{F} - \mathcal{F}'$ is a permutation-invariant linear map. Let $\rho_{A_1^n B_1^n R''} \in \mathrm{Pos}(A^n B^n R'')$ be any extension of $\rho_{A_1^n B_1^n}$. Then the state $\bar{\rho}_{A_1^n B_1^n} = \frac{1}{n!} \sum_{\pi \in S_n^{\text{perm}}} \mathcal{W}_\pi(\rho_{A_1^n B_1^n})$ is permutation-invariant, and for any purification $\bar{\rho}_{A_1^n B_1^n R'}$ of that state, we have*

$$\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R''})\left(\rho_{A_1^n B_1^n R''}\right)\right\|_1 \leq \frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'})\left(\bar{\rho}_{A_1^n B_1^n R'}\right)\right\|_1. \tag{5.13}$$

Lemma 5.2.4. *Let $\rho_{A_1^n B_1^n} \in \mathrm{Pos}(A_1^n B_1^n)$ and $\tau_{A_1^n B_1^n} \in \mathrm{Pos}(A_1^n B_1^n)$ be such that $\rho_{A_1^n B_1^n} \leq g_{n,x} \tau_{A_1^n B_1^n}$ for some $g_{n,x} > 0$. Let $\rho_{A_1^n B_1^n R'}$ be any extension of $\rho_{A_1^n B_1^n}$, and let $\tau_{A_1^n B_1^n R}$ be any purification of $\tau_{A_1^n B_1^n}$. Then for any two maps $\mathcal{F}, \mathcal{F}' \in \mathrm{T}(A_1^n B_1^n, K)$,*

$$\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'})\left(\rho_{A_1^n B_1^n R'}\right)\right\|_1 \leq g_{n,x}\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R})\left(\tau_{A_1^n B_1^n R}\right)\right\|_1 \tag{5.14}$$

Combing these results, we obtain the following lemma which we utilize in the next subsection.

Lemma 5.2.5. *Let $\mathcal{F}, \mathcal{F}' \in \mathrm{T}(A_1^n B_1^n, K)$ be such that $\mathcal{F} - \mathcal{F}'$ is a permutation-invariant map. Let $\rho_{A_1^n B_1^n R''} \in \mathrm{Pos}(A^n B^n R'')$ with $\mathrm{Tr}_{B^n R''}\left(\rho_{A_1^n B_1^n R''}\right) = (\sigma_A)^{\otimes n}$. Then there exists a probability measure $d\sigma_{AB}$ on the set of extensions σ_{AB} of σ_A such that*

$$\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R''})\left(\rho_{A_1^n B_1^n R''}\right)\right\|_1 \leq g_{n,x}\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R})\left(\tau_{A_1^n B_1^n R}\right)\right\|_1, \tag{5.15}$$

where $\tau_{A_1^n B_1^n R}$ is any purification of $\tau_{A_1^n B_1^n} = \int d\sigma_{AB}\ \sigma_{AB}^{\otimes n}$, and $x = d_A^2 d_B^2$.

Proof. Lemma 5.2.3 lets us assume without loss of generality that the input state to a permutation-invariant QKD protocol is permutation-invariant on $A_1^n B_1^n$. Thus, the input states to such protocols satisfy the de Finetti reductions (Corollary 5.1.2) described in Section 5.1. Using Lemma 5.2.4 on this de Finetti reduction allows us to prove the following lemma after combining Lemmas 5.2.3 and 5.2.4 and Corollary 5.1.2. □

5.2.2 Reducing Security of QKD protocols to the IID case

Lemma 5.2.5 allows us to reduce the $\varepsilon^{\text{secret}}$-secrecy with prepare-and-measure QKD protocol for any arbitrary input state (satisfying the fixed marginal property on A), to the $\varepsilon^{\text{secret}}$-secrecy of the protocol when the input state is a purification $\tau_{A^nB^nR}$ of a mixture of IID states $\tau_{A^nB^n}$ with the same fixed marginal on A. In this subsection, we will rigorously reduce the $\varepsilon^{\text{secret}}$-secrecy of a QKD protocol acting on $\tau_{A^nB^nR}$ to that of a QKD protocol against IID collective attacks. Note that Ref. [5] presents two variants of this reduction. One is applicable to both variable-length and fixed-length protocols and is independent of the proof technique used for the IID collective attack security analysis. The other variant is slightly tighter, but applies only to fixed-length protocols and requires the IID collective attack proof to follow a specific structure. In this thesis, we present only the former, as it is the more general of the two.

We first state the following theorem relating security against IID collective attacks to security against the purification $\tau_{A_1^nB_1^nR}$ of a mixture of IID collective attacks. It is this step which was incorrectly argued in Ref. [36].

Theorem 5.2.1 (Postselection Theorem for Variable-length)**.** *Consider the QKD Protocol defined via* $\{\mathcal{E}_{\text{QKD}}^{(\ell)}, \sigma_A\}$ *where* $\mathcal{E}_{\text{QKD}}^{(\ell)} \in \text{CPTP}(A_1^nB_1^n, K_AK_B\widehat{C}_1^nC_{\text{EC}}C_{\text{EV}}H_{\text{PA}}H_{\text{EV}})$ *is such that the* $\varepsilon^{\text{secret}}$*-secrecy condition (Definition 3.6.2) holds for all IID states* $\rho_{A_1^nB_1^nE_1^n} = \sigma_{ABE}^{\otimes n}$ *satisfying* $\text{Tr}_{BE}(\sigma_{ABE}) = \sigma_A$*. Let the state* $\tau_{A_1^nB_1^n}$ *be given by*

$$\tau_{A_1^nB_1^n} = \int \sigma_{AB}^{\otimes n} d\sigma_{AB}, \tag{5.16}$$

where $d\sigma_{AB}$ *is some probability measure on the set of non-negative extensions* σ_{AB} *of* σ_A *and* $\tau_{A_1^nB_1^nR}$ *be a purification of* $\tau_{A_1^nB_1^n}$*. Let* $\mathcal{E}_{\text{QKD}}^{(\ell')}$ *be a variable-length QKD protocol map identical to* $\mathcal{E}_{\text{QKD}}^{(\ell)}$*, except that it hashes to a length*

$$\ell'(\cdot) = \max\left\{\lfloor \ell(\cdot) - 2\log(g_{n,x}) - 2\log(1/2\widetilde{\varepsilon})\rfloor, 0\right\} \tag{5.17}$$

instead of $\ell(\cdot)$*, where* $x = d_A^2d_B^2$*. Then,*

$$\frac{1}{2}\left\|\left(\left(\text{Tr}_{K_B}\circ\mathcal{E}_{\text{QKD}}^{(\ell')} - \text{Tr}_{K_B}\circ\mathcal{E}_{\text{QKD}}^{(\ell'),\text{ideal}}\right)\otimes \text{id}_R\right)(\tau_{A_1^nB_1^nR})\right\|_1 \leq \sqrt{8\varepsilon^{\text{secret}}} + \widetilde{\varepsilon}. \tag{5.18}$$

The same result also holds for the protocols that include the random permutation step on the measurement outcomes, that is, for $\mathcal{E}_{\text{QKD}}^{(\ell,\text{perm})}$*.*

Note that, while the above result is stated in terms of QKD Protocol, it only requires that the final stage is implemented via privacy amplification. The precise details of the earlier steps do not matter (and hence the same proof works both for $\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}$ and $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$. Moreover although all our proofs were stated for prepare-and-measure QKD protocols, they are also applicable to entanglement-based QKD protocols by choosing the fixed marginal to be trivial. This improves upon Ref. [36], whose results apply only to entanglement-based QKD protocols.

Proof. Recall that in the variable-length protocol, multiple events may occur. Either the protocol aborts and does not produce any key, or it accepts and produces a key of length some length. We use $\Omega(\hat{c}_1^n)$ to refer to the event that $\hat{c}_1^n$ is observed in the public announcements. In this case, if error-verification passes, a key of length $\ell(\hat{c}_1^n)$ (or $\ell'(\hat{c}_1^n)$, depending on the protocol) is produced. We model aborts as producing a key of zero length, and denote that event via $\Omega_{\mathrm{len}=0}$. Thus, we write the output states for $\mathcal{E}_{\mathrm{QKD}}^{(\ell')}, \mathcal{E}_{\mathrm{QKD}}^{(\ell'),\mathrm{ideal}}$, for the input state $\tau_{A_1^n B_1^n R}$, as

$$\begin{aligned}
\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell')} \otimes \mathrm{id}_R\right)(\tau_{A_1^n B_1^n R}) &= \sum_{\hat{c}_1^n : \ell'(\hat{c}_1^n) > 0} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}) \tau^{\ell'(\hat{c}_1^n)}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} R | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}} \\
&\quad + \Pr(\Omega_{\mathrm{len}=0}) \tau^{(\perp)}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} R | \Omega_{\mathrm{len}=0}} \\
\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell'),\mathrm{ideal}} \otimes \mathrm{id}_R\right)(\tau_{A_1^n B_1^n R}) &= \sum_{\hat{c}_1^n : \ell'(\hat{c}_1^n) > 0} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}) \tau^{(l'(\hat{c}_1^n),\mathrm{ideal})}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} R | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}} \\
&\quad + \Pr(\Omega_{\mathrm{len}=0}) \tau^{(\perp,\mathrm{ideal})}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} R | \Omega_{\mathrm{len}=0}}.
\end{aligned} \tag{5.19}$$

Similarly, we write the output states for $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}}$ acting upon the input state $\tau_{A_1^n B_1^n E_1^n}$

$$\tau_{A_1^n B_1^n E_1^n} = \int \sigma_{ABE}^{\otimes n} \mathrm{d}\sigma, \tag{5.20}$$

as

$$\begin{aligned}
\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell)} \otimes \mathrm{id}_{E_1^n}\right)(\tau_{A_1^n B_1^n E_1^n}) &= \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}) \tau^{(\ell(\hat{c}_1^n))}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}} \\
&\quad + \Pr(\Omega_{\mathrm{len}=0}) \tau^{(\perp)}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega_{\mathrm{len}=0}} \\
\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}} \otimes \mathrm{id}_{E_1^n}\right)(\tau_{A_1^n B_1^n E_1^n}) &= \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}) \tau^{(\ell(\hat{c}_1^n),\mathrm{ideal})}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega_{\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}}} \\
&\quad + \Pr(\Omega_{\mathrm{len}=0}) \tau^{(\perp,\mathrm{ideal})}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n | \Omega(\mathrm{len}=0)}.
\end{aligned} \tag{5.21}$$

For each possible observation $\hat{c}_1^n$, we get the following term (which is multiplied by $\Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}})$) in the secrecy expression we wish to bound,

$$\zeta(\hat{c}_1^n) \coloneqq \frac{1}{2}\left\| \tau^{(\ell(\hat{c}_1^n))}_{K_A \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_1^n | \Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}}} - \tau^{(\ell(\hat{c}_1^n),\text{ideal})}_{K_A \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_1^n | \Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}}} \right\|_1. \tag{5.22}$$

Note that without loss of generality, we can assume that $\zeta(\hat{c}_1^n) < 1$, if equality occurs, then the required bound in Eq. (5.27) for the proof follows trivially). The converse bound for privacy amplification [38, Theorem 7.7] allows us to bound the smooth min entropy of the state prior to privacy amplification. Intuitively, we are simply using a statement that shows that if privacy amplification results in an output key that is secret, then the starting state must have atleast some amount of smooth min entropy. This allows us to obtain :

$$H_{\min}^{\sqrt{2\zeta(\hat{c}_1^n) - \zeta(\hat{c}_1^n)^2}}(\mathbf{S}|\widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{EV}} E_1^n)_{\tau|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}} \geq \ell(\hat{c}_1^n). \tag{5.23}$$

We now work with the above bound.

Since we require $\tau_{A_1^n B_1^n R}$ to be a purification, we purify $\tau_{A_1^n B_1^n E_1^n}$ using V as the purifying system. Thus, $E_1^n V$ is identified with R in the theorem statement. Since each $\sigma_{ABE}^{\otimes n}$ in Eq. (5.20) belongs to $\text{Sym}^n\left(\mathbb{C}^{d_A^2 d_B^2}\right)$, $\tau_{A_1^n B_1^n E_1^n}$ is supported on $\text{Sym}^n\left(\mathbb{C}^{d_A^2 d_B^2}\right)$. Thus, the dimension of the purifying register V is bounded by $\dim(V) \leq \dim(\text{Sym}^n\left(\mathbb{C}^{d_A^2 d_B^2}\right)) = g_{n,x}$ with $x = d_A^2 d_B^2$. Then, using the chain rule from [116, Eq. (8)] to split off this extra quantum register, we have

$$\begin{aligned} H_{\min}^{\sqrt{2\zeta(\hat{c}_1^n) - \zeta(\hat{c}_1^n)^2}}(\mathbf{S}|\widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{EV}} E_1^n V)_{\tau|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}} &\geq H_{\min}^{\sqrt{2\zeta(\hat{c}_1^n) - \zeta(\hat{c}_1^n)^2}}(\mathbf{S}|\widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{EV}} E_1^n)_{\tau|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}} \\ &\quad - 2\log(\dim(V)) \\ &\geq \ell(\hat{c}_1^n) - 2\log(g_{n,x}) \end{aligned} \tag{5.24}$$

Therefore, consider the modified protocol $\mathcal{E}_{\text{QKD}}^{(\ell')}$ that hashes to

$$\ell'(\cdot) = \max\left\{\lfloor \ell(\cdot) - 2\log(g_{n,x}) - 2\log(1/2\widetilde{\varepsilon})\rfloor, 0\right\}, \tag{5.25}$$

instead of $\ell(\cdot)$. In this case, using the Leftover Hashing Lemma (see Lemma 3.5.1) for

smooth min entropy for the terms where $\ell'(\hat{c}_1^n) > 0$, we have

$$\begin{aligned}
&\frac{1}{2}\left\|\tau^{(\ell'(\hat{c}_1^n))}_{K_A\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n V|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}} - \tau^{(\ell'(\hat{c}_1^n),\mathrm{ideal})}_{K_A\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n V|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}\right\|_1 \\
&\leq \frac{1}{2} 2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{2\zeta(\hat{c}_1^n)-\zeta(\hat{c}_1^n)^2}}(\mathbf{S}|\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{EV}} E_1^n V)_{\tau|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}} - \ell'(\hat{c}_1^n)\right)} + 2\sqrt{2\zeta(\hat{c}_1^n)-\zeta(\hat{c}_1^n)^2} \qquad (5.26) \\
&\leq \frac{1}{2} 2^{\log(2\widetilde{\varepsilon})} + 2\sqrt{2\zeta(\hat{c}_1^n)-\zeta(\hat{c}_1^n)^2} \\
&= \widetilde{\varepsilon} + 2\sqrt{2\zeta(\hat{c}_1^n)-\zeta(\hat{c}_1^n)^2}
\end{aligned}$$

Therefore, bringing all the terms together, we obtain

$$\begin{aligned}
&\frac{1}{2}\left\|\left(\left(\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell')} - \mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell'),\mathrm{ideal}}\right)\otimes \mathrm{id}_{E_1^n V}\right)\left(\tau_{A_1^n B_1^n E_1^n V}\right)\right\|_1 \\
&= \sum_{\hat{c}_1^n:\ell'(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\frac{1}{2}\left\|\tau^{(\ell'(\hat{c}_1^n))}_{K_A\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n V|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}} - \tau^{(\ell'(\hat{c}_1^n),\mathrm{ideal})}_{K_A\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} E_1^n V|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}\right\|_1 \qquad (5.27) \\
&\leq \sum_{\hat{c}_1^n:\ell'(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\left(\widetilde{\varepsilon} + 2\sqrt{2\zeta(\hat{c}_1^n)-\zeta(\hat{c}_1^n)^2}\right) \qquad (5.28) \\
&\leq \sum_{\hat{c}_1^n:\ell'(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\left(\widetilde{\varepsilon} + 2\sqrt{2\zeta(\hat{c}_1^n)}\right) \qquad (5.29) \\
&= \sum_{\hat{c}_1^n:\ell'(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\widetilde{\varepsilon} + \sqrt{8}\sum_i \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\sqrt{\zeta(\hat{c}_1^n)} \qquad (5.30) \\
&\leq \widetilde{\varepsilon} + \sqrt{8}\sqrt{\sum_{\hat{c}_1^n:\ell'(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\zeta(\hat{c}_1^n)} \qquad (5.31) \\
&\leq \widetilde{\varepsilon} + \sqrt{8}\sqrt{\varepsilon^{\mathrm{secret}}} \qquad (5.32)
\end{aligned}$$

where Eq. (5.27) follows from the definition of secrecy, Eq. (5.28) follows from Eq. (5.26). Eqs. (5.29) and (5.30) follow from basic algebra. In Eq. (5.31) we use the concavity of the square root function and Jensen's inequality, whereas Eq. (5.32) follows from:

$$\sum_{\hat{c}_1^n:\ell'(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\zeta(\hat{c}_1^n) \leq \sum_{\hat{c}_1^n:\ell(\hat{c}_1^n)>0} \Pr(\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}})\zeta(\hat{c}_1^n) = \varepsilon^{\mathrm{secret}} \qquad (5.33)$$

where we use the fact that $\ell'(\hat{c}_1^n) > 0 \implies \ell(\hat{c}_1^n) > 0$. This concludes the proof. □

Through a series of lemmas and theorems, we have reduced the security proof of a QKD protocol against arbitrary attacks to the security proof of a similar QKD protocol against IID collective attacks. There are two costs to be paid for this lift. One is a cost paid to the $\varepsilon^{\text{secret}}$ as stated in Lemma 5.2.5. The other is a cost paid to the hash length that can be chosen as stated in Theorem 5.2.1. We bring together the entire reduction formally in the following corollary.

Corollary 5.2.1. *Consider the QKD Protocol defined via* $\{\mathcal{E}^{(\ell)}_{\text{QKD}}, \sigma_A\}$ *where* $\mathcal{E}^{(\ell)}_{\text{QKD}} \in \text{CPTP}(A_1^n B_1^n, K_A K_B \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}})$ *is a map such that the* $\varepsilon^{\text{secret}}$*-secrecy condition holds for all IID states* $\rho_{A^n B^n E^n} = \sigma_{ABE}^{\otimes n}$ *satisfying* $\text{Tr}_{BE}(\sigma_{ABE}) = \sigma_A$ *((Definition 3.6.3)). That is,*

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\text{Tr}_{K_B} \circ \mathcal{E}^{(\ell)}_{\text{QKD}} - \text{Tr}_{K_B} \circ \mathcal{E}^{(\ell),\text{ideal}}_{\text{QKD}} \right) \otimes \text{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 \leq \varepsilon^{\text{secret}}, \\ &\forall\, \rho_{ABE} \in \text{S}_=(ABE) \text{ such that } \text{Tr}_{BE}(\rho_{ABE}) = \sigma_A. \end{aligned} \tag{5.34}$$

Let $\mathcal{E}^{(\ell',\text{perm})}_{\text{QKD}}$ *be a variable-length QKD protocol map identical to* $\mathcal{E}^{(\ell)}_{\text{QKD}}$*, except that*

1. *it hashes to a length* $\ell'(\cdot)$ *instead of* $\ell(\cdot)$*,*
2. *includes the random permutation step on the classical* X_1^n, Y_1^n *(see Lemma 5.2.1), announced in the register* C_{perm}*.*

Suppose $\ell'(\cdot) = \max\left\{ \lfloor \ell(\cdot) - 2\log(g_{n,x}) - 2\log(1/2\widetilde{\varepsilon}) \rfloor, 0 \right\}$*, where* $x = d_A^2 d_B^2$*. Then the QKD protocol* $\{\mathcal{E}^{(\ell',\text{perm})}_{\text{QKD}}, \sigma_A\}$ *is* $g_{n,x}\left(\sqrt{8\varepsilon^{\text{secret}}} + \widetilde{\varepsilon}\right)$*-secret with fixed marginal* σ_A*. That is,*

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\text{Tr}_{K_B} \circ \mathcal{E}^{(\ell',\text{perm})}_{\text{QKD}} - \text{Tr}_{K_B} \circ \mathcal{E}^{(\ell',\text{perm}),\text{ideal}}_{\text{QKD}} \right) \otimes \text{id}_{\hat{\boldsymbol{E}}} \right) \left[\rho_{A_1^n B_1^n \hat{\boldsymbol{E}}} \right] \right\|_1 \leq g_{n,x}\left(\sqrt{8\varepsilon^{\text{secret}}} + \widetilde{\varepsilon}\right), \\ &\forall\, \rho_{A_1^n B_1^n \hat{\boldsymbol{E}}} \in \text{S}_=(A_1^n B_1^n \hat{\boldsymbol{E}}) \text{ such that } \rho_{A_1^n} = \sigma_A^{\otimes n}. \end{aligned} \tag{5.35}$$

Proof. Since $\mathcal{E}^{(\ell',\text{perm})}_{\text{QKD}} - \mathcal{E}^{(\ell',\text{perm}),\text{ideal}}_{\text{QKD}}$ is permutation-invariant (from Lemma 5.2.1), Lemma 5.2.5 states that there exists a probability measure $d\sigma_{AB}$ on the set of extensions σ_{AB} of σ_A such that

$$\begin{aligned} &\frac{1}{2}\left\| \left(\left(\mathcal{E}^{(l',\text{perm})}_{\text{QKD}} - \mathcal{E}^{(l',\text{perm}),\text{ideal}}_{\text{QKD}} \right) \otimes \text{id}_{E_1^n} \right) \left(\rho_{A_1^n B_1^n E_1^n} \right) \right\|_1 \\ &\leq g_{n,x} \frac{1}{2}\left\| \left(\left(\mathcal{E}^{(l',\text{perm})}_{\text{QKD}} - \mathcal{E}^{(l',\text{perm}),\text{ideal}}_{\text{QKD}} \right) \otimes \text{id}_R \right) \left(\tau_{A_1^n B_1^n R} \right) \right\|_1, \end{aligned} \tag{5.36}$$

where $\tau_{A_1^n B_1^n R}$ is any purification of $\tau_{A_1^n B_1^n} = \int d\sigma_{AB}\ \sigma_{AB}^{\otimes n}$, and $x = d_A^2 d_B^2$. We then use Theorem 5.2.1, which allows us to only prove security against IID states. Then, we utilize

Lemma 5.2.2 to argue that for IID states, the security of the protocol with the permutation is the same as the security of the protocol without the permutation. This concludes the proof. □

The above corollary can now be directly reduced the secrecy analysis of QKD protocols that satisfy the permutation invariance condition. Thus, we make rigorous a verbal argument made in Ref. [36] in Theorem 5.2.1. In doing so, we notice that the key secrecy parameter is worse than predicted by Ref. [36]. In particular, Ref. [36] obtains a secrecy parameter of $\approx g_{n,x}\varepsilon^{\text{secret}}$ against arbitrary attacks, as compared to $g_{n,x}\sqrt{\varepsilon^{\text{secret}}}$ which we obtain, where $\varepsilon^{\text{secret}}$ refers to the secrecy parameter obtained against IID collective attacks.

5.2.3 Improvements from block-diagonal symmetry

In situations where the QKD protocol satisfies additional properties, one can repeat the previous analysis as shown below to obtain improved performance. We first state when a QKD protocol is IID-block-diagonal, in preparation for using our improved de Finetti result from Corollary 5.1.3.

Definition 5.2.2 (IID-block-diagonal maps)**.** Let $\{\Pi_i\}_{i=1}^k$ be a set of orthogonal projectors on A. A linear map $\Delta \in \mathrm{T}(A_1^n, B_1)$ is **IID-block-diagonal**, if

$$\sum_{\vec{i}\in[k]^n} \Delta \circ \mathcal{P}_{\vec{i}} = \Delta \tag{5.37}$$

where $\mathcal{P}_{\vec{i}}(\cdot) = \bigotimes_{j=1}^n \Pi_{i_j}(\cdot)\bigotimes_{j=1}^n \Pi_{i_j}$.

Corollary 5.2.2. *Consider the QKD Protocol defined via* $\{\mathcal{E}_{\text{QKD}}^{(\ell)}, \sigma_A\}$ *where* $\mathcal{E}_{\text{QKD}}^{(\ell)} \in \mathrm{CPTP}(A_1^n B_1^n, K_A K_B \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} H_{\text{PA}} H_{\text{EV}})$ *is such that the* $\varepsilon^{\text{secret}}$*-secrecy condition (Definition 3.6.3) holds for all IID states* $\rho_{A^n B^n E^n} = \sigma_{ABE}^{\otimes n}$ *satisfying* $\mathrm{Tr}_{BE}(\sigma_{ABE}) = \sigma_A$.

Let $\mathcal{E}_{\text{QKD}}^{(\ell',\text{perm})}$ *be a variable-length QKD protocol map identical to* $\mathcal{E}_{\text{QKD}}^{(\ell,\text{perm})}$*, except that it*

1. *it hashes to a length* $\ell'(\cdot)$ *instead of* $\ell(\cdot)$*,*
2. *includes the random permutation step on the classical* X_1^n, Y_1^n *(see Lemma 5.2.1), announced in the register* C_{perm}*.*
3. *and* $\mathcal{E}_{\text{QKD}}^{(\ell',\text{perm})} - \mathcal{R}_{\text{ideal}} \circ \mathcal{E}_{\text{QKD}}^{(\ell',\text{perm})}$ *is an IID-block-diagonal map with respect to projections* $\{\Pi_i^A \otimes \Pi_j^B\}_{i,j=1}^{k_A,k_B}$ *of dimension* $\{d_i^A d_j^B\}_{i,j=1}^{k_A,k_B}$*.*

Suppose $\ell'(\cdot) = \max\{\lfloor \ell(\cdot) - 2\log(g_{n,x}) - 2\log(1/2\widetilde{\varepsilon})\rfloor, 0\}$, *where* $x = \sum_{i,j=1}^{k_A,k_B} (d_i^A)^2 (d_j^B)^2$. *Then* $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \sigma_A\}$ *is* $g_{n,x}\left(\sqrt{8\varepsilon^{\mathrm{secret}}} + \widetilde{\varepsilon}\right)$*-secret.*

Proof. The proof follows from a similar series of steps as Corollary 5.2.1, but using the de Finetti reduction form Corollary 5.1.3 instead of Corollary 5.1.2. □

5.3 Postselection technique for optical protocols

So far, we have shown how the postselection technique can be used to reduce the analysis to proving secrecy against IID collective attacks. However, our lift statements (Corollaries 5.2.1 and 5.2.2) depend explicitly on the dimensions of Alice's and Bob's systems. This creates a problem when dealing with optical protocols. In this section, we will see how to extend our analysis to handle such protocols, in particular decoy-state BB84.

If we naively apply the source-replacement scheme from Chapter 7, then Alice's shield system $\hat{A}$ (see Section 3.6.1) - a system that remains inside her lab - is infinite dimensional for phase-randomized weak coherent pulses. Likewise, Bob's threshold detectors act on infinite-dimensional Hilbert spaces. Thus, neither d_A nor d_B is finite.

In this section, we will formally state how squashing maps and source maps can be used to reduce the protocol to one involving finite-dimensional systems. It may be helpful to revise Sections 3.6.2 and 3.6.3 at this point. We note that squashing maps and source maps are often applied at the level of the single-round optimization problem in many works [117, 9, 118, 6]. That approach is tenable when the underlying security proof technique does not depend on the dimensions[4]. This is not the case for us, and therefore additional care is required.

Thus, we will now combine the use of source maps and squashing maps with our analysis. We will first use these tools to reduce the protocol to a finite-dimensional one, after which it can be analyzed using the analysis from previous sections. For this, it is convenient to view an instance of QKD Protocol as $\{\widetilde{\mathcal{E}}_{\mathrm{QKD}}^{(\ell)}, \sigma_{XA'}\}$, where Alice first creates the classical quantum state $\sigma_{XA'}^{\otimes n}$, which is followed by Eve's attack, and $\widetilde{\mathcal{E}}_{\mathrm{QKD}}^{(\ell)}$ is the protocol map that implements Bob's measurements, and all subsequent classical postprocessing (see Definitions 3.6.5 and 3.6.6). Note that we will include a more general version of these statements in Section 7.4.

[4]Although we note that there are still nuances when it comes to handling truly infinite dimensions, since a statement that holds for arbitrary finite dimensional states does not necessarily hold for infinite dimensional states, see [3, Appendix A]

We will first obtain the following lemma concerning source maps.

Lemma 5.3.1 (Source maps)**.** *Let $\{\sigma_k\} \subset \mathrm{S}_=(A')$ be the set of states prepared by Alice in a QKD protocol given by $\{\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}, \sigma_{XA'}\}$. Consider a related QKD protocol $\{\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}, \xi_{XA''}$ that is identical to the first one in all cases except source preparation, where it prepares ξ_k instead of σ_k. Suppose that there exists a **source map** $\Psi \in \mathrm{CPTP}(A'', A')$ relating the real states $\{\sigma_k\}$ to a set of virtual states $\{\xi_k\} \subset \mathrm{S}_= A''$ such that $\sigma_k = \Psi[\xi_k]$ for all k. Then $\varepsilon^{\mathrm{secure}}$-security for the virtual protocol $\{\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}, \xi_{XA''}\}$ implies $\varepsilon^{\mathrm{secure}}$-security for the real protocol $\{\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}}, \sigma_{XA'}\}$.*[5]

Proof. For any attack $\mathcal{A} \in \mathrm{CPTP}((A')^n_1, B^n_1 \hat{\boldsymbol{E}})$, we have

$$\begin{aligned}
&\frac{1}{2}\left\| \left(\left(\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} - \mathcal{R}_{\mathrm{ideal}} \circ \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \right) \otimes \mathcal{A} \right) \left[\sigma_{X^n_1 (A')^n_1} \right] \right\|_1 \\
&= \frac{1}{2}\left\| \left(\left(\widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} - \mathcal{R}_{\mathrm{ideal}} \circ \widetilde{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \right) \otimes \mathcal{A} \circ \Psi^{\otimes n} \right) \left[\xi_{X^n_1 (A'')^n_1} \right] \right\|_1 \\
&\leq \varepsilon^{\mathrm{secure}}.
\end{aligned} \tag{5.38}$$

where we simply used the stated property of the source map for the second line, and the definition of security for the final line, where we have that $\mathcal{A} \circ \Psi^{\otimes n} \in \mathrm{CPTP}((A'')^n_1, B^n_1 \hat{\boldsymbol{E}})$ is a valid attack that Eve can perform on the protocol with the virtual states. . □

The original squashing map constructions [81, 62, 63, 82] prove the applicability of squashing models by showing that their usage lower bounds the key rate under the assumption of IID collective attacks. However, this alone is *insufficient* to apply the squashing model to make Bob's system finite-dimensional and apply the postselection technique. Thus, we prove the following lemma.

Lemma 5.3.2 (Squashing)**.** *Consider the QKD protocol $\left\{ \bar{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \circ \left(\mathcal{M}^{\mathrm{meas}}_{\{\Gamma^{(B)}_k\}} \right)^{\otimes n}, \sigma_{XA'} \right\}$, where $\mathcal{M}^{\mathrm{meas}}_{\{\Gamma^{(B)}_k\}}$ is a channel that measures the B systems and stores the outcome in Y, and $\bar{\mathcal{E}}^{(\ell)}_{\mathrm{QKD}} \in \mathrm{CPTP}(X^n_1 Y^n_1, \widehat{C}^n_1 C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ implements the rest of the QKD protocol. Suppose there exists quantum channels (squashing maps, see Definition 3.6.7) $\Lambda \in \mathrm{CPTP}(B, Q)$ and measurement channels $\mathcal{M}^{\mathrm{meas}}_{\{F^Q_i\}} \in \mathrm{CPTP}(Q, Y)$ such that*

$$\mathcal{M}^{\mathrm{meas}}_{\left\{F^{(Q)}_i\right\}} \circ \Lambda = \mathcal{M}^{\mathrm{meas}}_{\left\{M^{(B)}_i\right\}} \tag{5.39}$$

[5] One can obtain the same result for secrecy instead.

Then, the $\varepsilon^{\text{secure}}$-security of the squashed QKD protocol, given by $\left\{\bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(B)}_k\}}\right)^{\otimes n}, \sigma_{XA'}\right\}$ *implies the $\varepsilon^{\text{secure}}$-security of the original QKD protocol, given by* $\left\{\bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(B)}_k\}}\right)^{\otimes n}\right\}$.

Proof. We use the fact that the first step of the QKD protocol is to measure Bob's received state, i.e, the protocal map is given by $\bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(B)}_k\}}\right)^{\otimes n}$. Thus, for any attack $\mathcal{A} \in \text{CPTP}((A')^n_1, B^n_1 \hat{\boldsymbol{E}})$ we have

$$\begin{aligned}
&\frac{1}{2}\left\|\left(\left(\bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(B)}_k\}}\right)^{\otimes n} - \mathcal{R}_{\text{ideal}} \circ \bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(B)}_k\}}\right)^{\otimes n}\right) \otimes \mathcal{A}\right)\left[\sigma_{X^n_1 (A')^n_1}\right]\right\|_1 \\
&= \frac{1}{2}\left\|\left(\left(\bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(Q)}_k\}}\right)^{\otimes n} - \mathcal{R}_{\text{ideal}} \circ \bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(Q)}_k\}}\right)^{\otimes n}\right) \otimes \Lambda^{\otimes n} \circ \mathcal{A}\right)\left[\sigma_{X^n_1 (A')^n_1}\right]\right\|_1 \\
&= \frac{1}{2}\left\|\left(\left(\bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(Q)}_k\}}\right)^{\otimes n} - \mathcal{R}_{\text{ideal}} \circ \bar{\mathcal{E}}^{(\ell)}_{\text{QKD}} \circ \left(\mathcal{M}^{\text{meas}}_{\{\Gamma^{(Q)}_k\}}\right)^{\otimes n}\right) \otimes \mathcal{A}^{\text{Sq}}\right)\left[\sigma_{X^n_1 (A')^n_1}\right]\right\|_1 \\
&\leq \varepsilon^{\text{secure}}
\end{aligned} \tag{5.40}$$

where the second line follows from Eq. (5.39), and the last line follows redefining $\mathcal{A}^{\text{Sq}} = \Lambda^{\otimes n} \circ \mathcal{A}$. The required statement follows from the fact that $\mathcal{A}^{\text{Sq}} \in \text{CPTP}((A')^n_1, Q^n_1 \hat{\boldsymbol{E}})$ is a valid attack on the protocol with the squashed POVM measerements. □

Using Squashing with postselection technique

We now briefly discuss a subtle issue that arises when using the postselection technique with squashing arguments. The subtlety comes from having to prove the security against *all* attacks in the protocol with squashed measurements.

First, note that not all squashing models proceed via the construction of an explicit squashing map Λ. In particular, the universal squashing model [81] only allows the replacement of the original measurements with squashed measurements for the purposes of estimating certain statistical quantities. Moreover, the dimension-reduction method [82] does not proceed via a squashing map argument. As a result, they cannot be combined with the postselection technique through Lemma 5.3.2.[6]

[6]Since the dimension-reduction method is currently the only known approach for reducing CVQKD to finite dimensions, the applicability of the postselection technique to CVQKD remains an open problem.

Existing multiphoton-to-qubit squashing maps, such as those constructed in Ref. [62], are only known to exist under highly restrictive assumptions on the detector model. In particular, they require perfectly matched (or exactly equal) efficiencies and dark count rates across all detectors, and are therefore not robust to realistic device imperfections.

Consequently, in practical settings the only viable candidate is the flag-state squasher. Moreover, recent works [78, 119] establish the existence of a flag-state squasher even when detector parameters are only known to lie within a characterized range. It is therefore natural to attempt to combine the flag-state squasher with the postselection technique. However, a direct application of Lemma 5.3.2 using the standard flag-state squasher leads to a trivial (zero) key rate, due to the existence of classical flags as described in Section 3.6.3.

For the postselection technique specifically, a new "weight-preserving flag-state squasher" variant of the flag-state squasher was introduced in Ref.[5]. This construction modifies the standard flag-state squasher in a way that allows the entire squashing map to be given to Eve, while still enabling the application of Lemma 5.3.2 together with the postselection technique. We do not describe this construction in detail here, nor do we use this modified squasher in this thesis. Instead, for the numerical results presented in this chapter, we employ the qubit squasher introduced in Ref.[62]. The purpose of the present discussion is to highlight a subtle but crucial issue in combining squashing models with postselection, and to motivate the need for such modified squashing maps. We note that Refs. [119, 78] present an alternative approach that enables the use of the flag-state squasher together with postselection, even in the presence of detector imperfections, that utilizes the weight-preserving flag-state squasher. That method is technically involved, and we refer the interested reader to the cited works for further details.

With these clarifications in place, we now have all the necessary tools to apply our results to the qubit BB84 and decoy-state BB84 protocols, which we do in the next subsection.

5.4 Application to BB84 protocols

So far we have made rigorous the framework to apply the postselection technique to optical prepare-and-measure protocols. In this section, we will first outline a recipe in Section 5.4.1 that can be used to apply the postselection technique to optical protocols. Then, in Sections 5.4.2 and 5.4.3 we apply that recipe to the Qubit BB84 and decoy-state BB84 protocols.

5.4.1 Recipe

We use Corollaries 5.2.1 and 5.2.2, which state that given a variable-length security proof against IID collective attacks with key lengths $\ell(\hat{c}_1^n)$ and secrecy parameter $\varepsilon^{\text{secret}}$, the postselection technique can be used to provide a security proof against coherent attacks with key lengths $\ell(\hat{c}_1^n) - 2\log(g_{n,x}) - 2\log(1/2\widetilde{\varepsilon})$ and secrecy parameter $g_{n,x}(\sqrt{8\varepsilon^{\text{secret}}} + \widetilde{\varepsilon})$. Here, $\widetilde{\varepsilon}$ is a parameter that can be chosen freely and $g_{n,x}$ can be thought of as the cost of using the postselection technique that depends on the dimensions of the systems. In the presence of additional protocol structure, this cost can be reduced as detailed in the corollary statements.

In practice, this can be used as follows:

1. Choose a target secrecy parameter $\varepsilon^{\text{secret}}$ based on the application in mind.
2. Determine the protocol-dependent upper bound on the cost of using the postselection technique as $g_{n,x} = \binom{n+x-1}{x-1} \leq \left(\frac{e(n+x-1)}{x-1}\right)^{x-1}$. Here, x depends on the dimensions of the systems, and the structure in the protocol. For a generic protocol, $x = d_A^2 d_B^2$ as described in Corollary 5.2.1. In the presence of block-diagonal structure this can be improved as stated in Corollary 5.2.2.
3. Pick value of free parameter $\widetilde{\varepsilon}$ (in principle this value can be optimised over). For our calculations, we choose this to be $\widetilde{\varepsilon} = \varepsilon^{\text{secret}}/2$
4. Compute key lengths $\ell(\cdot)$ through an IID security proof, with secrecy parameter $\frac{(\varepsilon^{\text{secret}} - g_{n,x}\widetilde{\varepsilon})^2}{8g_{n,x}^2}$. For our calculations, we choose $\varepsilon_{\text{PA}} = \varepsilon_{\text{AT}}$ for the IID key length calculations.
5. Use key lengths $\ell(\hat{c}_1^n) - 2\log(g_{n,x}) - 2\log(1/2\widetilde{\varepsilon})$ as the final hash length for the protocol. This protocol is secure against coherent attacks.

Application to optical protocols using Qubit squuasher

For detection setups with threshold detectors, an appropriate squasher must be used to squash Bob's system down to finite-dimensions. If we use the qubit squasher from Ref. [62], Bob measures a 3-dimensional system what is made of the vacuum and qubit space. Moreover, Bob is block-diagonal, and thus the dimensional-dependent term x in 2 is given by (Corollary 5.2.2)

$$x = d_A^2 \left(1^2 + 2^2\right). \tag{5.41}$$

For the qubit BB84 protocol, one can also further reduce d_A to 2 instead of 4, as argued in the next chapter. Hence, for Qubit BB84, we have $x = 2^2(5)$.

For decoy-state protocols, we use the tagging source map, and therefore consider tagged states as described in Eq. (3.32). For most encodings such as polarization, time-bin, etc. (see Ref. [5] for formal details, and Ref. [119] for improvements), the dimensional-dependent term x in Step. 2 is given by

$$x = N_{\text{int}}^2(N_{\text{ph}} + 2)d_{\bar{A}}^2(1^2 + 2^2), \tag{5.42}$$

where N_{int} is the number of intensities used in the protocol, and $d_{\bar{A}}$ is the dimension of Alice's subsystem that she measures (recall that $A = \bar{A}\hat{A}$). We set $N_{\text{ph}} = 3$, and hence we obtain $x = 3^2(3 + 2)4^2(1^2 + 2^2)$, for the decoy-state BB84 calculations.

5.4.2 Qubit BB84

We plot key rates with and without the postselection lift for the qubit BB84 protocol in Fig. 5.1. We plot variable-length key rates for the typical observations of the channel, i.e $\mathbf{F}^{\text{obs}}$ set to be the expected honest behaviour of the channel. Alice and Bob both choose each basis with probability 0.5, and the probability of a `test` round is given by $\gamma = 0.1$. We consider a channel with 2° misalignment, and depolarization probability of 2%. Key rates are plotted against loss, with the target $\varepsilon^{\text{secret}} = \varepsilon_{\text{EV}} = 10^{-10}$. We use the same formula for key rate computations as Section 4.4, suitably modifying the parameters as required by the postselection technique.

5.4.3 Decoy-state BB84

We plot key rates with and without the postselection lift for the decoy-state BB84 protocol in Fig. 5.1. We plot variable-length key rates for the typical observations of the channel, i.e $\mathbf{F}^{\text{obs}}$ set to be the expected honest behaviour of the channel. Alice and Bob both choose each basis with probability 0.9, and the probability of a `test` round is given by $\gamma = 0.1$. We set the decoy intensities to be $\mu_1 = 1, \mu_2 = 0.01, \mu_3 = 0.001$, with all three intensities sent with equal probability in the `test` rounds, and only μ_1 being used in the `gen` rounds. We plot key rates for a loss-only channel, with the $\varepsilon^{\text{secret}} = \varepsilon_{\text{EV}} = 10^{-10}$. We use the same formula for key rate computations as Section 4.5 (which relies on Ref. [6]), suitably modifying the parameters as required by the postselection technique.

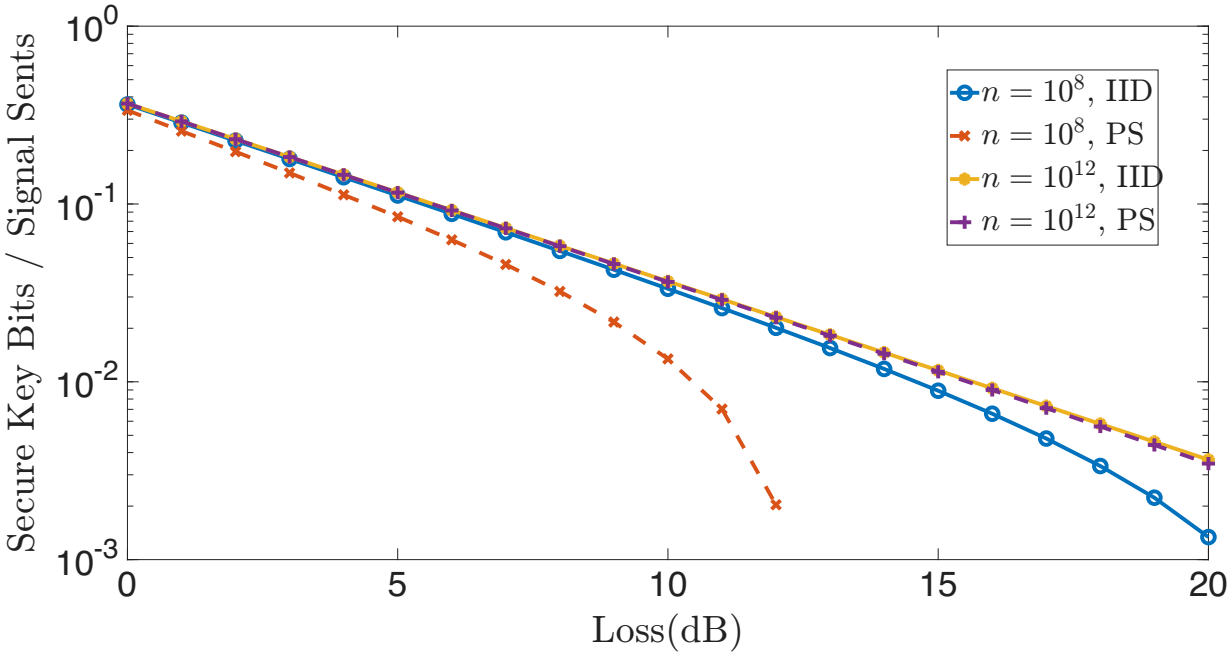


Figure 5.1: Key rate for variable-length qubit BB84 protocol plotted against loss, with and without the postselection lift to coherent attacks.

We see that the usage of the postselection technique significantly reduces the key rate compared to IID collective attacks. The main impact is due to the large value of $g_{n,x}$. For a plot that shows the impact of this dimension on the key rate performance, see [5, Fig 2].

5.5 Summary and Outlook

Overall, this chapter provides the first complete, robust, and practically applicable formulation of the postselection technique[7] for quantum key distribution. It resolves several longstanding gaps in the literature and enables rigorous security proofs against coherent attacks for realistic prepare-and-measure protocols.

The postselection technique is remarkably easy to use in practice. One simply needs to ensure that the protocol explicitly includes a random permutation of the classical data as one of its steps, thereby guaranteeing permutation invariance of the overall protocol.

[7]The author is not entirely sure why this technique was named so, as it has nothing to do with postselection of data.

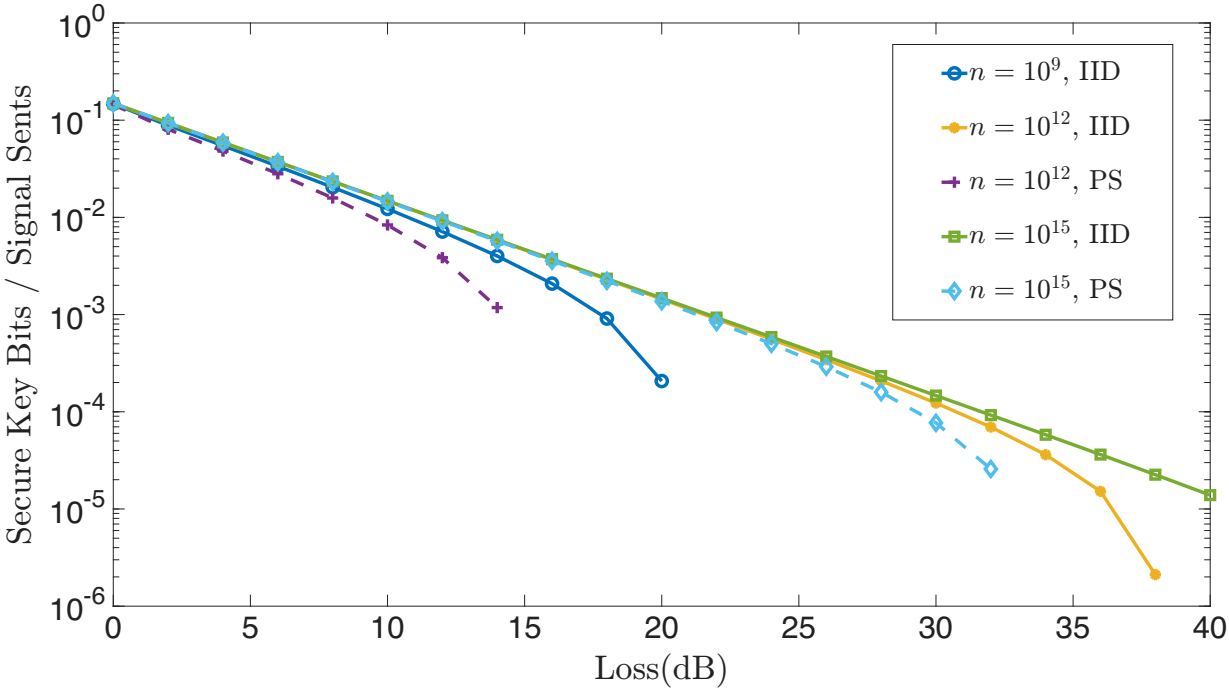


Figure 5.2: Key rate for variable-length decoy-state BB84 protocol plotted against loss, with and without the postselection lift to coherent attacks.

Once this condition is satisfied, Corollary 5.2.1 can be applied to reduce the entire security analysis to the IID collective attack setting. We emphasize that this reduction is entirely independent of how one chooses to perform the IID security analysis. After this reduction, one may proceed with *any* IID security analysis of choice. This includes, for instance, approaches based on uncertainty relations or phase error correction [120].[8]

Despite these strengths, the postselection technique has several fundamental drawbacks. First, recall that the technique starts from a global state $\rho_{A_1^n B_1^n \hat{\boldsymbol{E}}}$ describing Eve's attack on all n rounds. In this picture, Eve's attack is applied first, which results in the post-attack state that is to be analyzed, and only afterward are public announcements made. As a consequence, protocols that rely on *on-the-fly* announcements, where Alice and Bob announce public information before all signals have been sent and received, cannot be handled in a straightforward manner within this framework.

[8]We note, however, that if one wishes to pursue a phase error correction approach at this stage, it is generally preferable to rely directly on the underlying de Finetti reductions to simplify the sampling process, as done for example in Refs. [121, 122, 123], rather than relying directly on the lifting theorems.

Second, permutation invariance formally requires permuting the quantum systems $A_1^n B_1^n$. In practice, one permutes only the classical measurement data obtained from these systems, and this is sufficient to justify permutation invariance if Alice and Bob perform the same measurements in each round. However, it is unclear how this technique can be extended to scenarios involving correlated measurement effects, such as detector dead times or after pulsing [83, 78], or correlated source imperfections [80, 124].

Finally, the postselection technique yields highly pessimistic key rates, primarily due to the large value of the overhead factor $g_{n,x}$. Although the improved de Finetti reductions developed in this chapter significantly mitigate this issue, the resulting key rates remain below those achievable using phase error rate based methods and the MEAT framework studied in the next two chapters.

In summary, while the postselection technique provides a conceptually clean and broadly applicable route to coherent-attack security, its limitations in handling adaptive announcements, correlated imperfections, and finite-size performance are significant drawbacks.

Chapter 6

Entropic Uncertainty Relations and Phase Error Estimation

> Where we *really* break free from the shackles of IID collective attacks; where we confront Eves's global attack head-on; and where we enthusiastically consider a large number of fictitious measurements, and agonizingly obtain estimates on their measurement outcomes.

Security proofs of QKD based on entropic uncertainty relations (EUR) [44, 34, 125, 7] and on the phase error correction approach [89, 90, 7] yield some of the highest key rates against coherent attacks in the finite-size regime. Historically, these techniques were among the earliest to provide analyses of coherent attacks, and it is only more recently that EAT-based methods (which we discuss in Chapter 7) have begun to achieve comparable (and in many cases superior [6]) key rates. Moreover, these approaches are widely used in practice, due in part to their conceptual simplicity and the availability of closed-form or largely analytic key rate expressions.

However, while this simplicity and elegance are most apparent in idealized BB84 scenarios, they come at a significant cost when practical imperfections are taken into account, as we shall see in this chapter. Although source imperfections [126, 127, 128, 129] have been extensively studied within the phase error correction framework, detector imperfections have only recently been addressed for either proof technique [2].

In particular, prior to Ref. [2] (which is the work on which this chapter is based), these proof techniques required the probability of detection in Bob's measurement setup

to be independent of the basis choice. This assumption is commonly referred to as **basis-independent loss**, while violations of this assumption are known as **basis-efficiency mismatch** or **detection-efficiency mismatch**. Satisfying basis-independent loss requires the efficiencies and dark count rates of Bob's detectors to be *exactly* identical. Consequently, justifying this assumption in practice requires exact characterization of identical detectors, which is not achievable. Meanwhile, there have been several experimental demonstrations [130, 131, 132, 133, 134], exploiting basis-efficiency mismatch for attacks on QKD systems.

As a result, these proof techniques remained inapplicable to practical prepare-and-measure (and entanglement-based) QKD scenarios involving realistic detectors.[1] Extending EUR and phase error correction based proof techniques to realistic detector models has remained a well-known open problem in the field for nearly two decades. While a variety of partial results exist [135, 136, 137, 138, 63, 139, 140, 141, 47], none addressed the finite-size regime against coherent attacks prior to Ref. [2]; see [2, Table 1] for a detailed overview of the historical developments.

In this chapter, we prove the security of the decoy-state BB84 protocol with an active detection setup *without* assuming basis-independent loss. We do so by showing that the phase error rate can be suitably bounded even without the assumption. We explicitly define metrics δ_1, δ_2 that quantify the deviation from the ideal case, and bound the phase error rate in terms of these deviations. Our framework is general, and can be applied to any (IID) detector model of one's choice, as long as the relevant metrics δ_1, δ_2 can be suitable bounded. We explicitly compute these metrics for the case of detectors with basis-efficiency mismatch and unequal dark count rates. To do so, we assume the the canonical model of detectors described in Sections 3.3 and 6.6.2. The block-diagonal structure of the detector POVMs significantly aids the computation of these metrics. Moreover, we compute these metrics directly from the experimental characterization of the detection efficiencies and dark count rates of the detectors. Our results extend the security of QKD to the following practical scenarios:

1. Bob's detectors are *not* identical, but the values of efficiency (η_{b_i} for basis b and outcome i) and dark count rates (d_{b_i}) are known. Note that while this is a useful toy model, such scenarios are impractical since they require η_{b_i}, d_{b_i} to be known exactly. We treat the dark count rate as a part of the POVM element, as described in Section 6.6.2.

[1] By contrast, measurement-device-independent QKD (MDI-QKD) [55] is able to address *all* detector imperfections and detector side channels, since it assumes the detectors to be completely under Eve's control. However, it is much more complex to implement and prepare-and-measure QKD protocols remain the dominant implementation.

2. Bob's detectors are *not* identical, and the values of efficiency and dark count rates are only known to be in some range $\eta_{b_i} \in [\eta_{\text{det}}(1-\Delta_\eta), \eta_{\text{det}}(1+\Delta_\eta)], d_{b_i} \in [d_{\text{det}}(1-\Delta_{\text{dc}}), d_{\text{det}}(1+\Delta_{\text{dc}})]$. While this is again a useful toy model, a detectors response (η_{b_i}, d_{b_i}) to incoming photons typically depends on the spatio-temporal modes of incoming photons, which are in Eve's control.

3. Bob's detectors are *not* identical, and the values of efficiency and dark count rates are only known to be in some range. Moreover, these values depend on the spatio-temporal modes (labelled by $\mathbf{d}$) of the incoming photons, and can therefore be chosen by Eve [131, 63, 133, 134]. This is expressed mathematically as $\eta_{b_i}(\mathbf{d}) \in [\eta_{\text{det}}(\mathbf{d})(1-\Delta_\eta), \eta_{\text{det}}(\mathbf{d})(1+\Delta_\eta)], d_{b_i}(\mathbf{d}) \in [d_{\text{det}}(1-\Delta_{\text{dc}}), d_{\text{det}}(1+\Delta_{\text{dc}})]$. Note that in this model, the range of allowed values of the loss can depend on the spatio-temporal mode, whereas the dark count rates for all the modes lie in the same range.

Our metrics δ_1, δ_2 involve an optimization over all possible values of η_{b_i}, d_{b_i} in their respective ranges. Moreover, for our model of multi-mode detectors, we find that our methods yield the same values for Case 2 and Case 3. Thus, our methods address one practically important detector side-channel as a by-product.

Organization of this chapter

This chapter is organized as follows. We begin by stating a fairly abstract theorem (Theorem 6.1.1) on the variable-length security of QKD Protocol, which serves as basis for proving variable-length security in EUR based approaches. (This section may be skipped on a first reading, as its role will become clearer once the phase error rate bounds derived in later sections have been studied.) We will then see how suitable bounds on the phase error rate suffice for proving security, and describe some details about our notation and phase error rates in Section 6.2. In Section 6.3, we show how such bounds can be obtained in the case where the basis-independent loss assumption is satisfied. In Section 6.4, we show how analogous bounds can be obtained when the basis-independent loss assumption is *not* satisfied. Finally, in Section 6.5, we extend the analysis to prove variable-length security for the decoy-state BB84 protocol with imperfect detectors In Section 6.6 we apply our results to study the effect of basis-mismatch on decoy-state BB84. In Section 6.7 we present some concluding remars.

6.1 Variable length security in EUR

In this subsection, we will state a theorem regarding the variable-length security of QKD Protocol, analogous to [2, Theorem 4], that is suitable for use with the EUR technique. Recall that the QKD Protocol makes public announcements in the register $\widehat{C}_1^n$, and we use $\hat{c}_1^n$ to denote the value stored in $\widehat{C}_1^n$, and $\Omega(\hat{c}_1^n)$ denote the event that $\hat{c}_1^n$ was observed in $\widehat{C}_1^n$ registers. Recall further that our goal is to lower bound the smooth min entropy of the raw key string i.e, $H_{\min}^{\bar{\varepsilon}}(\mathbf{S}|\widehat{C}_1^n\hat{\boldsymbol{E}})_\rho$. Ofcourse, from Section 3.5.1, we know that we have to condition carefully on various events in order to get non-trivial results. In the EUR case, we will also have the smoothing parameter itself also depend on the probability of the event being conditioned on. We will also need to consider various unobserved events, which we denote using $\Omega(\vec{p})$. These refer to events that are well defined, but which we do not directly have access to (such as number of single-photon rounds in the protocol etc).

We are now ready to state the theorem statement. Note that the proof uses the same essential idea as [109, Supplementary Note A] and Refs. [107, 108], but is more general, and carefully handles conditioning on events. The proof is provided in Appendex. C. The usage of this theorem is explained after the theorem statement.

Theorem 6.1.1 (Variable-length security for EUR based methods)**.** *In QKD Protocol, let $\Omega(\vec{p})$ denote a well-defined event on the state $\rho_{\mathbf{SS}_B\widehat{C}_1^n C_{\mathrm{EC}}C_{\mathrm{EV}}H_{\mathrm{PA}}}$ just before privacy amplification. Therefore, $\Omega(\hat{c}_1^n,\vec{p})$ denotes well-defined events, where $\hat{c}_1^n$ denotes the value of the public announcement register $\widehat{C}_1^n$ in the protocol, and $\vec{p}$ denotes values that are not directly observed in the protocol. For every value of $\hat{c}_1^n$, let $\mathcal{V}(\hat{c}_1^n)$ be a set of possible values of $\vec{p}$.*

Let $\zeta(\hat{c}_1^n,\vec{p})\in[0,1)$ be such that the following bound on the smooth min entropy of the preamplification string holds,

$$H_{\min}^{\sqrt{\zeta(\hat{c}_1^n,\vec{p})}}(\mathbf{S}|\widehat{C}_1^n\hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n,\vec{p})}\geq\beta(\hat{c}_1^n)\qquad\qquad\forall\hat{c}_1^n,\forall\vec{p}\in\mathcal{V}(\hat{c}_1^n). \tag{6.1}$$

where the smoothing parameters $\zeta(\hat{c}_1^n,\vec{p})$ satisfy

$$\sum_{\hat{c}_1^n}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)}\Pr(\Omega(\hat{c}_1^n,\vec{p}))\zeta_{(\hat{c}_1^n,\vec{p})}+\sum_{\hat{c}_1^n}\sum_{\vec{p}\notin\mathcal{V}(\hat{c}_1^n)}\Pr(\Omega(\hat{c}_1^n,\vec{p}))\leq\varepsilon_{\mathrm{AT}}^2. \tag{6.2}$$

Let the output key length be given by

$$\ell(\hat{c}_1^n):=\max\left\{\left\lfloor\beta(\hat{c}_1^n)-\lambda_{\mathrm{EC}}(\hat{c}_1^n)-2\log\left(\frac{1}{\varepsilon_{\mathrm{PA}}}\right)-\left\lceil\log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil+2\right\rfloor,0\right\}. \tag{6.3}$$

Then QKD Protocol is $(2\varepsilon_{\mathrm{AT}}+\varepsilon_{\mathrm{PA}}+\varepsilon_{\mathrm{EV}})$-secure.

A typical use of this theorem is as follows. The bound on the smooth min entropy given by $\beta(\hat{c}_1^n)$ will depend on the phase error rate bound we obtain, via the entropic uncertainty relations. The value $\zeta(\hat{c}_1^n, \vec{p})$ will denote the probability of our computed phase error bound failing conditioned on observing $\hat{c}_1^n, \vec{p}$. Then, Eq. (6.2) is simply stating that we the probability that probability of the phase error rate bound failing is small. We have to include $\vec{p}$ since, our phase error rate bounds sometimes depend on statistics obtained from decoy-analysis, which are not known exactly, but instead estimated from $\hat{c}_1^n$.

6.2 Protocol Description and phase error rates

In this section we describe the protocol we study in this chapter. It is a specific instantiation of the Qubit BB84 protocol from Section 3.2.1, where we introduced specialized notation that is necessary for the EUR based analysis. This is due to the fact that EUR-based security proofs, as we shall see, are naturally suited to scenarios in which one basis (the X basis) is always used for testing, while the other basis (the Z basis) is always used for key generation, with a small sample potentially reserved for estimating the error-correction parameters. This stands in contrast to the protocol variations described in Section 3.2.1, which typically feature separate test and key-generation rounds, with both bases used in both types of rounds.[2]

We will first describe the protocol briefly, and then specify how it emerges as a specific instance of QKD Protocol. We consider a protocol where Alice prepares qubit states, but Bob uses threshold detectors for measurements.

1. **State Preparation:** Alice decides to send states in the basis Z (X) with probability $p_{(\mathsf{Z})}^{(A)}(p_{(\mathsf{X})}^{(A)})$. If she chooses the Z basis, she sends states $\{|0\rangle_{A'}, |1\rangle_{A'}\}$ with equal probability. If she chooses the X basis, she sends states $\{|+\rangle_{A'}, |-\rangle_{A'}\}$ with equal probability. Notice that this ensures

$$\rho_{A'|\mathsf{X}} = \frac{|+\rangle\langle+| + |-\rangle\langle-|}{2} = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \rho_{A'|\mathsf{Z}} = \frac{\mathbb{I}_{A'}}{2} \tag{6.4}$$

   where $\rho_{A'|b_A}$ denotes the the state sent out from Alice's lab given that she chooses a basis b_A. Essentially, Eq. (6.4) says that the Alice's signal states leak no information about the basis chosen by Alice. This can be shown rigorously as follows.

[2]We emphasize, however, that Theorem 6.1.1 itself remains completely general. The above restriction is imposed only at the level of the concrete protocol specification, as we now begin deriving explicit phase error rate bounds.

Using the source-replacement scheme [57, 142], Alice's signal preparation is equivalent to her first preparing the state $|\Psi_+\rangle = \frac{|00\rangle_{AA'}+|11\rangle_{AA'}}{\sqrt{2}}$ followed by measurements on the A system. Now, if Alice prepares the states from Eq. (6.4), her POVM elements corresponding to the basis b_A signal states sum to $p^{(A)}_{(b_A)}\mathbb{I}_A$. Because of this fact, one can view Alice's measurement process, *after* using the source-replacement scheme, as equivalent to choosing the basis $\mathsf{Z}(\mathsf{X})$ with probability $p^{(A)}_{(\mathsf{Z})}(p^{(A)}_{(\mathsf{X})})$, followed by measuring using the POVM $\{\Gamma^{(A)}_{(b_A,0)}, \Gamma^{(A)}_{(b_A,1)}\}$, for a given basis b_A. This reflects the fact that Eve has no knowledge of the basis used.

The POVM elements are given by

$$\begin{aligned} \Gamma^{(A)}_{(\mathsf{Z},0)} &= |0\rangle\langle 0|\,, \quad \Gamma^{(A)}_{(\mathsf{Z},1)} = |1\rangle\langle 1| \\ \Gamma^{(A)}_{(\mathsf{X},0)} &= |+\rangle\langle +|\,, \quad \Gamma^{(A)}_{(\mathsf{X},1)} = |-\rangle\langle -|\,. \end{aligned} \tag{6.5}$$

Therefore, we now have a setup where the state $\rho_{A^nB^n}$ is shared between Alice and Bob, followed by basis choice and measurements by Alice.

Remark 6.2.1. *Without loss of generality, one can always use the source-replacement scheme, and delay Alice's measurements until after Eve's attack has been completed, for any set of signal states. However, this process might result in POVM elements for Alice whose sum (for a specific basis) is not proportional to identity. In this case, Alice's measurements are incompatible with active basis choice after the source-replacement scheme. We utilize the fact that Alice implements active basis choice when using the EUR statement (Theorem 2.2.1), and in bounding the phase error rate (Sections 6.3 and 6.4). It is precisely for this reason that Eq. (6.4) is needed.*

We note that there exist many methods to address imperfect state preparation (Eq. (6.4) does not hold), [129, 127, 126, 128]. The approach there is fairly involved and involves a scenario where Alice prepares two different source-replaced states, depending on whether it is a Z round or a X round. In this chapter, we will always consider the simpler case outlined above, and focus our attention on detector imperfections.

2. **Measurement:** Bob chooses to measure in the $\mathsf{Z}(\mathsf{X})$ basis with probability $p^{(B)}_{(\mathsf{Z})}(p^{(B)}_{(\mathsf{X})})$. For each basis choice, Bob has two threshhold detectors, each of which can click or not-click. Bob maps double clicks to 0/1 randomly (this is essential, see Remark 6.2.2), and thus has 3 POVM elements in each basis b, which we denote using $\{\Gamma^{(B)}_{(b,\perp)}, \Gamma^{(B)}_{(b,0)}, \Gamma^{(B)}_{(b,1)}\}$ which correspond to the inconclusive-outcome, 0-outcome, and the 1-outcome. In this

work, we will use the following notation to write joint POVM elements,

$$\begin{aligned}
\Gamma_{(b_A,b_B),(i,j)} &\coloneqq \Gamma^{(A)}_{(b_A,i)} \otimes \Gamma^{(B)}_{(b_B,j)}, \\
\Gamma_{(b_A,b_B),(\neq)} &\coloneqq \Gamma^{(A)}_{(b_A,0)} \otimes \Gamma^{(B)}_{(b_B,1)} + \Gamma^{(A)}_{(b_A,1)} \otimes \Gamma^{(B)}_{(b_B,0)}, \\
\Gamma_{(b_A,b_B),(=)} &\coloneqq \Gamma^{(A)}_{(b_A,0)} \otimes \Gamma^{(B)}_{(b_B,0)} + \Gamma^{(A)}_{(b_A,1)} \otimes \Gamma^{(B)}_{(b_B,1)}, \\
\Gamma_{(b_A,b_B),(\perp)} &\coloneqq \mathbb{I}_A \otimes \Gamma^{(B)}_{(b_B,\perp)},
\end{aligned} \tag{6.6}$$

where Alice's POVMs are defined in Eq. (6.5), and Bob's in Section 6.6.2.

Remark 6.2.2. *As we will see in Section 6.3, the mathematical assumption on Bob's detector setup needed for phase error estimation is actually given by*

$$\Gamma^{(B)}_{(\mathsf{X},\perp)} = \Gamma^{(B)}_{(\mathsf{Z},\perp)}. \tag{6.7}$$

This means that the probability of a round being inconclusive (i.e discarded) is independent of the basis for all input states. Notice that Eq. (6.7) depends on the choice of classical post-processing on Bob's side. In particular, it can be trivially satisfied by mapping no-click and double-click events to 0 *and* 1 *randomly (so that* $\Gamma^{(B)}_{(\mathsf{X},\perp)} = \Gamma^{(B)}_{(\mathsf{Z},\perp)}$ *is zero). However, such a protocol cannot produce a key when loss is greater than* 50%*, and is therefore impractical. In general, if one assumes the canonical model of detectors (see Section 6.6.2), and maps double-clicks to 0/1 randomly, then Eq. (6.7) requires the loss and dark count rates in each detector-arm to be equal. This is why this condition is referred to as "basis-independent loss", and its violation is referred to as "detection-efficiency mismatch" in the literature. Note that even for identical detectors, one is forced remap double-click events to satisfy Eq. (6.7).*

3. **Classical Announcements and Sifting:** For all rounds, Alice and Bob announce the basis they used. Furthermore, Bob announces whether he got a conclusive outcome ($\{\Gamma^{(B)}_{(b,0)}, \Gamma^{(B)}_{(b,1)}\}$), or inconclusive ($\{\Gamma^{(B)}_{(b,\perp)}\}$). A round is said to be "conclusive" if Alice and Bob used the same basis, and Bob obtained a conclusive outcome.

   All rounds where Alice sent X are used for testing, and Alice and Bob announce their measurement outcomes. These rounds are used to estimate the phase error rate. We let n_{X} be the number of X basis conclusive rounds, and let $e^{\text{obs}}_{\mathsf{X}}$ be the observed error rate in these rounds.

   All rounds where Alice sent Z are used for key generation.[3] Rounds where no-detect

[3]Note that, in practice, a very small fraction of these rounds can be used to estimate the Z-basis error rate, which in turn can be used to determine $\lambda_{\text{EC}}(\mathbf{F}^{\text{obs}})$, the amount of error correction required. However, this sample need not be estimated accurately for the purposes of security, and therefore we may choose to use only a very small fraction of rounds for this purpose.

events occur are discarded, and one is left with n_{K} key generation rounds used for key generation.

All these classical announcements are stored in the register $\widehat{C}_1^n$, and $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}}, e_{\mathsf{X}}^{\text{obs}}, e_{\mathsf{Z}}^{\text{obs}})$ denotes the event that $n_{\mathsf{X}}, n_{\mathsf{K}}, e_{\mathsf{X}}^{\text{obs}}, e_{\mathsf{Z}}^{\text{obs}}$ values are observed in the protocol.

Remark 6.2.3. *In this chapter, we use bold letters, such as $\boldsymbol{x}$ to denote a classical random variable, and x to denote a particular value it takes. Furthermore, we will use $\Omega(x)$ to denote the event that $\boldsymbol{x} = x$. Thus our protocol involves random variables $\boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}}, \boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}$, which take values $n_{\mathsf{X}}, n_{\mathsf{K}}, e_{\mathsf{X}}^{\text{obs}}, e_{\mathsf{X}}^{\text{key}}$ in any given run.*

We use $\ell(n_{\mathsf{X}}, n_{\mathsf{K}}, e_{\mathsf{X}}^{\text{obs}}, e_{\mathsf{Z}}^{\text{obs}})$ to denote the key length, and $\lambda_{\text{EC}}(n_{\mathsf{X}}, n_{\mathsf{K}}, e_{\mathsf{X}}^{\text{obs}}, e_{\mathsf{Z}}^{\text{obs}})$ to denote the error-correction protocol parameter in this thesis, with the understanding that $n_{\mathsf{X}}, n_{\mathsf{K}}, e_{\mathsf{X}}^{\text{obs}}, e_{\mathsf{Z}}^{\text{obs}}$ is obtained from $\hat{c}_1^n$.

The above protocol is a specific instantiation of QKD Protocol, and the various probabilities can be related via simple algebraic manipulation. In particular:

- $\Pr(\texttt{test})$ in QKD Protocol is equal to $p_{(\mathsf{X})}^{(A)}$.
- $\Pr(a|\texttt{test}) = \frac{1}{2}$ in QKD Protocol whenever a corresponds to a X basis state, and $\Pr(a|\texttt{test}) = 0$ whenever a corresponds to Z basis state.
- $\Pr(a|\texttt{gen}) = \frac{1}{2}$ in QKD Protocol if a corresponds to a Z basis state, and 0 otherwise.

6.2.1 Requirements on phase error estimation

We now turn our attention to the phase error rate. Note that in a QKD protocol, one starts with a fixed but unknown state $\rho_{A^n B^n \hat{\boldsymbol{E}}}$ that represents Eve's attack. As the protocol evolves, we get n_{K} states where Alice and Bob measured in the Z basis, and Bob got a detection event. The phase error rate is defined by the error rate in these rounds, if Alice and Bob instead choose to measure these rounds in the complementary X basis. Describing this formally requires viewing measurements by Alice and Bob as multi-step measurements, and is undertaken throughout this chapter.

In this way, the state gives rise to random variables $\boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}}, \boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}$. Here $\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}$ denotes the random variable corresponding to the phase error rate in the key generation rounds, when Alice and Bob measure those rounds (virtually) in the X basis. (The phase error rate is explained in greater detail in Sections 6.3 and 6.4). To obtain security, one must obtain

a high probability upper bound on the phase error rate $\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}$. We assume that one has a way to obtain the following statement (which we prove in Sections 6.3 and 6.4):

$$\Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}})\right) \leq \varepsilon_{\mathrm{AT}}^2. \tag{6.8}$$

This states that the phase error rate is upper bounded (with high probability) by a suitable function $\mathcal{B}_{\delta_1,\delta_2}$ of the observed error rate in the X basis rounds, and the number of test and key generation rounds. We will obtain a suitable $\mathcal{B}_{\delta_1,\delta_2}$ satisfying Eq. (6.8) in Sections 6.3 and 6.4, with and without the basis-independent loss assumption. The function $\mathcal{B}_{\delta_1,\delta_2}$ depends on the metrics δ_1, δ_2 that quantify the deviation from ideal behavior for a given protocol description.

Remark 6.2.4. *When working with random variables that are obtained via measurements on quantum states, the joint distributions of random variables can only be specified when those random variables can exist at the same time, via some physical measurements on the state. For example, one cannot speak of the joint distribution of* X *and* Z *measurement outcomes on the same state, since such a joint distribution does not exist. In the entirety of this thesis, all the random variables whose joint distribution is used in our arguments can indeed exist at the same time.*

Given an upper bound on the phase error rate (Eq. (6.8)), we have the following theorem regarding the variable-length security of the QKD protocol described above, which follows from the bound Eq. (6.8) and Theorem 6.1.1 and the EUR statement [44].

Theorem 6.2.1. *Consider QKD Protocol with the details as specified in Section 6.2. Suppose that the phase error rate bound from Eq. (6.8) holds, and the protocol produces an output key of length*

$$\begin{aligned} l(\hat{c}_1^n) \coloneqq \max\Bigg(0, \\ \left\lfloor n_K \left(1 - h\left(\mathcal{B}_{\delta_1,\delta_2}(e_{\mathsf{X}}^{\mathrm{obs}}, n_{\mathsf{X}}, n_{\mathsf{K}})\right)\right) - \lambda_{\mathrm{EC}}(\hat{c}_1^n) - 2\log(1/\varepsilon_{\mathrm{PA}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil + 2 \right\rfloor \Bigg). \end{aligned} \tag{6.9}$$

Then the QKD protocol is $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}})$*-secret, and* $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}} + \varepsilon^{\mathrm{correct}})$*-secure.*

Proof. For this proof, we will not need to consider the $\vec{p}$ from Theorem 6.1.1.[4] We define $\zeta(\hat{c}_1^n)$ to be the probability that the phase error bound fails, *conditioned* on $\Omega(\hat{c}_1^n)$, i.e,

$$\zeta(\hat{c}_1^n) = \Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}}) | \Omega(\hat{c}_1^n)\right), \tag{6.10}$$

[4]Formally, we can simply set $\vec{p}$ to be a dummy variable that always takes fixed value, and $\mathcal{V}(\hat{c}_1^n)$ to always be a set containing that fixed value.

Then, the Eq. (6.2) is satisfied since the overall probability of the phase error bound failing is small (from Eq. (6.8)). Further, we set $\beta(\hat{c}_1^n) = n_{\mathsf{K}}\left(1 - h(\mathcal{B}_{\delta_1,\delta_2}(e_{\mathsf{X}}^{\text{obs}}, n_{\mathsf{X}}, n_{\mathsf{K}}))\right)$, which ensures that $\ell(\hat{c}_1^n)$ form Eq. (6.9) matches the specification from Theorem 6.1.1 (see Eq. (6.3)).

Thus, we only need to prove that $\beta(\hat{c}_1^n)$ lower bounds the smooth min entropy as as described in Eq. (6.1).

To do so, focus on the state $\rho_{A_1^{n_{\mathsf{K}}} B_1^{n_{\mathsf{K}}} \widehat{C}_1^n \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n)}$, which is the state on the detected key generation rounds. This state can be obtained by transforming Bob's measurement procedure to consist of two steps, and then only implementing the first step measurement which determines the detect vs no-detect outcome. Such a state can be rigorously obtained using Lemma 6.3.1. For the purposes of this proof, we only need the fact that it is well defined. We will obtain a bound on the smooth min entropy of the key generated from this state.

Suppose Alice measures her n_{K} systems in the Z basis (this is what happens in the actual protocol). The post-measurement state is given by $\rho_{\mathbf{S} B_1^{n_{\mathsf{K}}} \widehat{C}_1^n \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n)}$. Suppose she measures it in the X basis, and let the post-measurement state be given by $\rho^{\text{virt}}_{\widetilde{\mathbf{S}} B_1^{n_{\mathsf{K}}} \widehat{C}_1^n \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n)}$. This X measurement is not actually done in the protocol, and is only required for the theoretical proof. Using the entropic uncertainty relation [44] (see Theorem 2.2.1), we can relate the smooth min and max entropies $\left(\text{with smoothing parameter } \sqrt{\zeta(\hat{c}_1^n)}\right)$ of the two states obtained via Z and X measurements as

$$H_{\min}^{\sqrt{\zeta(\hat{c}_1^n)}}(\mathbf{S}|\widehat{C}_1^n \hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n)} + H_{\max}^{\sqrt{\zeta(\hat{c}_1^n)}}(\widetilde{\mathbf{S}}|B_1^{n_{\mathsf{K}}})_{\rho^{\text{virt}}|\Omega(\hat{c}_1^n)} \geq n_{\mathsf{K}} c_q. \tag{6.11}$$

where $c_q := \log\left(\frac{1}{\max_{i,j} \left\|\Gamma^{(A)}_{(\mathsf{X},i)} \Gamma^{(A)}_{(\mathsf{Z},j)}\right\|_\infty^2}\right)$[5]. We have deliberately chosen an appropriate smoothing parameter in the above equation.

Remark 6.2.5. *Notice that the value of c_q only depends on the POVM's used by Alice, after using the source-replacement scheme, and is equal to 1 in this work. Thus, we set $c_q = 1$ in the remainder of this work. Moreover, directly using the EUR in this context requires Alice to implement an active basis choice measurement, which requires perfect signal state preparation. However, as stated earlier, several techniques of dealing with imperfect source preparation exist.*

[5]We need to apply the entropic uncertainty relations on the n_{K} round measurements. However, for IID measurements, this can be then simplified easily to be n_{K} times the computation for a single round measurement

We now wish so simply the max entropy term in the above expressions. We can make Bob measure his systems B in the X basis to obtain the classical outcome $Y_1^{n_\mathsf{K}}$. Then, using data processing Lemma 2.2.10 , we obtain

$$\begin{aligned} &H_{\min}^{\sqrt{\zeta(\hat{c}_1^n)}}(\mathbf{S}|\widehat{C}_1^n\hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n)} \\ +&H_{\max}^{\sqrt{\zeta(\hat{c}_1^n)}}(\widetilde{\mathbf{S}}|Y_1^{n_\mathsf{K}})_{\rho^{\text{virt}}|\Omega(\hat{c}_1^n)} \geq n_\mathsf{K}. \end{aligned} \tag{6.12}$$

Recall that we have a probabilistic upper bound on $\boldsymbol{e}_\mathbf{X}^{\mathbf{key}}$ (the error rate in $\widetilde{\mathbf{S}}, Y_1^{n_\mathsf{K}}$) conditioned on the event $\Omega(\hat{c}_1^n)$. This bound fails with probability $\zeta(\hat{c}_1^n)$ (see Eq. (6.10)). Thus, using Lemma C.2.2 along with this fact, we obtain:

$$H_{\max}^{\sqrt{\zeta(\hat{c}_1^n)}}(\widetilde{\mathbf{S}}|Y_1^{n_\mathsf{K}})_{\rho^{\text{virt}}|\Omega(\hat{c}_1^n)} \leq n_\mathsf{K} h\left(\mathcal{B}_{\delta_1,\delta_2}(e_\mathsf{X}^{\text{obs}}, n_\mathsf{X}, n_\mathsf{K})\right), \tag{6.13}$$

which along with Eq. (6.12) gives us

$$H_{\min}^{\sqrt{\zeta(\hat{c}_1^n)}}(\mathbf{S}|\widehat{C}_1^n\hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n)} \geq n_\mathsf{K}(1 - h\left(\mathcal{B}_{\delta_1,\delta_2}(e_\mathsf{X}^{\text{obs}}, n_\mathsf{X}, n_\mathsf{K})\right)). \tag{6.14}$$

This is the required bound on the smooth min entropy of the raw key, where the RHS is exactly what we have defined to be $\beta(\hat{c}_1^n)$. This concludes the proof. □

Thus all that is left to do is obtain the required bound on the phase error rate.

6.3 Phase error estimation for BB84 with perfect detectors

We will now prove Eq. (6.8) for an implementation that satisfies the basis-independent loss assumption. It is useful to refer to Fig. 6.2 for this section. To prove Eq. (6.8), we will need to modify the actual protocol to an equivalent protocol (in the sense of being the same quantum to classical channel). To do so we will use Lemma 6.3.1 below to reformulate Alice and Bob's measurements to consist of two steps. The first step will implement a basis-*independent* filtering operation that discards the inconclusive outcomes, while the second step will complete the measurement procedure. Then the required claim will follow from random sampling arguments on the second step measurements. We start by explaining the two-step protocol measurements.

6.3.1 Protocol Measurements

We will first use the following lemma to divide Alice and Bob's measurement procedure into two steps. For the proof, we refer the reader to Appendix. C.

Lemma 6.3.1 (Filtering POVMs)**.** *Let $\{\Gamma_k | k \in \mathcal{A}\}$ be a POVM on a register Q, and let $\{\mathcal{A}_i\}_{i \in \mathcal{P}_\mathcal{A}}$ be a partition of $\mathcal{A}$, and let $\rho \in \mathrm{S}_=(Q)$ be a state. The classical register storing the measurement outcomes when ρ is measured using $\{\Gamma_k\}_{k \in \mathcal{A}}$ is given by*

$$\rho_{\text{final}} \coloneqq \sum_{k \in \mathcal{A}} \mathrm{Tr}(\Gamma_k \rho) \, |k\rangle\langle k| \, . \tag{6.15}$$

This measurement procedure is equivalent (in the sense of being the same quantum to classical channel) to the following two-step measurement procedure: First doing a coarse-grained "filtering" measurement of i, using POVM $\{\tilde{F}_i\}_{i \in \mathcal{P}_\mathcal{A}}$, where

$$\begin{aligned} \tilde{F}_i &\coloneqq \sum_{j \in \mathcal{A}_i} \Gamma_j, \qquad \textit{leading to the post-measurement state} \\ \rho'_{\text{intermediate}} &= \sum_{i \in \mathcal{P}_\mathcal{A}} \sqrt{\tilde{F}_i} \rho \sqrt{\tilde{F}_i}^\dagger \otimes |i\rangle\langle i| \, . \end{aligned} \tag{6.16}$$

Upon obtaining outcome i in the first step, measuring using POVM $\{G_k\}_{k \in \mathcal{A}_i}$ where

$$\begin{aligned} G_k &\coloneqq \sqrt{\tilde{F}_i}^+ \Gamma_k \sqrt{\tilde{F}_i}^+ + P_k \qquad \textit{leading to the post-measurement classical state} \\ \rho'_{\text{final}} &= \sum_{i \in \mathcal{P}_\mathcal{A}} \sum_{k \in \mathcal{A}_i} \mathrm{Tr}\left(G_k \sqrt{\tilde{F}_i} \rho \sqrt{\tilde{F}_i} \right) |k\rangle\langle k| \, , \end{aligned} \tag{6.17}$$

where F^+ denotes the pseudo-inverse of F, and P_k are any positive operators satisfying $\sum_{k \in \mathcal{A}_i} P_k = \mathbb{I} - \Pi_{\tilde{F}_i}$, where $\Pi_{\tilde{F}_i}$ denotes the projector onto the support of $\tilde{F}_i$.

Consider the POVMs $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ defined in Eq. (6.6), which correspond to Bob obtaining a conclusive outcome and Alice and Bob obtaining an error, Bob obtaining a conclusive outcome and Alice and Bob not obtaining an error, and Bob obtaining an inconclusive outcome respectively, for basis choices b_A, b_B. Without loss of generality, we can use Lemma 6.3.1 to equivalently describe Alice and Bob's measurement procedure as consisting of two steps.

1. First, they measure using POVM $\{\tilde{F}_{(b_A,b_B),(\text{con})}, \tilde{F}_{(b_A,b_B),(\perp)}\}$ which determines whether they obtain a conclusive and inconclusive measurement outcome.

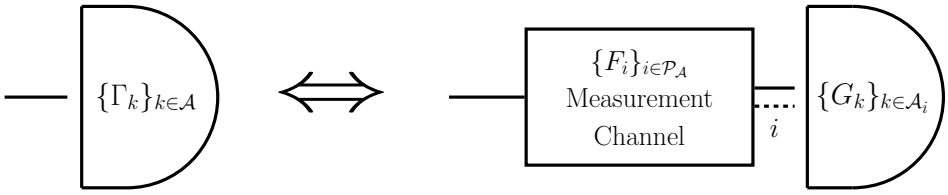


Figure 6.1: Schematic for the two-step measurement procedure from Lemma 6.3.1. Note that the second step measurement $\{G_k\}_{k\in\mathcal{A}_i}$ depends on the outcome of the first step measurement.

2. Then, if they obtain a conclusive outcome, they measure using a second POVM $\{G^{\text{con}}_{(b_A,b_B),(=)}, G^{\text{con}}_{(b_A,b_B),(\neq)}\}$.

We use the convention that whenever an explicit basis (X/Z) is written in the subscript of these POVMs, it refers to the basis used by both Alice and Bob. We refer to the first-step measurements as "filtering" measurements, since they determine whether Bob gets a conclusive outcome (which may be kept or discarded depending on basis choice), or an inconclusive outcome (which is always discarded). Furthermore, due to the construction of the POVM from Lemma 6.3.1, we have

$$\tilde{F}_{(b_A,b_B),(\perp)} = \mathbb{I}_A \otimes \Gamma^{(B)}_{(b_B,\perp)}. \tag{6.18}$$

6.3.2 Constructing Equivalent Protocol

We will now construct an equivalent protocol that is described in Fig. 6.2.

1. If one has $\Gamma^{(B)}_{(\mathsf{X},\perp)} = \Gamma^{(B)}_{(\mathsf{Z},\perp)}$, then we find that the filtering measurements $\tilde{F}_{(b_A,b_B),(\text{con})}$ is independent of the basis choices (b_A, b_B). Let this basis-independent POVM element be $\tilde{F}$. If the filtering measurement does not depend on the basis choice, then implementing the basis choice followed by filtering measurement is the same as implementing the filtering measurement followed by basis choice. Thus, we can delay basis choice until after the filtering measurements have been performed. This can also be formally argued using Lemma 6.3.1. This allows us to obtain the first node of Fig. 6.2, where we measure using $\{\tilde{F}, \mathbb{I} - \tilde{F}\}$.

2. This is then followed by random basis choices and assignment to test vs key by Alice and Bob. All X basis rounds are used for testing, while almost all Z basis rounds are used for key generation (and a small fraction is used to estimate $e^{\text{obs}}_{\mathsf{Z}}$). Thus, we get

the second node of Fig. 6.2. Note that the estimate $e_{\mathsf{Z}}^{\text{obs}}$ of the error rate in the key bits is only used to determine the amount of error-correction required and does not affect the secrecy of the protocol. However, $e_{\mathsf{Z}}^{\text{obs}}$ and the choice of error-correction protocol is important to ensure that error-verification succeeds with high probability.

3. The n_{X} testing rounds are measured using $\{G^{\text{con}}_{(\mathsf{X}),(=)}, G^{\text{con}}_{(\mathsf{X}),(\neq)}\}$, and the error rate in these rounds is denoted by $e_{\mathsf{X}}^{\text{obs}}$. This is the error rate we observe. This is the **Testing (X)** node of Fig. 6.2.

4. The n_{K} key generation rounds can be measured (virtually) using the same POVM $\{G^{\text{con}}_{(\mathsf{X}),(=)}, G^{\text{con}}_{(\mathsf{X}),(\neq)}\}$. The error rate in these rounds is denoted by $e_{\mathsf{X}}^{\text{key}}$ and is the phase error rate we wish to estimate. This is the **Key (X)** node of Fig. 6.2.

5. The actual n_{K} key generation rounds are measured in the Z basis to obtain the raw key. This is the **Key (Z)** node of Fig. 6.2.

6.3.3 Sampling

We will now turn our attention to the sampling part of the argument, and obtain an estimate $\mathcal{B}_{0,0}$ on the phase error rate that satisfies Eq. (6.8). To do so, we will make use of the following Lemma, which uses the Serfling bound [143]. For the proof, we refer the Appendix. C.3.1.

Lemma 6.3.2 (Serfling with IID sampling)**.** *Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_n$ be bit-valued random variables. Suppose each position i is mapped to the "test set" ($i \in \boldsymbol{J}_t$) with probability p_t, and the "key set" ($i \in \boldsymbol{J}_k$) with probability p_k. Let $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$ be the event that exactly n_{X} positions are mapped to test, and exactly n_{K} positions are mapped to key. Then, conditioned on the event $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$, the following statement is true:*

$$\Pr\left(\sum_{i\in\boldsymbol{J}_k}\frac{\boldsymbol{X}_i}{n_{\mathsf{K}}} \geq \sum_{i\in\boldsymbol{J}_t}\frac{\boldsymbol{X}_i}{n_{\mathsf{X}}} + \gamma_{\text{serf}}\right)_{|\Omega(n_{\mathsf{X}},n_{\mathsf{K}})} \leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(n_{\mathsf{X}},n_{\mathsf{K}})}, \tag{6.19}$$

$$f_{\text{serf}}(n_{\mathsf{X}}, n_{\mathsf{K}}) := \frac{n_{\mathsf{K}} n_{\mathsf{X}}^2}{(n_{\mathsf{K}}+n_{\mathsf{X}})(n_{\mathsf{X}}+1)}.$$

To use the lemma, we will identify $X_i = 1$ with error, and $X_i = 0$ with the no-error outcome, when the conclusive rounds are measured in the X basis. The test data will correspond to $e_{\mathsf{X}}^{\text{obs}}$, whereas the key data will correspond to $e_{\mathsf{X}}^{\text{key}}$.

Remark 6.3.1. *There are two important aspects to the sampling argument. First, the Serfling bound applies in the situation where one chooses a random subset of fixed-length for testing. However, the above procedure (and many QKD protocols) randomly assigns each round to testing vs key generation. Thus, Serfling must be applied with some care, and that is what is done here*[6]*. This observation has been missing in many prior works. Second, since we are interested in a variable-length protocol, we require slightly different statements than standard fixed-length security proofs (Eq. (6.8)). However, these can also be obtained by simple (almost trivial) modifications to existing arguments and yield the same results as before. Both these issues are addressed in the proof of Lemma 6.3.2 in Section C.3.*

Let us consider the second node in the equivalent protocol constructed in Fig. 6.2, where rounds are now randomly assigned for testing (X basis) or key generation (Z basis and key generation). (The remaining rounds are used for estimating the Z basis error rate or discarded and are unimportant for this discussion). Consider the state $\rho_{|\Omega(n_{\mathsf{X}},n_{\mathsf{K}})}$, where the number of rounds to be used to testing and key generation is fixed. Using Lemma 6.3.2 on this state, we obtain

$$\Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}} + \gamma_{\text{serf}}\right)_{|\Omega(n_{\mathsf{X}},n_{\mathsf{K}})} \leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(n_{\mathsf{X}},n_{\mathsf{K}})}, \tag{6.20}$$

Furthermore we can choose

$$\gamma_{\text{serf}}^{\varepsilon_{\text{AT}}}(n_{\mathsf{X}},n_{\mathsf{K}}) \coloneqq \sqrt{\frac{\ln(1/\varepsilon_{\text{AT}}^2)}{2f_{\text{serf}}(n_{\mathsf{X}},n_{\mathsf{K}})}} \implies e^{-2\left(\gamma_{\text{serf}}^{\varepsilon_{\text{AT}}}(n_{\mathsf{X}},n_{\mathsf{K}})\right)^2 f_{\text{serf}}(n_{\mathsf{X}},n_{\mathsf{K}})} = \varepsilon_{\text{AT}}^2. \tag{6.21}$$

Thus we can choose

$$\mathcal{B}_{0,0}(e_{\mathsf{X}}^{\text{obs}}, n_{\mathsf{X}}, n_{\mathsf{K}}) = e_{\mathsf{X}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT}}}(n_{\mathsf{X}}, n_{\mathsf{K}}) \tag{6.22}$$

to be our bound for the phase error rate, where the $(0,0)$ subscript indicates that the bound is only valid when there is no deviation from basis-independent loss. Finally, since the bound is valid for any event $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$, we can get rid of this conditioning in Eq. (6.20), to obtain Eq. (6.8) via

$$\begin{aligned}
\Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \mathcal{B}_{0,0}(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}})\right) &= \sum_{n_{\mathsf{X}},n_{\mathsf{K}}} \Pr(\Omega(n_{\mathsf{X}},n_{\mathsf{K}}))\Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \mathcal{B}_{0,0}(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, n_{\mathsf{X}}, n_{\mathsf{K}})\right)_{|\Omega(n_{\mathsf{X}},n_{\mathsf{K}})} \\
&\leq \sum_{n_{\mathsf{X}},n_{\mathsf{K}}} \Pr(\Omega(n_{\mathsf{X}},n_{\mathsf{K}}))\varepsilon_{\text{AT}}^2 \\
&= \varepsilon_{\text{AT}}^2
\end{aligned} \tag{6.23}$$

[6]It is also worthwhile to note that if one is interested in estimating the QBER *independent* of basis, then the standard serfling argument is directly applicable (for instance in [34]).

Thus, for the above choice of $\mathcal{B}_{0,0}(e_{\mathsf{X}}^{\text{obs}}, n_{\mathsf{X}}, n_{\mathsf{K}})$, the variable-length security of the protocol follows from Theorem 6.2.1.

6.4 Phase error estimation for BB84 with imperfect detectors

In this section, we will prove Eq. (6.8) for an implementation that *does not satisfy* the basis-independent loss assumption. The argument is similar to the one presented in Section 6.3, with important additions. It is helpful to refer to Fig. 6.3 for this section. We will first explain the idea behind the proof, before stating the proof itself.

Proof Idea

We will use Lemma 6.3.1 in Section 6.4.1 to construct an equivalent measurement procedure (in the sense that it is the same quantum to classical channel) for the protocol, which consists of three steps. The first step measurement is done using the POVM $\{\tilde{F}, \mathbb{I} - \tilde{F}\}$ and implements basis-*independent* filtering (discarding) operations. ($\tilde{F}$ here plays the same role as in Section 6.3, but is defined differently). In particular it is the largest common filtering operation over both basis choices.

Due to basis-efficiency mismatch, we will have a second step measurement that implements filtering operations that depend on the basis choice. (This will typically result in a small number of discards for a small amount of basis-dependent loss in the detectors). Once both filtering steps are done, the measurements on the remaining rounds can be completed using the third step measurements which determines the exact measurement outcomes on the detected rounds.

Turning our attention to Fig. 6.3, the state first undergoes the basis-independent filtering measurement in the first node. This is then followed by random basis choice and assignment to testing and key generation at the second node. The testing rounds are further measured using second step X basis filtering POVM and third step X basis POVM at the **Testing* ($\mathbf{X} \to \mathbf{X}$)** node. Similarly, the key generation rounds are measured using second step Z basis filtering POVM and third step Z basis POVM. Note that we use $(b_{\text{2nd}} \to b_{\text{3rd}})$ to denote the basis choice b_{2nd} for the second step filtering measurement, and basis choice b_{3rd} for the third step measurement, for both Alice and Bob.

We will consider virtual measurements on the key generation rounds corresponding to $\mathbf{X} \to \mathbf{X}$ and $\mathbf{Z} \to \mathbf{X}$. These are represented using dotted boxes and lines in the figure. These

measurements are not performed in the protocol, but are only required in our proof. We will then associate an error rate with all these choices of measurements, which corresponds to the number of rounds that resulted in an error divided by the total number of rounds on which the measurements were done.

We see a variety of error rates in Fig. 6.3. These errors are classified based on three criteria:

1. The basis used by Alice *and* Bob in the second and third step measurements (written in the subscript),
2. Whether the $\perp$s due to the second step measurements have been discarded from the total number of rounds or not (e vs $\tilde{e}$),
3. Whether they were done on testing rounds (obs in superscript), or key generation rounds (key in superscript).

The proof will follow by building a connection from our observed error rate ($e_{\mathsf{X}}^{\text{obs}}$), to the phase error rate ($e_{\mathsf{X}}^{\text{key}}$). These connections are highlighted using curved blue arrows in the figure. Note that we only observe the error rate $e_{\mathsf{X}}^{\text{obs}}$ in the protocol.

In particular, we will relate the error rates before and after discarding for the testing rounds ($\tilde{e}_{\mathsf{XX}}^{\text{obs}} \leftrightarrow e_{\mathsf{X}}^{\text{obs}}$) by simply noting that we discard rounds in the second-step measurements. On the other hand, we will relate $\tilde{e}_{\mathsf{ZX}}^{\text{key}} \leftrightarrow e_{\mathsf{X}}^{\text{key}}$ by bounding the number of discards that can happen in the second step filtering measurements. This relation will depend on δ_2, which will be the metric that quantifies the "smallness" of the POVM element corresponding to the discard outcome. $\tilde{e}_{\mathsf{XX}}^{\text{obs}}$ and $\tilde{e}_{\mathsf{XX}}^{\text{key}}$ correspond to error rates corresponding to exactly the same measurement, and assigned to test vs key randomly. Thus, they can be related using Serfling (Lemma 6.3.2), exactly as in Section 6.3. $\tilde{e}_{\mathsf{XX}}^{\text{key}}$ and $\tilde{e}_{\mathsf{ZX}}^{\text{key}}$ correspond to error rates on the same state, but with slightly different POVMs, and thus are expected to be similar. This can be rigorously argued using Lemma 6.4.1, where we use δ_1 to quantify the "closeness" of these POVMs. Combining all these relations, we will ultimately obtain Eq. (6.42).

We will now convert the above sketch into a rigorous proof. We start by explaining the three step protocol measurements.

6.4.1 Protocol Measurements

Fix the basis b_A, b_B used by Alice and Bob. As in Section 6.3.1, consider the POVM $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ defined in Eq. (6.6), which correspond to Bob obtaining

a conclusive outcome (and Alice and Bob obtaining an error), Bob obtaining a conclusive outcome (and Alice and Bob not obtaining an error), and Bob obtaining an inconclusive outcome respectively. Since $\Gamma_{(b_A,b_B),(\perp)}$ now depends on the basis choices, we cannot proceed in the same way as before. This reflects the fact that the discarding is basis dependent. Thus we will reformulate the measurement process in a different way.

To do so, consider a $\tilde{F}$ such that

$$\tilde{F} \geq \Gamma_{(b_A,b_B),(=)} + \Gamma_{(b_A,b_B),(\neq)} \quad \forall (b_A, b_B) \tag{6.24}$$

This $\tilde{F}$ will play the role of a common "basis-independent filtering measurement". While any choice satisfying the above requirement will suffice, for the best results, $\tilde{F}$ must fulfil Eq. (6.24) as tightly as possible.

Remark 6.4.1. *Since basis-mismatch rounds are discarded anyway, it is possible to argue that we only need $\tilde{F}$ to satisfy $\Gamma_{(b_A,b_B),(=)} + \Gamma_{(b_A,b_B),(\neq)} \leq \tilde{F}$ for $b_A = b_B$. This involves constructing a slightly different equivalent protocol where the first node decides basis match vs mismatch. The basis match events then undergo the usual filtering followed by basis choice, while the mismatch events are discarded without any filtering. If this modified requirement results in a value of $\tilde{F}$ that is "smaller" then the original choice, then this will lead to tighter key rates. Intuitively, this is due to the fact that a smaller value of $\tilde{F}$ means that more loss is attributed to the basis-independent filtering.*

To reformulate the measurement procedure, start by considering the four-outcome POVM given by $\{\mathbb{I} - \tilde{F}, \tilde{F} - \Gamma_{(b_A,b_B),(=)} - \Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\neq)}\}$, where the first two outcomes correspond to discard, the third correspond to a conclusive no-error outcome, and the fourth corresponds to a conclusive error. This four-outcome measurement followed by classical grouping of the first two outcomes is then equivalent to the original three-outcome measurement in the protocol.

Now, we can use Lemma 6.3.1 to reformulate the four-outcome measurement as occurring in two steps. In the first step, Alice and Bob measure using POVM $\{\tilde{F}, \mathbb{I}-\tilde{F}\}$ and discard the latter outcomes. If they obtain the $\tilde{F}$ outcome, they then complete the measurement using POVM $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$, corresponding to discard, conclusive no-error and conclusive error outcomes respectively.

We then use Lemma 6.3.1 again to reformulate this three-outcome measurement to consist of two steps. First, they measure using $\{F_{(b_A,b_B),(\text{con})}, F_{(b_A,b_B),(\perp)}\}$ which determines whether they obtain a conclusive or inconclusive measurement outcome. Then, if they obtain a conclusive outcome, they measure using the POVM $\{G^{\text{con}}_{(b_A,b_B),(=)}, G^{\text{con}}_{(b_A,b_B),(\neq)}\}$. Thus we now have a three-step measurement procedure, described in Table 6.1.

Since basis-mismatch signals are anyway discarded in the protocol, from this point onwards, we will only be concerned with POVMs that correspond to Alice and Bob choosing the same basis. As before, we will use the convention that whenever a basis is explicitly written as X/Z (or denoted using $b_1 b_2$), it represents *both* Alice and Bob's basis choices.

It will be convenient to recombine the second and third step measurement into a single measurement step with three outcomes. For brevity we introduce the following notation to write this POVM $\{G^{\text{con,F}}_{(b_1b_2),(\neq)}, G^{\text{con,F}}_{(b_1b_2),(=)}, \mathbb{I} - F_{(b_1),(\text{con})}\}$ where

$$\begin{aligned} G^{\text{con,F}}_{(b_1b_2),(\neq)} &= \sqrt{F_{(b_1),(\text{con})}}\, G^{\text{con}}_{(b_2),(\neq)} \sqrt{F_{(b_1),(\text{con})}}, \\ G^{\text{con,F}}_{(b_1b_2),(=)} &= \sqrt{F_{(b_1),(\text{con})}}\, G^{\text{con}}_{(b_2),(=)} \sqrt{F_{(b_1),(\text{con})}}. \end{aligned} \tag{6.25}$$

where the subscript b_1b_2 determines the basis for the second step and third step measurements by *both* Alice and Bob, and the superscript F indicates the merging of the two measurement steps. (Note that if $b_1 = b_2 = b$, then this simply reverses the earlier action of Lemma 6.3.1 that split $\{\tilde{F}_{(b,b),(\perp)}, \tilde{F}_{(b,b),(=)}, \tilde{F}_{(b,b),(\neq)}\}$ to generate the second and third-step measurements. However, we will consider fictitious measurements where $b_1 \neq b_2$ in our proof. To describe such measurements, it is indeed necessary to split $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$ into two separate steps.)

Symbol	Meaning
$\{\tilde{F}, \mathbb{I} - \tilde{F}\}$	First step measurement. Implements basis-independent filter.
$\{F_{(b_A,b_B),(\text{con})}, \mathbb{I} - F_{(b_A,b_B),(\text{con})}\}$.	Second step measurement. Implements filtering that is basis dependent.
$\{G^{\text{con}}_{(b_A b_B),(=)}, G^{\text{con}}_{(b_A b_B),(\neq)}\}$	Third step measurement corresponding to no-error and error.
$\{G^{\text{con,F}}_{(b_1 b_2),(\neq)}$, $G^{\text{con,F}}_{(b_1 b_2),(=)}, \mathbb{I} - F_{(b_1),(\text{con})}\}$	Combined second and third step measurement, corresponding to no-error, error and discard.
$\tilde{n}_{\mathsf{X}}$	Number of testing rounds after basis-independent filter only
$\tilde{n}_{\mathsf{K}}$	Number of key generation rounds after basis-independent filter only
n_{X}	Actual number of testing rounds
n_{K}	Actual number of key generation rounds

Table 6.1: Different symbols used in our proof. Note that b_A, b_B refer to basis choice of Alice and Bob. However, b_1, b_2 refer to the basis used by *both* Alice and Bob, for the second and third step measurements. Whenever a basis is explicitly written as X/Z (or b_1, b_2) it represents *both* Alice and Bob's basis choices.

6.4.2 Constructing an equivalent protocol

We will now construct the equivalent protocol from Fig. 6.3. The construction is similar to the one from Section 6.3.2, albeit with some important modifications.

1. As in Section 6.3.2, we observe that the first step measurement is conducted using $\{\tilde{F}, \mathbb{I} - \tilde{F}\}$ and is independent of basis. Therefore, we can delay basis choice until after this measurement has been completed, and the $\mathbb{I} - \tilde{F}$ outcomes are discarded. That is the first node of Fig. 6.3.

2. The remaining rounds undergo random basis choice. Basis mismatch rounds are discarded, all X basis rounds are used for testing, while Z basis rounds are used for key generation (with a tiny sample used for estimating $e^{\text{obs}}_{\mathsf{Z}}$). This allows us to obtain the second node of Fig. 6.3. Again, as in Section 6.3.2, the estimate we obtain on $e^{\text{obs}}_{\mathsf{Z}}$

does not affect the secrecy claim of the protocol, since $e_{\mathsf{Z}}^{\text{obs}}$ is only used to determine the amount of error-correction to be performed.

Note that unlike Section 6.3.2, we have to perform *two* measurements on the testing and key generation rounds after the second node, and these rounds are *not* guaranteed to result in a conclusive outcome. We describe these measurements in detail below.

Testing Rounds after basis-independent Filter

We will now complete the measurement steps on the test rounds (which take place in the **Testing* ($\mathbf{X} \to \mathbf{X}$)** box in Fig. 6.3). Let us consider the X basis rounds used for testing at this stage. Let $\tilde{n}_{\mathsf{X}}$ be the number of such rounds. Note that some of these rounds will be discarded during the remainder of the protocol, and therefore we do not know the value of $\tilde{n}_{\mathsf{X}}$ in the actual protocol. However, we will see that we do not need to.

These rounds must undergo the second step filtering measurement using $\{F_{(\mathsf{X}),(\text{con})}, \mathbb{I} - F_{(\mathsf{X}),(\text{con})}\}$, where the rounds which yield the latter outcome are discarded. Now, the remaining rounds are measured using the third step $\{G^{\text{con}}_{(\mathsf{X}),(=)}, G^{\text{con}}_{(\mathsf{X}),(\neq)}\}$ that determines whether Alice and Bob observe an error or no error. Recall that we use the convention that whenever a basis is explicitly written as X/Z, it refers to *both* Alice and Bob measuring in the same basis.

Combining the second and third measurement step, we see that measuring $\tilde{n}_{\mathsf{X}}$ rounds using the above two-step procedure is equivalent to measuring directly using $\left\{G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}, G^{\text{con,F}}_{(\mathsf{XX}),(=)}, \mathbb{I} - F_{(\mathsf{X}),(\text{con})}\right\}$ (see Eq. (6.25)), with the outcomes corresponding conclusive and error, conclusive and no-error and inconclusive respectively. We write $\tilde{e}^{\text{obs}}_{\mathsf{XX}}$ be the error rate in these rounds, which is the fraction of rounds that resulted in the $G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}$-outcome. The subscript XX reflects the fact that this is the error rate when the second step and third step measurements are in X basis. Note that we do not actually observe this error rate in the protocol. We write $e^{\text{obs}}_{\mathsf{X}}$ as the error rate in these rounds after discarding the $\perp$ outcomes. This is the error rate we actually observe in the protocol.

Key Generation Rounds after basis-independent Filter

We will now complete the virtual measurement steps on the key generation rounds, that lead to the phase error rate (which take place in the **Key* ($\mathbf{Z} \to \mathbf{X}$)** box in Fig. 6.3). Let us consider the Z basis rounds selected for key generation at this stage. Let $\tilde{n}_{\mathsf{K}}$ be

the number of such rounds. Note that some of these rounds will be discarded during the remainder of the protocol, and therefore we do not actually know the value of $\tilde{n}_{\mathsf{K}}$ in the protocol. However, as in the case of $\tilde{n}_{\mathsf{X}}$, we do not need to.

These rounds must undergo the second step filtering measurement using $\{F_{(\mathsf{Z}),(\mathrm{con})}, \mathbb{I} - F_{(\mathsf{Z}),(\mathrm{con})}\}$, where the rounds which yield the latter outcome are discarded. Now, we wish to obtain the phase error rate when the remaining rounds are measured using the third step $\{G^{\mathrm{con}}_{(\mathsf{X}),(\neq)}, G^{\mathrm{con}}_{(\mathsf{X}),(=)}\}$ that determines whether Alice and Bob observe an error or no error.

Again, the above two-step measurement procedure is equivalent to measuring directly using $\left\{G^{\mathrm{con,F}}_{(\mathsf{ZX}),(\neq)}, G^{\mathrm{con,F}}_{(\mathsf{ZX}),(=)}, \mathbb{I} - F_{(\mathsf{Z}),(\mathrm{con})}\right\}$ (see Eq. (6.25)), with the outcomes corresponding conclusive and error, conclusive and no-error and inconclusive respectively. We let $\tilde{e}^{\mathrm{key}}_{\mathsf{ZX}}$ be the error rate in these rounds, which is the fraction of rounds that resulted in the $G^{\mathrm{con,F}}_{(\mathsf{ZX}),(\neq)}$-outcome. Again, the subscripts denote the fact that this is the error rate when the second step measurement is in the Z basis and the third step measurement is in the X basis. The phase error rate $e^{\mathrm{key}}_{\mathsf{X}}$ is the error rate in these rounds after discarding the $\perp$ outcomes.

Remark 6.4.2. *When basis-efficiency mismatch is present, one must figure out the phase error rate in the key generation rounds, which are filtered using the* Z *basis. However the rounds for testing are filtered using the* X *basis. These filtering steps are not identical. Therefore it becomes very difficult to prove rigorous bounds on the phase error rate based on the observed data. The main contributions of this chapter is a rigorous derivation of such bounds, without relying on asymptotic behavior or IID assumptions.*

Since the measurements in the key generation rounds leading to $\tilde{e}^{\mathrm{key}}_{\mathsf{ZX}}$ are not identical to the one in the testing rounds which leads to $\tilde{e}^{\mathrm{obs}}_{\mathsf{XX}}$, one cannot directly use Serfling (Lemma 6.3.2) to relate the two, as we did in Section 6.3.3. Therefore, we introduce another set of virtual measurements (which take place in the **Key* (X → X)** box in Fig. 6.3), corresponding to X basis second and third step measurements. Thus we obtain another error rate $\tilde{e}^{\mathrm{key}}_{\mathsf{XX}}$. This is the error rate corresponding to the case where these $\tilde{n}_{\mathsf{K}}$ rounds are measured using $\left\{G^{\mathrm{con,F}}_{(\mathsf{XX}),(\neq)}, G^{\mathrm{con,F}}_{(\mathsf{XX}),(=)}, \mathbb{I} - F_{(\mathsf{X}),(\mathrm{con})}\right\}$ (the same measurement that testing rounds are subject to).

6.4.3 Cost of removing the basis-independent loss assumption

In removing the basis-independent loss assumption from phase error estimation, we will need to define metrics δ_1, δ_2, which will quantify the deviation from ideal behavior. We will now explain how these metrics are defined.

Consider the POVM elements $G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)}$ and $G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}$ defined via Eq. (6.25), which combine the second and third step measurements. In Section 6.3 they were exactly equal. We define δ_1 to quantify the closeness of these POVM elements as

$$\delta_1 := 2\left\| G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)} - G^{\text{con,F}}_{(\mathsf{XX}),(\neq)} \right\|_\infty, \tag{6.26}$$

and use it in Lemma 6.4.1 (to be discussed later) in our proof.

Consider the second step measurements, where outcomes corresponding to POVM element $\mathbb{I} - F_{(\mathsf{Z}),(\text{con})}$ are discarded. In Section 6.3, there was no need of the second step filtering measurement, which is equivalent to having $F_{(\mathsf{Z}),(\text{con})} = \mathbb{I}$. We define δ_2 to quantify the amount of deviation from this case as

$$\delta_2 := \left\| \mathbb{I} - F_{(\mathsf{Z}),(\text{con})} \right\|_\infty. \tag{6.27}$$

Thus δ_2 controls the likelihood of discards in the second step filtering measurements.

Having defined δ_1, δ_2 as metrics of the deviation from the basis-independent loss assumption, we now move on to consider the relations between the error rates in the next subsection.

6.4.4 Sampling

Let us recall the error-rates we have defined so far:

1. $e^{\text{obs}}_{\mathsf{X}}$ is the fraction of the n_{X} testing rounds that resulted in the $G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}$ outcome. We have access to $e^{\text{obs}}_{\mathsf{X}}$ in the protocol, since it is something we actually observe.

2. $\tilde{e}^{\text{obs}}_{\mathsf{XX}}$ is the fraction of the $\tilde{n}_{\mathsf{X}}$ testing rounds (after basis-independent filter only) that result in $G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}$-outcome. $e^{\text{obs}}_{\mathsf{X}}$ is obtained from $\tilde{e}^{\text{obs}}_{\mathsf{XX}}$ after some rounds are discarded in the second step measurements.

3. $\tilde{e}^{\text{key}}_{\mathsf{XX}}$ is the fraction of the $\tilde{n}_{\mathsf{K}}$ key generation rounds (after basis-independent filter only) that result in $G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}$-outcome.

4. $\tilde{e}^{\text{key}}_{\mathsf{ZX}}$ is the fraction of the $\tilde{n}_{\mathsf{K}}$ key generation rounds (after basis-independent filter only) that result in $G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)}$-outcome.

5. $e^{\text{key}}_{\mathsf{X}}$ is the fraction of the n_{K} key generation rounds that result in $G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)}$-outcome. This is the quantity we wish to estimate. $e^{\text{key}}_{\mathsf{X}}$ is obtained from $\tilde{e}^{\text{key}}_{\mathsf{ZX}}$ after some rounds are discarded in the second step measurements.

We wish to prove Eq. (6.8) that relate $\boldsymbol{e}_{\mathbf{X}}^{\mathbf{obs}}$ to $\boldsymbol{e}_{\mathbf{X}}^{\mathbf{key}}$. We do this by relating the various error-rates together as $\boldsymbol{e}_{\mathbf{X}}^{\mathbf{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}} \leftrightarrow \tilde{\boldsymbol{e}}_{\mathbf{ZX}}^{\text{key}} \leftrightarrow \boldsymbol{e}_{\mathbf{X}}^{\mathbf{key}}$. We will consider the event $\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})$, even though we do not actually observe it in the protocol. In the end, all random variables and events not directly observed in the protocol will disappear from our final expressions.

- $\boldsymbol{e}_{\mathbf{X}}^{\mathbf{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}}$: Recall from the **Testing*(X → X)** node in Fig. 6.3, that $\boldsymbol{e}_{\mathbf{X}}^{\mathbf{obs}} = \boldsymbol{N}_{G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}} / \boldsymbol{n}_{\mathbf{X}}$ and $\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}} = \boldsymbol{N}_{G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}} / \tilde{\boldsymbol{n}}_{\mathbf{X}}$. The required relation follows from the fact that we discard rounds to go from $\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}}$ to $\boldsymbol{e}_{\mathbf{X}}^{\mathbf{obs}}$, i.e we have $\Pr(\boldsymbol{n}_{\mathbf{X}} \leq \tilde{\boldsymbol{n}}_{\mathbf{X}})_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} = 1$. Therefore, we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}} \geq \boldsymbol{e}_{\mathbf{X}}^{\mathbf{obs}}\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} = 0. \tag{6.28}$$

- $\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}} \leftrightarrow \tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}}$: These error rates correspond to measurement outcomes using the *same* POVM, but with random assignment to testing vs key generation. Thus we can apply Lemma 6.3.2 (Serfling) in exactly the same manner as in Section 6.3.3, conditioned on the event $\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})$. In doing so, we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}} \geq \tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}} + \gamma_{\text{serf}}\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} \leq e^{-2\gamma_{\text{serf}}^2 f_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})}. \tag{6.29}$$
Using the definition from Eq. (6.21), we have
$$\gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) = \sqrt{\frac{\ln(1/\varepsilon_{\text{AT-a}}^2)}{2 f_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})}} \implies e^{-\left(\gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\right)^2 2 f_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} = \varepsilon_{\text{AT-a}}^2. \tag{6.30}$$
Therefore, we obtain
$$\Pr\left(\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}} \geq \tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{obs}} + \gamma_{\text{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} \leq \varepsilon_{\text{AT-a}}^2 \tag{6.31}$$

- $\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}} \leftrightarrow \tilde{\boldsymbol{e}}_{\mathbf{ZX}}^{\text{key}}$: We utilize the definition of δ_1 stated in Section 6.4.3. Since the POVM elements generating $\tilde{\boldsymbol{e}}_{\mathbf{ZX}}^{\text{key}}$ ($G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)}$) and $\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}}$ ($G^{\text{con,F}}_{(\mathsf{XX}),(\neq)}$) are close, we expect the bounds obtained on $\tilde{\boldsymbol{e}}_{\mathbf{ZX}}^{\text{key}}$ and $\tilde{\boldsymbol{e}}_{\mathbf{XX}}^{\text{key}}$ to also be close. This is made precise in the following lemma proved in Appendix. C.3.1.

  Lemma 6.4.1 (Similar measurements lead to similar observed frequencies)**.** *Let $\rho_{Q^n} \in \mathrm{S}_{=}(Q^{\otimes n})$ be an arbitrary state. Let $\{P, \mathbb{I} - P\}$ and $\{P', \mathbb{I} - P'\}$ be two sets of POVM elements, such that $\|P' - P\|_\infty \leq \delta$. Then,*
$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + 2\delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_{P}}{n} \geq e\right) + F_{\text{bin}}(n, 2\delta, c), \tag{6.32}$$

for $e \in [0,1]$, where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathbb{I}-P\}$, and

$$F_{\text{bin}}(n,\delta,c) := \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}. \tag{6.33}$$

Thus, using Lemma 6.4.1 and δ_1 defined in Eq. (6.26), we obtain

$$\Pr\left(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{ZX}} \geq e+\delta_1+c_1\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \leq \Pr\left(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{XX}} \geq e\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} + F_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1,c_1). \tag{6.34}$$

We would like $F_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1,c_1)$ to be equal to a constant $\varepsilon^2_{\text{AT-b}}$ on the right hand side of the above expression. To do so, we note that $F_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1,c_1)$ is a monotonic (and therefore invertible) function of c_1. Thus, we can choose c_1 to be a function $\gamma^{\varepsilon_{\text{AT-b}}}_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1)$ such that

$$F_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1,\gamma^{\varepsilon_{\text{AT-b}}}_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1)) = \varepsilon^2_{\text{AT-b}}. \tag{6.35}$$

Using this as a definition $\gamma^{\varepsilon_{\text{AT-b}}}_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1)$, we obtain

$$\Pr\left(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{ZX}} \geq e+\delta_1+\gamma^{\varepsilon_{\text{AT-b}}}_{\text{bin}}(\tilde{n}_{\mathsf{K}},\delta_1)\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \leq \Pr\left(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{XX}} \geq e\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} + \varepsilon^2_{\text{AT-b}}. \tag{6.36}$$

Note that γ_{bin} can be easily computed numerically by relating $F_{\text{bin}}(n,\delta,c)$ (and its inverse) to the cumulative binomial distribution and using root finding algorithms.

- $\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{ZX}} \leftrightarrow \boldsymbol{e}^{\text{key}}_{\mathsf{X}}$: We will use the fact that the filtering measurements result in a very small number of discards.

  First, note that $\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{ZX}} = \boldsymbol{N}_{G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)}}/\tilde{\boldsymbol{n}}_{\mathsf{K}}$, and $\boldsymbol{e}^{\text{key}}_{\mathsf{X}} = \boldsymbol{N}_{G^{\text{con,F}}_{(\mathsf{ZX}),(\neq)}}/\boldsymbol{n}_{\mathsf{K}}$. Thus, we have $\tilde{\boldsymbol{e}}^{\text{key}}_{\mathsf{ZX}}/\boldsymbol{e}^{\text{key}}_{\mathsf{X}} = \boldsymbol{n}_{\mathsf{K}}/\tilde{\boldsymbol{n}}_{\mathsf{K}}$.

  Recall that $\boldsymbol{n}_{\mathsf{K}}$ is obtained by discarding rounds from $\tilde{\boldsymbol{n}}_{\mathsf{K}}$ based on $\{F_{(\mathsf{Z}),(\text{con})}, \mathbb{I} - F_{(\mathsf{Z}),(\text{con})}\}$ measurements. We will essentially show that very few rounds are discarded in this step, using Eq. (6.27). To do so, we prove the following Lemma in Appendix. C.3.1.

  Lemma 6.4.2 (Small POVM measurement)**.** *Let $\rho_{Q^n} \in \mathrm{S}_{=}(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I-P\}$ be a POVM such that $\|P\|_\infty \leq \delta$. Then*

  $$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq \delta + c\right) \leq F_{\text{bin}}(n,\delta,c) := \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}, \tag{6.37}$$

  where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathbb{I}-P\}$.

Then, using Lemma 6.4.2 with $P = \mathbb{I} - F_{(\mathsf{Z}),(\mathrm{con})}$ and δ_2 defined in Eq. (6.27), we obtain

$$\begin{aligned}\Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\mathbf{ZX}} \leq \boldsymbol{e}^{\mathbf{key}}_{\mathbf{X}}(1-\delta_2-c_2)\right)_{\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} &= \Pr\left(\frac{\tilde{n}_{\mathsf{K}} - \boldsymbol{n}_{\mathbf{K}}}{\tilde{n}_{\mathsf{K}}} \geq \delta_2 + c_2\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\ &= \Pr\left(\frac{\boldsymbol{N}_{\mathbb{I}-F_{(\mathsf{Z}),(\mathrm{con})}}}{\tilde{n}_{\mathsf{K}}} \geq \delta_2 + c_2\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\ &\leq F_{\mathrm{bin}}(\tilde{n}_{\mathsf{K}}, \delta_2, c_2).\end{aligned} \tag{6.38}$$

Again, we would like $F_{\mathrm{bin}}(\tilde{n}_{\mathsf{K}}, \delta_2, c_2)$ to be a constant value $\varepsilon^2_{\text{AT-c}}$. Thus, we replace c_2 with $\gamma^{\varepsilon_{\text{AT-c}}}_{\mathrm{bin}}(\tilde{n}_{\mathsf{K}}, \delta_2)$ and obtain

$$\Pr\left(\tilde{\boldsymbol{e}}^{\mathrm{key}}_{\mathbf{ZX}} \leq \boldsymbol{e}^{\mathbf{key}}_{\mathbf{X}}(1-\delta_2-\gamma^{\varepsilon_{\text{AT-c}}}_{\mathrm{bin}}(\tilde{n}_{\mathsf{K}}, \delta_2))\right)_{|\Omega(\tilde{n}_{\mathsf{K}},\tilde{n}_{\mathsf{K}})} \leq \varepsilon^2_{\text{AT-c}} \tag{6.39}$$

Thus we have relationships Eqs. (6.28), (6.31), (6.36) and (6.39) between all the error rates, whose complements hold with high probability. These can all be combined using straightforward but cumbersome algebra (see Section C.4), to obtain

$$\Pr\left(\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X}} \geq \frac{\boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\mathrm{bin}}(\tilde{n}_{\mathsf{K}}, \delta_1)}{(1-\delta_2-\gamma^{\varepsilon_{\text{AT-c}}}_{\mathrm{bin}}(\tilde{n}_{\mathsf{K}}, \delta_2))}\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \leq \varepsilon^2_{\text{AT-b}} + \varepsilon^2_{\text{AT-a}} + \varepsilon^2_{\text{AT-c}}. \tag{6.40}$$

Using the above expression requires us to know the values of $\tilde{n}_{\mathsf{K}}$ and $\tilde{n}_{\mathsf{X}}$ which we do not. This problem is easily resolved by noting all the γs are decreasing functions of $\tilde{n}_{\mathsf{K}}$ and $\tilde{n}_{\mathsf{X}}$, and that $\tilde{n}_{\mathsf{K}}(\tilde{n}_{\mathsf{X}})$ cannot be smaller than $n_{\mathsf{K}}(n_{\mathsf{X}})$ (since we discard rounds to from the former to the latter) . Thus, we can replace $\tilde{n}_{\mathsf{K}}$ with $\boldsymbol{n}_{\mathbf{K}}$ and $\tilde{n}_{\mathsf{X}}$ with $\boldsymbol{n}_{\mathbf{X}}$ and obtain

$$\Pr\left(\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X}} \geq \frac{\boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(\boldsymbol{n}_{\mathbf{X}}, \boldsymbol{n}_{\mathbf{K}}) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\mathrm{bin}}(\boldsymbol{n}_{\mathbf{K}}, \delta_1)}{(1-\delta_2-\gamma^{\varepsilon_{\text{AT-c}}}_{\mathrm{bin}}(\boldsymbol{n}_{\mathbf{K}}, \delta_2))}\right)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \leq \varepsilon^2_{\text{AT-b}} + \varepsilon^2_{\text{AT-a}} + \varepsilon^2_{\text{AT-c}} \tag{6.41}$$

We set $\varepsilon^2_{\text{AT-a}} + \varepsilon^2_{\text{AT-b}} + \varepsilon^2_{\text{AT-c}} = \varepsilon^2_{\text{AT}}$, and obtain the choice of $\mathcal{B}_{\delta_1,\delta_2}$:

$$\mathcal{B}_{\delta_1,\delta_2}(e^{\mathrm{obs}}_{\mathsf{X}}, n_{\mathsf{X}}, n_{\mathsf{K}}) := \frac{e^{\mathrm{obs}}_{\mathsf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\mathrm{serf}}(n_{\mathsf{X}}, n_{\mathsf{K}}) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\mathrm{bin}}(n_{\mathsf{K}}, \delta_1)}{(1-\delta_2-\gamma^{\varepsilon_{\text{AT-c}}}_{\mathrm{bin}}(n_{\mathsf{K}}, \delta_2))}, \tag{6.42}$$

where functions $\gamma_{\text{bin}}, \gamma_{\text{serf}}$ are defined in Eq. (6.35) and Eq. (6.21) respectively. Since Eq. (6.41) is valid for all events $\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})$, the above choice satisfies Eq. (6.8) via

$$\begin{aligned}\Pr\Big(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}})\Big) &\leq \sum_{\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}}} \Pr(\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}))\Pr\Big(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}}, \boldsymbol{n}_{\mathsf{X}}, \boldsymbol{n}_{\mathsf{K}})\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\ &\leq \sum_{\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}}} \Pr(\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}))\varepsilon_{\text{AT}}^2 = \varepsilon_{\text{AT}}^2.\end{aligned} \tag{6.43}$$

Remark 6.4.3. *Let us investigate the behavior of Eq. (6.42) in the limit $\delta_1, \delta_2 \to 0$. Recall that $\gamma_{\text{bin}}^{\varepsilon_{\text{AT}}}(n, \delta)$ was defined as the value of c such that $F_{\text{bin}}(n, \delta, c) = \sum_{i=n(\delta+c)}^{n} \binom{n}{k}\delta^i(1-\delta)^{n-i} \leq \varepsilon_{\text{AT}}^2$. However, notice that $\delta \to 0 \implies F_{\text{bin}}(n, \delta, c) \to 0$ for any value of c. Therefore, $\delta \to 0 \implies \gamma_{\text{bin}}(n, \delta) \to 0$. Setting these limits in Eq. (6.42), we recover the result Eq. (6.22) for the case where the basis-independent loss assumption is satisfied.*

Thus we now have a phase error estimation bound that is valid even in the presence of basis-efficiency mismatch. (A self-contained statement describing this as a sampling result can be found in [2, Theorem 2])

6.5 Application to decoy-state BB84

So far in this chapter, we have focused our attention on the BB84 protocol implemented using perfect single-photon sources for pedagogical reasons. In this section, we will extend our techniques and obtain a variable-length security proof for decoy-state BB84 [69, 70, 144, 145, 71] with imperfect detectors. We base our security proof approach on that of Lim et al [97], while fixing some technical errors in that work (see Ref. [2, Section 5]).

6.5.1 Protocol specification

The decoy-state BB84 protocol modifies the following steps of the protocol described in QKD Protocol.

1. **State Preparation:** Alice decides to send states in the $\mathsf{Z}(\mathsf{X})$ basis with probability $p_{(\mathsf{Z})}^{(A)}$ ($p_{(\mathsf{X})}^{(A)}$). She additionally chooses a signal intensity $\mu_k \in \{\mu_1, \mu_2, \mu_3\}$ with some

predetermined probability p_{μ_k} [7]. She prepares a phase-randomized weak laser pulse based on the chosen values, and sends the state to Bob. We assume $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$. This requirement on the intensity values, as well as the total number of intensities, is not fundamental. It is used in deriving the analytical bounds in the decoy-state analysis. Note the all decoy intensities are used in both bases.

2. **Measurement:** Bob chooses the basis $\mathsf{Z}(\mathsf{X})$ with probability $p^{(B)}_{(\mathsf{Z})}(p^{(B)}_{(\mathsf{X})})$ and measures the incoming state. This step of the protocol is identical to that from Section 6.2.

3. **Classical Announcements and Sifting:** For all rounds, Alice and Bob announce the bases they used. Furthermore, Bob announces whether he got a conclusive outcome $(\{\Gamma^{(B)}_{(b,0)}, \Gamma^{(B)}_{(b,1)}\})$, or an inconclusive outcome $(\{\Gamma^{(B)}_{(b,\perp)}\})$. A round is said to be "conclusive" if Alice and Bob used the same basis, and Bob obtained a conclusive outcome. As before X basis rounds are used for testing, and Z basis rounds are used for key generation (with a tiny fraction used for obtaining $e^{\text{obs}}_{\mathsf{Z}}$).

   On all X basis rounds, Alice and Bob announce their measurement outcomes and intensity choices. We let n_{X,μ_k} be the number of X basis conclusive rounds where Alice chose intensity μ_k, and let $e^{\text{obs}}_{\mathsf{X},\mu_k}$ be the observed error rate in these rounds. For brevity, we use the notation $n_{\mathsf{X},\mu_{\vec{k}}} = (n_{\mathsf{X},\mu_1} \dots n_{\mathsf{X},\mu_3})$ to denote observations from all intensities. (We use similar notation for $e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}$, $n_{\mathsf{K},\mu_{\vec{k}}}$ etc).

   On all Z basis, Alice announces her intensity choices, and these rounds are used for key generation. We let n_{K} rounds be the total number of Z basis conclusive rounds used for key generation.

   All announcements are stored in the register $\widehat{C}^n_1$. We use $\Omega(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{Z}})$ to denote the event that $n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{Z}}$ values are observed in the protocol.

The remaining steps of the protocol are the same as in QKD Protocol. In particular, based on the observations $n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{Z}}$, Alice and Bob implement one-way error-correction using $\lambda_{\text{EC}}(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{Z}})$ bits of communication, followed by error-verification, and privacy amplification to produce a key of $\ell(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{Z}})$ bits. Additionally note that our protocol generates key from *all* intensities, instead of having a single "signal" intensity for key generation.

[7] This probability can depend on the basis used without affecting the results of this work. To incorporate this, one simply has to track the correct probability distribution through all the calculations.

6.5.2 Required and actual phase error estimation bound

In order to prove security for our decoy-state QKD protocol, we will need to bound two quantities. First, we must obtain a lower bound on the number of single-photon events that lead to key generation $\boldsymbol{n}_{\mathsf{K},\mathbf{1}}$ (since as we argued in Section 3.3.4 that multi-photon rounds leak all info to Eve). Second, we must obtain an upper bound on the phase error rate within these single-photon key generation rounds, given by $\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X},\mathbf{1}}$. This can be represented mathematically as

$$\Pr\left(\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X},\mathbf{1}} \geq \mathcal{B}_e(\boldsymbol{e}^{\text{obs}}_{\mathbf{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_{\vec{k}}}, \boldsymbol{n}_{\mathsf{K},\boldsymbol{\mu}_{\vec{k}}}) \quad \vee \quad \boldsymbol{n}_{\mathsf{K},\mathbf{1}} \leq \mathcal{B}_1(\boldsymbol{n}_{\mathsf{K},\boldsymbol{\mu}_{\vec{k}}})\right) \leq \varepsilon^2_{\text{AT}}, \tag{6.44}$$

where $\vee$ denotes the logical OR operator, and $\mathcal{B}_e, \mathcal{B}_1$ are functions that provide these bounds as a function of the observed values.

This statement will be used in the proof of Theorem 6.5.1 to prove the variable-length security of our protocol. We will derive the required bounds $(\mathcal{B}_e, \mathcal{B}_1)$ in Eq. (6.44) in two steps. First we will use decoy analysis to convert from observations corresponding to different intensities (which we have access to) to those corresponding to different photon numbers (which we do not have access to). We will be concerned with three outcomes $\{\mathsf{X}_{\neq}, \mathsf{X}, \mathsf{K}\}$, corresponding to X basis conclusive error outcome, X basis conclusive outcome, and Z basis conclusive outcome used for key generation respectively. Thus, at the end of the first step we will obtain

$$\Pr\left(\boldsymbol{e}^{\text{obs}}_{\mathbf{X},\mathbf{1}} \geq \frac{\mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n}_{\mathbf{X}_{\neq},\boldsymbol{\mu}_{\vec{k}}})}{\mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_{\vec{k}}})} \;\vee\; \boldsymbol{n}_{\mathbf{X},\mathbf{1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_{\vec{k}}}) \;\vee\; \boldsymbol{n}_{\mathsf{K},\mathbf{1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\mathsf{K},\boldsymbol{\mu}_{\vec{k}}})\right) \leq 9\varepsilon^2_{\text{AT-d}} \tag{6.45}$$

where $\mathcal{B}^{\text{decoy}}_{\text{min}-m}$ and $\mathcal{B}^{\text{decoy}}_{\text{max}-m}$ are functions that compute bounds on the m-photon components of the input statistics. Note that we use $\boldsymbol{n}_{\mathbf{X}_{\neq},\boldsymbol{\mu}_{\vec{k}}} = (\boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_1} \times \boldsymbol{e}^{\text{obs}}_{\mathbf{X},\boldsymbol{\mu}_1}, \ldots, \boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_{N_{\text{int}}}} \times \boldsymbol{e}^{\text{obs}}_{\mathbf{X},\boldsymbol{\mu}_{N_{\text{int}}}})$ to denote the number of rounds resulting both Alice and Bob using the X basis and obtaining an error, for each intensity (and we will assume implicit conversion between these two notations). The 9 on the RHS comes from the fact that we implement decoy analysis on 3 different events and we have 3 intensities. We will prove Eq. (6.45) in Appendix. Section C.5.

Remark 6.5.1. *Note that the only parameters actually observed in the protocol are given by* $n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}}$. *Variables like* $\boldsymbol{e}^{obs}_{\mathbf{X},\mathbf{1}}$ *are not actually directly observed, but instead are derived from observations.*

In this second step, we will use $\boldsymbol{e}^{\text{obs}}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{K},\mathbf{1}}$ to bound the single photon phase error rate $\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X},\mathbf{1}}$. Notice this is exactly what we showed Sections 6.3 and 6.4. In particular, with $\mathcal{B}_{\delta_1,\delta_2}$ directly obtained from Eq. (6.42), we have

$$\Pr\left(\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X},\mathbf{1}} \geq \mathcal{B}_{\delta_1,\delta_2}(\boldsymbol{e}^{\text{obs}}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{K},\mathbf{1}})\right) \leq \varepsilon^2_{\text{AT-s}}. \tag{6.46}$$

where $\varepsilon^2_{\text{AT-s}}$ denotes the failure probability of the "single-photon" part of our estimation.

However, note that we do not directly observe $\boldsymbol{e}^{\text{obs}}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{K},\mathbf{1}}$ in the decoy-state protocol (unlike Section 6.4). Thus we would like to replace these values with the bounds computed from our decoy analysis (Eq. (6.45)). This is straightforward to do, since $\mathcal{B}_{\delta_1,\delta_2}$ is an increasing function of $\boldsymbol{e}^{\text{obs}}_{\mathbf{X},\mathbf{1}}$, and decreasing function of $\boldsymbol{n}_{\mathbf{X},\mathbf{1}}, \boldsymbol{n}_{\mathbf{K},\mathbf{1}}$. This can be done formally by a straightforward application of the union bound for probabilities ($\Pr(\Omega_1 \vee \Omega_2) \leq \Pr(\Omega_1) + \Pr(\Omega_2)$) applied to Eqs. (6.45) and (6.46). Doing so allows us to conclude that the probability of *any* of the bounds in Eqs. (6.45) and (6.46) failing is smaller than $9\varepsilon^2_{\text{AT-d}} + \varepsilon^2_{\text{AT-s}}$. Then we use the fact that if *none* of the bounds inside the probabilities in Eqs. (6.45) and (6.46) fail, then this implies that the bounds inside the probability in Eq. (6.47) below must hold. Formally, we obtain

$$\begin{aligned}\Pr\Bigg(\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X},\mathbf{1}} \geq \mathcal{B}_{\delta_1,\delta_2}\left(\frac{\mathcal{B}^{\text{decoy}}_{\max-1}(\boldsymbol{n}_{\mathbf{X}\neq,\boldsymbol{\mu}_{\vec{k}}})}{\mathcal{B}^{\text{decoy}}_{\min-1}(\boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_{\vec{k}}})}, \mathcal{B}^{\text{decoy}}_{\min-1}(\boldsymbol{n}_{\mathbf{X},\boldsymbol{\mu}_{\vec{k}}}), \mathcal{B}^{\text{decoy}}_{\min-1}(\boldsymbol{n}_{\mathbf{K},\boldsymbol{\mu}_{\vec{k}}})\right) \quad \vee \\ \boldsymbol{n}_{\mathbf{K},\mathbf{1}} \leq \mathcal{B}^{\text{decoy}}_{\min-1}(\boldsymbol{n}_{\mathbf{K},\boldsymbol{\mu}_{\vec{k}}})\Bigg) \leq 9\varepsilon^2_{\text{AT-d}} + \varepsilon^2_{\text{AT-s}} =: \varepsilon^2_{\text{AT}}\end{aligned} \tag{6.47}$$

which is the required statement. Thus, it is now enough to prove Eq. (6.45) in order to prove Eq. (6.47) (equivalently Eq. (6.44)), for which we turn to decoy analysis. The decoy analysis is a standard tool, and is explained in Section C.5 in Chapter C.

6.5.3 Variable-length security statement for decoy-state

Having proved Eq. (6.44), we now have the following theorem regarding variable-length security of the decoy-state BB84 protocol, which we can prove using Theorem 6.1.1.

Theorem 6.5.1 (Variable-length security of decoy-state BB84 [2])**.** *Suppose Eq. (6.44) is satisfied and let* $\lambda_{\text{EC}}(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}})$ *be a function that determines the number of*

bits used for error-correction in the QKD protocol. Define

$$\ell(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}}) \coloneqq \max\Bigg(0, \Bigg\lfloor \mathcal{B}_1\left(n_{\mathsf{K},\mu_{\vec{k}}}\right)\left(1 - h\left(\mathcal{B}_e\left(e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}\right)\right)\right) \\ - \lambda_{\mathrm{EC}}(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}}) - 2\log(1/2\varepsilon_{\mathrm{PA}}) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil \Bigg\rfloor\Bigg) \tag{6.48}$$

where $h(x)$ is the binary entropy function for $x \leq 1/2$, and $h(x) = 1$ otherwise. Then the variable-length decoy-state QKD protocol that produces a key of length $\ell(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}})$ using $\lambda_{\mathrm{EC}}(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}})$ bits for error-correction, upon the event $\Omega(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{obs}_{\mathsf{X},\mu_{\vec{k}}}, e^{obs}_{\mathsf{Z}}) \wedge \Omega_{\mathrm{EV}}$ is $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EV}})$-secure.

Proof. The proof follows from a straightforward application of Theorem 6.1.1. We identity $\hat{c}_1^n$ with $n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\mathrm{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\mathrm{obs}}_{\mathsf{Z}}$ and $n_{\mathsf{K},1}$ with $\vec{p}$, and consider events $\Omega(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\mathrm{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\mathrm{obs}}_{\mathsf{Z}}, n_{\mathsf{K},1})$, and we define

$$\begin{aligned} \zeta(\hat{c}^1, \vec{p}) &= \Pr\Big(\boldsymbol{e}^{\mathbf{key}}_{\mathbf{X},\mathbf{1}} \geq \mathcal{B}_e(\hat{c}_1^n) \quad \vee \quad \boldsymbol{n}_{\mathbf{K},\mathbf{1}} \leq \mathcal{B}_1(\hat{c}_1^n)\Big)_{\Omega(\hat{c}_1^n, n_{\mathsf{K},1})}, \\ \mathcal{V}(\hat{c}_1^n) &= \{m \in \mathbb{N} | m > \mathcal{B}_1(\boldsymbol{n}_{\mathbf{K},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}})\}. \end{aligned} \tag{6.49}$$

With this identification, the requirement from Eq. (6.2) can be shown to be satisfied. The required bound on the min entropy from Eq. (6.1) also follows from the use of the EUR relation and suitable chain rules to isolate the single-photon contribution. For more details, we refer the reader to Ref. [2, Proof of Theorem 3]. □

6.6 Results

We will now apply our results to a decoy-state BB84 protocol with realistic detectors. To do so, we start by outlining a recipe for using this work to compute key rates in Section 6.6.1. We will then specify the canonical model for our detectors with efficiency mismatch in Section 6.6.2. This model is the same as that specified in Section 3.3, but is specified in more detail. We will apply the recipe to our model in Section 6.6.3. Finally, we will plot the key rate we obtain in Section 6.6.4.

6.6.1 Recipe for computing key rates in the presence of basis-efficiency mismatch

In this subsection, we provide straightforward instructions for using the results of this chapter to compute key rates for decoy-state BB84 in the presence of basis-efficiency mismatch. We will start by explaining the computation of (upper bounds on) δ_1, δ_2 for a given model of the measurement POVMs in the protocol. To do so, one has to break up the measurement process implemented by Alice and Bob into multiple steps via multiple uses of Lemma 6.3.1. This is done as follows:

1. Start with POVM $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\perp)}\}$ which describe Alice and Bob measuring in the (b_A, b_B) basis, and obtaining a conclusive error, a conclusive no-error, and an inconclusive outcome respectively. (In this work, we apply this recipe on the POVMs defined in Eq. (6.54).)

2. Pick a $\tilde{F} \geq \Gamma_{(b_A,b_B),(\neq)} + \Gamma_{(b_A,b_B),(=)}$ for all (b_A, b_B). Consider the four-outcome POVM $\{\mathbb{I} - \tilde{F}, \tilde{F} - \Gamma_{(b_A,b_B),(=)} - \Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\neq)}\}$. Group the last three outcomes together, and use Lemma 6.3.1 to divide this measurement into two steps. In the first step, $\{\tilde{F}, \mathbb{I} - \tilde{F}\}$ is measured and latter outcomes discarded. The remaining rounds are measured using $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$ where

$$\begin{aligned}
\tilde{F}_{(b_A,b_B),(\perp)} &= \sqrt{\tilde{F}}^{+} (\tilde{F} - \Gamma_{(b_A,b_B),(\neq)} - \Gamma_{(b_A,b_B),(\neq)}) \sqrt{\tilde{F}}^{+} + \mathbb{I} - \Pi_{\tilde{F}} \\
\tilde{F}_{(b_A,b_B),(\neq)} &= \sqrt{\tilde{F}}^{+} \Gamma_{(b_A,b_B),(\neq)} \sqrt{\tilde{F}}^{+} \\
\tilde{F}_{(b_A,b_B),(=)} &= \sqrt{\tilde{F}}^{+} \Gamma_{(b_A,b_B),(=)} \sqrt{\tilde{F}}^{+}
\end{aligned} \tag{6.50}$$

   where $\Pi_{\tilde{F}}$ denotes the projector onto the support of $\tilde{F}$.

3. Consider the new POVM $\{\tilde{F}_{(b_A,b_B),(\perp)}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$. Using Lemma 6.3.1 again, divide this POVM measurement into two steps. The first step is implemented using $\{F_{(b_A,b_B),(\text{con})}, F_{(b_A,b_B),(\perp)}\}$ and decides whether the outcome is conclusive or inconclusive. The conclusive outcomes are further measured using $\{G^{\text{con}}_{(b),(\neq)}, G^{\text{con}}_{(b),(=)}\}$.

These POVM elements are given by

$$\begin{aligned} F_{(b_A,b_B),(\mathrm{con})} &= \tilde{F}_{(b_A,b_B),(\neq)} + \tilde{F}_{(b_A,b_B),(=)} \\ F_{(b_A,b_B),(\perp)} &= \tilde{F}_{(b_A,b_B),(\perp)} \\ G^{\mathrm{con}}_{(b_A,b_B),(\neq)} &= \sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+} \tilde{F}_{(b_A,b_B),(\neq)} \sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+} \\ G^{\mathrm{con}}_{(b_A,b_B),(=)} &= \sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+} \tilde{F}_{(b_A,b_B),(=)} \sqrt{F_{(b_A,b_B),(\mathrm{con})}}^{+} + \mathbb{I} - \Pi_{F_{(b_A,b_B),(\mathrm{con})}} \\ &= \mathbb{I} - G^{\mathrm{con}}_{(b_A,b_B),(\neq)} \end{aligned} \tag{6.51}$$

where $\Pi_{F_{(b_A,b_B),(\mathrm{con})}}$ is the projector onto the support of $F_{(b_A,b_B),(\mathrm{con})}$. This projector plays a trivial rule in the measurement itself, and is only included to ensure that we obtain a valid POVM.

4. Compute

$$\begin{aligned} \delta_1 =& 2\left\| \sqrt{F_{(\mathsf{Z}),(\mathrm{con})}} G^{\mathrm{con}}_{(\mathsf{X}),(\neq)} \sqrt{F_{(\mathsf{Z}),(\mathrm{con})}} - \sqrt{F_{(\mathsf{X}),(\mathrm{con})}} G^{\mathrm{con}}_{(\mathsf{X}),(\neq)} \sqrt{F_{(\mathsf{X}),(\mathrm{con})}} \right\|_\infty \\ \delta_2 =& \left\| \mathbb{I} - F_{(\mathsf{Z}),(\mathrm{con})} \right\|_\infty \end{aligned} \tag{6.52}$$

where we recall that whenever the basis is explicitly written as X/Z, it represents both Alice and Bob's basis choices.

5. For the analysis of practical scenarios, where the detector parameters η_{b_i}, d_{b_i} are not known exactly but are instead known to be in some range, one must also additionally maximize Eq. (6.52) over all possible choices of parameters η_{b_i}, d_{b_i}.

Once δ_1, δ_2 are computed via the procedure above, we can compute key rates as follows. The key rate expression for the decoy-state BB84 protocol is given by Eq. (6.48). To use this expression, refer to Eqs. (6.44) and (6.47) (which are notationally equivalent). The bounds for the decoy analysis in Eq. (6.47) are in turn found in Eqs. (C.37) to (C.39), whereas the bound for the phase error estimation is found in Eq. (6.42). For the BB84 protocol where Alice sends single photons, the key rate is given by Eqs. (6.9) and (6.42).

6.6.2 Detector Model

In this section, we specify the canonical model of Bob's detectors (for active BB84) we use in this work. Let η_{b_i}, d_{b_i} denote the efficiency and dark count rate of Bob's POVM corresponding to basis b, and bit i. We first define Bob's double click POVM for basis $b \in \{\mathsf{Z}, \mathsf{X}\}$ to

be $\Gamma^{(B)}_{(b,\mathrm{dc})} = \sum_{N_0,N_1=0}^{\infty}(1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_b$, where $|N_0,N_1\rangle\langle N_0,N_1|_b$ is the state with N_0 photons in the mode 1, and N_1 photons in mode 2, where the modes are defined with respect to basis b. For example, for polarization-encoded BB84, $|2,1\rangle\langle 2,1|_{\mathsf{Z}}$ would signify the state with 2 horizontally-polarised photons and 1 vertically polarised photon. Recall that double clicks are mapped to single clicks randomly in our protocol. Thus, we can write Bob's POVM elements as

$$\begin{aligned}
\Gamma^{(B)}_{(b,\perp)} &= \sum_{N_0,N_1=0}^{\infty}(1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1}\,|N_0,N_1\rangle\langle N_0,N_1|_b \\
\Gamma^{(B)}_{(b,0)} &= (1-d_{b_1})\sum_{N_0,N_1=0}^{\infty}(1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1}\,|N_0,N_1\rangle\langle N_0,N_1|_b + \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})} \\
\Gamma^{(B)}_{(b,1)} &= (1-d_{b_0})\sum_{N_0,N_1=0}^{\infty}(1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_b + \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})}.
\end{aligned} \tag{6.53}$$

Decoy methods allow us to restrict out attention to rounds where Alice sent single photons. Thus her Hilbert space is qubit while Bob holds two optical modes. The joint Alice-Bob POVM elements for the basis b can be constructed via Eqs. (6.5), (6.6) and (6.53) and are

given by

$$\begin{aligned}
\Gamma_{(b,b),(\perp)} =& \mathbb{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} (1-d_{b_0})(1-d_{b_1})(1-\eta_{b_0})^{N_0}(1-\eta_{b_1})^{N_1} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
\Gamma_{(b,b),(\neq)} =& \left|0\right\rangle\!\left\langle 0\right|_b \otimes (1-d_{b_0}) \sum_{N_0,N_1=0}^{\infty} (1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1}) \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \left|1\right\rangle\!\left\langle 1\right|_b \otimes (1-d_{b_1}) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \mathbb{I}_A \otimes \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})} \\
\Gamma_{(b,b),(=)} =& \left|0\right\rangle\!\left\langle 0\right|_b \otimes (1-d_{b_1}) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_{b_0})(1-\eta_{b_0})^{N_0})(1-\eta_{b_1})^{N_1} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \left|1\right\rangle\!\left\langle 1\right|_b \otimes (1-d_{b_0}) \sum_{N_0,N_1=0}^{\infty} (1-\eta_{b_0})^{N_0}(1-(1-d_{b_1})(1-\eta_{b_1})^{N_1}) \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \mathbb{I}_A \otimes \frac{1}{2}\Gamma^{(B)}_{(b,\mathrm{dc})},
\end{aligned} \tag{6.54}$$

where $\left|0\right\rangle\!\left\langle 0\right|_b$ on Alice's system is the $\left|0\right\rangle$ state encoded in basis b. Note that this is different from the vacuum state $\left|0,0\right\rangle\!\left\langle 0,0\right|_b$ on Bob's system, the state with 0 photons in all modes.

In any practical protocol, the detection efficiencies η_{b_i} and dark count rates d_{b_i} cannot be characterized exactly. Therefore, instead of assuming exact knowledge of these parameters, we assume that they are characterized upto some tolerances $\Delta_\eta, \Delta_{\mathrm{dc}}$ given by

$$\begin{aligned}
\eta_{b_i} &\in [\eta_{\mathrm{det}}(1-\Delta_\eta), \eta_{\mathrm{det}}(1+\Delta_\eta)], \\
d_{b_i} &\in [d_{\mathrm{det}}(1-\Delta_{\mathrm{dc}}), d_{\mathrm{det}}(1+\Delta_{\mathrm{dc}})].
\end{aligned} \tag{6.55}$$

6.6.3 Computing bounds on δ_1, δ_2.

The upper bounds on δ_1, δ_2 are straightforward cumborsome algebra, and we refer the reader to [2, Appendix G]. The main idea is to utilize the block-diagonal structure in photon number, and compute the bounds separately for each block.

Active BB84 detection setup without any hardware modification

In this case, we obtain

$$\begin{aligned}\delta_1 &\leq \max\left\{\left(1-\frac{1-(1-d_{\min})^2}{1-(1-d_{\max})^2}\right)\frac{d_{\max}(2-d_{\min})}{1-(1-d_{\min})^2}, 4\left|1-\sqrt{1-(1-d_{\min})^2(1-r_\eta)}\right|\right\},\\ \delta_2 &\leq \max\left\{1-\frac{1-(1-d_{\min})^2}{1-(1-d_{\max})^2}, (1-d_{\min})^2(1-r_\eta)\right\},\end{aligned} \tag{6.56}$$

where

$$\begin{aligned} r_\eta &= \eta_{\min}/\eta_{\max}\\ d_{\max} &= \max\{d_{X_0}, d_{X_1}, d_{Z_0}, d_{Z_1}\} \leq d_{\det}(1+\Delta_{\mathrm{dc}}),\\ d_{\min} &= \min\{d_{X_0}, d_{X_1}, d_{Z_0}, d_{Z_1}\} \geq d_{\det}(1-\Delta_{\mathrm{dc}}),\\ \eta_{\max} &= \max\{\eta_{X_0}, \eta_{X_1}, \eta_{Z_0}, \eta_{Z_1}\} \leq \eta_{\det}(1+\Delta_\eta),\\ \eta_{\min} &= \min\{\eta_{X_0}, \eta_{X_1}, \eta_{Z_0}, \eta_{Z_1}\} \geq \eta_{\det}(1-\Delta_\eta).\end{aligned} \tag{6.57}$$

Thus, upper bounds on δ_1, δ_2 can be computed using Eq. (6.56) and the bounds in Eq. (6.57). It is these bounds that we use to compute key rates.

Random Swapping of 0 and 1 Detectors

In Ref. [141] it was argued that random swapping of the 0 and the 1 detector can be used to remove basis-efficiency mismatch for single-photon pulses entering Bob's detectors. Note that this trick *only works for the single-photon subspace*. We will now adapt our analysis to the case where Bob randomly swaps the 0 and the 1 detector.

In the scenario where we randomly swap the 0 and the 1 detectors, we make certain physically motivated assumptions (Eq. (6.58)) about the detector setup. In particular, we assume that the dark count rate is a property of the detector only. Furthermore, we assume that the basis choice setting does not change the detector parameters. This means that the dark count rate and detection efficiency in both bases is the same (though these can be different for each detector). Thus, we have

$$\begin{aligned} \eta_{X_0} &= \eta_{Z_0} =: \eta_0\\ \eta_{X_1} &= \eta_{Z_1} =: \eta_1\\ d_{X_0} &= d_{Z_0} =: d_0\\ d_{X_1} &= d_{Z_1} =: d_1.\end{aligned} \tag{6.58}$$

We will see that this indeed allows us to obtain improved results, even though it does not completely remove efficiency mismatch. In particular, the leading order terms in δ_1, δ_2 are improved in the new bounds obtained in Eqs. (6.59) and (6.60). Note that our metrics δ_1, δ_2 do not improve unless we make these assumptions. These assumptions are also implicit in the claims presented in Ref. [141].

If the random swapping is implemented, the Bob's POVM elements also need to be suitably modified, as described in [2, Section 6.4.2], and the δ_1, δ_2 computations are undertake for these modified POVMs.

$$\begin{aligned} \delta_1 &\leq 4\left(1-\sqrt{1-(1-d_{\text{mult}})^2\frac{(1-r_\eta)^2}{2}}\right), \\ \delta_2 &\leq (1-d_{\text{mult}})^2\frac{(1-r_\eta)^2}{2}, \end{aligned} \tag{6.59}$$

where

$$\begin{aligned} d_{\text{mult}} &= 1-\sqrt{(1-d_0)(1-d_1)} \geq d_{\min}, \\ r_\eta &= \frac{\eta_{\min}}{\eta_{\max}} \geq \frac{1-\Delta_\eta}{1+\Delta_\eta}. \end{aligned} \tag{6.60}$$

Thus, upper bounds on δ_1, δ_2 in case of random swapping of detectors can be computed using Eq. (6.59) and the bounds in Eq. (6.60). We see that these bounds are better than the earlier bounds from Eq. (6.56). On inspecting our calculations, we find that the zero-photon component of δ_1, δ_2 goes to zero due to $d_X = d_Z$. Furthermore, random swapping in addition to the assumption of $\eta_X = \eta_Z$ leads to the single-photon contribution also being zero. Thus, we are left with the two-photon contribution.

6.6.4 Plots

We plot finite size key rates for the decoy-state BB84 protocol described in Section 6.5. We choose typical protocol parameters and plot the key rate for the expected observations for the given channel model. For all plots, we set the basis choice probabilities to be $p^{(A)}_{(\mathsf{Z})} = p^{(B)}_{(\mathsf{Z})} = 0.5$ and $p^{(A)}_{(\mathsf{X})} = p^{(B)}_{(\mathsf{X})} = 0.5$, We set the detector parameters to be $\eta_{\text{det}} = 0.7$ and $d_{\text{det}} = 10^{-6}$. We set the misalignment angle to be 2°. We set the number of bits used for error-correction to be $\lambda_{\text{EC}}(n_{\mathsf{X},\mu_{\vec{k}}}, n_{\mathsf{K},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{X},\mu_{\vec{k}}}, e^{\text{obs}}_{\mathsf{Z}}) = f_{\text{EC}} n_{\mathsf{K}} h(e^{\text{obs}}_{\mathsf{Z}})$, where $f_{\text{EC}} = 1.16$ is the error-correction efficiency. The decoy intensities are chosen to be $\mu_1 = 1$, $\mu_2 = 0.1$, and $\mu_3 = 0.01$. Each intensity is chosen with equal probability. We set the overall security parameter to be $\varepsilon^{\text{secure}} = 2 \times 10^{-10}$, with $\varepsilon_{\text{EV}} = 10^{-10}$, and $\varepsilon^{\text{secret}} = 10^{-10}$. Then, the

various ε values can be further distributed as : $\varepsilon_{\text{PA}} = 10^{-10}/2$, $\varepsilon_{\text{AT}} = 10^{-10}/4$, and $\varepsilon_{\text{AT-a}} = \varepsilon_{\text{AT-b}} = \varepsilon_{\text{AT-c}} = \varepsilon_{\text{AT-d}} = 10^{-10}/4\sqrt{12}$. Due to machine precision issues arising from small values of $\varepsilon_{\text{AT}}^2$, we use Hoeffdings inequality to bound γ_{bin} (Eq. (6.35)) instead of using the cumulative binomial distribution (which is tighter). As before, note that several of these parameters can be optimized over for the best key rate results. We do not do that here, since we wish to simply study the impact of efficiency mismatch on the key rates.

1. In Fig. 6.4, we plot the finite size key rate against loss for various values of detector characterizations $\Delta_\eta, \Delta_{\text{dc}}$ for $n_{\text{total}} = 10^{12}$ number of total signals. For $\Delta_\eta = \Delta_{\text{dc}} = 0$, we have $\delta_1 = \delta_2 = 0$. Therefore the phase error rate bound from Eq. (6.42) reduces to the scenario where the basis-independent loss assumption is satisfied (Eq. (6.22)). For non-zero values of $\Delta_\eta, \Delta_{\text{dc}}$, the key rate is reduced. This is mostly due to the increase in the bound for the phase error rate from Eq. (6.42) from δ_1. We find that random swapping leads to a dramatic improvement in performance.

2. In Fig. 6.5, we plot the finite size key rate against loss for various values of total signals sent. We set $\Delta_\eta = \Delta_{\text{dc}} = 0.05$. We find that we get close to asymptotic key rates already at $n = 10^{12}$ signals sent.

3. In Fig. 6.6, we plot the finite size key rate against detector characterization parameters $\Delta_\eta, \Delta_{\text{dc}}$. We find that our methods can tolerate a significant amount of error in detector characterization. In fact, with random swapping of detectors, we get positive key rate for $n = 10^{12}$ signals sent for $\Delta_\eta, \Delta_{\text{dc}}$ upto 0.35.

We also refer the reader to Ref. [119] for an improvement over these results.

6.6.5 Extension to multi-mode case

The analysis presented so far assumes that the detector behavior, while possibly varying between rounds or exhibiting correlations, is described by a single mode characterized by bounded loss and dark count rates η_{b_i} and d_{b_i}, as specified in Eq. (6.55). Thus, we have presented an analysis of Case 2 from the introduction to this chapter. This analysis allows us to drastically reduce the requirements on device characterization: the proof technique is now robust to imperfect characterization. However, physical implementations of QKD protocols are vulnerable to side-channel attacks where Eve can control, to a limited extent, the POVMs used. For example, by controlling the frequency, spatial mode [146, 133] or arrival time [134] of the light, Eve can partially choose the detector efficiencies and induce a suitable basis-efficiency mismatch. This is the scenario described by Case 3.

While our proof technique advances the theory to the point where this case can be handled in principle, a complete analysis first requires the physical modeling of multi-mode detectors, which remains an open problem. In this section, we outline how the results of this work can be applied to a simple multi-mode model.

We expand our detector model (and Bob's Hilbert space) to account for spatio-temporal modes [63] as

$$\Gamma^{\text{multi}}_{(b_A,b_B),(k)} = \bigoplus_{\mathbf{d}} \Gamma_{(b_A,b_B),(k)}(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}), \tag{6.61}$$

where $\mathbf{d}$ denotes the spatio-temporal mode, and $\Gamma_{(b_A,b_B),(k)}(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\})$ denotes the single-mode POVM element corresponding to that mode, and is given by Eq. (6.54). The multi-mode detector has loss $\eta_{b_i}(\mathbf{d})$ for this mode, and a dark count rate of $d_{b_i}(\mathbf{d})$.

The block-diagonal structure with respect to $\mathbf{d}$ in the above equation reflects the fact that our model assumes no interference between any pair of spatio-temporal modes during the measurement process. In particular, it captures the possibility that an adversary may exploit different times-of-arrival, frequencies, or angles of incidence to attack the system, provided that each instance corresponds to a definite spatio-temporal mode and no coherent superpositions across modes, or multi-excitation states that simultaneously occupy several modes are used. Even with these limitations, the model protects against a wide range of known classical side-channel attacks. For instance, the time-shift attack [131, 134] is fully captured within this model, as it simply corresponds to Eve selecting different times-of-arrival to exploit the time-dependent efficiency mismatch of the gated detectors. Thus, the block-diagonal model represents a first step toward a more complete analysis of realistic side-channels. This perspective also captures other potential attack strategies, such as modifying the temperature of the detection setup.

Remark 6.6.1. *We stress that our results in this subsection should be interpreted within the context of this model, and may not accurately describe the physical reality of multi-mode detectors. Nevertheless, while we only consider models of the above form in this work, our proof provides a framework to accommodate more complicated models of multi-mode detectors with off-diagonal blocks, as long as one can suitably bound δ_1, δ_2. In general, this would require a model of the detectors, and characterization of the detectors over all the modes. For examples of such attempts to experimentally characterize all the modes, see Ref. [146, 133].*

Due to the block-diagonal structure of the above POVM element Eq. (6.61), and the fact that δ_1, δ_2 are ∞-norms which can be computed on each block-diagonal part separately, it is straightforward to see that our computation of δ_1, δ_2 is directly applicable to the above scenario. To see this, note that our metrics are obtained by first

constructing POVMs corresponding to a multi-step measurement process, as outlined in Section 6.6.1. This construction preserves the block-diagonal structure of Eq. (6.61). Thus, if $\delta_1(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}), \delta_2(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\})$ are the values of these metrics computed according to Eq. (6.52), for the appropriate single-mode POVMs, then the metrics for the multi-mode case are given by

$$\begin{aligned} \delta_1^{\text{multi}} &= \max_{\mathbf{d}} \delta_1(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}), \\ \delta_2^{\text{multi}} &= \max_{\mathbf{d}} \delta_2(\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}). \end{aligned} \tag{6.62}$$

If the values of $\{\eta_{b_i}(\mathbf{d}), d_{b_i}(\mathbf{d})\}$ are characterized and satisfy Eq. (6.55) for all $\mathbf{d}$, then Eq. (6.62) is exactly the same as the computation as in Step (5) of Section 6.6.1 (which corresponds to computing δ_1, δ_2 for Case 2 (see start of this chapter).

This means that the recipe from Section 6.6.1, and the computed key rates from Section 6.6.4 are valid for the scenario where Eve can choose the value of η_{b_i}, d_{b_i} in the specified ranges (Eq. (6.55)), via some extra spatio-temporal modes. Most importantly, our analysis does not depend on the *number* of such spatio-temporal modes. Thus, we are able to address scenarios where Eve has an arbitrary number of spatio-temporal modes, to induce (a bounded amount of) basis-efficiency mismatch in the detector.

Remark 6.6.2. *As discussed above, our methods are such that allowing Eve to choose the detector parameters within the characterized range yields the same key rate as having fixed detector parameters that are characterized within the same range. However, this observation need not be fundamental, and may be a consequence of the proof technique used in this work. This is because intuitively, we expect scenarios where Eve cannot choose the detector parameters (from within their respective ranges), to lead to higher key rates than scenarios where she can, since she is strictly stronger in the latter scenario. Moreover, while we do not know of a physical mechanism by which Eve can choose dark count rates, we allow Eve to choose them along with the detection efficiency.*

We have picked this model for its theoretical simplicity. However, more realistic models such as the one introduced in [141, Section 3] can also be analysed with the results in this work. Finally we note that this work does not apply to *all* detector side-channels. For instance, our model does not fit Trojan horse attacks [147]. Moreover, some blinding attacks on detectors [148] lead to complete knowledge of Bob's detection events to Eve. In this case, our methods naturally lead to trivial key rates, since no key generation is possible.

6.7 Summary and Outlook

In this chapter, we presented a finite-size security proof of the decoy-state BB84 protocol in the presence of imperfectly characterized and bounded adversarial control over basis-efficiency mismatch, using a phase error rate based approach. In doing so, we addressed a longstanding and well-known assumption underlying security proofs within the entropic uncertainty relation (EUR) and phase error correction frameworks. Prior to this work, security proofs within these frameworks were fundamentally unstable: even infinitesimal amounts of basis-efficiency mismatch were sufficient to invalidate the analysis. (This issue does not arise for measurement-device-independent QKD, and is not addressed in this chapter for entanglement-based protocols.) By allowing for bounded adversarial control over the efficiency mismatch, our methods also provide a framework for addressing an important class of detector side channels that had remained unresolved in existing security proofs for standard prepare-and-measure QKD with trusted detection setups.

We applied our framework to the decoy-state BB84 protocol and demonstrated that practical key rates can still be achieved in the finite-size regime, even in the presence of basis-efficiency mismatch. In addition, we quantitatively investigated mitigation strategies such as random swapping of detectors, which reduce the effective mismatch and thereby improve performance. Taken together, these results represent a significant step toward both the protocol-level security of EUR-based proof techniques and the implementation-level security of QKD systems employing trusted detectors.

Detector Models: The rigorous results obtained in this chapter for multi-mode detectors rely on a specific detector model. While this model already captures several realistic features, we expect the framework to be adaptable to more refined and experimentally accurate models in future work. In particular, computing key rates within our framework requires bounds on the parameters δ_1 and δ_2. Although our current analysis relies on simplifying assumptions to obtain these bounds, there is clear scope for improvement. More refined detector characterizations could lead to tighter bounds and improved key rates. More broadly, extending the framework to encompass a wider range of detector imperfections—well characterized by state-of-the-art experimental techniques—would significantly broaden the applicability of the results.

Connections to subsequent work: We note that the results of this chapter have already informed subsequent work on QKD security analysis. For example, basis-efficiency mismatch becomes more subtle in passive detection setups, where the beam splitter implementing the

basis choice exhibits photon-number-dependent behavior. Ref. [83] builds directly on the framework developed here and extends it to passive protocols. Furthermore, certain classes of correlated detector imperfections can be handled using the methods outlined in Ref. [2] (not presented in this thesis), which were later applied rigorously in Ref. [83].

Another natural extension is the integration of our methods with established techniques for addressing source imperfections [126, 127, 129]. Such a combination would yield a security proof robust to both source and detector imperfections. A result of this form has recently been obtained in Ref. [80]. Thus, these results form a foundation for a growing body of results addressing detector imperfections in QKD security proofs.

Relatedly, Ref. [78] presents a complementary approach to detector imperfections based on the flag-state squasher. That work demonstrates that the flag-state squasher can be used to replace imperfect detectors with ideal (squashed) ones even in the presence of imperfectly characterized loss and dark count rates, and outlines a pathway toward handling correlated detector effects. Moreover, elements from all these works [78, 2, 83] can be combined to yield tighter versions of the results in this chapter, as shown in Ref. [119]. A reader interested in detector imperfections is encouraged to refer to Ref. [119].

Limitations of Phase Error Based Methods: Notice that the problem of efficiency mismatch is, in fact, specific to phase error based proof techniques. Other approaches, such as postselection or entropy accumulation–based methods, do not rely on symmetry assumptions[8] about the underlying POVMs and therefore do not suffer from this issue. This highlights a fundamental limitation of phase error based approaches.

While phase error based methods yield rigorous and often analytically tight bounds on the key rate, they rely heavily on symmetries that are specific to idealized BB84 implementations. Any deviation from perfect symmetry - whether originating from source imperfections or detector imperfections - can invalidate the original analysis.

Although such deviations from symmetry can, in principle, be handled through careful and technically involved arguments, the resulting security statements are rarely modular. Instead, they depend intricately on the precise protocol details and on the specific physical model under consideration, with even small modifications often requiring a substantial reworking of the entire proof.[9] From the perspective of this thesis, this lack of modularity constitutes the primary drawback of phase error based security proofs. At the same time,

[8]The postselection requirement on permutation invariance can be satisfied via protocol design.

[9]This observation is supported by the length and complexity of Refs. [129, 83], which, despite their technical sophistication, ultimately remain tailored to BB84-like protocols.

these methods have been studied extensively and are widely used, largely because they are relatively simple to apply and because many relevant source imperfections have been thoroughly analyzed in the literature [129, 128, 127, 149], and which can potentially be combined with the analysis of this chapter.

In the next chapter, we turn to MEAT, which provides with a security proof approach that is tight, modular, and significantly more general than any we have seen so far.

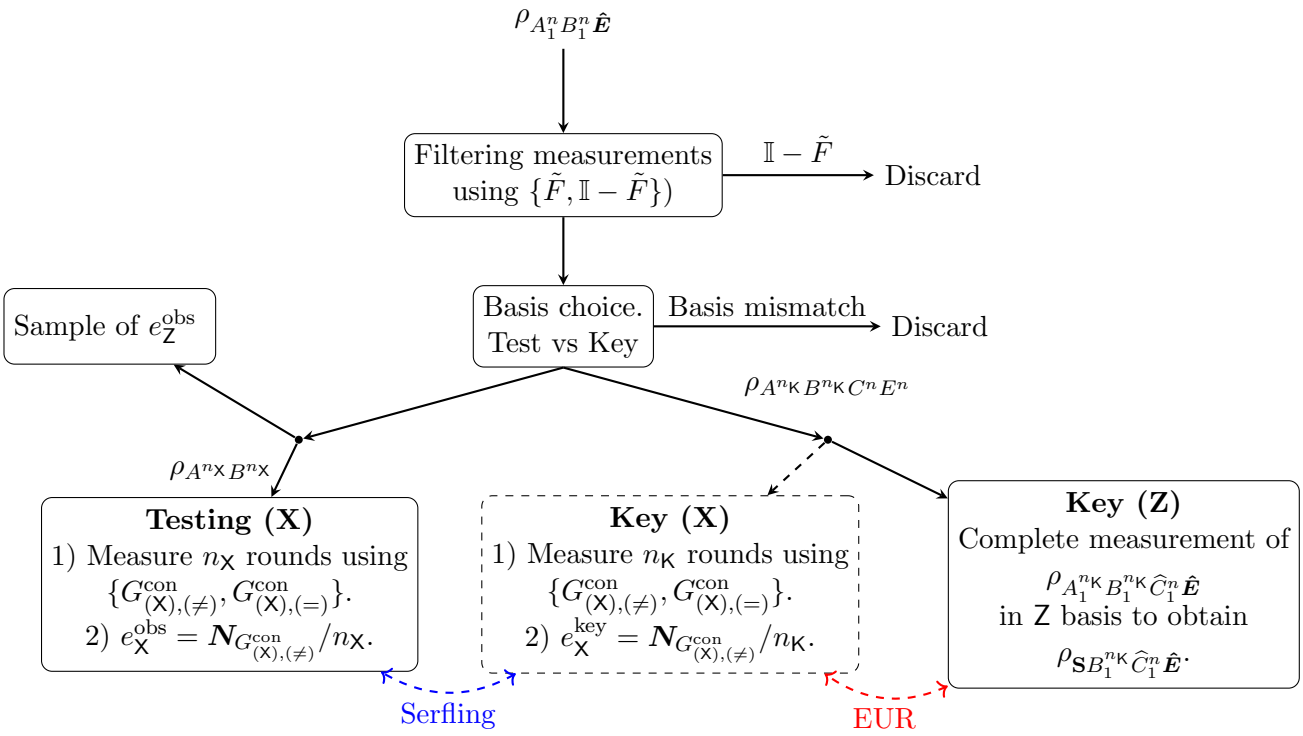


Figure 6.2: Protocol flowchart for the equivalent protocol from Section 6.3, where basis-independent loss assumption (Eq. (6.7)) is satisfied. The dotted arrows and boxes represent virtual measurements that do not actually happen in the real protocol. Connections between different boxes are highlighted using curved arrows. We use the Serfling bound (Lemma 6.3.2) to obtain a bound on the phase error rate from observations. The phase error rate is then used to bound the smooth min entropy using the EUR statement. We use $\boldsymbol{N}_P$ to denote the number of P measurement outcomes, where P denotes a POVM element. For clarity, we have omitted the conditioning on events in the figure (but not in our proof). The basis used for measurements is indicated in each box, and refers to the basis used by *both* Alice and Bob.

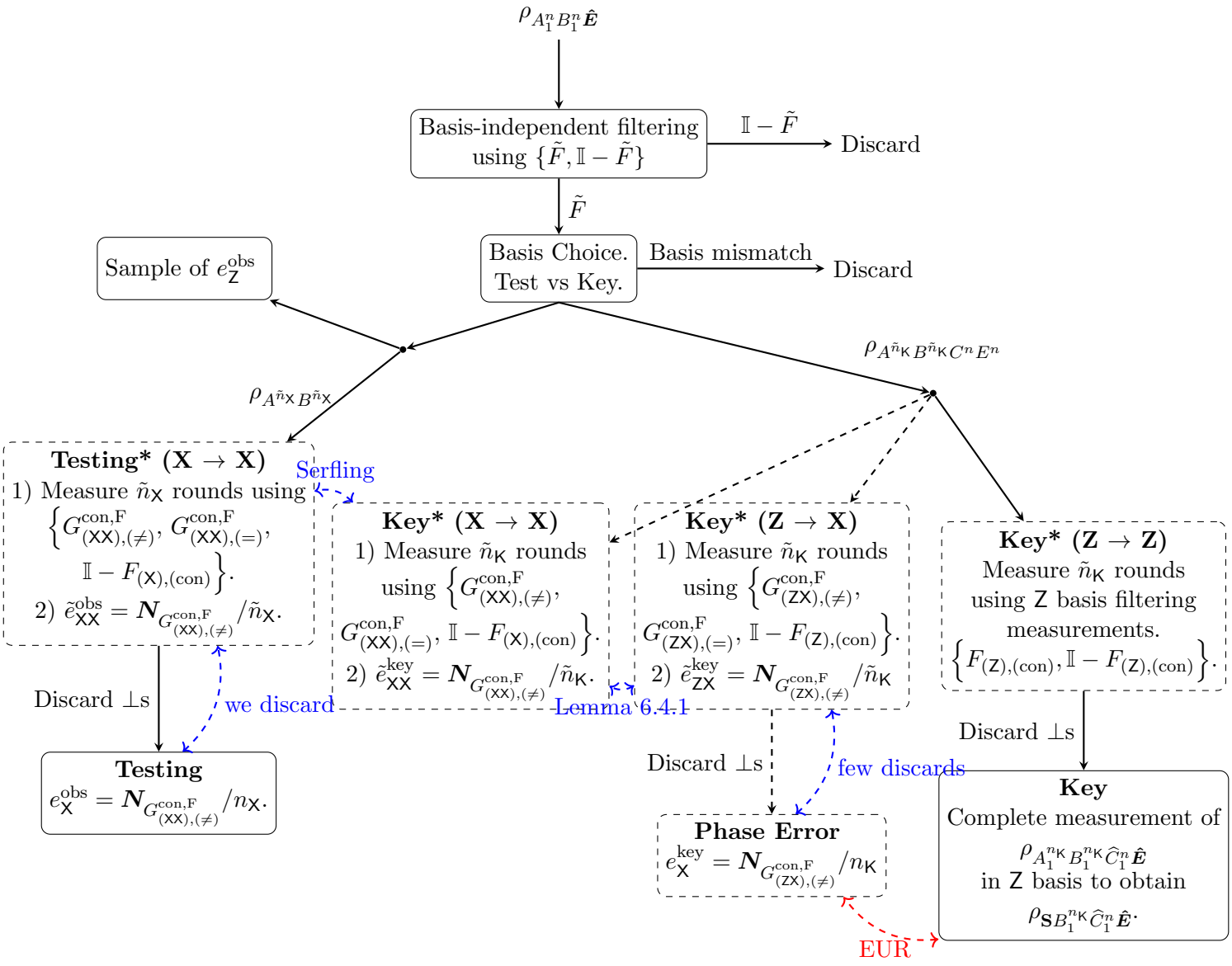


Figure 6.3: Protocol flowchart for the equivalent protocol from Section 6.4, where basis-independent loss assumption (Eq. (6.7)) is not satisfied. For the POVMs, the reader may refer to Table 6.1 or Section 6.4.1. Compared to Fig. 6.3, the testing and key generation rounds go through an additional second step filtering measurement that depends on the basis used. The basis used in these measurements in indicated in each box, and indicates the basis used by *both* Alice and Bob.

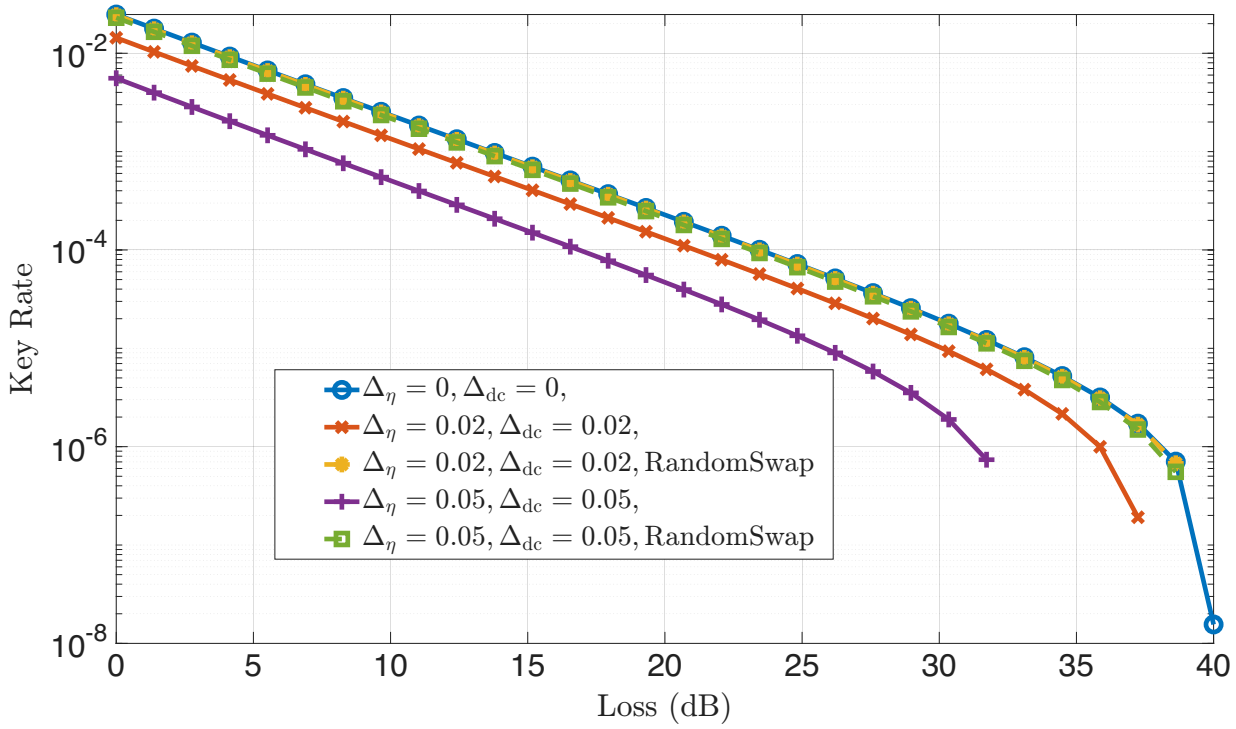


Figure 6.4: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol, against loss. We plot key rates for $n = 10^{12}$ number of total signals sent, for various values of $\Delta_\eta, \Delta_{\rm dc}$. We find that random swapping of the 0 and 1 detectors drastically improves the key rates obtained.

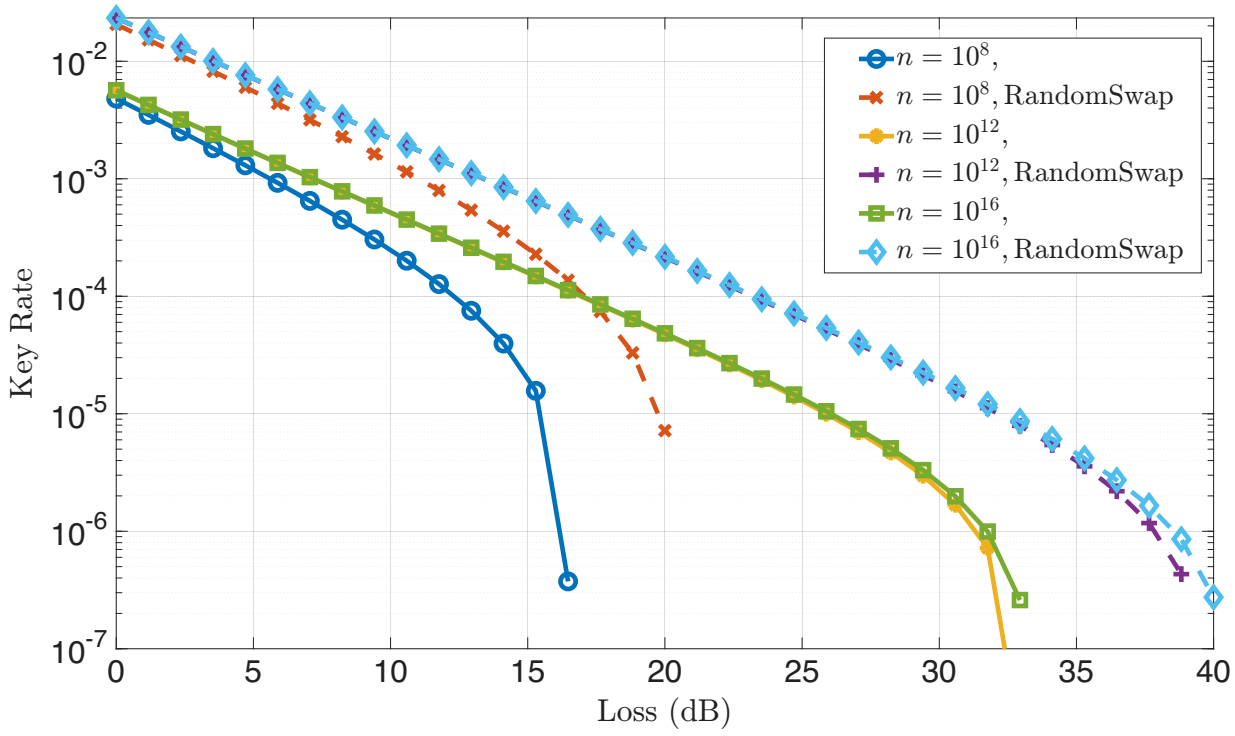


Figure 6.5: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against loss. We plot key rates for various values of total number of signals sent (n), for $\Delta_\eta = \Delta_{\text{dc}} = 0.05$.

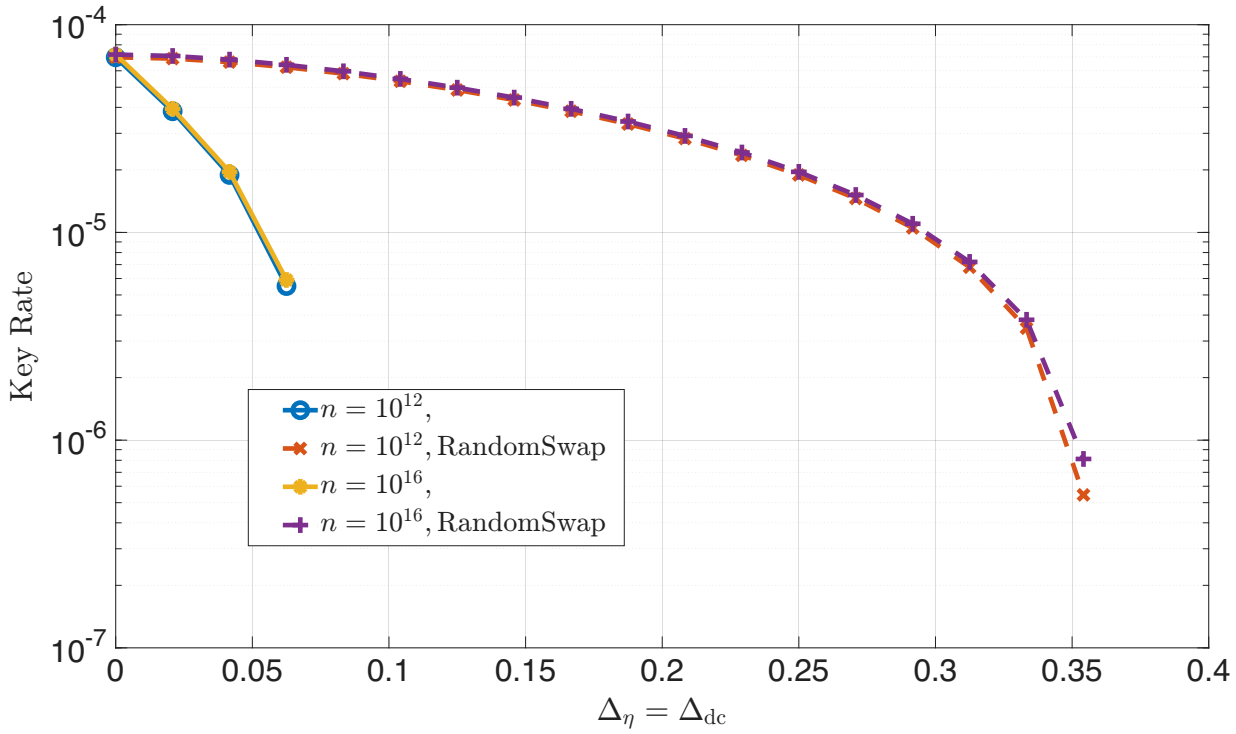


Figure 6.6: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against detector characterization parameters $\Delta_\eta, \Delta_{\mathrm{dc}}$. We plot key rates for a channel with 25dB loss.

Chapter 7

Security using Marginal-constrained Entropy Accumulation Theorem

> Where we invoke the MEAT and obtain a solution to a surprisingly large number of our problems; and where we present a complete and rigorous security analysis framework that accommodates almost all features a reasonable person could hope for in QKD.

In this chapter, we present a rigorous and complete security proof for a generic QKD protocol using the marginal-constrained entropy accumulation theorem (MEAT) [11], which can be applied to the decoy-state BB84 protocol [70, 69, 144, 21]. To support this goal, our approach extends far beyond this specific case: we will consolidate several key elements required for a modern QKD security analysis into a unified and modular framework. Our treatment will encompasses all the major components essential for the analysis of realistic QKD protocols, including classical authentication and postprocessing [150, 151], finite-size effects [95, 152, 153, 154, 155, 107, 145, 97, 34, 93, 85, 41], source-replacement schemes [56, 57], source maps [58], squashing maps [59, 60, 61, 62, 63] and decoy-state methods. Consequently, the framework we develop can be readily adapted to obtain security proofs for other QKD protocols, as we illustrate throughout this chapter. In particular, Section 7.3.7 provides a concrete recipe that can be followed to derive security proofs for a broad class of QKD protocols. We emphasize that this analysis relies heavily on a body of prior work in which many of the individual ingredients required for QKD security proofs were developed (and often combined) over the last few decades. The primary contribution of this chapter is the clean and fully explicit integration of these ingredients into a single, coherent, rigorous

and complete security analysis. This chapter is based on Ref. [3].

Need for a self-contained, rigorous security proof for QKD. Over the past few decades, quantum key distribution (QKD) has evolved from a theoretical concept [21] into a mature technology poised for deployment and commercial use. A critical milestone that must be achieved before QKD can be widely adopted is the certification of QKD devices by a relevant certification authority. A key ingredient of this step is the existence of a rigorous and complete security proof for the underlying QKD protocol, which can be scrutinized and vetted by the wider community [24]. Such a proof must satisfy several key criteria, as outlined in Refs. [24, 7]:

- It must specify a complete protocol relevant to practical implementations.
- It must clearly state all assumptions about the devices used.
- It must precisely state the security criterion to be satisfied.
- It must provide a rigorous mathematical proof that, under the stated assumptions, the protocol achieves the desired level of security with the specified parameters.

As discussed in Ref. [7], no existing security analysis fully meets all of the above requirements simultaneously. A recent attempt to address this gap is Ref. [33], which is currently under active scrutiny by the community. Ref. [34] presents another exemplary and fully rigorous security proof; however, it applies to an idealized qubit-based BB84 protocol and does not address the practical decoy-state setting. In this chapter, we will present our attempt at filling this gap.

Reasons for using MEAT. We employ the recently developed marginal-constrained entropy accumulation theorem (MEAT) [11] for our analysis. This approach is motivated by its ability to yield tight key rates [9], accommodate a broad range of protocol variations, and maintain a modular structure (see Section 7.3.7). Moreover, it enables the framework developed here to be readily extended to incorporate device imperfections, providing a systematic foundation for future implementation-level security analyses. The main drawbacks of this approach are its relatively recent development (limited external scrutiny) and its reliance on numerical optimization to extract key rates. We believe, however, that the former limitation will naturally diminish with time and further community validation. Furthermore, the required numerical optimizations are performed only once during the security analysis phase, and not during the execution of the QKD protocol itself. Overall,

the use of the MEAT enables us to incorporate a number of important features (explained in more detail later in this chapter) such as on-the-fly announcements, fully adaptive key-rates, ability to handle channel variability, and robustness to source and detector imperfections, while maintaining compatibility with a wide range of state preparation, measurement, and classical post-processing choices (which are also allowed to vary across rounds).

Prior work. We note that the MEAT [11] is a recent variant of the entropy accumulation theorem [41, 77, 86]. Moreover, the MEAT was first applied to the security analysis of decoy-state BB84 in Ref. [9], which also developed numerical techniques for the evaluation of finite-size key rates (see also Ref. [49]), and which we leverage in this chapter. The key rates obtained in the present work match those reported in Ref. [9]. Ref. [9] treats both variable-length and fixed-length protocols, and explicitly analyzes phase and intensity imperfections. In comparison, the analysis presented here does not explicitly model device imperfections (although it can be extended to do so). However, it is able to handle on-the-fly announcements (which arises from the way the MEAT is invoked in the security analysis) and is more general in its treatment of several structural aspects of the security proof, such as squashing maps and source maps. Moreover, it addresses certain technical issues related to classical authentication, timing of various operations, and the treatment of infinite-dimensional systems and makes explicit a few additional formal steps in the analysis.[1] The emphasis of the present work is therefore complementary: we aim to provide a fully specified protocol together with a rigorous, self-contained security analysis in which all assumptions, protocol steps, and proof components are made explicit and assembled into a single coherent framework, which is not the goal of Ref. [9].

Organization of this chapter

This chapter is organized as follows. In Section 7.1, we describe the QKD protocol to be analyzed. We do not attempt to specify a complete protocol here, but specify it in as much detail as required for the security analysis. In particular, we present a general formulation of a QKD protocol without fixing the specific states, measurements, or classical post-processing steps — leaving these components abstract. Note that a fully specified protocol can be obtain via suitable instantiation of various parameters described in Table 7.1 (see [3, Section 4.2]). In Section 7.2, we summarize the relevant tools and definitions from quantum information theory that are used in our security analysis of the QKD protocol. In Section 7.3, we rigorously establish the security of the generic QKD protocol (as defined

[1] The manuscript Ref. [3] on which this chapter is based presents an even more detailed analysis.

in Section 7.1) under the assumption that Alice sends finite-dimensional states and Bob performs finite-dimensional measurements. This culminates in Theorem 7.3.3, which states the central security result. In Section 7.4, we address the infinite-dimensional nature of practical implementations and introduce the notions of source maps and squashing maps to reduce the analysis to the finite-dimensional case. This enables the analysis to be extended to optical protocols such as decoy-state BB84. To extract concrete key rates, our results require solving a finite-dimensional convex optimization problem. In practice, any suitable numerical method may be employed, provided it satisfies certain requirements - namely, that it guarantees a reliable lower bound for the relevant minimization problem. However, such methods are quite involved. In this chapter, we directly utilize the work of Kamin et al Ref. [9], which computes key rates for decoy-state BB84, in Section 7.5. Finally, in Section 7.6, we present our concluding remarks.

7.1 Generic Protocol Specification

In this section, we describe a generic QKD protocol whose security will be proven later in Section 7.3. When supplemented with detailed specifications, and after fixing the values of various free parameters, this generic protocol turns into a particular instance of the decoy-state BB84 protocol. As usual, we assume that the protocol begins with Alice and Bob having access to local randomness stored in classical registers, which they use to implement the steps of the QKD protocol. The adversary is uncorrelated to this randomness, which is only accessible to the honest parties, and is never leaked to the adversary (even after the termination of the QKD protocol).[2] We do not explicitly describe the generation and use of these local random numbers in the QKD protocol execution; they are implicitly utilized in choosing the signal states sent, basis choices, and choosing seeds for hashing. Thus, the assumption that Alice and Bob correctly implement the prescribed state preparation and measurements (and later, hash choices) implicitly assumes that they have access to adequate randomness for doing so. We note that the assumption of perfect random numbers can be relaxed by utilizing random number generators that are ε_{rng}-close to perfect, in the composable security framework.[3]

[2]While this randomness is sometimes used to generate states or classical messages that are publicly released at some point (when explicitly specified in the protocol), what we mean by this requirement is that the "raw" values of the randomness are never made accessible to the adversary.

[3]Random number generators are often designed to output uniformly random numbers. However, the QKD protocol may need to transform this output into nonuniform random values, as some steps such as signal preparation or basis choice are often based on nonuniform probability distributions. This can be done at essentially small cost, using the "interval algorithm" described in [156] or a variant thereof in [157].

In what follows, when specifying the protocol steps and during the security analysis in Section 7.3, we restrict attention to the idealized setting in which the authentication mechanism behaves honestly, meaning that every authenticated classical message sent by one party is received correctly by the other party at some later time. This is the standard assumption adopted in QKD security analyses. Under this assumption, Alice and Bob agree on all public announcements. Consequently, the public communication can be represented by a single classical register that is accessible to all parties, including Eve, rather than by separate registers corresponding to each party's local copy of the public information. This assumption can be relaxed to more realistic authentication models; we discuss such extensions in Chapter 8.

During the execution of the protocol, the parties exchange the following classical communication which is described in the protocol steps below:

$$\widehat{C}_1^n, F_{\mathrm{K}}, F_{\mathrm{EC}}, C_{\mathrm{EC}}, H_{\mathrm{EV}}, C_{\mathrm{EV}}, F_{\mathrm{EV}}, H_{\mathrm{PA}}. \tag{7.1}$$

The final output of the protocol consists of the secret keys K_A and K_B, generated by Alice and Bob, respectively. All parameters required to instantiate an instance of this Generic QKD Protocol are given in Table 7.1. Note that the Generic QKD Protocol considered here is a more general version of the QKD Protocol from Chapter 3. It uses similar notation, but allows the state preparation, measurements, and classical processing to vary across rounds, as well as on-the-fly announcements, unlike QKD Protocol. This is because earlier proof techniques cannot handle these features, whereas the MEAT can. We also specify the protocol in greater detail (such as those pertaining to the timing of operations), and consequently introduce additional registers and explicitly defined functions.

Note that we do *not* assume that Alice and Bob have synchronized clocks for our security analysis. All timings that we refer to in this description refer to the global or true time in which these events occur, and not to Alice's and Bob's local time. Thus, we do not require Alice or Bob to have access to these global time values. They are simply introduced here since they are required in our theoretical proof.

Protocol 2 (Generic QKD Protocol)**.**

1. For rounds j from 1 to n, Alice and Bob perform the following operations:

   (a) **State preparation and transmission:** In round j, Alice performs the following steps.

Symbol	Meaning
$n \in \mathbb{N}$	Total number of rounds of the QKD protocol.
$\sigma_k^{(j)} \in \mathrm{S}_=(A')$	The kth signal state sent by Alice, in round j.
$p_k^{(j)} \in [0,1]$	Probability with which Alice sends kth signal state in round j.
$M_k^{(j)} \in \mathrm{Pos}(B_j)$	The POVM element corresponding to for outcome k of Bob's measurement in the jth round.
$f_{\mathrm{ann}}^{(j)} : \mathcal{X} \otimes \mathcal{Y} \to \widehat{\mathcal{C}}$	Function mapping Alice and Bob's local data (X_j, Y_j) to public announcements, for the jth round.
$f_{\mathrm{kmap}}^{(j)}(\cdot,\cdot) : \mathcal{X} \times \widehat{\mathcal{C}} \to \mathcal{S}$	Function implementing the mapping Alice's local data stored in X_j to S_j, based on public announcements stored in $\widehat{C}_j$, for round j.
$\lambda_{\mathrm{EC}}(\cdot) : \widehat{\mathcal{C}}^n \to \mathbb{N}$	Function that determines the number of transcripts of error-correction protocol, as a function of public announcements $\widehat{C}_1^n$.
$\ell(\cdot) : \widehat{\mathcal{C}}^n \to \mathbb{N}$	Function that determines the number of bits of output key, as a function of public announcements $\widehat{C}_1^n$.
$\varepsilon_{\mathrm{EV}} \in [0,1]$	Epsilon for error-verification. Determines output length of hash family used in error-verification, and the final correctness parameter.
$\varepsilon_{\mathrm{PA}} \in [0,1]$	Epsilon for privacy amplification. The exact input and output lengths are determined by the protocol during runtime.
$\mathcal{F}_{\mathrm{hash}}\,(l_{\mathrm{in}}, l_{\mathrm{out}})$	Universal$_2$ hash family from l_{in} bits to l_{out} bits. Used for error-verification. The exact input and output lengths are determined by the protocol during runtime.
$\mathcal{F}_{\mathrm{hash}}^{\mathrm{ideal}}\,(l_{\mathrm{in}}, l_{\mathrm{out}})$	Ideal universal$_2$ hash family from l_{in} bits to l_{out} bits. Used for privacy-amplification.

Table 7.1: Parameters required to define an instance of Generic QKD Protocol.

i. Alice prepares one of $\bar{d}_A$ possible signal states $\{\sigma_k^{(j)}\}_k$, according to the probability distribution $p_k^{(j)}$, where $\sigma_k^{(j)} \in \mathrm{S}_=(A'_j)$.[4] This step requires

[4]In this protocol specification, and in our proof, Alice is allowed send different states with different probabilities in the different rounds j, as long as the distributions are independent across rounds.

the use of local randomness. (Note that we assume that the adversary is uncorrelated with the state preparation; in particular, they do not hold any purification of the signal state, nor is any such purification made available to the adversary at any point during or after the protocol.)

ii. She stores the label k for her choice of the signal state in a classical register X_j. The register X_j has the alphabet $\mathcal{X}$.

iii. Alice sends the signal state to Bob via an insecure quantum channel.

iv. We let t_j^{A} be the (global) time this state leaves Alice's lab.

(b) **Measurements:** In round j, Bob performs the following steps:

i. Bob measures his received state using a POVM $\{M_k^{(B_j)}\}_{k=1\ldots\bar{d}_B}$, obtains one of d_B possible outcomes, and stores his results in a classical register Y_j (which has alphabet $\mathcal{Y}$). Depending on the exact detection setup used, this step may require the use of local randomness.[5]

ii. We let t_j^{B} be the (global) time this measurement is completed.

(c) **Public announcement:** Alice and Bob engage in public announcements in parallel to their signal transmission and measurement steps described above. Alice and Bob perform the following steps for each round j:

i. Bob sends a fixed message to Alice indicating that he has completed the measurement for the jth round, after he has done so.[6]

ii. Alice and Bob engage in further interactive public communication, which depends on the classical registers X_j, Y_j as well as the values announced so far. The first message in this exchange is sent by Alice at time t_j^{ann}, but only after two conditions are met: (i) she has already transmitted the jth quantum state to Bob, and (ii) she has received Bob's message confirming that his measurement for that round is complete. This ordering guarantees that announcements never precede the corresponding quantum transmission or measurement. Consequently, under the honest authentication setting, the relation $t_j^{\mathrm{ann}} > t_j^{\mathrm{A}}, t_j^{\mathrm{B}}$ is always satisfied.

iii. This classical communication can be two-way and may differ from round to round. We use $\widehat{C}_j$ (which has alphabet $\widehat{\mathcal{C}}$) to denote the classical register storing all public announcements in the jth round. For clarity, we stress that

[5] Note that we also allow Bob's measurement POVMs to depend on the rounds j.

[6] Note that this is a fixed message which is already known to Eve, since she knows the time at which Bob measures. Thus, this message leaks no information to the adversary, and we can exclude it from the public announcement registers.

$\widehat{C}_j$ is determined solely by the Alice's and Bob's classical data of that round, namely the registers X_j and Y_j, and can be computed by some function $f_{\text{ann}}^{(j)}$ acting on X_j, Y_j.[7]

Remark 7.1.1. *We stress that we do* not *require Alice and Bob to complete the announcements for round j, before proceeding to signal preparation and measurement for the next round. We only require that the announcements for round j occur at some time after signal preparation and measurement for that round. This feature of allowing Alice and Bob to perform public announcements* before *all signals are sent are received, is referred to as* ***on-the-fly*** *announcements. In particular, Alice and Bob may announce their classical registers either immediately after each round or in grouped form, where several rounds are announced together in a block of size M_{block} rounds. In the latter, $\widehat{C}_j$ for all rounds $(k_{\text{block}}-1)M_{\text{block}} < j \leq k_{\text{block}}M_{\text{block}}$ is announced simultaneously, at some time after the signal preparation and measurement of the $k_{\text{block}}M_{\text{block}}$th round. Grouping announcements in this way can reduce the overall consumption of authentication keys (see Section 8.4). As shown in Section 7.3, the security analysis remains valid under either choice.*

(d) **Sifting and key map:** Alice uses knowledge of previous public announcements (and local randomness, if needed), to map her register X_1^n to the **pre-amplification string S**.

i. Alice maps her local data X_j to the classical registers S_j (which has alphabet $\mathcal{S}$), using public announcements $\widehat{C}_j$. This is described by a function $f_{\text{kmap}}^{(j)}$ acting on $X_j, \widehat{C}_j$.[8]

ii. She then applies a deterministic rule, based solely on $\widehat{C}_j$, to discard certain rounds from S_j. This produces the (potentially shortened) pre-amplification string, which is stored in the register $\mathbf{S}$.[9] In this work, we consider protocols where Alice's remapping and discarding are defined so that whenever a value

[7] For the security analysis, we only require that $\widehat{C}_j$ should be obtained by applying a CPTP map on X_j, Y_j. Thus, we can also allow $f_{\text{ann}}^{(j)}$ to be a stochastic map. Of course, since these public announcements are carried out by two separate parties, each of which starts with access to X_j and Y_j respectively, this imposes constraints on the types of announcement functions $f_{\text{ann}}^{(j)}$ that can be actually implemented in the protocol.

[8] As with f_{ann}, we only require this mapping to be CPTP. Thus we can allow f_{kmap} to be a stochastic map.

[9] Thus, the register $\mathbf{S}$ takes values from the set of all possible strings of length less than or equal to n, and composed of symbols from the alphabet of the register S_j that are *not* discarded. In most common

of S_j will be discarded (based on $\widehat{C}_j$), S_j is set to a fixed placeholder symbol $\perp$. Since Alice determines the mapping to S_j, she can directly encode the rounds to be discarded in this way.[10]

iii. This step can be performed at any time, as long as Alice has the necessary registers $(X_j, \widehat{C}_j)$ to perform the required operations.

After all the announcements and sifting and key map operations are completed, the state of the protocol is given by

$$\rho_{\mathbf{S}S_1^n X_1^n Y_1^n \widehat{C}_1^n E_n}. \tag{7.2}$$

where E_n denotes Eve's quantum side information at the end of her attack on the n rounds (which may contain a copy of the announcements $\widehat{C}_1^n$). Alice moves on to the next step in the protocol only after all public announcements are completed, i.e, after she has sent her last message and received the last message for the public announcements corresponding to round n. Note that since Alice and Bob only perform announcements after they signal preparation and measurement for that round, this implies that Alice and only moves on to the next step after all signal preparation and measurements are completed.[11]

Remark 7.1.2. *We make the following clarification regarding the treatment of classical registers in this analysis. During the state preparation, transmission, and measurement phases, all public announcements are recorded in the registers $\widehat{C}_j$. For each such announcement, we provide Eve with an explicit copy, denoted $\widetilde{C}_j$ (introduced later in our security analysis), which she may choose to store, process, or discard. Consequently, all public announcements made during these phases are already included in Eve's final quantum system E_n at the end of the quantum communication stage. Thus, we do not necessarily need to explicitly specify that Eve has access to $\widehat{C}_1^n$ (although doing so does not cause any difference to the security analysis, since Eve is allowed to copy all announcements and keep them in E_n anyway).*

scenarios, S_j takes values in $\{0, 1, \perp\}$ (based on $\widehat{C}_j$,X_j), and the last outcome refers to the outcome that is discarded. Thus, $\mathbf{S}$ stores a binary string of length up to n bits.

[10] In principle, this means that Alice could implement the discarding step by inspecting the sequence S_1^n alone, without separately referring to the announcements $\widehat{C}_1^n$.

[11] In our protocol, it is Alice who sends the next message containing (i) the length of the output key to be produced and (ii) a parameter related to error correction, to Bob. If desired, this step could instead be initiated by Bob via a message to Alice; in that case, Bob would analogously proceed only after sending (and receiving) the final message associated with the public announcements.

In the remaining steps of the protocol, only classical communication takes place. We model these by introducing classical registers that are also accessible to Eve. If Eve wishes, she may use these classical registers together with her existing quantum system E_n to generate an updated system E'_n. However, all operations performed by Alice and Bob during this stage act solely on their own classical registers and thus commute with any operation Eve might apply to her systems. Consequently, we may, without loss of generality, postpone all of Eve's remaining operations until after the protocol has completed. Moreover, since the trace distance is non-increasing under CPTP maps, it follows that if the required security criterion holds for the state before *Eve's postponed operations, then it also holds for the state* after *she applies them (which corresponds to the actual state she obtains as a result of her attack). Hence it suffices to focus solely on analyzing the former state; in other words, we can suppose without loss of generality that Eve does not act on these classical registers at all (other than storing them).*

2. **Variable length decision:** Alice and Bob use predetermined functions of the public announcements $\widehat{C}_1^n$ to determine parameters for error correction and key generation. We use $\hat{c}_1^n$ to denote the value stored in the classical register $\widehat{C}_1^n$.

   (a) Alice computes the value $\lambda_{\mathrm{EC}}(\hat{c}_1^n) \in \mathbb{N}$ (a parameter that will be used during error correction) and stores it in F_{EC}.

   (b) Alice computes the length of the output key to be produced, given by $\ell(\hat{c}_1^n) \in \mathbb{N}$, using a predetermined function $\ell(\cdot)$, and stores this in the register F_{K}.

   (c) Alice sends $F_{\mathrm{K}}, F_{\mathrm{EC}}$ to Bob using the authenticated classical channel.

   The state in the protocol, conditioned on observing a specific value in the $\widehat{C}_1^n$ registers, is given by

$$\rho_{\mathbf{S}S_1^n X_1^n Y_1^n \widehat{C}_1^n F_{\mathrm{K}} F_{\mathrm{EC}} E_n | \Omega(\hat{c}_1^n)}, \tag{7.3}$$

   where $\Omega(\hat{c}_1^n)$ denotes the event that the value $\hat{c}_1^n$ is observed in the $\widehat{C}_1^n$ registers. Note that the functions $\ell(\cdot)$ and $\lambda_{\mathrm{EC}}(\cdot)$ are related, since $\ell(\cdot)$ must account for the amount of information leaked during error correction, which is quantified by $\lambda_{\mathrm{EC}}(\cdot)$. The relationship is established by the security proof.

Abort Condition: *If F_{K} stores $\ell(\hat{c}_1^n) = 0$, Alice and Bob abort the protocol. That is, they replace their key registers with $\perp$s and send* `abort` *for all future communication.*[12]

[12] In this case one would want Alice and Bob to avoid wasting authentication keys on messages since they

3. **Error correction:** Alice and Bob perform an error-correction subprotocol that results in Bob outputting a guess for Alice's pre-amplification string, by performing the following steps:

   (a) Alice and Bob read the value of $\lambda_{\mathrm{EC}}(\hat{c}_1^n)$ from the classical register F_{EC}.

   (b) They run an error-correction subprotocol that is designed such that the total number of possible communication transcripts is at most $2^{\lambda_{\mathrm{EC}}(\hat{c}_1^n)}$.[13]

   (c) The error correction procedure can have any number of communication rounds. Alice's steps can depend on her local information $\mathbf{S}, S_1^n, X_1^n$, prior public announcements $\widehat{C}_1^n$, and announcements during the error-correction procedure itself. Bob's steps can depend on his local information Y_1^n, public announcements $\widehat{C}_1^n$, and announcements during the error-correction procedure.

   (d) The communication transcript is stored in the classical register C_{EC}.

   (e) At the end of this procedure, Bob outputs a classical string stored in $\mathbf{S}_B$, intended as his estimate of Alice's pre-amplification string stored in $\mathbf{S}$. The protocol ensures that $\mathbf{S}$ and $\mathbf{S}_B$ are of the same length.[14]

   (f) From this point on, we ignore the registers S_1^n, X_1^n, Y_1^n. This is justified because these registers are either explicitly deleted by Alice and Bob after their use, or they no longer play any role in the subsequent steps of the protocol. In either case, they are never leaked to the adversary.

   The state in the protocol, conditioned on observing a specific value in the $\widehat{C}_1^n$ registers, is given by

$$\rho_{\mathbf{S}\mathbf{S}_B\widehat{C}_1^n C_{\mathrm{EC}} F_{\mathrm{K}} F_{\mathrm{EC}} E_n | \Omega(\hat{c}_1^n)}. \tag{7.4}$$

4. **Error verification:** Alice and Bob perform universal$_2$ hashing and compare the hash values, by performing the following:

   (a) Alice and Bob look at the length $l_{\text{pre-PA}}$ of the string in $\mathbf{S}$ ($\mathbf{S}_B$ for Bob). This determines the universal$_2$ hash family from the set of $l_{\text{pre-PA}}$-length strings to

intend to abort in the end anyway and instead simply jump to the end of the protocol. While this should not pose any real issue, we do not attempt to formalize this detail here.

[13] For one-way error-correction protocols that leak a fixed number of bits $\lambda_{\mathrm{EC}}^{\mathrm{fixed}}$, the number of possible transcripts is $2^{\lambda_{\mathrm{EC}}^{\mathrm{fixed}}}$.

[14] Since Alice's procedure of discarding rounds from S_1^n is based on public announcements $\widehat{C}_i^n$, Bob can compute this length himself, and ensure that his guess is of the same length.

$\lceil \log(1/\varepsilon_{\text{EV}}) \rceil$ bits, which we denote using $\mathcal{F}_{\text{hash}}\left(l_{\text{pre-PA}}, \lceil \log(1/\varepsilon_{\text{EV}}) \rceil\right)$.[15]

(b) Alice uses her local randomness to choose a hash function from the chosen universal$_2$ hash family. She announces the choice of the function chosen in the classical register H_{EV}.

(c) Alice announces the result of the hash function applied to $\mathbf{S}$, in the classical register C_{EV}.

(d) Bob uses the announcement H_{EV} to choose the same hash function as Alice, and applies it to his guess $\mathbf{S}_{\text{B}}$. Bob compares his computed hash value with Alice's announced value in C_{EV}, and outputs the binary result of the match in the register F_{EV}. Bob sends 1 in F_{EV} to indicate a match, and 0 for a mismatch.

Abort Condition: *If F_{EV} indicates a mismatch, Alice and Bob abort the protocol. That is, they replace their key registers with $\perp$s and send* `abort` *for all future communication.* The state in the protocol, conditioned on $\Omega(\hat{c}_1^n)$ and error-verification passing, is given by

$$\rho_{\mathbf{S}\mathbf{S}_B \widehat{C}_1^n C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{EV}} E_n | \Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}}}. \tag{7.5}$$

where $\wedge$ denotes the logical 'and' operator and Ω_{EV} denotes the event that error-verification passes, i.e F_{EV} indicates a match.

5. **Privacy amplification:** Alice and Bob perform *ideal* universal$_2$[16] hashing on their pre-amplification strings to generate the output key, as follows:

(a) Alice looks at the length $l_{\text{pre-PA}}$ of the string in $\mathbf{S}$, and the register F_{K} to determine the length $\ell(\hat{c}_1^n)$ of the output key. This determines the ideal universal$_2$ hash family from the set of $l_{\text{pre-PA}}$-length strings to $\ell(\hat{c}_1^n)$ bits, which we denote using $\mathcal{F}_{\text{hash}}^{\text{ideal}}\left(l_{\text{pre-PA}}, \ell(\hat{c}_1^n)\right)$.

(b) Alice uses her local randomness to choose a hash function from the chosen universal$_2$ hash family. She announces the choice of the function chosen in the classical register H_{PA}. Bob uses the announcement H_{PA} to choose the same function as Alice.

[15] More generally, one could also use a δ-almost-universal family. In this case, $\varepsilon_{\text{EV}} = \delta$, and $\lceil \log(1/\varepsilon_{\text{EV}}) \rceil$ is replaced by the number of the bits in the output of the chosen hash family.

[16] Recall that ideal universal$_2$ (see Definition 2.4.1) corresponds to the case where the collision probability of the hash is *equal* to $1/|D'|$, where D' is the codomain of the hash family. Note that this requirement can be relaxed to universal$_2$ by sacrificing one additional bit of output key, see Remark 3.5.1 for a discussion.

(c) Alice (Bob) applies the hash function to the $\mathbf{S}$ ($\mathbf{S}_{\mathrm{B}}$) register, and stores the result in the K_A (K_B) registers.

(d) From this point on in the protocol, we ignore the registers $\mathbf{S}, \mathbf{S}_B$, since they are longer play any role in the subsequent steps of the protocol and are never leaked to the adversary.

The state in the protocol, conditioned on $\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}$, is given by

$$\rho_{K_A K_B \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} F_{\mathrm{K}} F_{\mathrm{EC}} F_{\mathrm{EV}} H_{\mathrm{EV}} H_{\mathrm{PA}} E_n | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}}. \tag{7.6}$$

We prove the security of Generic QKD Protocol, in terms of the parameters used to describe it (see Table 7.1), in Section 7.3. Note that with the details specified in Section 3.3, one can now instantiate the Generic QKD Protocol as a polarization-encoded, decoy-state BB84 protocol.

7.2 Additional Background

In this section, we collect some additional definitions and background from information theory that will be used in our proof. We start with defining f-weighted Rényi entropies.

Definition 7.2.1. (f-weighted Rényi entropies [11, Definition 4.1] [86, Definition 4.1]) Let $\rho \in \mathrm{S}_{=}(\widehat{C}QQ')$ be a state where $\widehat{C}$ is classical with alphabets $\widehat{\mathcal{C}}$. A **tradeoff function on** $\widehat{C}$ is simply a function $f : \widehat{\mathcal{C}} \to \mathbb{R}$; equivalently, we may denote it as a real-valued tuple $\mathbf{f} \in \mathbb{R}^{|\widehat{\mathcal{C}}|}$ where each term in the tuple specifies the value $f(\hat{c})$. Given a tradeoff function f and a value $\alpha \in (0,1) \cup (1,\infty)$, we define the **$f$-weighted entropy of order** α for ρ as

$$\widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q')_\rho := \frac{\alpha}{1-\alpha} \log \left(\sum_{\hat{c}} \rho(\hat{c})\, 2^{\left(\frac{1-\alpha}{\alpha}\right)\left(\widetilde{H}_\alpha^{\uparrow}(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{c})\right)} \right), \tag{7.7}$$

Note that the f-weighted Rényi entropy reduces to the usual Rényi entropy when the function f is set to be zero for all inputs [38, Proposition 5.1]. To gain some intuition of this quantity, we can define the notion of "log-mean-exponential" of a random variable with respect to a base $b \in (0,\infty)$ as:

$$\operatorname*{lme}_{P_X,b}[g(X)] := \log_b \left(\sum_x P_X(x)\, b^{g(x)} \right). \tag{7.8}$$

With this, Eq. (7.7) can be written as

$$\widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q')_\rho = \operatorname*{lme}_{\boldsymbol{\rho}_{\widehat{C}}, b}\left[\widetilde{H}_\alpha^{\uparrow,f}(Q|Q')_{\rho_{|\widehat{c}}} - f(\widehat{C})\right], \quad \text{where } b = 2^{1-\alpha} \in (0,\infty). \tag{7.9}$$

This means non-negativity of $\widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q')_\rho \geq 0$ is equivalent to having $f(\widehat{C})$ lower bound $\widetilde{H}_\alpha^{\uparrow}(Q|Q')_{\rho_{|\widehat{C}}}$ in a log-mean-exponential sense.

Lemma 7.2.1. *(Data-processing [11, Lemma 4.4]) Let $\rho \in \mathrm{S}_=(\widehat{C}QQ')$ be classical on $\widehat{C}$, let f be a tradeoff function on $\widehat{C}$, and take any $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty]$. Then for any channel $\mathcal{E} \in \mathrm{CPTP}(Q', Q'')$,*

$$\widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q'')_{\mathcal{E}[\rho]} \geq \widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q')_\rho. \tag{7.10}$$

If $\mathcal{E}$ is an isometry, then we have equality in the above bound.

Lemma 7.2.2. *(Data-processing on non-conditioning register) Let $\rho \in \mathrm{S}_=(\widehat{C}QQ')$ be classical on $\widehat{C}$, let f be a tradeoff function on $\widehat{C}$, and take any $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty]$. Then for any unital channel $\mathcal{F} \in \mathrm{CPTP}(Q, Q'')$, i.e, $\mathcal{F}$ maps the identity operator $\mathbb{I}_Q$ to $\mathbb{I}_{Q'}$, we have*

$$\widetilde{H}_\alpha^{\uparrow,f}(Q''|\widehat{C}Q')_{\mathcal{F}[\rho]} \geq \widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q')_\rho. \tag{7.11}$$

If $\mathcal{F}$ is an isometry, then we have equality in the above bound.

Proof. Let $\alpha \in \left(\frac{1}{2}, 1\right]$, then we have

$$\begin{aligned} &\widetilde{H}_\alpha^{\uparrow}(Q|Q')_{\rho_{|\hat{c}}} \leq \widetilde{H}_\alpha^{\uparrow}(Q''|Q')_{\mathcal{F}[\rho_{|\hat{c}}]} \qquad ;\forall \hat{c} \in \widehat{C} \\ &\implies \rho(\hat{c}) 2^{\left(\frac{1-\alpha}{\alpha}\right)\left(\widetilde{H}_\alpha^{\uparrow}(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{c})\right)} \leq \rho(\hat{c}) 2^{\left(\frac{1-\alpha}{\alpha}\right)\left(\widetilde{H}_\alpha^{\uparrow}(Q''|Q')_{\mathcal{F}[\rho_{|\hat{c}}]} - f(\hat{c})\right)}, \end{aligned} \tag{7.12}$$

where the first line is an application of data processing for unital channels [38, Corollary 5.1]. Note that the inequality is saturated if $\mathcal{F}$ is an isometry. Summing over all values of $\hat{c}$, followed by taking log and multiplying both sides by $\frac{\alpha}{1-\alpha}$, yields the desired results. The proof for $\alpha > 1$ follows similarly. □

Lemma 7.2.3. *(Monotonicity in tradeoff function [4, Lemma 6.4]) (Monotonicity in f) Let $\rho \in \mathrm{S}_=(\widehat{C}QQ')$ be classical on $\widehat{C}$, let f, g be tradeoff functions on $\widehat{C}$ such that for all $\hat{c} \in \widehat{C}$ we have $f(\hat{c}) \leq g(\hat{c})$. Then, for any $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty]$, we have*

$$\widetilde{H}_\alpha^{\uparrow,g}(Q|\widehat{C}Q')_\rho \leq \widetilde{H}_\alpha^{\uparrow,f}(Q|\widehat{C}Q')_\rho. \tag{7.13}$$

We also reproduce below the core result of the MEAT framework [11]. The A registers are renumbered to reflect their role in this work, and we include only the statements that are required for our analysis.

Theorem 7.2.1. *(MEAT [11, Theorem 4.1a]) For each $j \in \{1, 2, \cdots, n\}$, take a state $\sigma^{(j)} \in \mathrm{S}_{=}(A_j)$, and a channel $\mathcal{M}_j \in \mathrm{CPTP}(A_j E_{j-1}, S_j \widehat{C}_j E_j)$, such that $\widehat{C}_j$ are classical. Let ρ be a state of the form $\rho_{S_1^n \widehat{C}_1^n E_n} = \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1[\omega_{A_1^n E_0}]$ for some $\omega \in \mathrm{S}_{=}(A_1^n E_0)$, such that $\omega_{A_1^n} = \sigma_{A_1}^{(1)} \otimes \cdots \otimes \sigma_{A_n}^{(n)}$. For each j, suppose that for every value $\hat{c}_1^{j-1}$, we have a tradeoff function $f_{|\hat{c}_1^{j-1}}$ on registers $\widehat{C}_j$. Define*

$$\begin{aligned} \kappa_{\hat{c}_1^{j-1}} &:= \inf_{\nu \in \Sigma_j} \widetilde{H}_\alpha^{\uparrow, f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j E_j \widetilde{E})_\nu, \\ \Sigma_j &:= \left\{ \mathcal{M}_j \left[\omega_{A_j E_{j-1} \widetilde{E}}\right] \;\middle|\; \omega \in \mathrm{S}_{=}(A_j E_{j-1} \widetilde{E}) \text{ s.t. } \omega_{A_j} = \sigma_{A_j}^{(j)} \right\}, \end{aligned} \tag{7.14}$$

with $\widetilde{E}$ being a register of large enough dimension to serve as a purifying register for any of the $A_j E_j$ registers. Define the following "normalized" tradeoff function on $\widehat{C}_1^n$:

$$\hat{f}_{\text{full}}(\hat{c}_1^n) := \sum_{j=1}^{n} \hat{f}_{|\hat{c}_1^{j-1}}(\hat{c}_j), \quad \text{where} \quad \hat{f}_{|\hat{c}_1^{j-1}}(\hat{c}_j) := f_{|\hat{c}_1^{j-1}}(\hat{c}_j) + \kappa_{\hat{c}_1^{j-1}}. \tag{7.15}$$

Then for any $\alpha \in (1, \infty]$ we have

$$H[\hat{f}_{\text{full}}](S_1^n|\widehat{C}_1^n E_n)_\rho \geq 0. \tag{7.16}$$

7.3 Proving security of QKD Protocol using MEAT

In this section, we embark upon proving the security of the Generic QKD Protocol. We will first begin by expressing the Generic QKD Protocol as a sequence of CPTP maps, before analyzing the sequence of maps using MEAT [11, Theorem 4.1a].

7.3.1 Expressing the protocol as a sequence of channels

The analysis in this section is identical to the analysis found in [11, Section 5]. The goal of this subsection is to reduce the QKD protocol we are interested in analyzing to one which can be expressed as a sequence of channels as described in Lemma 7.3.4 and Fig. 7.1, in preparation for the application of MEAT [11, Theorem 4.1a].

Modifying timings of the QKD protocol

Let us consider the Generic QKD Protocol described in Section 7.1. In this case, the protocol can be equivalently expressed as the following Prepare-and-measure protocol, which will be the object of our subsequent analysis. Note that since we will only be modifying certain timings and signal-preparation steps of this protocol, only the relevant parameters are listed explicitly below.

Protocol 3 (Prepare-and-measure protocol)**.**

Parameters:

$$\begin{aligned} n \in \mathbb{N}_0 \quad &: \quad \text{Total number of rounds} \\ \{\sigma^{(j)}_{X_j A'_j}\}_{j=1}^n \quad &: \quad \text{Classical-quantum states prepared by Alice} \\ \{t_j^A, t_j^B, t_j^{\text{ann}}\}_{j=1}^n \quad &: \quad \text{Timings of various steps (see below)} \end{aligned}$$

We assume that the times listed above satisfy the following conditions (see Remark 7.3.1) :

- For each $j \in \{1, 2, \ldots, n\}$, we have $t_j^A, t_j^B < t_j^{\text{ann}}$.
- Each of the sequences $\{t_j^A\}_{j=1}^n$, $\{t_j^B\}_{j=1}^n$, and $\{t_j^{\text{ann}}\}_{j=1}^n$ is monotonically increasing.

We do not impose *any* other restrictions on those timings; for instance, the sequences $\{t_j^A\}_{j=1}^n$, $\{t_j^B\}_{j=1}^n$, and $\{t_j^{\text{ann}}\}_{j=1}^n$ can be "interleaved" with each other in an arbitrary fashion as long as the first condition is satisfied. In particular, we do *not* require the public announcements to have blocksize $M_{\text{block}} = 1$; larger blocksizes are permitted precisely because such interleaving is allowed.

Protocol steps:

1. Alice and Bob perform the following steps for every $j \in \{1, 2, \ldots, n\}$.
   (a) **State preparation and transmission:** At time t_j^A, independently for each round, Alice prepares some state $\sigma_k^{(j)} \in S_=(A'_j)$ with probability $p_k^{(j)}$, and stores k in the classical register X_j. She then sends out A'_j via a public quantum channel, after which Eve may interact freely with it. This is represented via the preparation of the state $\sigma^{(j)}_{X_j A'_j} = \sum_{k=1}^{d_A} p_k^{(j)} |k\rangle\langle k|_{X_j} \otimes \sigma_k^{(j)}$.
   (b) **Measurements:** At time t_j^B, Bob receives some quantum register from Eve and measures it using some POVM, storing the outcome in a register Y_j.

(c) **Public announcement:** At time t_j^{ann}, Alice and Bob commence announcements for round j, based only on the values X_jY_j. We denote all such public information as a classical register $\widehat{C}_j$. Formally, $\widehat{C}_j$ can be viewed as the output of a CPTP map acting on the registers X_jY_j.

(d) **Sifting and key map:** At any time after t_j^{ann}, Alice computes a classical value S_j based only on her raw data X_j and the public announcements $\widehat{C}_j$. This value S_j will later be used to generate her final key via privacy amplification.

2. Alice and Bob apply various further classical procedures such as discarding values from S_1^n, variable-length decision, error correction, error verification, and privacy amplification as described in Generic QKD Protocol.

Remark 7.3.1. *Note that these conditions on the timings are extremely minimal. The first condition states that the announcements in round j only happen after Alice has sent the state in that round and Bob has measured it. This is enforced in our protocol by design: Alice only starts announcing after she has received Bob's announcement, which in turn only occurs after Bob has finished measuring. Moreover, under the honest authentication assumption, Eve cannot cause Alice to announce prematurely by impersonating Bob. The second condition is simply a basic time-ordering condition on the sequences of preparations, measurements, and announcements* individually*, without otherwise constraining them with respect to each other. These can be enforced by each party locally. In particular, these conditions do* not *limit the repetition rate as in the existing generalized EAT-based proofs [85], which require the protocol to ensure that Eve has access to only one signal at a time (i.e, Alice can only send the state for the next round after Bob has measured the current round).*

For the security proof, as we will see later, we are interested in analyzing the state at the end of Step 1 in the Prepare-and-measure protocol. However, the structure of the above protocol is not yet compatible with the MEAT. Hence we first perform some modifications to the above protocol, which modify the timings $t_j^{\text{A}}, t_j^{\text{B}}, t_j^{\text{ann}}$ of various steps to new values $\tilde{t}_j^{\text{A}}, \tilde{t}_j^{\text{B}}, \tilde{t}_j^{\text{ann}}$ satisfying:

$$\tilde{t}_1^{\text{A}} = \cdots = \tilde{t}_n^{\text{A}} < \tilde{t}_1^{\text{B}} < \tilde{t}_1^{\text{ann}} < \tilde{t}_2^{\text{B}} < \tilde{t}_2^{\text{ann}} < \cdots < \tilde{t}_n^{\text{ann}}. \tag{7.17}$$

To perform the above modification, we

- Do not modify Bob's measurement timings, i.e, we set $\tilde{t}_j^{\text{B}} = t_j^{\text{B}}$.

- Move forward all of Alice's preparations such that they happen before Bob's first measurement.
- Move forward all announcements for round j such that they happen right after Bob's measurement for that round, i.e, $\tilde{t}_j^{\mathrm{B}} < \tilde{t}_j^{\mathrm{ann}} < \tilde{t}_{j+1}^{\mathrm{B}}$. In this step, we ensure that *all* announcements for round j happen at $\tilde{t}_j^{\mathrm{ann}}$,

Thus, in the modified protocol, Alice prepares and sends out all states at time $\tilde{t}_1^{\mathrm{A}} = \tilde{t}_n^{\mathrm{A}}$. Eve is allowed to perform any operation she wants on these states. After all states have been sent, Bob begins receiving and measuring states. After he measures the first state, Alice and Bob perform all announcements for round j. Bob then measures the second state and so on.

We stress that we have not lost any generality in considering the modified protocol. This is because moving the timings of Alice's preparations and public announcements to an earlier time does not reduce Eve's capabilities in any way: any action that Eve could have done in Prepare-and-measure protocol is also possible in the modified protocol, since at any point she always has access to more registers in the modified protocol, and she is free to ignore them until the time she would have interacted with them in the original protocol. This argument lets us write the following lemma.

Lemma 7.3.1 (Modified Protocol)**.** *Consider Generic QKD Protocol with timings $t_j^{\mathrm{A}}, t_j^{\mathrm{B}}, t_j^{\mathrm{ann}}$ such that $t_j^{\mathrm{A}}, t_j^{\mathrm{B}} < t_j^{\mathrm{ann}}$, and each of the sequences $\{t_j^A\}_{j=1}^n$, $\{t_j^B\}_{j=1}^n$, and $\{t_j^{\mathrm{ann}}\}_{j=1}^n$ is monotonically increasing. Consider the modified protocol that is identical to Generic QKD Protocol except that the timings $\tilde{t}_j^{\mathrm{A}}, \tilde{t}_j^{\mathrm{B}}, \tilde{t}_j^{\mathrm{ann}}$ satisfy Eq. (7.17). Any Alice-Bob-Eve state that can be obtained in the original protocol, can also be obtained in the modified protocol.*

Proof. As described above. □

Therefore, for the purposes of proving security, we can now focus on analyzing the modified version. In the modified version, Alice prepares and sends out all states before Bob's first measurement, i.e, she prepares the global state

$$\begin{aligned} \sigma_{X_1^n (A')_1^n} &= \bigotimes_{j=1}^{n} \sigma^{(j)}_{X_j A'_j}, \\ \sigma^{(j)}_{X_j A'_j} &= \sum_{k=1}^{d_A} p_k^{(j)} \, |k\rangle\langle k|_{X_j} \otimes (\sigma_k^{(j)})_{A'_j}, \end{aligned} \tag{7.18}$$

before sending the $(A')_1^n$ systems to Eve. The evolution of the state in the modified protocol can now be described using the following lemma. Note that it is this protocol with modified timings for which for we prove certain results in later sections. For this reason, we also formalize the notion of this protocol in terms of its internal maps and states (Definition 7.3.1), and we express the relevant security requirement directly in terms of the maps that arise in the state evolution (Definition 7.3.2).

Lemma 7.3.2 (State evolution for modified protocol)**.** *Consider the Generic QKD Protocol with timings $t_j^{\mathrm{A}}, t_j^{\mathrm{B}}, t_j^{\mathrm{ann}}$ such that $t_j^{\mathrm{A}}, t_j^{\mathrm{B}} < t_j^{\mathrm{ann}}$, and each of the sequences $\{t_j^A\}_{j=1}^n$, $\{t_j^B\}_{j=1}^n$, and $\{t_j^{\mathrm{ann}}\}_{j=1}^n$ is monotonically increasing. Consider the modified protocol that is identical to the Generic QKD Protocol except that the timings $\tilde{t}_j^{\mathrm{A}}, \tilde{t}_j^{\mathrm{B}}, \tilde{t}_j^{\mathrm{ann}}$ satisfy Eq. (7.17). Then, the evolution of the state through the modified protocol can be described as follows:*

1. *Alice prepares the global state $\sigma_{X_1^n (A')_1^n}$ as in Eq. (7.18). She sends $(A')_1^n$ to Eve. Eve thus starts with $E_0 = (A')_1^n$.*[17]

   She keeps X_1^n to herself, and sends the $(A')_1^n$ systems to Eve, which we relabel to be E_0.

2. *For each round $j \in \{1, \ldots, n\}$, the following maps are applied:*

   (a) *In each round j, Eve implements her attack $\mathcal{A}_j \in \mathrm{CPTP}(E_{j-1}, B_j E'_j)$.*

   (b) *The B_j system is forwarded to Bob. Bob performs measurements on the B_j system, and stores the outcome in the Y_j register (Alice already has the X_j register). They perform public announcements for the round j, which are stored in the register $\widehat{C}_j$. A copy of the public announcements is given to Eve in the register $\widetilde{C}_j$. Alice and Bob perform sifting to generate the S_j registers. This entire process can be described by a map $\widetilde{\mathcal{G}}_j^{\mathrm{full}} \in \mathrm{CPTP}(X_j B_j, S_j X_j Y_j \widehat{C}_j \widetilde{C}_j)$.*

   (c) *The E'_j register and the $\widetilde{C}_j$ register is combined into a unified E_j register, which is passed into Eve's attack channel for the next round $\mathcal{A}_{j+1}$.*[18]

   Thus, the state after the application of these maps is given by

$$\rho_{S_1^n X_1^n Y_1^n \widehat{C}_1^n E_n} = \left(\widetilde{\mathcal{G}}_n^{\mathrm{full}} \circ \mathcal{A}_n \ldots \widetilde{\mathcal{G}}_1^{\mathrm{full}} \circ \mathcal{A}_1\right) \left[\sigma_{X_1^n (A')_1^n}\right] \tag{7.19}$$

[17] Of course, Eve may always start with additional auxiliary systems. However, since these systems are completely uncorrelated (i.e., in a trivial tensor-product form) with all the other registers in the QKD protocol, they can simply be added by Eve whenever needed, for instance when she implements her first attack channel $\mathcal{A}_1$.

[18] When $j = n$ is the last round, there is no $\mathcal{A}_{j+1}$ that is applied.

3. *Alice performs the final sifting step, generating the register* $\mathbf{S}$ *from* S_1^n *and* $\widehat{C}_1^n$.

4. *Alice and Bob perform steps such as the variable-length decision, error-correction, error-verification and privacy amplification. The final sifting operation, and the above procedures are all classical operations that are described by a map* $\mathcal{M}_{\text{CPP}} \in \text{CPTP}(X_1^n Y_1^n S_1^n \widehat{C}_1^n, K_A K_B F_{\text{K}} F_{\text{EC}} C_{\text{EC}} H_{\text{EV}} F_{\text{EV}} H_{\text{PA}})$.

Proof. The proof follows from the description of the Generic QKD Protocol with the modified timings. □

At this stage, it is convenient to use work with the following equivalent definitions of QKD protocols and security. These are generalized versions of Definitions 3.6.5 and 3.6.6, since they allow the protocol to have on-the-fly announcements.

Definition 7.3.1. We use $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \sigma_{X_1^n (A')_1^n}\right\}$ to define an instance of the time-modified Generic QKD Protocol, where $\widetilde{\mathcal{G}}_j^{\text{full}}, \mathcal{M}_{\text{CPP}}, \sigma_{X_1^n (A')_1^n}$ are defined in Lemma 7.3.2.

We can also restate the security definition Definition 3.1.1 in terms of this sequence of channels.

Definition 7.3.2 (QKD security as sequence of channels)**.** Let $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \sigma_{X_1^n (A')_1^n}\right\}$ define a QKD protocol that is described through the series of maps from Lemma 7.3.2. Let $\mathcal{R}_{\text{ideal}}$ be the map that produces the ideal output state as defined in Section 3.1. Then, the QKD protocol is $\varepsilon^{\text{secure}}$-secure if, for all Eve's attack channels $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E'_j)$, the following inequality is satisfied:

$$\left\| \left(\mathcal{M}_{\text{CPP}} \circ \widetilde{\mathcal{G}}_n^{\text{full}} \circ \mathcal{A}_n \circ \cdots \circ \widetilde{\mathcal{G}}_1^{\text{full}} \circ \mathcal{A}_1 - \mathcal{R}_{\text{ideal}} \circ \mathcal{M}_{\text{CPP}} \circ \widetilde{\mathcal{G}}_n^{\text{full}} \circ \mathcal{A}_n \circ \cdots \circ \widetilde{\mathcal{G}}_1^{\text{full}} \circ \mathcal{A}_1 \right) \left[\sigma_{X_1^n (A'')_1^n}\right] \right\|_1 \leq \varepsilon^{\text{secure}}. \tag{7.20}$$

Here, without loss of generality, we can assume that $E_j, E'_j = \mathcal{H}_\infty$ is infinite-dimensional; embedding any smaller spaces in $\mathcal{H}_\infty$ if necessary.

Applying the source-replacement scheme

In the above description, the starting state is one where Alice holds the classical register X_1^n storing the labels for the states she sent in the protocol. This state then goes through the sequence of channels described in the above lemma. While the MEAT can be be applied

to this sequence as well, doing so yields trivial results. Intuitively, this is because the application of the MEAT results in a single-round optimization that involves granting Eve access to an arbitrary purification of the system under Alice's control, which is a common feature in QKD security analysis (which we saw in earlier chapters). In this scenario, that would allow Eve to hold a purifying system for X_j which is simply a copy of X_j. This issue is straightforwardly remedied by the use of the source-replacement scheme [56, 57], which equivalently describes Alice's initial operation as preparing an entangled states followed by performing measurements on it. This is obtained in the following lemma. Note that this is again a generalized version of Lemma 3.6.1 that accounts for on-the-fly announcements.

Lemma 7.3.3 (Shield System and Source Replacement)**.** *Consider a protocol where Alice first prepares the global state*

$$\begin{aligned} \sigma_{X_1^n (A')_1^n} &= \bigotimes_{j=1}^{n} \sigma^{(j)}_{X_j A'_j} \\ \sigma^{(j)}_{X_j A'_j} &= \sum_{k=1}^{d_A} p_k^{(j)} \, |k\rangle\langle k|_{X_j} \otimes (\sigma_k^{(j)})_{A'_j} \end{aligned} \tag{7.21}$$

where $\{|k\rangle\}_{X_j}$ *denotes the classical basis of* X_j*. She keeps* X_1^n *to herself, and sends the* $(A')_1^n$ *systems to Eve. Then, the state* $\sigma_{X_1^n (A')_1^n}$ *can equivalently be obtained by*

1. *Preparing the global state*

$$\begin{aligned} \sigma_{\bar{A}_1^n \hat{A}_1^n (A')_1^n} &= \bigotimes_{j=1}^{n} \sigma^{(j)}_{\bar{A}_j \hat{A}_j A'_j} \\ \sigma^{(j)}_{\bar{A}_j \hat{A}_j A'_j} &= \sum_{k,i=1}^{d_A} \sqrt{p_i^{(j)} p_k^{(j)}} \, |i\rangle\langle k|_{\bar{A}} \otimes \left|\sigma_i^{(j)}\right\rangle\!\left\langle\sigma_k^{(j)}\right|_{\hat{A}_j A'_j} \end{aligned} \tag{7.22}$$

   where $\left|\sigma_k^{(j)}\right\rangle_{\hat{A}_j A'_j}$ *denotes a purification of the state* $(\sigma_k^{(j)})_{A'_j}$*,* $\{|k\rangle\}_{k=1,\ldots,d_A}$ *is an orthonomal basis for* $\bar{A}$*, and* $\hat{A}_j$ *is referred to as the shield system.*

2. *Sending the state* $(A')_1^n$ *to Eve,*

3. *For each* $j \in \{1, \ldots, n\}$*, measuring the* $\bar{A}_j \hat{A}_j$ *systems using the POVM* $\{|k\rangle\langle k|_{\bar{A}_j} \otimes \mathbb{I}_{\hat{A}_j}\}_{k \in \{1,\ldots,d_A\}}$*, and storing the result in* X_j*.*

Proof. For any round j, first consider the single round states $\sigma_{X_j A'_j}$ and $\sigma_{\bar{A}_j \hat{A}_j A'_j}$ as defined in Eqs. (7.21) and (7.22). Simple algebra tell us that measuring $\sigma_{\bar{A}_j \hat{A}_j A'_j}$ with the POVM $\{|k\rangle\langle k|_{\bar{A}_j} \otimes \mathbb{I}_{\hat{A}_j}\}_{k \in \{1,\ldots,d_A\}}$, and storing the result in X_j would result exactly in $\sigma_{X_j A'_j}$. The n-round case follows similarly by considering the n-round states and n-round IID POVM instead. □

Note that $\left|\sigma_k^{(j)}\right\rangle_{\hat{A}_j A'_j}$ can be *any* purification of $(\sigma_k^{(j)})_{A'_j}$. Crucially, we now observe that after the usage of the source replacement scheme to describe signal preparation using Lemma 7.3.3, Alice's operations are now equivalent to her preparing a global pure state $\sigma_{\bar{A}_1^n \hat{A}_1^n (A')_1^n}$, and then performing a suitable measurement on the $\bar{A}_j$ registers to produce classical data in the X_j systems. This has the critical property that Alice's measurements on the $\bar{A}_j$ systems commute with all other operations that do not depend on the X_j registers. In particular, Alice's measurements commutes with Eve's attack, and thus we can delay her measurements and assume that she does her measurements at the same time as Bob. This allows us to focus our analysis to that of the following virtual entanglement-based protocol, which produces the *same exact* final state as the modified protocol from Lemma 7.3.1 (or the evolution of the state described in Lemma 7.3.2). This will be the protocol we analyze in subsequent sections. A security proof for this protocol implies the security proof of Generic QKD Protocol via Lemmas 7.3.1 to 7.3.3.

Remark 7.3.2. *Note that in the arguments above, we modify the timings of Alice's operations* twice *- first by moving them earlier in time, and then by moving some of them later in time. Specifically, we initially argue that without loss of generality, one can assume that all state preparations are performed at the start of the protocol. This modification gives more power to Eve and thus only strengthens our security claims. Next, we apply the source-replacement technique, replacing Alice's state sending operations with the preparation of a global entangled state, part of which is sent to Eve ($(A')_1^n$), part of which is kept with Alice but not measured ($\hat{A}_1^n$), and part of which is kept with Alice and measured ($\bar{A}_1^n$). Finally, we argue that since Alice's measurements commute with all operations except the public announcements (which depend on X_1^n), those measurements can be postponed to after Eve's attack and just before public announcements for that round, without affecting Eve's strategy. Note that Alice's global state preparation still occurs at the initial time.*

Protocol 4 (Virtual entanglement-based protocol)**.** .

Parameters:

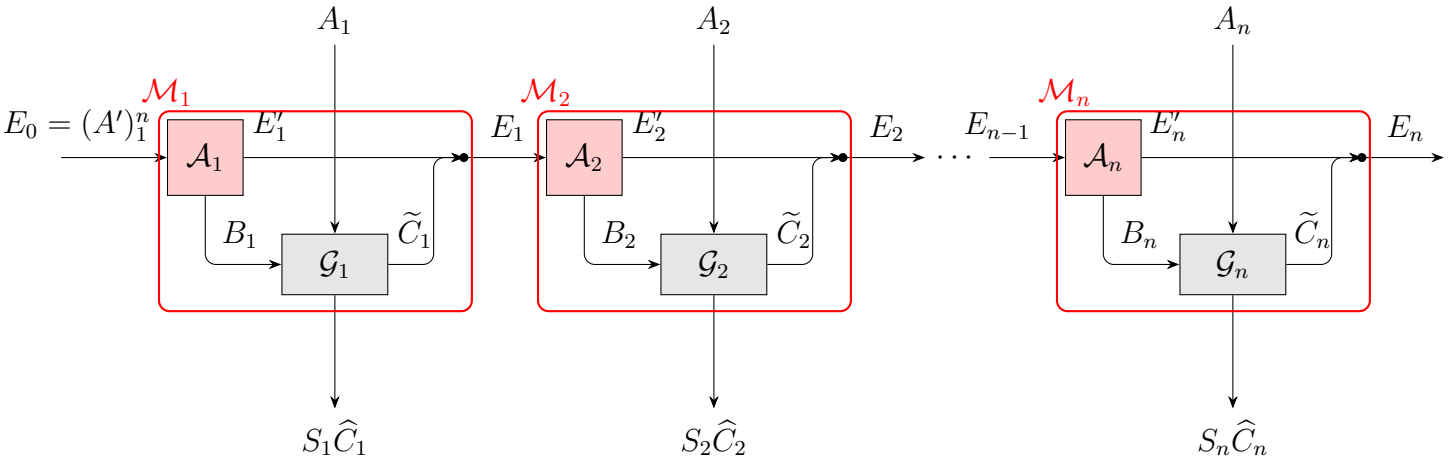


Figure 7.1: The evolution of the state through Eve's attack channels $\{\mathcal{A}_j\}$, and Alice and Bob's operations $\{\mathcal{G}_j\}$ for the Virtual entanglement-based protocol. The evolution of states is also described in Lemma 7.3.4. Note that the announcements $\widehat{C}_j$ are made available to Eve through an explicit copy $\widetilde{C}_j$, which gets merged with E'_j to form E_j.

$$
\begin{aligned}
n \in \mathbb{N}_0 \quad &: \quad \text{Total number of rounds} \\
\{\sigma^{(j)}_{\bar{A}_j \hat{A}_j A'_j}\}_{j=1}^n \quad &: \quad \text{Pure quantum states prepared by Alice} \\
\{\tilde{t}_j^A = \tilde{t}_j^B, \tilde{t}_j^{\text{ann}}\}_{j=1}^n \quad &: \quad \text{Timings of various steps (see below), satisfying } \tilde{t}_1^{\text{B}} < \\
& \qquad \tilde{t}_1^{\text{ann}} < \tilde{t}_2^{\text{B}} < \tilde{t}_2^{\text{ann}} < \cdots < \tilde{t}_n^{\text{ann}}.
\end{aligned}
$$

Protocol steps:

1. **State preparation and transmission:** Alice prepares a global pure state $\sigma_{\bar{A}_1^n \hat{A}_1^n (A')_1^n} = \bigotimes_{j=1}^n \sigma^{(j)}_{\bar{A}_j \hat{A}_j A'_j}$. She sends out all of the $(A')_1^n$ registers to Eve. She keeps $\bar{A}_1^n \hat{A}_1^n$ with herself.

2. Alice and Bob perform the following steps for every $j \in \{1, 2, \ldots, n\}$.

   (a) **Measurements:** At time $\tilde{t}_j^{\text{B}}$, Bob receives quantum register B_j from Eve, and performs a measurement on it, storing the outcome in the register Y_j. At the same time[19] , Alice performs a measurement in the computational basis on the $\bar{A}_j$ system, and stores the measurement outcome in the X_j register.

[19]Since this is a purely virtual protocol used only within the security proof, there is no need for Alice and Bob to physically implement these operations simultaneously.

(b) **Public Announcements:** At time $\tilde{t}_j^{\text{ann}}$, Alice and Bob perform some public announcements which may be interactive. We denote all public announcements for round j with the register $\widehat{C}_j$. A copy of these announcements in the register $\widetilde{C}_j$ is made available to Eve.

(c) **Sifting and key map:** At time $\tilde{t}_j^{\text{ann}}$, Alice maps her private data X_j and public announcements $\widehat{C}_j$ to a classical value S_j.

3. Alice and Bob apply various further classical procedures such as variable-length decision, error correction, error certification, and privacy amplification as described in Generic QKD Protocol.

It is convenient to view the above Virtual entanglement-based protocol as a sequence of maps, depicted in Fig. 7.1 and described in the following Lemma 7.3.4.

Lemma 7.3.4 (Describing evolution of states for QKD protocol from Virtual entanglement-based protocol)**.** *The evolution of the state in the QKD protocol can be treated as occurring as follows:*

1. *Alice prepares the state $\sigma_{\bar{A}_1^n \hat{A}_1^n (A')_1^n}$, and sends A'^n_1 to Eve. We treat this as E_0.*
2. *For each round j from 1 to n, the following maps are applied:*
   (a) *In each round j, Eve implements her attack $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E'_j)$.*
   (b) *The B_j system is forwarded to Bob. Alice and Bob then perform measurements on the $\bar{A}_j$ and B_j systems, and store them in registers X_j and Y_j, and perform public announcements $\widehat{C}_j$. A copy $\widetilde{C}_j$ of the announcements $\widehat{C}_j$ is given to Eve. They perform sifting to generate the S_j registers. This entire process can be described by a map $\mathcal{G}_j^{\text{full}} \in \text{CPTP}(A_j B_j, S_j X_j Y_j \widehat{C}_j \widetilde{C}_j)$, where $A_j = \bar{A}_j \hat{A}_j$ denotes the registers that do not leave Alice's lab. We let $\mathcal{G}_j \in \text{CPTP}(A_j B_j, S_j \widehat{C}_j \widetilde{C} j)$ denote the map $\mathcal{G}_j := \text{Tr}_{X_j Y_j} \circ \mathcal{G}_j^{\text{full}}$, i.e. $\mathcal{G}_j^{\text{full}}$ with its output registers restricted to the secret register and public announcements.*
   (c) *The E'_j register and the $\widetilde{C}_j$ register is combined into a unified E_j register, which is passed into Eve's attack channel for the next round $\mathcal{A}_{j+1}$.*[20]

[20] When $j = n$, there is no $\mathcal{A}_{n+1}$ that is applied.

Thus, the state after the application of these maps is given by

$$\begin{aligned}\rho_{S_1^n X_1^n Y_1^n \widehat{C}_1^n E_n} &= \left(\mathcal{G}_n^{\text{full}} \circ \mathcal{A}_n \dots \mathcal{G}_1^{\text{full}} \circ \mathcal{A}_1\right)\left[\sigma_{\bar{A}_1^n (\hat{A})_1^n (A')_1^n}\right] \\ \rho_{S_1^n \widehat{C}_1^n E_n} &= \left(\mathcal{G}_n \circ \mathcal{A}_n \dots \mathcal{G}_1 \circ \mathcal{A}_1\right)\left[\sigma_{\bar{A}_1^n (\hat{A})_1^n (A')_1^n}\right].\end{aligned} \tag{7.23}$$

Furthermore, we have $\mathcal{G}_j^{\text{full}} = \widetilde{\mathcal{G}}_j^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\{|k\rangle\langle k|_{\bar{A}_j} \otimes \mathbb{I}_{\hat{A}}\}}$*, where* $\mathcal{M}^{\text{meas}}_{\{|k\rangle\langle k|_{\bar{A}_j} \otimes \mathbb{I}_{\hat{A}}\}} \in \text{CPTP}(\bar{A}_j \hat{A}_j, X_j)$ *is a channel that measures the* $\bar{A}_j$ *system using POVM* $\{|k\rangle\langle k|_{\bar{A}_j} \otimes \mathbb{I}_{\hat{A}}\}_k$ *and stores the outcome in the* X_j *system (see Definition 2.1.8), and* $\widetilde{\mathcal{G}}_j^{\text{full}}$ *does all remaining operations except the initial measurement by Alice, and is the same as in Lemma 7.3.2.*

3. *Alice performs the final sifting step, generating the register* $\mathbf{S}$ *from* S_1^n *and* $\widehat{C}_1^n$*.*

4. *Alice and Bob perform steps such as the variable-length decision, error-correction, error-verification and privacy amplification. The final sifting operation, and the above procedures are together described by a map* $\mathcal{M}_{\text{CPP}} \in \text{CPTP}(X_1^n Y_1^n S_1^n \widehat{C}_1^n, K_A K_B F_{\text{K}} F_{\text{EC}} C_{\text{EC}} H_{\text{EV}} F_{\text{EV}} H_{\text{PA}})$*.*

Proof. The proof follows directly from the description of Virtual entanglement-based protocol. Recall that this protocol is obtained from Prepare-and-measure protocol (with the modified timings specified in Lemma 7.3.1) by replacing the state preparation step through the source-replacement scheme (Lemma 7.3.3). The state evolution of Prepare-and-measure protocol with the modified timings is given in Lemma 7.3.2. The required state evolution for Virtual entanglement-based protocol is then obtained by applying the same modification (arising from the source-replacement scheme) to the state evolution from Lemma 7.3.2. □

7.3.2 Dimensions of Eve's systems

Our goal is to prove that the security statement holds for *all* possible attacks by Eve. Concretely, this requires showing that the security definition (Definition 7.3.2) is satisfied for *every* possible attack channel $\mathcal{A}_j$. A subtlety arises here: since $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E'_j)$, our analysis must also account for the *dimensions* of the auxiliary spaces E'_j that Eve may introduce. In principle, these spaces could even be infinite-dimensional. Moreover, Alice's state preparation $(\hat{A}_j, A'_j)$ and Bob's measurements (B_j) may themselves involve infinite-dimensional systems. However, the MEAT theorem is formulated only under the assumption that all registers are finite-dimensional. To reconcile this mismatch, we proceed as follows:

1. **Dimensions of Alice and Bob:** We first assume that Alice prepares finite-dimensional states and Bob performs finite-dimensional measurements. The proof in this section is restricted to this finite-dimensional Alice and Bob setting. Later, in Section 7.4, we show how these restrictions can be lifted by introducing appropriate source maps and squashing maps. With this, the only remaining issue is the dimensionality of Eve's systems.

2. **Security against arbitrary but finite-dimensional Eve:** Next, we fix an arbitrary finite dimension d_j for each E'_j. For this setting, we consider a sequence of attack channels $\{\mathcal{A}_j\}_j$ with $\mathcal{A}_j \in \mathrm{CPTP}(E'_{j-1}\widetilde{C}_{j-1}, E'_j B_j)$ and establish security in a way that does not depend on the particular choice of $\{\mathcal{A}_j\}_j$. Critically, the resulting security statement we obtain is independent of the values of d_j. Hence, security holds against all attacks where Eve's systems are finite-dimensional.

3. **Infinite-dimensional Eve:** Finally, we extend the argument to infinite-dimensional systems. Intuitively, since our security statement holds for arbitrary finite dimensions d_j of Eve's systems, one can take the limit $d_j \to \infty$ to recover the result when Eve uses infinite-dimensional systems. This limiting argument is made rigorous in [3, Appendix A], and is not included in this thesis.

Thus, in the following subsections, we fix a finite dimension d_j for each E'_j. Note that this issue of specifying Eve's dimension is primarily a technical nuisance rather than a conceptual obstacle. Intuitively, in a protocol where state preparation, measurements, and announcements are all finite-dimensional, Eve cannot do better than implement some unitary operation in each round as part of her attack. In such a setting, she only ever requires finite-dimensional registers. For a fully rigorous analysis, one must formalize a suitable version of this intuition [3, Appendix A].

Remark 7.3.3. *Let us focus on the infinite-dimensional aspects of Eve. Note that this issue does not arise when using the post-selection technique (Chapter 5): because that approach has an explicit dimension dependence, one must first reduce the protocol itself to a finite-dimensional Alice-Bob setting. After this reduction, Eve's attack can be taken to consist of holding a purification of a finite-dimensional state, which can (without loss of generality) be assumed to be finite-dimensional as well.*

In contrast, the EUR approach in Chapter 6 has no explicit dimension dependence. In that setting, the finite dimensional Alice-Bob setting results in Eve holding some purification of this state, and security is straightforward. However, since there is no dimension dependence, our analysis in Chapter 6 is applied without any squashing operation, where

Bob measures infinite-dimensional systems. Thus, it invokes several entropy statements that are technically stated only for finite-dimensional systems, but applied them to infinite-dimensional systems. We note that this is a common technical gap in many analyses, where statements proved for arbitrary finite-dimensional systems without explicit dimensional dependence are applied to infinite-dimensional systems. This discrepancy can be resolved using the approach from [3, Appendix A]

7.3.3 Security proof for Generic QKD Protocol (finite-dimensional case)

Recall that we are in the setting where Alice prepares finite-dimensional states, Bob performs finite-dimensional measurements and each E'_j has dimension d_j. We start by fixing the set of attack channels $\{\mathcal{A}_j\}_j$, and consider the fixed state obtained corresponding to this attack. As usual, we first use Lemma 3.1.1 to break up the security requirement into secrecy and correctness. The fact that the protocol is $\varepsilon^{\text{correct}}$-correct follows in exactly the same manner as the proof of Lemma 3.4.1. Thus, we focus only on proving secrecy.

Let us first consider the event $\Omega(\hat{c}_1^n)$, defined as the event that the public announcements $\widehat{C}_1^n$ took the value $\hat{c}_1^n$. Observe that in the protocol, the privacy amplification step is performed conditioned on the value $\hat{c}_1^n$ (and conditioned on error verification accepting), i.e. it is applied on the state $\rho_{\mathbf{S}C_{\text{EC}}C_{\text{EV}}F_{\text{K}}F_{\text{EC}}F_{\text{EV}}H_{\text{EV}}E_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}}$. Hence we would be interested in lower bounding the Rényi entropy of register $\mathbf{S}$ in this state, which will be used in the application of the Leftover Hashing Lemma (Lemma 3.5.1). However, the formulation of MEAT [11, Theorem 4.1a] that we use later in Theorem 7.3.2 is best suited in analyzing *sequential* processes, and thus allows us to lower bound the Rényi entropy of register S_1^n of the state $\rho_{S_1^nC_{\text{EC}}C_{\text{EV}}F_{\text{K}}F_{\text{EC}}F_{\text{EV}}H_{\text{EV}}E_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}}$. Since S_1^n and $\mathbf{S}$ can be transformed into one another by using the public announcements $\widehat{C}_1^n$, we expect the two entropies to be equal. This can be argued using the following lemma.

Lemma 7.3.5 (Equality of entropies of S_1^n and $\mathbf{S}$)**.** *For any event $\Omega(\hat{c}_1^n)$, consider the state just after the key map and sifting steps in the QKD protocol (see Lemma 7.3.4), given by $\rho_{\mathbf{S}S_1^nX_1^nY_1^n\widehat{C}_1^nE_n}$. Then, the following statement holds:*

$$\widetilde{H}_\alpha^\uparrow(\mathbf{S}|E_n)_{\rho_{|\Omega(\hat{c}_1^n)}} = \widetilde{H}_\alpha^\uparrow(S_1^n|E_n)_{\rho_{|\Omega(\hat{c}_1^n)}}. \tag{7.24}$$

Moreover, this equality continues to hold at any later point in the protocol prior to privacy

amplification. In particular,

$$\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|C_{\mathrm{EC}}C_{\mathrm{EV}}F_{\mathrm{K}}F_{\mathrm{EC}}F_{\mathrm{EV}}H_{\mathrm{EV}}E_n)_{\rho_{|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}} = \widetilde{H}^{\uparrow}_{\alpha}(S_1^n|C_{\mathrm{EC}}C_{\mathrm{EV}}F_{\mathrm{K}}F_{\mathrm{EC}}F_{\mathrm{EV}}H_{\mathrm{EV}}E_n)_{\rho_{|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}}, \tag{7.25}$$

where we consider a version of the protocol in which the register S_1^n is not deleted after use in the above equation.

Proof. Recall that the protocol generates $\mathbf{S}$ from S_1^n by applying a deterministic discard rule based on $\widehat{C}_1^n$. In particular, S_1^n can be transformed into $\mathbf{S}$ by discarding certain positions (as specified by $\widehat{C}_1^n$), and $\mathbf{S}$ can be transformed back into S_1^n by inserting $\perp$ symbols at the appropriate locations (again determined by $\widehat{C}_1^n$). Since we are considering states conditioned on specific values of $\widehat{C}_1^n$, the two states are related by isometries $V_{\mathbf{S}\to S_1^n}$ and $V_{S_1^n\to\mathbf{S}}$ (both of which depend on $\hat{c}_1^n$), such that

$$\begin{aligned} V_{\mathbf{S}\to S_1^n}\rho_{\mathbf{S}E_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}V^{\dagger}_{\mathbf{S}\to S_1^n} &= \rho_{S_1^nE_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}} \\ V_{S_1^n\to\mathbf{S}}\rho_{S_1^nE_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}V^{\dagger}_{S_1^n\to\mathbf{S}} &= \rho_{\mathbf{S}E_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}}. \end{aligned} \tag{7.26}$$

Then, the required statement follows from the fact that Rényi entropies are invariant under isometries on the first system (Lemma 7.2.2).[21] Note that the statement holds throughout the protocol, since the same isometries exist at every stage. □

We will now state the following theorem, which states that if the f-weighted Rényi entropy of the private string S_1^n is positive, then the secrecy requirement can be satisfied by a suitable choice of the $l(\cdot)$ and $\lambda_{\mathrm{EC}}(\cdot)$ functions. This suggests that the f-weighted Rényi entropy is a particularly useful object of study for the purposes of QKD security analysis. The proof of the following theorem is essentially the same as the one developed in Ref. [87] (reproduced with permission in Ref. [9]), and that work should be cited as the source whenever possible.

Theorem 7.3.1 (f-weighted entropy to variable-length secrecy)**.** *Consider the state just after the key map step in Virtual entanglement-based protocol that is obtained from the Generic QKD Protocol. Consider any $\alpha \in (1,2)$, and let $\hat{f}_{\mathrm{full}}$ be any tradeoff function on the classical registers $\widehat{C}_1^n$ such that*

$$\widetilde{H}^{\uparrow,\hat{f}_{\mathrm{full}}}_{\alpha}(S_1^n|\widehat{C}_1^nE_n)_{\rho} \geq 0, \tag{7.27}$$

[21] Note that we only require the isometry to hold in one direction for this proof to work.

and let $l(\hat{c}_1^n)$ *be given by*

$$l(\hat{c}_1^n) = \max\left\{0, \left\lfloor \hat{f}_{\text{full}}^{\text{QKD}}(\hat{c}_1^n) - \lambda_{\text{EC}}(\hat{c}_1^n) - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}}\right)\right\rceil - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\text{PA}}}\right) + 2\right\rfloor\right\}, \quad (7.28)$$

where $\hat{f}_{\text{full}}^{\text{QKD}}$ *"lower-bounds"* $\hat{f}_{\text{full}}$*, i.e, satisfies*

$$\hat{f}_{\text{full}}^{\text{QKD}}(\hat{c}_1^n) \leq \hat{f}_{\text{full}}(\hat{c}_1^n) \qquad \forall \hat{c}_1^n. \quad (7.29)$$

Then, the state obtained by performing sifting, error-correction and privacy amplification on this state as described in Generic QKD Protocol is ε_{PA}*-secret.*

Proof. Recall that for proving ε_{PA}-secrecy, one has to show that that the distance between the real and the ideal Alice-Eve states is smaller than ε_{PA}, i.e,

$$\sum_l \Pr(\Omega_{\text{len}=l})\frac{1}{2}\left\|\rho_{K_A C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_n|\Omega_{\text{len}=l}} - \tau_{K_A}^{(l)} \otimes \rho_{C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_n|\Omega_{\text{len}=l}}\right\|_1 \leq \varepsilon_{\text{PA}} \quad (7.30)$$

where we recall that $\tau_{K_A}^{(l_A)} = \sum_{k\in\{0,1\}^{l_A}} \frac{1}{2^{l_A}} |k\rangle\langle k|$ was defined in Eq. (8.4) to be the ideal output key state. The required statement follows from the following series of inequalities (explained in the paragraph later):

$$\sum_{l=0}^{\infty} \Pr(\Omega_{\text{len}=l})\frac{1}{2}\left\|\rho_{K_A C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_n|\Omega_{\text{len}=l}} - \tau_{K_A}^{(l)} \otimes \rho_{C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_n|\Omega_{\text{len}=l}}\right\|_1 \quad (7.31)$$

$$\leq \sum_{\{\hat{c}_1^n | \ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}}) \times \quad (7.32)$$

$$\frac{1}{2}\left\|\rho_{K_A C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}} - \tau_{K_A} \otimes \rho_{C_{\text{EC}} C_{\text{EV}} F_{\text{K}} F_{\text{EC}} F_{\text{EV}} H_{\text{PA}} H_{\text{EV}} E_n|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}}\right\|_1$$

$$\leq \sum_{\{\hat{c}_1^n | \ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}}) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(\mathbf{S}|C_{\text{EC}} C_{\text{EV}} F_{\text{EC}} F_{\text{EV}} F_{\text{K}} H_{\text{EV}} E_n)_{\rho|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}} - \ell(\hat{c}_1^n)+2\right)} \quad (7.33)$$

$$= \sum_{\{\hat{c}_1^n | \ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\text{EV}}) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(\mathbf{S}|C_{\text{EC}} C_{\text{EV}} H_{\text{EV}} E_n)_{\rho|\Omega(\hat{c}_1^n)\wedge\Omega_{\text{EV}}} - \ell(\hat{c}_1^n)+2\right)} \quad (7.34)$$

$$\leq \sum_{\{\hat{c}_1^n | \ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n)) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(\mathbf{S}|C_{\text{EC}} C_{\text{EV}} H_{\text{EV}} E_n)_{\rho|\Omega(\hat{c}_1^n)} - \ell(\hat{c}_1^n)+2\right)} \quad (7.35)$$

Here, Eq. (7.31) just restates the quantity we wish to bound. In Eq. (7.32), we rewrite the sum over all possible values of $\hat{c}_1^n$, and use the triangle inequality and the fact that the distance between the real and ideal states is zero when the protocol does not produce a key. Hence, we only need to keep events corresponding to a key of non-zero length being generated in the sum over $\hat{c}_1^n$. In Eq. (7.33), we used the Leftover Hashing Lemma (Lemma 3.5.1). In Eq. (7.34), we used the fact that values of $F_{\mathrm{EC}}, F_{\mathrm{EV}}, F_{\mathrm{K}}$ are uniquely determined by the event $\Omega(\hat{c}_1^n)$, and therefore can be removed from the conditioning registers without penalty.[22] Eq. (7.35) follows by using $\rho_{|\Omega(\hat{c}_1^n)\wedge\Omega_{\mathrm{EV}}} = \rho_{(|\Omega(\hat{c}_1^n))|\Omega_{\mathrm{EV}}}$, and a direct application of Lemma 2.2.3 to get rid of the conditioning on Ω_{EV}, where we absorb the correction term into the probability before the exponential. Continuing this chain of inequalities, we get

$$\leq \sum_{\{\hat{c}_1^n|\ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n)) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(\mathbf{S}|H_{\mathrm{EV}}E_n)_{\rho|\Omega(\hat{c}_1^n)} - \lambda_{\mathrm{EC}}(\hat{c}_1^n) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \ell(\hat{c}_1^n)+2\right)} \tag{7.36}$$

$$\leq \sum_{\{\hat{c}_1^n|\ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n)) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(\mathbf{S}|E_n)_{\rho|\Omega(\hat{c}_1^n)} - \lambda_{\mathrm{EC}}(\hat{c}_1^n) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \ell(\hat{c}_1^n)+2\right)} \tag{7.37}$$

$$\leq \sum_{\{\hat{c}_1^n|\ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n)) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(\mathbf{S}|E_n)_{\rho|\Omega(\hat{c}_1^n)} - \hat{f}_{\mathrm{full}}(\hat{c}_1^n) + \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\mathrm{PA}}}\right)\right)} \tag{7.38}$$

$$\leq \varepsilon_{\mathrm{PA}} \sum_{\{\hat{c}_1^n|\ell(\hat{c}_1^n)>0\}} \Pr(\Omega(\hat{c}_1^n)) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n|E_n)_{\rho|\Omega(\hat{c}_1^n)} - \hat{f}_{\mathrm{full}}(\hat{c}_1^n)\right)} \tag{7.39}$$

$$\leq \varepsilon_{\mathrm{PA}} \sum_{\hat{c}_1^n} \Pr(\Omega(\hat{c}_1^n)) 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^\uparrow(S_1^n|E_n)_{\rho|\Omega(\hat{c}_1^n)} - \hat{f}_{\mathrm{full}}(\hat{c}_1^n)\right)} \tag{7.40}$$

$$= \varepsilon_{\mathrm{PA}}\, 2^{\frac{1-\alpha}{\alpha}\left(\widetilde{H}_\alpha^{\uparrow,\hat{f}_{\mathrm{full}}}(S_1^n|\widehat{C}_1^n E_n)_\rho\right)} \tag{7.41}$$

$$\leq \varepsilon_{\mathrm{PA}}. \tag{7.42}$$

Eq. (7.36) follows by using Lemma 2.2.4 to split off the error-correction and error-verification registers. Eq. (7.37) then follows since we can now remove the H_{EV} register which stored the hash-choice for error verification, since it is independent of the rest of the registers,

[22] This can be seen formally by observing that when we condition on $\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}$, one can transform between the state with the $F_{\mathrm{EC}}, F_{\mathrm{EV}}, F_{\mathrm{K}}$ registers and the state without them using a CPTP map in either direction. In both directions, the CPTP map acts only on the conditioning registers. Therefore, Lemma 2.2.2 applies both ways, yielding the desired equality.

without penalty, by using data processing in both directions. Eq. (7.38) follows from the fact that the output key length $\ell(\hat{c}_1^n)$ satisfies Eqs. (7.28) and (7.29). Eq. (7.39) is simple algebra. For Eq. (7.40), observe that we add more (positive) terms to the sum over $\hat{c}_1^n$, and thus the resulting quantity must be larger. Eq. (7.41) follows from the definition of f-weighted Rényi entropy from Definition 7.2.1. Eq. (7.42) follows from $\alpha > 1$ and the fact that the $\hat{f}_{\text{full}}$-weighted Rényi entropy is positive, i.e, Eq. (7.27). This concludes our proof. □

Thus, the task reduces to finding a tradeoff function $\hat{f}_{\text{full}}$ such that

$$\widetilde{H}_\alpha^{\uparrow, \hat{f}_{\text{full}}}(S_1^n \mid \widehat{C}_1^n E_n)_\rho \geq 0.$$

This is precisely the setting in which the MEAT can be applied, as we show in the next subsection. We will first carry out this analysis for a fixed attack by the adversary, and subsequently remove this restriction by performing a worst-case analysis over all possible attacks.

Remark 7.3.4. *Recall that the above requirement is demanding that $\hat{f}_{\text{full}}(\hat{c}_1^n)$ lower bounds $\widetilde{H}_\alpha^{\uparrow}(S_1^n|E_n)$ in the log-mean-exponential sense (see Section 7.2). This is a somewhat weaker requirement than the one imposed in the variable length security proofs of Chapter 4, where a statistical estimator $b_{\text{stat}}(\hat{c}_1^n)$ was required to lower bound $\widetilde{H}_\alpha^{\uparrow}(S_1^n|E_n)$ with high probability.*

7.3.4 Security via application of MEAT

Theorem 7.3.2 (Obtaining $\hat{f}_{\text{full}}$ satisfying Eq. (7.27))**.** *Let $\rho_{S_1^n \widehat{C}_1^n E_n}$ be the state obtained in the QKD protocol, i.e, via Eq. (7.23) from Lemma 7.3.4 or Fig. 7.2. For each j, and every value of $\hat{c}_1^{j-1}$, let $f_{|\hat{c}_1^{j-1}}$ be a tradeoff function on the register $\widehat{C}_j$, and define $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right)$ as:*

$$\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right) := \inf_{\nu \in \Sigma_j(\mathcal{A}_j)} \widetilde{H}_\alpha^{\uparrow, f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j E_j \widetilde{E})_\nu \tag{7.43}$$

where

$$\Sigma_j(\mathcal{A}_j) := \left\{ \mathcal{G}_j \circ \mathcal{A}_j\left(\omega_{A_j E_{j-1} \widetilde{E}}\right) \;\middle|\; \omega_{A_j} = \sigma_{A_j}^{(j)} \right\}, \tag{7.44}$$

where $\widetilde{E}$ is a purifying register any of the $A_j E_{j-1}$ registers. Then the following "normalized" tradeoff function on $\hat{C}_1^n$:

$$\hat{f}_{\text{full}}(\hat{c}_1^n) := \sum_{j=1}^{n} \left(f_{|\hat{c}_1^{j-1}}(\hat{c}_j) + \kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right)\right) \tag{7.45}$$

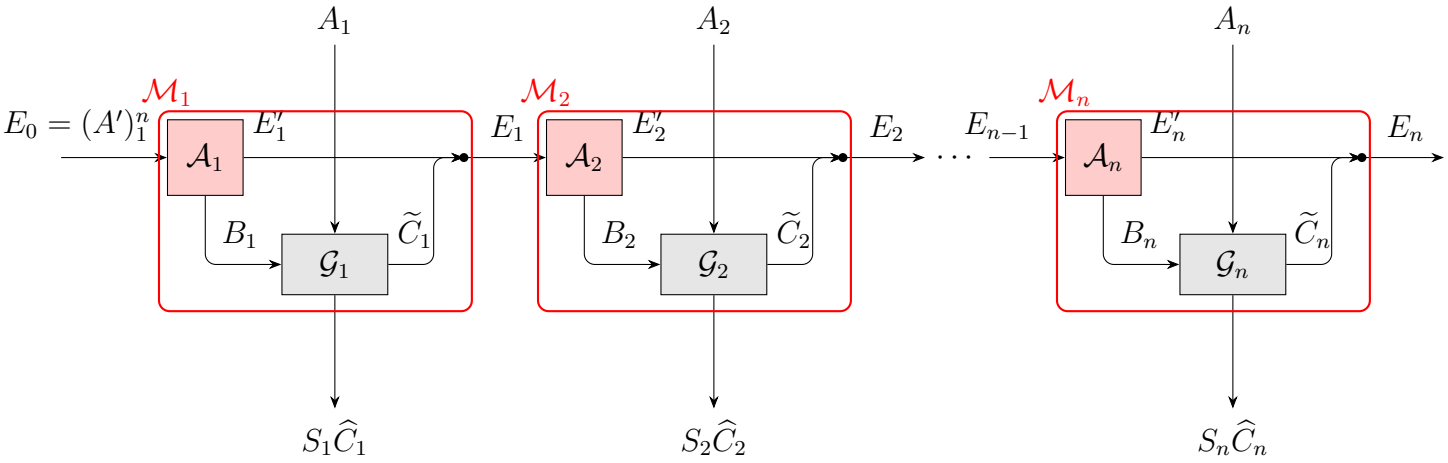


Figure 7.2: (Same as Fig. 7.1). The evolution of the state through Eve's attack channels $\{\mathcal{A}_j\}$, and Alice and Bob's operations $\{\mathcal{G}_j\}$ for the Virtual entanglement-based protocol. The evolution of states is also described in Lemma 7.3.4. Note that the announcements $\widehat{C}_j$ are made available to Eve through an explicit copy $\widetilde{C}_j$, which gets merged with E_j' to form E_j. The MEAT [11, Theorem 4.1a] is applied for the sequence of channels $\{\mathcal{M}_j\}$.

satisfies

$$\widetilde{H}_\alpha^{\uparrow,\hat{f}_{\text{full}}}(S_1^n|\widehat{C}_1^n E_n) \geq 0. \tag{7.46}$$

Proof. The statement follows from a direct application of [11, Theorem 4.1a], and we simply describe how that theorem can be applied here. The final state $\rho_{S_1^n\widehat{C}_1^n E_c}$ is of the form

$$\rho_{S_1^n\widehat{C}_1^n E_c} = \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1 \left(\rho_{A_1^n E_0}\right) \tag{7.47}$$

where $\rho_{A_1^n E_0}$ is the global source-replaced state defined in Eq. (7.22), where we identify $A_j = \bar{A}_j\hat{A}_j$ as the register that does not leave Alice's lab, and $E_0 = (A')_1^n$ as the set of states that leave Alice's lab. Furthermore, $\rho_{A_1^n} = \bigotimes_{j=1}^n \sigma_{A_j}^{(j)}$, and $\mathcal{M}_j = \mathcal{G}_j \circ \mathcal{A}_j \in \text{CPTP}(E_{j-1}A_j, S_j\widehat{C}_j E_j)$. The statement thus follows directly from [11, Theorem 4.1a], where the symbols $\mathcal{M}_j, E_j, \widehat{C}_j, \widetilde{E}, \hat{f}_{\text{full}}, f_{|\hat{c}_1^{j-1}}$ correspond to the same symbols used in that theorem. The only difference is that A_j here should be identified with A_{j-1} in Ref. [11], and we explicitly write $\mathcal{M}_j$ as a concatenation of two maps, $\mathcal{G}_j \circ \mathcal{A}_j$. □

Thus, we are now at a stage where, for a given sequence of attack channels $\{\mathcal{A}_j\}$ and operations by Alice and Bob in each round $\{\mathcal{G}_j\}$, an appropriate "global" tradeoff function

$\hat{f}_{\text{full}}$ satisfying $\widetilde{H}_\alpha^{\uparrow,\hat{f}_{\text{full}}}(S_1^n|\widehat{C}_1^n E_n)_\rho \geq 0$ can be obtained via Theorem 7.3.2.

Remark 7.3.5. *Recall that the statement $\widetilde{H}_\alpha^{\uparrow,\hat{f}_{\text{full}}}(S_1^n|\widehat{C}_1^n E_n)_\rho \geq 0$ can be understood as the function $\hat{f}_{\text{full}}$ lower bounding the entropy $\widetilde{H}_\alpha^{\uparrow}(S_1^n \mid \widehat{C}_1^n E_n)_\rho$ in the log-mean-exponential sense (see Eq. (7.8)). In this light, it is helpful to think of $f_{|\hat{c}_1^{j-1}}$ as assigning a preliminary "score" to the public announcement in each round. Intuitively, a good choice assigns larger values to test-round announcements that indicate little or no adversarial interference (as opposed to announcements indicating errors), and to generation-round announcements indicating that the round is kept (as opposed to discarded). One is free to start with any such preliminary score that one desires (which may or may not be compatible with the above intuition), and such a score need not have the desired property of lower bounding the relevant Rényi entropy. This preliminary score must then be reduced by the amount $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right)$. The resulting per-round contributions can subsequently be combined to yield the global tradeoff function $\hat{f}_{\text{full}}$, which indeed satisfies the required property of providing a lower bound on $\widetilde{H}_\alpha^{\uparrow}(S_1^n \mid \widehat{C}_1^n E_n)_\rho$ in the log-mean-exponential sense.*

However, the function $\hat{f}_{\text{full}}$ obtained from Theorem 7.3.2 depends on the attack performed, and therefore this result is still not yet sufficient to yield security of the QKD protocol. To circumvent this issue, we require the following definition, that constructs a lower bound on $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right)$ by minimizing over all possible attacks.

Remark 7.3.6. *Since our goal is to prove security against arbitrary attacks by Eve (subject to $E'j$ having dimension d_j), we must in principle optimize $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right)$ over all channels $\mathcal{A}_j \in \mathrm{CPTP}(E_{j-1}, B_j E'_j)$. This is indeed the fundamental task we carry out.*

That said, in many scenarios it is possible to restrict attention to a subset of CPTP maps without loss of generality. For example, when squashing maps are used to reduce a protocol with an infinite-dimensional measurement to an equivalent protocol with a finite-dimensional one (see Section 7.4), Eve's effective attack channel is given by composing her original channel with the squashing map. Depending on the details of the squashing map, these composed channels may lie in a subset

$$\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E'_j) \subseteq \mathrm{CPTP}(E_{j-1}, B_j E'_j).$$

This motivates the general definition adopted here.

Note to readers: For a first reading, it is perfectly fine to regard $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E'_j)$ as the full set of CPTP maps. The subtleties introduced by squashing-based reductions, which motivate restricting to smaller attack sets, are explained later in Section 7.4. Readers can return to this point after that discussion to fully appreciate these nuances.

Definition 7.3.3. Let $j \in \{1, \ldots, n\}$, let $f_{|\hat{c}_1^{j-1}}$ be a tradeoff function on $\widehat{C}_j$, let $\sigma_{A_j}^{(j)} \in \mathrm{S}_=(A_j)$, and let $\mathcal{G}_j \in \mathrm{CPTP}(A_j B_j, S_j \widehat{C}_j \widetilde{C} j)$. Let $\boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j) \subseteq \mathrm{CPTP}(E_{j-1}, B_j E_j')$ be a subset of all possible attack channels. Then, we define a value for $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}\right)$[23] over the set of attack channels via:

$$\begin{aligned} \kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j)\right) &\coloneqq \inf_{\mathcal{A}_j \in \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}} \kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right) \\ &\coloneqq \inf_{\nu \in \Sigma_j(\boldsymbol{\mathcal{A}}_j^{\mathrm{set}})} \widetilde{H}_\alpha^{\uparrow, f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j E_j \widetilde{E})_\nu \end{aligned} \tag{7.48}$$

where

$$\Sigma_j(\boldsymbol{\mathcal{A}}_j^{\mathrm{set}}) \coloneqq \left\{ \mathcal{G}_j \circ \mathcal{A}_j\left(\omega_{A_j E_{j-1} \widetilde{E}}\right) \;\middle|\; \omega_{A_j} = \sigma_{A_j}^{(j)},\ \mathcal{A}_j \in \boldsymbol{\mathcal{A}}_j^{\mathrm{set}} \right\}, \tag{7.49}$$

where $\widetilde{E}$ is a purifying register for any of the $A_j E_{j-1}$ registers.

Since

$$\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j')\right) \ \leq\ \kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j\right), \qquad \forall\ \mathcal{A}_j \in \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j')$$

one might be tempted to use the left-hand side to define $\hat{f}_{\mathrm{full}}$ and thereby the key length (via Eq. (7.28)), since that value would be the worst case value over all possible attacks. However, this formulation appears to depend on the dimensions assigned to Eve's side-information registers, and thus we would require an additional optimization over all possible choices of those dimensions as well. The goal of the next subsection is to present a reformulation of $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j')\right)$ that avoids these issues by getting rid of the dependence on the dimensions of Eve's registers.

7.3.5 Reformulating the minimization over attack channels

In order to reformulate $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j')\right)$ in a manner where the dependence on the Eve's dimensions disappears, it is convenient to consider two related notions of attack channels, as follows:

[23] In this work, each $\boldsymbol{\mathcal{A}}_j^{\mathrm{set}}$ is always associated with specific registers E_{j-1}, B_j, E_j', and should formally be written as $\boldsymbol{\mathcal{A}}_j^{\mathrm{set}}(E_{j-1}, B_j E_j')$. While we typically include this explicitly, we occasionally omit the register labels to avoid notational clutter.

- $\mathcal{A}_j \in \boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E_j') \subseteq \text{CPTP}(E_{j-1}, B_j E_j')$, which describe Eve's action from her side-information register E_{j-1} to Bob's system B_j together with a new side register E_j'. In particular, the set $\boldsymbol{\mathcal{A}}_j^{\text{set}}$ depends on the dimension we allow for Eve's side-information registers E_j'.

- $\mathcal{Q}_j \in \boldsymbol{\mathcal{Q}}_j^{\text{set}} \subseteq \text{CPTP}(A_j', B_j)$, which describe maps directly from Alice's emitted signal A_j' to Bob's register B_j. Intuitively, Eve's attack in this perspective can be seen as first applying such a channel to the source-replacement state $\sigma^{(j)}_{A_j A_j'}$, after which we purify the post-attack output state, and give the purifying register to Eve. Notice that $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ does not depend on the dimensions we allow for Eve's side-information registers E_j'.

Instead of considering all attack channels in $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E_j')$ for the security analysis, we would instead like to consider all maps in $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$. In order to do so, we require $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ to satisfy a specific property stated in Definition 7.3.4. (Informally, we require that applying maps in $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ and then giving a purification to Eve is at least as powerful as applying maps in $\boldsymbol{\mathcal{A}}_j^{\text{set}}$). That is, for every attack in $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E_j')$, there exists a channel in $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ such that the outputs on the $A_j B_j$ system is the same. This is formalized in the following definition.

Definition 7.3.4 (Marginal of $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}' \widetilde{C}_j, B_j E_j')$)**.** Let $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}' \widetilde{C}_j, B_j E_j') \subseteq \text{CPTP}(E_{j-1}' \widetilde{C}_j, B_j E_j')$ and $\boldsymbol{\mathcal{Q}}_j^{\text{set}} \subseteq \text{CPTP}(A_j', B_j)$ be attack sets. We say that $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ is a **marginal** of $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}' \widetilde{C}_j, B_j E_j')$ if the following *marginalization property* holds: for every $\omega_{A_j E_{j-1} \widetilde{E}}$ such that $\omega_{A_j} = \sigma^{(j)}_{A_j}$ and $\widetilde{E}$ is a purifying register for the $A_j E_{j-1}$ registers, and every $\mathcal{A}_j \in \boldsymbol{\mathcal{A}}_j^{\text{set}}$, there exists a $\mathcal{Q}_j \in \boldsymbol{\mathcal{Q}}_j^{\text{set}}$ such that

$$\mathcal{Q}_j \left[\sigma^{(j)}_{A_j A_j'} \right] = \text{tr}_{E_j \widetilde{E}} \circ \mathcal{A}_j \left[\omega_{A_j E_{j-1} \widetilde{E}} \right]. \tag{7.50}$$

where $\sigma^{(j)}_{A_j A_j'}$ is the source-replacement state (see Eq. (7.22)). We say that the collection $\left\{ \boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}' \widetilde{C}_j, B_j E_j') \right\}_{E_{j-1}', E_j'}$ satisfies the **dimension-independent marginal property** with respect to $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ if, for all possible choices of the auxiliary dimension of Eve's registers E_j', E_{j-1}', the collection $\left\{ \boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}' \widetilde{C}_j, B_j E_j') \right\}_{E_{j-1}', E_j'}$ all possess the same marginal $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$.

In this way, $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ is dimension-independent, whereas $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}' \widetilde{C}_j, B_j E_j')$ depends explicitly on the dimension assigned to E_j'. Notice that any state $\mathcal{A}_j \left[\omega_{A_j E_{j-1} \widetilde{E}} \right]$ on the RHS

of Eq. (7.50), can be obtained from some purification of $\mathcal{Q}_j\left[\sigma^{(j)}_{A_jA'_j}\right]$, which is the LHS of Eq. (7.50), by a map acting only on the purifying system. Thus, due to data-processing (Lemma 7.2.1), it suffices to consider purifications of $\mathcal{Q}_j\left[\sigma^{(j)}_{A_jA'_j}\right]$ when performing the infimum over all attacks that appears in κ from Eq. (7.48). We formalize this in the following lemma.

Lemma 7.3.6. *Let* $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma^{(j)}_{A_j},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}^{\text{set}}_j(E_{j-1},B_jE'_j)\right)$ *be as defined in Definition 7.3.3, and let* $\boldsymbol{\mathcal{Q}}^{\text{set}}_j$ *be a marginal of* $\boldsymbol{\mathcal{A}}^{\text{set}}_j(E_{j-1},B_jE'_j)$ *in the sense of Definition 7.3.4. Then, for any* $\alpha\geq 1$ *we have:*

$$\begin{aligned}\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma^{(j)}_{A_j},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}^{\text{set}}_j(E_{j-1},B_jE_j)\right) &\geq \inf_{\mathcal{Q}_j\in\boldsymbol{\mathcal{Q}}^{\text{set}}_j}\widetilde{H}_\alpha^{\uparrow,f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]}\\ &= \inf_{\overline{\omega}\in\overline{\Sigma}_j\left(\boldsymbol{\mathcal{Q}}^{\text{set}}_j\right)}\widetilde{H}_\alpha^{\uparrow,f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\overline{\omega}_{A_jB_j}\right)\right]}\end{aligned} \tag{7.51}$$

where Pur *is a purifying function of* A_jB_j *onto* $\widehat{E}$*, and*

$$\overline{\Sigma}_j\left(\boldsymbol{\mathcal{Q}}^{\text{set}}_j\right) \coloneqq \left\{\mathcal{Q}_j\left[\sigma^{(j)}_{A_jA'_j}\right]\ \middle|\ \mathcal{Q}_j\in\boldsymbol{\mathcal{Q}}^{\text{set}}_j\right\}, \tag{7.52}$$

where $\sigma^{(j)}_{A_jA'_j}$ *is the source-replaced state from Eq. (7.22). If* $\boldsymbol{\mathcal{Q}}^{\text{set}}_j$ *satisfies the dimension-independent marginal property, i.e is the marginal of all* $\left\{\boldsymbol{\mathcal{A}}^{\text{set}}_j(E'_{j-1}\widetilde{C}_j,B_jE'_j)\right\}_{E'_{j-1},E'_j}$*, then Eq. (7.51) is obtained for any dimensions of Eve's side-information registers. Furthermore, the objective function in the RHS of the first line of Eq. (7.51) is convex in* $\mathcal{Q}_j$*, and in the second line of Eq. (7.51) is convex in* $\overline{\omega}_{A_jB_j}$*.*[24]

Proof. The first line of Eq. (7.51) is merely an equivalent reformulation of the second line, obtained by an affine transformation of the input variable $\bar{\omega}$ (which is the post-attack state) to $\mathcal{Q}_j$ (which is the attack channel). Since affine transformations preserve convexity, the convexity of the objective function in the first line follows. Thus, we focus on proving the inequality in Eq. (7.51). In other words, we show that

$$\inf_{\mathcal{A}_j\in\boldsymbol{\mathcal{A}}^{\text{set}}_j}\inf_{\omega\in\Sigma_j(\mathcal{A}_j)}\widetilde{H}_\alpha^{\uparrow,f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_jE_j\widetilde{E})_{\mathcal{G}_j\circ\mathcal{A}_j\left[\omega_{A_jE_{j-1}\widetilde{E}}\right]} \geq \inf_{\mathcal{Q}_j\in\boldsymbol{\mathcal{Q}}^{\text{set}}_j}\widetilde{H}_\alpha^{\uparrow,f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]}, \tag{7.53}$$

[24] If $\boldsymbol{\mathcal{Q}}^{\text{set}}_j$ is convex, then the RHS of Eq. (7.51) is a convex optimization problem.

where $\widetilde{E}$ is a register of large enough dimension to accommodate for purification of all A_jE_{j-1} registers. Let $\left(\omega^*_{A_jE_{j-1}\widetilde{E}}, \mathcal{A}^*_j\right)$ be a feasible point on the LHS of Eq. (7.53), and let $\omega^*_{A_jB_jE'_j\widetilde{E}} = \mathcal{A}^*_j\left[\omega^*_{A_jE_{j-1}\widetilde{E}}\right]$; noting that it satisfies $\omega^*_{A_j} = \sigma^{(j)}_{A_j}$. Since $\boldsymbol{\mathcal{Q}}^{\text{set}}_j$ is a marginal of $\boldsymbol{\mathcal{A}}^{\text{set}}_j$ in the sense of Definition 7.3.4, then Eq. (7.50) states that there exists a channel $\mathcal{Q}^*_j \in \boldsymbol{\mathcal{Q}}^{\text{set}}_j$ such that

$$\mathcal{Q}^*_j\left[\sigma^{(j)}_{A_jA'_j}\right] = \text{tr}_{E'_j\widetilde{E}} \circ \mathcal{A}_j\left[\omega^*_{A_jE_{j-1}\widetilde{E}}\right] = \omega^*_{A_jB_j}. \tag{7.54}$$

Let $\texttt{Pur}$ be a purifying function of A_jB_j onto $\widehat{E}$. Then, there exists a channel $\mathcal{N}_j \in \text{CPTP}(\hat{E}, E'_j\widetilde{E})$ such that $\omega^*_{A_jB_jE'_j\widetilde{E}} = \mathcal{N}_j\left[\texttt{Pur}\left(\mathcal{Q}^*_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]$ (see Lemma 2.1.1). Thus, we have:

$$\begin{aligned}
\widetilde{H}^{\uparrow, f_{|\hat{c}_1^{j-1}}}_{\alpha}(S_j|\widehat{C}_jE_j\widetilde{E})_{\mathcal{G}_j\circ\mathcal{A}_j\left[\omega^*_{A_jE_{j-1}\widetilde{E}}\right]} &= \widetilde{H}^{\uparrow, f_{|\hat{c}_1^{j-1}}}_{\alpha}(S_j|\widehat{C}_j\widetilde{C}_jE'_j\widetilde{E})_{\mathcal{G}_j\circ\mathcal{A}_j\left[\omega^*_{A_jE_{j-1}\widetilde{E}}\right]} \\
&= \widetilde{H}^{\uparrow, f_{|\hat{c}_1^{j-1}}}_{\alpha}(S_j|\widehat{C}_j\widetilde{C}_jE'_j\widetilde{E})_{\mathcal{G}_j\circ\mathcal{N}_j\left[\texttt{Pur}\left(\mathcal{Q}^*_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]} \\
&= \widetilde{H}^{\uparrow, f_{|\hat{c}_1^{j-1}}}_{\alpha}(S_j|\widehat{C}_j\widetilde{C}_jE'_j\widetilde{E})_{\mathcal{N}_j\circ\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}^*_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]} \\
&\geq \widetilde{H}^{\uparrow, f_{|\hat{c}_1^{j-1}}}_{\alpha}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}^*_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]}.
\end{aligned} \tag{7.55}$$

The first line simply rewrites E_j as $\widetilde{C}jE'_j$, and the second line replaces $\mathcal{A}_j[\omega^*_{A_jE_{j-1}\widetilde{E}}]$ with $\mathcal{N}_j\left[\texttt{Pur}\left(\mathcal{Q}^*_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]$ $\boldsymbol{\mathcal{A}}^{\text{set}}_j$ since they are equal. The third line holds due to the fact that the maps $\mathcal{N}_j$ and $\mathcal{G}_j$ commute (since they act on different registers), and the last line follows from data processing inequality (Lemma 7.2.1). Thus, for any feasible point on the LHS, we can find a feasible point on the RHS such that the LHS is greater than or equal to the RHS. This proves the first inequality in Eq. (7.51).

The convexity of the objective function in the second line of Eq. (7.51) was established in [11, Lemma 4.10]. □

Note that [3, Corollary 8.9] shows that regardless of the choice of $\boldsymbol{\mathcal{A}}^{\text{set}}_j(E_{j-1}, B_jE'_j)$, the set $\boldsymbol{\mathcal{Q}}^{\text{set}}_j$ can always be taken to be $\text{CPTP}(A'_j, B_j)$ (although doing so when using the flag-state squasher leads to trivial key rates; there a non-trivial restriction needs to be

imposed on $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$). Furthermore, we note that although Lemma 7.3.6 only establishes an inequality, this inequality is typically saturated for all scenarios considered in chapter. Thus, we can instead focus on computing the objective function formulated in terms of $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$, where the dimension of Eve's side-information registers plays no role. We are now ready to bring all the pieces together and present the final security statement for the protocol under study.

7.3.6 Final security statement

We now state the final security statement concerning the security of Generic QKD Protocol.

Theorem 7.3.3 (Security statement for Generic QKD Protocol under finite-dimensional Alice–Bob setting)**.** *Consider the Generic QKD Protocol where Alice's transmitted systems (A'_j) are finite-dimensional and Bob performs finite-dimensional measurements (B_j is finite-dimensional). For this protocol, after applying the source-replacement scheme (Lemma 7.3.3), let $\sigma^{(j)}_{A_jA'_j}$ denote the resulting source states in round j, and let $\mathcal{G}_j$ denote the operations Alice and Bob perform in round j. (These are the same as those that appear in the corresponding Virtual entanglement-based protocol, with state evolution described in Lemma 7.3.4). For each j and every value of $\hat{c}_1^{j-1}$, let $f_{|\hat{c}_1^{j-1}}$ denote a tradeoff function[25] on the register $\widehat{C}_j$. Let $\kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)$ be any value satisfying*

$$\kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right) \leq \inf_{\mathcal{Q}_j \in \boldsymbol{\mathcal{Q}}_j^{\text{set}}} \widetilde{H}_\alpha^{\uparrow, f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}_j\left[\sigma^{(j)}_{A_jA'_j}\right]\right)\right]}, \tag{7.56}$$
$$\boldsymbol{\mathcal{Q}}_j^{\text{set}} = \text{CPTP}(A'_j, B_j),$$

where Pur *is a purifying function of A_jB_j onto $\widehat{E}$, and define*

$$\hat{f}^{\text{QKD}}_{\text{full}}(\hat{c}_1^n) \coloneqq \sum_{j=1}^{n} \left(f_{|\hat{c}_1^{j-1}}(\hat{c}_j) + \kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)\right). \tag{7.57}$$

Then, the protocol is $(\varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure (according to Definition 8.1.1) if the key length $\ell(\hat{c}_1^n)$ is chosen as

$$\ell(\hat{c}_1^n) = \max\left\{0, \left\lfloor \hat{f}^{\text{QKD}}_{\text{full}}(\hat{c}_1^n) - \lambda_{\text{EC}}(\hat{c}_1^n) - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}}\right)\right\rceil - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\text{PA}}}\right) + 2\right\rfloor\right\}. \tag{7.58}$$

[25] See Remark 7.3.5 for an intuitive interpretation of this function.

Proof. The required statement follows from an appropriate combination of all the statements we have shown previously, which we recall as follows. Recall that we only need to show the $\varepsilon_{\mathrm{PA}}$-secrecy of the protocol, since $\varepsilon_{\mathrm{EV}}$-correctness has already been shown in Lemma 3.4.1.

Reducing to Virtual entanglement-based protocol. We begin by applying Lemma 7.3.1, which allows us to construct a modified version of Generic QKD Protocol in which Alice's state preparation is moved earlier in time, such that it occurs before Bob's first measurement. As argued in Lemma 7.3.1, this can be done without loss of generality, and ensures that the security of this modified protocol implies the security of the original protocol. Next, we invoke Lemma 7.3.3, which shows that Alice's operations can be viewed as preparing a gobal source-replaced state $\sigma_{\bar{A}_1^n(\hat{A})_1^n(A')_1^n}$ (that is tensor-product across rounds) and then measuring the $\bar{A}_1^n$ systems. Since Alice's measurements commute with all operations except the public announcements (which, by design, occur only after Bob's measurement in each round), we can postpone Alice's measurements to occur simultaneously with Bob's.

After these modifications, the protocol for which we must prove security is given by Virtual entanglement-based protocol. In particular, it admits the structure of sequential channels described in Lemma 7.3.4 and Fig. 7.1, where $\{\mathcal{A}_j\}$ denotes the sequence of Eve's attack channels, and the maps $\{\mathcal{G}_j\}$ implement Alice and Bob's measurements, postprocessing and public announcements. We note that the arguments so far do not require Alice, Bob or Eve to be finite-dimensional.

Security analysis for state obtained in Virtual entanglement-based protocol. At this stage, we fix a particular sequence of attack channels, and analyze the output state corresponding to it. In particular, we also fix the dimensions of all of Eve's side-information registers (E'_j) to be some finite value d_j. We will later obtain a result that does not depend on any particular sequence of attack channels or dimensions, and holds for any sequence of attack channels that Eve may perform.

From Lemma 3.4.1 (which also applies to this protocol), we have that $\varepsilon_{\mathrm{EV}}$-correctness is satisfies. Thus, we are now concerned with proving $\varepsilon_{\mathrm{PA}}$-secrecy of the state. In Theorem 7.3.1, we show that if

$$\widetilde{H}_{\alpha}^{\uparrow,\hat{f}_{\mathrm{full}}}(S_1^n|\widehat{C}_1^n E_n) \geq 0, \tag{7.59}$$

then the function $\ell(\hat{c}_1^n)$ (see Eq. (7.28)) that determines the length of the output key given by

$$l(c_1^n) = \max\left\{0, \left\lfloor \hat{f}_{\mathrm{full}}^{\mathrm{QKD}}(\hat{c}_1^n) - \lambda_{\mathrm{EC}}(\hat{c}_1^n) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\mathrm{PA}}}\right) + 2 \right\rfloor \right\} \tag{7.60}$$

guarantees ε_{PA}-secrecy, provided that

$$\hat{f}_{\text{full}}^{\text{QKD}}(\hat{c}_1^n) \leq \hat{f}_{\text{full}}(\hat{c}_1^n) \quad \forall \hat{c}_1^n. \tag{7.61}$$

Thus, our task reduces to constructing a global tradeoff function $\hat{f}_{\text{full}}^{\text{QKD}}$ satisfying above property.

Applying MEAT. To do so, we turn to Theorem 7.3.2, where we apply MEAT to the sequence of channels described in Lemma 7.3.4 and Fig. 7.1. This yields a function $\hat{f}_{\text{full}}$ satisfying $\widetilde{H}_\alpha^{\uparrow,\hat{f}_{\text{full}}}(S_1^n|\widehat{C}_1^n E_n) \geq 0$, given by

$$\hat{f}_{\text{full}}(\hat{c}_1^n) \coloneqq \sum_{j=1}^{n} \left(f_{|\hat{c}_1^{j-1}}(\hat{c}_j) + \kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j \right) \right), \tag{7.62}$$

where $f_{|\hat{c}_1^{j-1}}$ are arbitrary tradeoff functions on $\widehat{C}_j$ (that we choose), and the constants $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j \right)$ are defined in Eq. (7.43). However, both $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j \right)$ and the resulting $\hat{f}_{\text{full}}$ constructed in this fashion depend on Eve's attack channels, and the dimensions of her registers. We would like to remove this dependence by performing a worst-case analysis over all possible attack channels $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E_j') = \text{CPTP}(E_{j-1}, B_j E_j')$ and all possible dimensions of Eve's registers.

Reformulations to remove dependence on Eve's dimensions and attack channels. To address this, we construct a different kind of attack channels, and denote this set via $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$. Here, we represent any attack as the application of one such channel to the source-replaced state, and then assume that Eve holds a purification of the resulting output state. We set $\boldsymbol{\mathcal{Q}}_j^{\text{set}} = \text{CPTP}(A_j', B_j)$, and apply Lemma 7.3.6. This, along with the definition of $\kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j \right)$ in the theorem statement, allows us to obtain

$$\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \mathcal{A}_j \right) \geq \inf_{\mathcal{Q}_j \in \boldsymbol{\mathcal{Q}}_j^{\text{set}}} \widetilde{H}_\alpha^{\uparrow, f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}_j\left[\sigma_{A_j A_j'}^{(j)}\right]\right)\right]} \geq \kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j \right), \tag{7.63}$$

for any attack $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E_{j-1}')$. Thus, if we use $\kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j \right)$ to define

$$\hat{f}_{\text{full}}^{\text{QKD}}(\hat{c}_1^n) \coloneqq \sum_{j=1}^{n} \left(f_{|\hat{c}_1^{j-1}}(\hat{c}_j) + \kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j \right) \right), \tag{7.64}$$

then the resultant global tradeoff function $\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}(\hat{c}_1^n)$ satisfies the required property Eq. (7.61). Moreover, neither $\kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)$ nor $\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}(\hat{c}_1^n)$ has any dependence on the dimensions of Eve's systems, or her choice of attack. Additionally, as pointed out in Lemma 7.3.6, the resulting optimization problem is finite-dimensional and convex. Thus, $\ell(\hat{c}_1^n)$, as defined in the theorem statement, is a valid choice for obtaining a $(\varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EV}})$-secure protocol when considering any attack in which Eve employs finite-dimensional side registers.

Relaxing the finite-dimensional Eve assumption. We now address the technicality that Eve could, in principle, use infinite-dimensional side registers in her attack. So far, we have proven security for all attacks where Eve's registers are finite-dimensional. However, since our security statement yields the same security parameter $(\varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EV}})$ regardless of the dimensions assigned to Eve's side registers, we can invoke the results of [3, Appendix A] to argue that the same security guarantee extends to the infinite-dimensional case. This concludes our proof. □

Having completed the security analysis for Generic QKD Protocol, we now turn to the next subsection to elaborate on certain aspects, highlight subtleties, and provide additional clarification.

7.3.7 Discussion

We have now proved Theorem 7.3.3, which guarantees the security of the Generic QKD Protocol against arbitrary attacks by Eve, as long as one can compute a lower bound on a finite-dimensional convex optimization. Our theorem holds for the case where Alice sends finite-dimensional states, and Bob measures finite-dimensional systems. Naturally, this security statement depends on the parameters specified in the protocol, and the secure output key length depends on these parameters. Before proceeding further, let us take stock of what has been accomplished so far and identify the remaining steps needed to complete the analysis and obtain a security proof for a practical decoy-state BB84 protocol. We have two main aspects that need to be addressed.

- **Infinite dimensions of Alice and Bob:** First, recall our earlier caveat: the MEAT is formally applicable only to finite-dimensional systems, even though its statement does not dependent on the dimensions of the underlying systems. However, QKD protocols are implemented using optical systems, which are naturally described by infinite-dimensional Hilbert spaces. In particular, Alice sends infinite-dimensional states,

and Bob POVM lives in an infinite-dimensional Hilbert space. Ref. [5] (Section 5.3) presented an argument to reduce to finite dimensions at the level of the security definition, that is, however it does not apply here due to on-the-fly announcements. Thus we generalize the approach in Ref. [5] to include on-the-fly announcements. This method is general and potentially compatible with a broad class of squashing maps and source maps. This is undertaken in Section 7.4. Once this reduction is complete, the resulting finite-dimensional protocol can be analyzed using MEAT, following the procedure outlined Sections 7.3.1 and 7.3.3 to 7.3.6.

- **Numerics:** Second, even after reducing to finite dimensions, computing the key rate still requires us to solve a highly non-trivial convex optimization problem. In essence, the difficulty arises from the fact that we aim to obtain a value that is provably *lower* than the infimum — i.e, a guaranteed lower bound. We state the numerical computations needed to compute key rates in Section 7.5, and refer the reader to [9, 49] for some recent work on this topic. We use the code from Ref. [9] to plot key rates.

Having discussed the above issues - which are addressed in more detail in subsequent sections - we now outline a general recipe for applying the results of the previous subsection to compute QKD key rates.

Recipe

Since the Generic QKD Protocol is highly general, the security of a wide variety of QKD protocols can be established using the results developed so far. To aid in this task, we include a practical "recipe" for applying our results to compute key rates for a protocol of interest. We present this recipe in a way that also accommodates squashing maps, source maps, and the optical modeling introduced in Section 7.4. For a first reading, the reader may safely skip the optical details and return to them after going through Section 7.4.

Recipe

1. Specify all details of the QKD protocol, and ensure that it fits the structure described in Generic QKD Protocol.

2. If required, apply the source map Lemma 7.4.1 to reduce to a protocol with a different state preparation by Alice.

3. If required, apply the squashing map Lemma 7.4.2 to reduce to a protocol where Bob performs a different measurement.

4. Consider the Virtual entanglement-based protocol, which is obtained after source-replacement and timing modifications as specified Section 7.3.1. In particular, this fixes $\sigma_{A_j}^{(j)}$, $\mathcal{G}_j$ for all $j \in \{1, \dots, n\}$, which describe Alice's (source-replaced) state preparation, and the round-by-round operations undertaken by Alice and Bob in round j.. Note that these quantities are obtained by considering the Virtual entanglement-based protocol version of the protocol obtained *after* the application of the source-map and squashing transformations.

5. For all $j \in \{1, \dots, n\}$ and $\hat{c}_1^{j-1}$, specify the tradeoff functions $f_{|\hat{c}_1^{j-1}}$ (or a deterministic procedure for specifying them, see Remark 7.3.10).

6. Determine $\boldsymbol{\mathcal{A}}_j^{\text{set}}(E_{j-1}, B_j E_j')$ (which depends the details of the squashing map used). From it, determine the corresponding $\boldsymbol{\mathcal{Q}}_j^{\text{set}}$ that satisfies the dimension-independent extension property (Definition 7.3.4). If we do not use squashing maps, this reduces to $\boldsymbol{\mathcal{Q}}_j^{\text{set}} = \text{CPTP}(A_j', B_j)$.

7. Compute a lower bound on $\kappa\left(f_{|\hat{c}_1^{j-1}},\ \sigma_{A_j}^{(j)},\ \mathcal{G}_j,\ \boldsymbol{\mathcal{A}}_j^{\text{set}}\right)$, given by

$$\inf_{\mathcal{Q}_j \in \boldsymbol{\mathcal{Q}}_j^{\text{set}}} \widetilde{H}_\alpha^{\uparrow, f_{|\hat{c}_1^{j-1}}}(S_j|\widehat{C}_j\widetilde{C}_j\widehat{E})_{\mathcal{G}_j\left[\texttt{Pur}\left(\mathcal{Q}_j\left[\sigma_{A_j A_j'}^{(j)}\right]\right)\right]} \tag{7.65}$$

   where $\texttt{Pur}$ is a purifying function from $A_j B_j$ onto $\widehat{E}$. Denote this lower bound by $\kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j\right)$.

8. Define $\hat{f}_{\text{full}}^{\text{QKD}} = \sum_{j=1}^n \left(f_{|\hat{c}_1^{j-1}}(\hat{c}_j) + \kappa^{\text{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j\right)\right)$.

9. Set the variable-length decision to be

$$\ell(\hat{c}_1^n) = \max\left\{0, \left\lfloor \hat{f}_{\text{full}}^{\text{QKD}}(\hat{c}_1^n) - \lambda_{\text{EC}}(\hat{c}_1^n) - \left\lceil \log\left(\frac{1}{\varepsilon_{\text{EV}}}\right)\right\rceil - \frac{\alpha}{\alpha - 1}\log\left(\frac{1}{\varepsilon_{\text{PA}}}\right) + 2 \right\rfloor\right\}. \tag{7.66}$$

   The resulting protocol is $(\varepsilon_{\text{PA}} + \varepsilon_{\text{EV}})$-secure.

We now highlight some subtleties and provide additional clarification in the following remarks.

Remark 7.3.7. *Notice that Theorem 7.3.3 is fairly general, since the Generic QKD Protocol is itself fairly general. For example, we can straightforwardly accommodate scenarios where Alice's state preparation is different in different rounds, since we allow for the $\sigma_{A_j}^{(j)}$ to vary from round to round, although we do require "independent"' state preparation across rounds, i.e, $\sigma_{A_1^n} = \sigma_{A_1}^{(1)} \otimes \cdots \otimes \sigma_{A_n}^{(n)}$. Interestingly, we can also accommodate fairly contrived protocols where Alice and Bob perform* different *protocol operations in each round - for example, a protocol that alternates between BB84 signal preparation and measurement in odd-numbered rounds and six-state signal preparation and measurement in even-numbered rounds. This manifests in the analysis as $\mathcal{G}_j$ now being different across rounds. This flexibility makes our analysis, which inherits these features from the abstract MEAT statement itself, extremely general. The only additional cost incurred is the need to perform more computations.*

Remark 7.3.8. *Note that when applying the above recipe, one may start with* any *choice of tradeoff functions $f_{|\hat{c}_1^{j-1}}$ that one desires — there are no constraints whatsoever on the original selection of these functions. This choice determines the the values of $\kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j\right)$, which in turn influences the normalized tradeoff function $\hat{f}_{\mathrm{full}}^{\mathrm{QKD}}$. While the theorem permits arbitrary choices of the tradeoff $f_{|\hat{c}_1^{j-1}}$, certain choices lead to superior key rates compared to other choices (in fact, a careful choice is typically important to achieve positive key rates). In particular, the* optimal *$f_{|\hat{c}_1^{j-1}}$, in the sense that it generates the best performance for a fixed honest behaviour of the channel, can be chosen following a procedure described in [9, Sec. VI] or [86, Sec. 5.3]. Since the initial choice of $f_{|\hat{c}_1^{j-1}}$ is not relevant for the security claim to hold, and only necessary for ensuring the best performance, we only briefly discuss the procedure to choose $f_{|\hat{c}_1^{j-1}}$ in Section 7.5.*

Remark 7.3.9. *Note that the above recipe, and Theorems 7.3.2 and 7.3.3, allows us to choose* different *tradeoff functions $f_{|\hat{c}_1^{j-1}}$ in different rounds, which can also depend on the observed public announcements of preceding rounds (although one has to determine how this choice is made beforehand). This allows for "fully adaptive" QKD protocols [158, 86], where the tradeoff functions $f_{|\hat{c}_1^{j-1}}$ can be updated over the the course of the protocol, a feature that is important when performing QKD over noisy, or unpredictable channels. This too, is a feature inherited from the abstract MEAT statement itself. However note that updating $f_{|\hat{c}_1^{j-1}}$ frequently leads to additional computation cost. The simplest scenario is the one where all $\sigma_{A_j}^{(j)}$s are identical, all $f_{|\hat{c}_1^{j-1}}$s are identical and have no dependence on $\hat{c}_1^{j-1}$, and all $\mathcal{G}_j$s are identical.*[26]

[26]Strictly speaking, these objects act on different registers and are therefore not equal as mathematical objects. Rather, we mean that each $\sigma_{A_j}^{(j)}$ and $\mathcal{G}_j$ is defined on a distinct but isomorphic copy of the same

Remark 7.3.10. *Since the function* $\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}$ *depends on all the* $f_{|\hat{c}_1^{j-1}}$ *and* $\kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)$, *it might seem as though the computation of* $\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}(\hat{c}_1^n)$ *requires the computation of all* $\kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)$ *for all the possible inputs, which is prohibitively expensive. However, as argued in Ref. [158], when applying the above result in practice, one only needs to compute* $\hat{f}_{\mathrm{full}}(\hat{c}_1^n)$ *on the specific sequence* $\hat{c}_1^n$ *observed in the protocol. This allows for an efficient, iterative procedure: for each round* j, *one examines the past announcements* $\hat{c}_1^{j-1}$, *makes some choice of* $f_{|\hat{c}_1^{j-1}}$ *(which depends on those values) and computes* $\kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)$, *then considers a similar computation for the* $(j+1)^{th}$ *round and so on. Note that there is no requirement to finish each of these computations before the next round occurs; in other words, they can be computed at any convenient time between generating the relevant data and the final privacy amplification step — this is because the computed values are only used to determine the key length for privacy amplification, and not for any other aspect of the protocol.*

Remark 7.3.11. *We remark that, when running the numerical routines from Ref. [9] for the decoy-state BB84 protocol, one observes that the quantity*

$$f_{|\hat{c}_1^{j-1}}(\cdot) \; + \; \kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma^{(j)}_{A_j}, \mathcal{G}_j\right)$$

can take fairly large positive or negative values. As a consequence, for some realizations of the public announcements $\hat{c}_1^n$, *the globally normalized tradeoff function* $\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}(\hat{c}_1^n)$, *and the key length* $\ell(\hat{c}_1^n)$ *may exceed the total number of rounds* n. *This behaviour may appear counterintuitive: the Rényi entropy of the pre-amplification string is always upper bounded by* n, *whereas* $\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}(\hat{c}_1^n)$ *has a qualitative interpretation as a lower bound on this quantity "on average". Nevertheless, this does not invalidate the security proof. The framework ensures that such extreme values arise only with sufficiently small probability, and our obtained security statement is still valid — recall for instance that the security definition (Definition 3.1.1) is averaged over the possible key lengths, and thus key lengths that occur with extremely small probability do not affect it much. (Similar properties hold for the "log-mean-exponential" interpretation (Eq. (7.9)) of the* f*-weighted entropy bounds, as these are also "averaged" quantities.) That said, for practical implementations, if one encounters an observation* $\hat{c}_1^n$ *for which*

$$\hat{f}^{\mathrm{QKD}}_{\mathrm{full}}(\hat{c}_1^n) > n,$$

underlying Hilbert space, and coincides with a fixed reference state and map under the corresponding canonical identification. Similarly, we mean that the functions $f_{|\hat{c}_1^{j-1}}$ coincide under the appropriate relabeling of the classical registers.

it is natural to propose that its value should be reduced to n (i.e. the maximal possible Rényi entropy); the protocol still straightforwardly remains secure in this case.[27] *Importantly, however, even without such corrective adjustments, the formal security guarantees from Theorem 7.3.3 are fully valid; the adjustment is purely for practical considerations such as implementation difficulties in producing an extremely long output key.*

We now turn our attention to the remaining steps outlined at the start of this subsection. In the next section, we consider the quantum optical nature of realistic implementations, which causes Alice's signal states and Bob's POVMs to reside in infinite-dimensional Hilbert spaces.

7.4 Extending Security to optical protocols

We will now outline the additional steps required to adapt our analysis to optical QKD implementations. We will do so by reducing the security analysis of the original protocol, where Alice's signal states and Bob's POVMs belong to infinite-dimensional Hilbert spaces, to a protocol where they belong to finite-dimensional Hilbert spaces. We start by focusing on Alice's signal states. This section will essentially generalize the analysis from Chapter 5 pertaining to the use of source maps (Section 3.6.2) and squashing maps (Section 3.6.3).

Lemma 7.4.1 (Source maps)**.** *Let* $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \sigma_{X_1^n(A')_1^n}\right\}$ *determine a QKD protocol (see Definition 7.3.1) where Alice prepares the global state*

$$\sigma_{X_1^n(A')_1^n} = \sum_{x_1^n} p(x_1^n) \, |x_1^n\rangle\langle x_1^n|_{X_1^n} \otimes \sigma_{(A')_1^n}^{(x_1^n)}.$$

Suppose there exists a quantum channel (source map) $\Psi \in \text{CPTP}((A'')_1^n, (A')_1^n)$ *and a set of* virtual states $\{\xi_{(A'')_1^n}^{(x_1^n)}\}_{x_1^n} \subset \text{S}_=((A'')_1^n)$ *such that*

$$\sigma_{X_1^n(A')_1^n} = (\text{id} \otimes \Psi)\left[\xi_{X_1^n(A'')_1^n}\right] \tag{7.67}$$

$$\text{where} \quad \xi_{X_1^n(A'')_1^n} = \sum_{x_1^n} p(x_1^n) \, |x_1^n\rangle\langle x_1^n|_{X_1^n} \otimes \xi_{(A'')_1^n}^{(x_1^n)}. \tag{7.68}$$

In other words, $\sigma_{(A')_1^n}^{(x_1^n)} = \Psi\left[\xi_{(A'')_1^n}^{(x_1^n)}\right]$ *for all* x_1^n*. Then if the protocol* $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \xi_{X_1^n(A'')_1^n}\right\}$ *using the virtual states is* $\varepsilon^{\text{secure}}$*-secure, the protocol* $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \sigma_{X_1^n(A')_1^n}\right\}$ *using the real states is also* $\varepsilon^{\text{secure}}$*-secure.*

[27] This can be argued using the monotonicity of f-weighted Rényi entropies wrt f, see Lemma 7.2.3.

Proof. If the virtual protocol $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \xi_{X_1^n(A'')_1^n}\right\}$ is $\varepsilon^{\text{secure}}$-secure, then for all attack channels $\{\mathcal{A}_j\}_{j=2}^n$ and $\mathcal{A}_1' \in \text{CPTP}((A'')_1^n, B_1E_1)$, we have (as in Definition 7.3.2)

$$\Big\| \Big(\mathcal{M}_{\text{CPP}} \circ \widetilde{\mathcal{G}}_n^{\text{full}} \circ \mathcal{A}_n \circ \cdots \circ \widetilde{\mathcal{G}}_1^{\text{full}} - \mathcal{R}_{\text{ideal}} \circ \mathcal{M}_{\text{CPP}} \circ \widetilde{\mathcal{G}}_n^{\text{full}} \circ \mathcal{A}_n \circ \cdots \circ \widetilde{\mathcal{G}}_1^{\text{full}} \Big) \circ \left(\text{id}_{X_1^n} \otimes \mathcal{A}_1'\right) \left[\xi_{X_1^n(A'')_1^n}\right] \Big\|_1 \leq \varepsilon^{\text{secure}}, \tag{7.69}$$

where we used Lemma 7.3.2 to represent the output state obtained in the protocol. We treat the first attack channel $\mathcal{A}_1'$ separately from the rest of the attack channels in our proof, since this attack channel is the one that can implement the source map. Consider the restricted subset of channels $\mathcal{C}_\Psi$, where we first apply the source map Ψ before applying an attack channel $\mathcal{A}_1 \in \text{CPTP}((A')_1^n, B_1E_1)$

$$\mathcal{C}_\Psi \coloneqq \{\mathcal{A}_1 \circ \Psi \,|\, \mathcal{A}_1 \in \text{CPTP}((A')_1^n, B_1E_1)\}\,. \tag{7.70}$$

Since Eq. (7.69) holds for all $\mathcal{A}_1'$, it also holds for any $\mathcal{A}_1' \in \mathcal{C}_\Psi$. Thus, for any $\mathcal{A}_1 \in \text{CPTP}(A_1'^n, B_1E_1)$, we set $\mathcal{A}_1' = \mathcal{A}_1 \circ \Psi$. With this identification, we have

$$\left(\text{id}_{X_1^n} \otimes \mathcal{A}_1'\right) \left[\xi_{X_1^n(A'')_1^n}\right] = \left(\text{id}_{X_1^n} \otimes \mathcal{A}_1 \circ \Psi\right) \left[\xi_{X_1^n(A'')_1^n}\right] = \left(\text{id}_{X_1^n} \otimes \mathcal{A}_1\right) \left[\sigma_{X_1^n(A')_1^n}\right]. \tag{7.71}$$

Now, using Eqs. (7.69) and (7.71) we obtain

$$\Big\| \Big(\mathcal{M}_{\text{CPP}} \circ \widetilde{\mathcal{G}}_n^{\text{full}} \circ \mathcal{A}_n \circ \cdots \circ \widetilde{\mathcal{G}}_1^{\text{full}} - \mathcal{R}_{\text{ideal}} \circ \mathcal{M}_{\text{CPP}} \circ \widetilde{\mathcal{G}}_n^{\text{full}} \circ \mathcal{A}_n \circ \cdots \circ \widetilde{\mathcal{G}}_1^{\text{full}} \Big) \circ \left(\text{id}_{X_1^n} \otimes \mathcal{A}_1\right) \left[\sigma_{X_1^n(A')_1^n}\right] \Big\|_1 \leq \varepsilon^{\text{secure}}, \tag{7.72}$$

for all attack channels $\mathcal{A}_1 \in \text{CPTP}((A')_1^n, E_1B_1)$, and for all $\{\mathcal{A}_j\}_{j=2}^n$. This proves that the real protocol is $\varepsilon^{\text{secure}}$-secure. □

For squashing maps, we obtain a similar result.

Lemma 7.4.2 (Squashing maps)**.** *Let* $\left\{\{\widetilde{\mathcal{G}}_j^{\text{full}}\}_{j=1}^n, \mathcal{M}_{\text{CPP}}, \xi_{X_1^n(A'')_1^n}\right\}$ *be a QKD protocol (see Definition 7.3.1) where Bob measures his received state in round* j *with the POVM* $\left\{M_i^{(B_j)}\right\}$*. That is, we have,* $\widetilde{\mathcal{G}}_j^{\text{full}} = \bar{\mathcal{G}}_j^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{(B_j)}\right\}}$*, where* $\mathcal{M}^{\text{meas}}_{\left\{M_i^{(B_j)}\right\}} \in \text{CPTP}(B_j, Y_j)$ *and* $\bar{\mathcal{G}}_j^{\text{full}} \in \text{CPTP}(X_jY_j, S_jX_jY_j\widehat{C}_j\widetilde{C}j)$*. Suppose there exists quantum channels (squashing maps)* $\Lambda_j \in \text{CPTP}(B_j, Q_j)$ *and measurement channels* $\mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_j}\right\}} \in \text{CPTP}(Q_j, Y_j)$ *such that*

$$\mathcal{M}^{\text{meas}}_{\left\{F_i^{(Q_j)}\right\}} \circ \Lambda_j = \mathcal{M}^{\text{meas}}_{\left\{M_i^{(B_j)}\right\}} \quad \textit{for all } j. \tag{7.73}$$

Moreover, suppose that the squashed protocol $\left\{\left\{\bar{\mathcal{G}}_j^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{(Q_j)}\right\}}\right\}_{j=1}^{n}, \mathcal{M}_{\text{CPP}}, \xi_{X_1^n(A'')_1^n}\right\}$ *using the measurement channel* $\mathcal{M}^{\text{meas}}_{\left\{F_i^{(Q_j)}\right\}}$ *is* $\varepsilon^{\text{secure}}$*-secure against all attacks* $\mathcal{A}_j^{\text{Sq}} \in \boldsymbol{\mathcal{A}}_j^{\text{set}}$*, where*

$$\boldsymbol{\mathcal{A}}_j^{\text{set}} \supset \Lambda_j \circ \text{CPTP}(E_{j-1}, B_j E_j) \quad \textit{for all } j. \tag{7.74}$$

Then the real protocol $\left\{\left\{\bar{\mathcal{G}}_j^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{(B_j)}\right\}}\right\}_{j=1}^{n}, \mathcal{M}_{\text{CPP}}, \xi_{X_1^n(A'')_1^n}\right\}$ *using the measurement channel* $\mathcal{M}^{\text{meas}}_{\left\{M_i^{(B_j)}\right\}}$ *is* $\varepsilon^{\text{secure}}$*-secure against all attacks* $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E_j)$ *in round* j*.*

Proof. We start with Eve's attack $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E_j)$ for the real protocol $\left\{\left\{\bar{\mathcal{G}}_j^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{(B_j)}\right\}}\right\}_{j=1}^{n}, \mathcal{M}_{\text{CPP}}, \xi_{X_1^n(A'')_1^n}\right\}$ and reduce its security to that of the squashed protocol as follows

$$\begin{aligned}
&\Big\| \Big(\mathcal{M}_{\text{CPP}} \circ \bar{\mathcal{G}}_n^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{B_n}\right\}} \circ \mathcal{A}_n \circ \cdots \circ \bar{\mathcal{G}}_1^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{B_1}\right\}} \circ \mathcal{A}_1 \\
&\qquad - \mathcal{R}_{\text{ideal}} \circ \mathcal{M}_{\text{CPP}} \circ \bar{\mathcal{G}}_n^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{B_n}\right\}} \circ \mathcal{A}_n \circ \cdots \circ \bar{\mathcal{G}}_1^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{M_i^{B_1}\right\}} \circ \mathcal{A}_1 \Big) \left[\xi_{X_1^n(A'')_1^n}\right] \Big\|_1 \\
=&\Big\| \Big(\mathcal{M}_{\text{CPP}} \circ \bar{\mathcal{G}}_n^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_n}\right\}} \circ \Lambda_n \circ \mathcal{A}_n \circ \cdots \circ \bar{\mathcal{G}}_1^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_1}\right\}} \circ \Lambda_1 \circ \mathcal{A}_1 \\
&\qquad - \mathcal{R}_{\text{ideal}} \circ \mathcal{M}_{\text{CPP}} \circ \bar{\mathcal{G}}_n^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_n}\right\}} \circ \Lambda_n \circ \mathcal{A}_n \circ \cdots \circ \bar{\mathcal{G}}_1^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_1}\right\}} \circ \Lambda_1 \circ \mathcal{A}_1 \Big) \left[\xi_{X_1^n(A'')_1^n}\right] \Big\|_1 \\
=&\Big\| \Big(\mathcal{M}_{\text{CPP}} \circ \bar{\mathcal{G}}_n^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_n}\right\}} \circ \mathcal{A}_n^{\text{Sq}} \circ \cdots \circ \bar{\mathcal{G}}_1^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_1}\right\}} \circ \mathcal{A}_1^{\text{Sq}} \\
&\qquad - \mathcal{R}_{\text{ideal}} \circ \mathcal{M}_{\text{CPP}} \circ \bar{\mathcal{G}}_n^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{Q_n}\right\}} \circ \mathcal{A}_n^{\text{Sq}} \circ \cdots \circ \bar{\mathcal{G}}_1^{\text{full}} \circ \mathcal{M}^{\text{meas}}_{\left\{F_i^{(Q_j)}\right\}} \circ \circ \mathcal{A}_1^{\text{Sq}} \Big) \left[\xi_{X_1^n(A'')_1^n}\right] \Big\|_1,
\end{aligned} \tag{7.75}$$

where the first equation follows from Eq. (7.73), and the second equation follows by relabelling $\mathcal{A}_j^{\text{Sq}} \coloneqq \Lambda_j \circ \mathcal{A}_j$. Note that $\mathcal{A}_j^{\text{Sq}} \in \boldsymbol{\mathcal{A}}_j^{\text{set}}$ follows from Eq. (7.74). Since this holds for every attack $\mathcal{A}_j \in \text{CPTP}(E_{j-1}, B_j E_j)$ for the real protocol, minimizing the final expression in Eq. (7.75) over all $\mathcal{A}_j^{\text{Sq}} \in \boldsymbol{\mathcal{A}}_j^{\text{set}} \subseteq \text{CPTP}(E_{j-1}, B_j E_j)$ is guaranteed to yield a value that is less than or equal to the result of minimizing the first expression in

Eq. (7.75) over all $\mathcal{A}_j \in \mathrm{CPTP}(E_{j-1}, B_j E_j)$. This completes the proof, by identifying these minimizations with the corresponding definitions of security given in Definition 7.3.2. □

Note that if one employs the simple qubit squasher to map the measurement register from B to Q, then one may simply take $\mathcal{A}_j^{\mathrm{Sq}} \in \boldsymbol{\mathcal{A}}_j^{\mathrm{set}} = \mathrm{CPTP}(E_{j-1}, Q_j E_j)$. We adopt this choice when computing key rates in Section 7.5.

When using the flag-state squasher, however, an additional restriction is required to prevent Eve from exploiting the classical flag registers alone (see Section 3.6.3). This can be implemented by restricting the allowed attack maps $\boldsymbol{\mathcal{A}}_j^{\mathrm{set}}$ to a proper subset of $\mathrm{CPTP}(E_{j-1}, Q_j E_j)$. Such a restriction is described in Ref. [3, Section 9]. While we do not formally incorporate this restriction here, our methods are fully compatible with the use of the flag-state squasher. For comparison, Ref. [9] also makes use of the flag-state squasher, but does so only after applying MEAT in the infinite-dimensional setting, at the level of a single-round optimization, which we avoid here.

7.5 Plots

To generate key rates from Theorem 7.3.3, we must compute the quantity $\kappa^{\mathrm{QKD}}\left(f_{|\hat{c}_1^{j-1}}, \sigma_{A_j}^{(j)}, \mathcal{G}_j\right)$ defined in Eq. (7.65). We have shown in Lemma 7.3.6 that this quantity can be expressed as a finite-dimensional convex optimization problem, making it suitable for numerical computation. If the protocol of interest is such that Alice and Bob perform the same operation in each round, then all the maps $\mathcal{G}_j$ are identical and states $\sigma_{A_j}^{(j)}$ are identical. Furthermore, one can choose the same tradeoff function $f_{|\hat{c}_1^{j-1}}$ for all $j, \hat{c}_1^{j-1}$. Thus the dependence on j disappears and in what follows we drop the subscript j and write it more compactly as $\kappa^{\mathrm{QKD}}(f, \sigma_A, \mathcal{G})$:

$$\kappa^{\mathrm{QKD}}(f, \sigma_A, \mathcal{G}) \leq \inf_{\mathcal{Q} \in \boldsymbol{\mathcal{Q}}^{\mathrm{set}}} \widetilde{H}_\alpha^{\uparrow, f}(S|\widehat{C}\widetilde{C}\widehat{E})_{\mathcal{G}[\mathtt{Pur}(\mathcal{Q}[\sigma_{AA'}])]}, \tag{7.76}$$

The above optimization problem is exactly the one solved in Ref. [159, 9].[28] Furthermore, one also has a choice in choosing the tradeoff functions $f_{\hat{c}_1^{j-1}}$. In fact, a suitable choice of

[28] Note that these works impose certain conditions in order to render the associated optimization problems more tractable. Informally, they require the probability of `test` rounds to be a fixed value, and they assign the same tradeoff score to all public announcements occurring in `gen` rounds. These assumptions are not severely restrictive in practice. We do not go into the details of these conditions here, except to note that the protocols considered in this thesis satisfy them.

these functions is critically important to obtain good performance, and a procedure for choosing optimal functions is provided in Ref. [9].

With these details in place, we are now ready to compute key rates using the machinery and codebase provided in Ref. [9]. We emphasize that all credit for the numerical methods and implementation belongs to the authors of that work. The plots presented here are intended purely for illustrative purposes and are generated using their publicly available code, with only minimal modifications on our part. Furthermore, Ref. [9] computes key rates for a larger class of protocols, including passive setups using the flag-state squasher, includes imperfections, and also optimized over many of the free parameters.

7.5.1 Qubit BB84

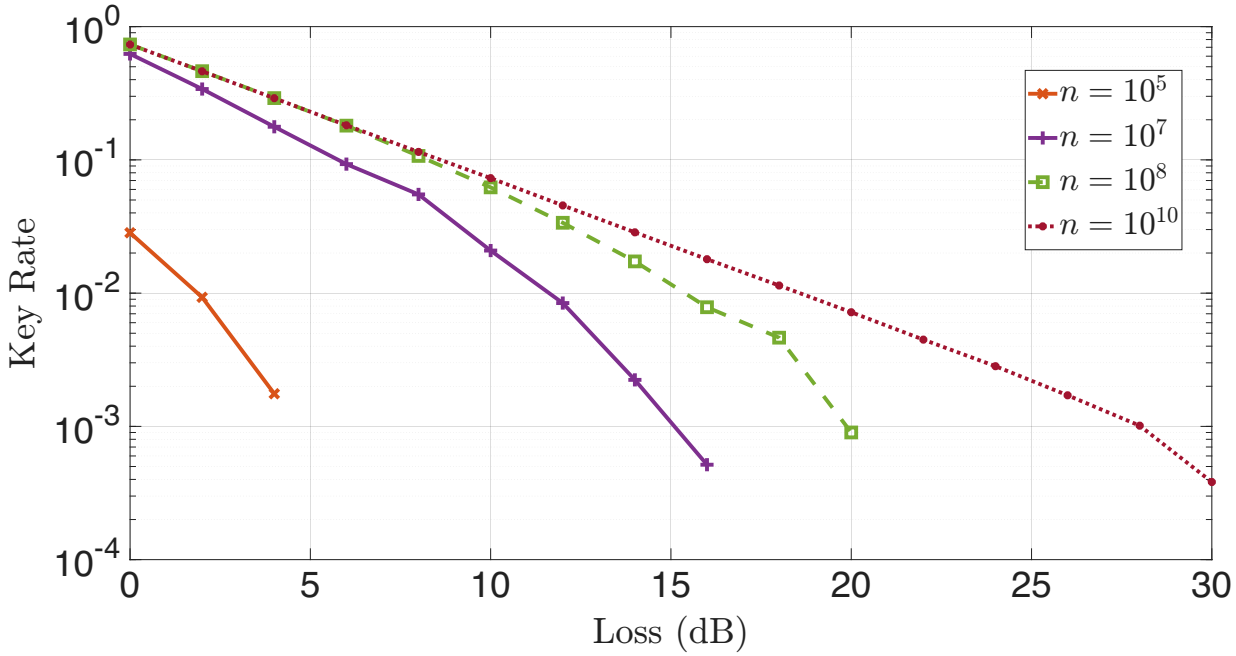


Figure 7.3: Key rate for variable-length qubit BB84 protocol plotted against loss, using MEAT, computed using open source code from Ref. [9].

We plot key rates for a loss-only channel in Fig. 7.3, for the qubit BB84 protocol. We set $\varepsilon_{\mathrm{PA}} = \varepsilon_{\mathrm{AT}} = 10^{-10}$ leading to an overall security parameter of $\varepsilon^{\mathrm{secure}} = 2 \times 10^{-10}$. A round is chosen to be a `test` round with probability $\gamma = 0.1$, and a `gen` round with probability $1 - \gamma$. For both `test` and `gen` rounds, Alice (and Bob) chooses the Z basis with probability

0.9 (X with probability 0.1), with each basis state sent with equal probability. We set $\lambda_{\mathrm{EC}}(\hat{c}_1^n) = f_{\mathrm{EC}} n H(S|Y\widehat{C})_{\mathrm{freq}(\hat{c}_1^n)}$ (meaning that the entropy is computed for the distribution implied by the announcements), with $f_{\mathrm{EC}} = 1.16$. We use the optimized values of α for each loss value, computed in Ref. [9].[29]. We plot key rates for the typical observations expected for the given channel parameters.

7.5.2 Decoy-state BB84

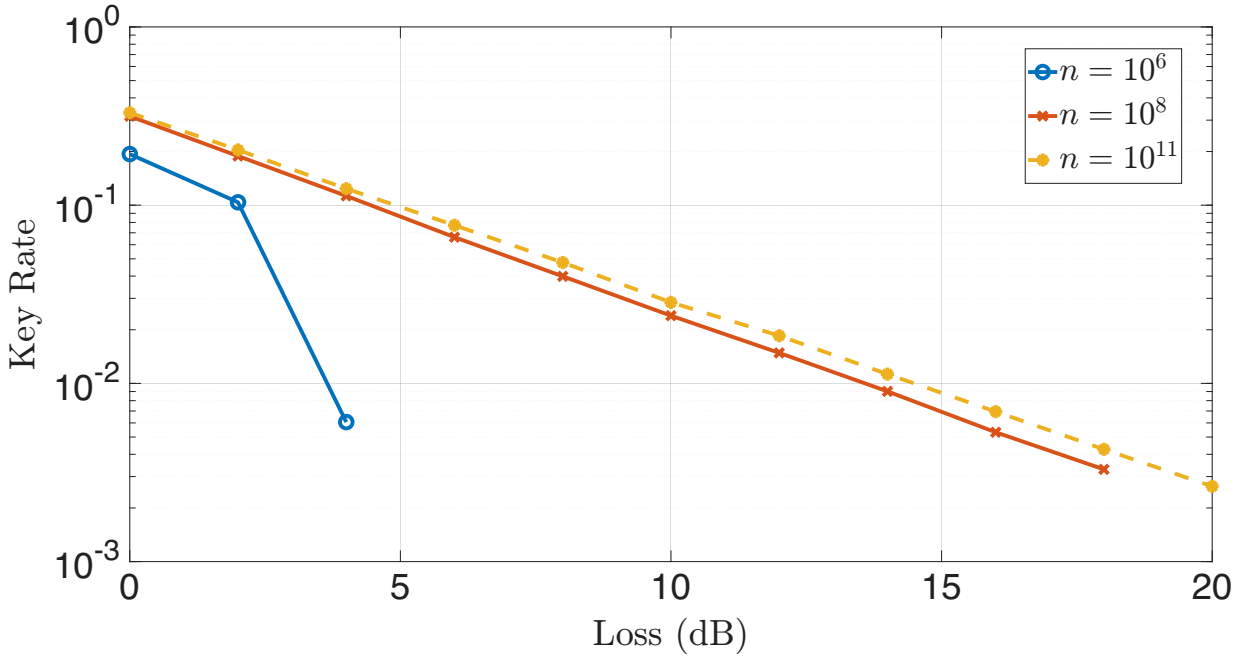


Figure 7.4: Key rate for the variable-length decoy-state BB84 protocol plotted as a function of loss, computed using MEAT. While key rates can, in principle, be evaluated at higher loss values, this becomes numerically challenging due to the optimization over the Rényi parameter. The results shown here are obtained using open-source code from Ref. [9]; we refer the reader to that work for additional plots covering a broader range of loss values.

We plot key rates for a loss-only channel in Fig. 7.4 for the decoy-state BB84 protocol. We set $\varepsilon_{\mathrm{PA}} = \varepsilon_{\mathrm{AT}} = 10^{-10}$ leading to an overall security parameter of $\varepsilon^{\mathrm{secure}} = 2 \times 10^{-10}$. The decoy intensities are given by $\mu_1 = 1, \mu_2 = 0.1, \mu_3 = 0.001$, and the probability of `test`

[29]Note that the protocol for which these optimal values were computed is a slightly different one from the one we consider here. This does not pose a problem, since every value of α yields a valid key rate.

rounds is set to $\gamma = 0.1$. We consider a protocol where, in `test` rounds, Alice sends X states with equal probability, using all three intensities (also with equal probabilities). In the `gen` rounds, Alice uses only m_1 intensity, and sends both Z states with equal probability. We set $\lambda_{\mathrm{EC}}(\hat{c}_1^n) = f_{\mathrm{EC}} n H(S|Y\widehat{C})_{\mathrm{freq}(\hat{c}_1^n)}$ (meaning that the entropy is computed for the distribution implied by the announcements), with $f_{\mathrm{EC}} = 1.16$. We plot key rates for the typical observations expected for the given channel parameters. For every key rate point, we optimize over α. We consider active detection setup by Bob, and use the qubit squasher, with double-clicks in each basis randomly mapped to single-clicks.

7.6 Summary and Outlook

The analysis presented in this chapter constitutes a very general and flexible application of the MEAT technique to QKD security analysis. It begins by considering an abstract formulation of a generic QKD protocol (Generic QKD Protocol) and establishes security under the assumption of finite-dimensional state preparation and measurements. This framework is then extended to practical optical implementations (which inherently involve infinite-dimensional systems) through the use of standard techniques such as squashing (Lemma 7.4.2) and source maps (Lemma 7.4.1). The framework is general and can, in principle, accommodate new classes of source and squashing maps that have not yet been formalized in the literature - for instance, those designed to model correlated imperfections. The entire analysis supports on-the-fly announcements, a feature that is important to efficiently utilize classical memory in implementations, and fully adaptive key rates (Remark 7.3.9), an aspect especially relevant for satellite QKD. Moreover, much of our analysis—such as the use of squashing, source maps, and the treatment of an infinite-dimensional Eve—is not tied to the specific formulation of MEAT used here. These components are likely to remain valid for future variations in QKD proof techniques, such as the new EAT variants, for example.

As an example of the modularity and flexibility of our approach, consider the security proof of the six-state protocol [160] implemented using, for instance, a single-photon source. This can be obtained straightforwardly by (1) expressing the protocol as an instance of our Generic QKD Protocol, (2) applying the appropriate squashing and source map[30], and (3) evaluating the resulting optimization problem using Ref. [9]. This procedure is outlined as a recipe in Section 7.3.7. In fact, the present framework can be applied to essentially the same protocol considered in Ref. [33], which likewise aims to provide a self-contained and

[30]Source maps are not required if the single-photon source is assumed to have ideal properties.

rigorous security analysis of decoy-state BB84, by following the steps outlined above. The only minor distinction is that Ref. [33] employs dual-universal$_2$ hash families for privacy amplification, whereas we require universal$_2$ hash families.

More generally, as discussed in Remark 7.3.9, our results also extend to fully adaptive protocols - a feature that is not currently available in any other proof technique. Moreover, it may prove particularly valuable for scenarios such as satellite QKD, where the channel behaviour changes with time. While this work provides the complete theoretical framework required for such analyses, a detailed study of various ways to update the optimal trade-off function and its impact on achievable key rates in time-varying channels is left for future work.

Another important direction for future work is the detailed treatment of device imperfections. A wide class of imperfections can, in principle, be incorporated within our framework, as outlined in [3, Section 11]. Integrating them rigorously with the above framework is an open and formidable task. Nonetheless, the framework and results presented in this work provide the essential tools and foundations for such an endeavor.

In summary, this chapter establishes a rigorous, extensible, and implementation-oriented foundation for the security analysis of practical QKD protocols. The key ingredient in this analysis is the generality and the MEAT statement itself, which then lends itself to a very general analysis of QKD protocols.

Chapter 8

Classical Authentication in QKD security proofs

> Where we consider classical communication and find that the security definition of QKD is wrong, and fix it; where we find that the corresponding security analysis of QKD is flawed too, and fix *that* as well; and where our proposed solution fixes both these problems retroactively.

QKD protocols rely on both quantum and classical communication. In particular, they require the use of authenticated classical channels to ensure the integrity of exchanged messages. A substantial body of work addresses this requirement, including information-theoretically secure authentication schemes [161], performance-optimized constructions [76, 162], and formulations within composable security frameworks [150]. Typically, in most existing QKD security proofs (see for instance [34, 33]), the classical authentication is assumed to behave "honestly": the authenticated channel never aborts, and all classical messages are delivered faithfully with their original timing preserved. All our security analysis in thesis so far has been under this assumption. We refer to this as the honest authentication setting. While this assumption simplifies security analyses, such an idealized channel cannot be realized in practice.

What can be constructed in practice is an authenticated channel that is close in functionality to one which either transmits each message faithfully or delivers a special symbol `auth-abort` to the receiving party, indicating that authentication has failed [65, 150]. An authentication abort occurs, for example, when the authentication tag attached to a

message does not match the expected value, which can happen if the message has been modified or if an adversary attempts to inject a new message without the correct tag. In either case, the receiver discards the message and registers `auth-abort`. Furthermore, an adversary (Eve) is permitted to delay, block, or reorder messages, or perform other timing-related manipulations—some of which may themselves result in an `auth-abort` being delivered to the receiver. We refer to this as the practical[1] authentication setting.

This discrepancy leads to the following issues in the QKD analysis:

1. First, the QKD protocol must now specify what happens when the authentication aborts. The natural choice here is to abort the protocol whenever authentication aborts (and attempt to communicate to the other party that one has aborted).

2. Second, only the receiving party is informed of the authentication aborts. Thus, Eve can generally force *one* party to abort in the QKD protocol while the other accepts (for instance by only interfering with the final message sent between the two parties).

3. Third, since the timing of messages may be modified, one can no longer assume a fixed ordering of actions performed by Alice and Bob. For instance, in the absence of synchronized clock assumptions in the security proof, Alice and Bob typically use messages to inform each other of completion of various operations in the protocol. If the timing of these messages is affected, then the ordering of actions performed by Alice and Bob is also affected.

These challenges arise in any setting where the authenticated classical channel may abort asymmetrically and where message timing is not rigidly preserved. Moreover, they require significant modifications to the security analysis:

- Due to Eve's ability to force asymmetric aborts in the realistic authentication setting, the usual security definition of QKD as specified in [65, 66, 7, 64, 95], which only covers symmetric aborts, cannot be satisfied. This observation has been noted in prior works, see for instance, [65, Section VII] [7, Section 5.2.1] [66].

- Even if one chooses to disregard the problem of one-sided aborts, it remains important to recognize that existing QKD security analyses rely (often implicitly) on a fixed time ordering of classical communications, which is not guaranteed in practice.

[1]By "practical" we mean a setting that is not itself perfectly achievable, but for which practical constructions can approximate the idealized functionality in the composable sense. See Section 8.2.1 for more discussion.

In this chapter, we address this gap as follows. In Section 8.1, we introduce the modified security definition for QKD protocols from Ref. [66], which remains valid even when authentication can lead to receiver-side aborts. This definition generalizes the usual trace-distance criterion (Definition 3.1.1) by explicitly incorporating asymmetric abort events. In Section 8.2.1, we specify a detailed model of interactive classical communication where authentication can result in one-sided aborts and where the adversary may modify the timing of classical messages (possibly resulting in authentication aborts). We also briefly discuss how such a model can be implemented in practice. We then consider the scenario where we have an arbitrary "core" QKD protocol, which is followed by a short authentication post-processing (APP) step, described in Section 8.2.3. Our goal is to analyze the security of the combined core QKD + APP protocol in the practical setting where authentication can lead to asymmetric aborts and where message timing may be influenced by the adversary. In Section 8.2.4, we state our main result: a reduction theorem showing that the security analysis of this combined protocol can be reduced to that of the core QKD protocol alone, under the assumption of honest authentication. This provides a clean separation between authentication and QKD security analysis, since one need not be concerned with authentication aborting or the timing of messages during classical communication while studying the security of the core QKD protocol. Moreover, it also retroactively lifts all prior QKD security proofs that were undertaken in the regime where the authentication was assumed to be honest to the more practical scenario, with the caveat that the protocol must now include the additional authentication post-processing step. The proof of this reduction is presented in Section 8.3. Finally, in Section 8.4, motivated by practical considerations of authentication key usage, we extend our analysis to the scenario of delayed authentication, where all classical communication during the core QKD protocol is undertaken using unauthenticated classical communication, and the entire communication transcript is authenticated at the end of the protocol. We also discuss the trade-offs associated with this choice. Concluding remarks are presented in Section 8.5.

We note that some prior works have analyzed the security of QKD protocols in conjunction with a realistic model of authentication, see, for example Ref. [163]. However, the analysis in that work is tailored to a specific QKD protocol combined with a specific authentication protocol. In contrast, we establish a general result that applies to generic QKD protocols.

8.1 Security Definition with asymmetric aborts

Let us recall some notation we used for stating the security definition in Chapter 3. Let us focus on the output state of a generic QKD protocol, defined on the registers $K_A K_B \boldsymbol{E}$, in the setting where asymmetric aborts are possible. Alice and Bob possess classical registers K_A and K_B. The classical registers K_A, K_B encode keys of arbitrary length for Alice and Bob — this is formalized by having K_A consist of a direct sum $K_A = \bigoplus_{l_A} K_A^{l_A}$, where $K_A^{l_A}$ is a classical register holding keys of length l_A, and analogously for K_B. We treat any party aborting as them storing a key of length 0 in their registers, which we denote with a special symbol $\perp$. The $\boldsymbol{E}$ register denotes all of Eve's information at the end of the QKD protocol, and may include a copy of the classical communications that occurred in the protocol. The precise modeling of the authenticated classical communication, message timing, and one-sided authentication aborts is not essential for the security definition of QKD, which is only concerned with the output state of the QKD protocol, and will therefore be deferred to Section 8.2.1. What matters for now is simply that the QKD protocol may output a state in which one party aborts while the other does not.

The output state of a generic QKD protocol can be written as [66]:

$$\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \coloneqq \bigoplus_{l_A, l_B \in \mathcal{K}} \Pr(\Omega_{l_A,l_B}) \rho^{\text{real}}_{K_A^{l_A} K_B^{l_B} \boldsymbol{E} | \Omega_{l_A,l_B}}, \tag{8.1}$$

where Ω_{l_A,l_B} denotes the event that Alice and Bob produce keys of lengths l_A and l_B, respectively, and $\mathcal{K}$ denotes the set of possible output key length combinations. The subregisters $K_A^{l_A}$ and $K_B^{l_B}$ store the keys of those specific lengths. As argued in Ref. [66], we restrict the set of possible output key length combinations to the following:

$$\mathcal{K} = \{(l_A, l_B) \mid l_A = l_B \ \vee \ l_A = 0 \ \vee \ l_B = 0\}. \tag{8.2}$$

That is, Alice and Bob either share keys of the same length, or at least one of them aborts the protocol.

The ideal output state $\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}}$ is defined to be the one obtained by acting a map $\mathcal{R}_{\text{ideal}} \in \text{CPTP}(K_A K_B, K_A K_B)$ acting on the real output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}$ as

$$\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} \coloneqq \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \right]. \tag{8.3}$$

Throughout this chapter, we adopt the convention that the ideal and real states of various kinds are related analogously to Eq. (8.3); that is, the ideal state is obtained by applying the map $\mathcal{R}_{\text{ideal}}$ to the corresponding real state. The action of the map $\mathcal{R}_{\text{ideal}}$ was defined in

Section 3.1 for scenarios where key lengths are the same. We simply extend that definition to the scenario where the key lengths are different. The map $\mathcal{R}_{\text{ideal}}$ performs the following operations:

- It looks at the length of the keys stored in registers K_A, K_B to compute l_A, l_B.
- It replaces the K_A, K_B registers with the state

$$\tau_{K_AK_B}^{l_A,l_B} := \begin{cases} \dfrac{1}{2^{l_A}} \displaystyle\sum_{k\in\{0,1\}^{l_A}} |kk\rangle\langle kk|_{K_AK_B}\,, & \text{if } l_A = l_B, \\ \tau_{K_A}^{l_A} \otimes \tau_{K_B}^{l_B} & \text{if } l_A \neq l_B, \end{cases} \tag{8.4}$$

$$\tau_{K_A}^{l_A} := \frac{1}{2^{l_A}} \sum_{k\in\{0,1\}^{l_A}} |k\rangle\langle k|_{K_A}\,, \qquad \tau_{K_B}^{l_B} := \frac{1}{2^{l_B}} \sum_{k\in\{0,1\}^{l_B}} |k\rangle\langle k|_{K_B}\,.$$

  That is, if the output lengths are the same, the key registers are replaced with perfectly uniform identical keys of that length, independent of all other registers (which the same action as before). If the output key lengths are not the same, the key registers are *individually* replaced with perfectly uniform keys of the corresponding lengths, independent of all other registers.

Thus intuitively, any key obtained from the ideal state is safe to use, regardless of symmetric or asymmetric aborts, since the key is always independent of Eve's side-information registers. Note that we have

$$\begin{aligned} \rho_{K_AK_B\boldsymbol{E}}^{\text{ideal}} &= \mathcal{R}_{\text{ideal}}\left[\rho_{K_AK_B\boldsymbol{E}}^{\text{real}}\right] \\ &= \sum_{\substack{l_A=l_B=l \\ l_A,l_B\in\mathcal{K}}} \Pr(\Omega_{l,l})\tau_{K_AK_B}^{l,l} \otimes \rho_{\boldsymbol{E}|\Omega_{l,l}}^{\text{real}} + \sum_{\substack{l_A\neq l_B \\ l_A,l_B\in\mathcal{K}}} \Pr(\Omega_{l_A,l_B})\tau_{K_B}^{l_A} \otimes \tau_{K_B}^{l_B} \otimes \rho_{\boldsymbol{E}|\Omega_{l_A,l_B}}^{\text{real}}. \end{aligned} \tag{8.5}$$

Moreover, $\mathcal{R}_{\text{ideal}}$ acts independently on each combination of key length subregisters, i.e, it can be written as

$$\mathcal{R}_{\text{ideal}} = \bigoplus_{l_A,l_B} \mathcal{R}_{\text{ideal}}^{(l_A,l_B)}, \qquad \text{where } \mathcal{R}_{\text{ideal}}^{(l_A,l_B)} \in \text{CPTP}(K_A^{l_A}K_B^{l_B}, K_A^{l_A}K_B^{l_B}). \tag{8.6}$$

We now state the security definition, which will require us to talk about protocols and their corresponding output states. We therefore set up some notation first. Let us

consider a protocol $\mathcal{P}$. What we will typically be concerned with is the set of output states produced by the protocol, which we denote by $\mathcal{W}(\mathcal{P})$. This set of possible output states depends on various assumptions ($\mathcal{W}$) under which we analyze the protocol. In this chapter, these assumptions will be related to the authenticated channel that is used during communication, and are explained in Section 8.2.1.[2] Thus, these assumptions fix the set of possible attacks Eve can perform, and the protocol $\mathcal{P}$ along with Eve's attack together determine a channel mapping the relevant input states to output states. When we write $\mathcal{W}(\mathcal{P})$, we refer to the set of all output states that can arise under all possible choices of Eve's attack. Moreover, when we compose two protocols via $\mathcal{P}_2 \circ \mathcal{P}_1$, the composed protocol is understood in the sense of channel composition, where the resulting channel is fixed by the protocol descriptions and Eve's attack on both protocols. This level of formalism is sufficient for our purposes. We can now state the QKD security definition.

Definition 8.1.1 (QKD Security with asymmetric aborts [66])**.** Let $\mathcal{P}_{\text{QKD}}$ be a QKD protocol, and let $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}$ be the output state of the QKD protocol, and let $\mathcal{W}(\mathcal{P}_{\text{QKD}})$ denote the set of possible output states of the QKD protocol. Let $\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}}$ be the ideal output state, obtained by acting the map $\mathcal{R}_{\text{ideal}}$ on the actual output state. That is

$$\begin{aligned} \rho^{\text{real}}_{K_A K_B \boldsymbol{E}} &:= \bigoplus_{l_A, l_B} \Pr(\Omega_{l_A, l_B}) \rho^{\text{real}}_{K_A^{l_A} K_B^{l_B} \boldsymbol{E} | \Omega_{l_A, l_B}} \\ \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \right]. \end{aligned} \tag{8.7}$$

Then, the (variable-length) QKD protocol is $\varepsilon^{\text{secure}}$-secure if, for all output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$, the following inequality is satisfied[3]:

$$\frac{1}{2} \left\| \rho^{\text{real}}_{K_A K_B \boldsymbol{E}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} \right\|_1 \leq \varepsilon^{\text{secure}}. \tag{8.8}$$

Note that Definition 8.1.1 generalizes the standard definition of QKD security (Definition 3.1.1) [64, 65, 66] (which corresponds to the case where $\Pr(\Omega_{l_A, l_B}) = 0$ whenever $l_A \neq l_B$ in Eq. (8.7)) to the case where the output state may have asymmetric aborts. Furthermore,

[2] For example, an assumption may be that Alice and Bob use unauthenticated classical communication, and Eve is allowed to tamper with classical messages. A different assumption may be that they use authenticated classical communication, and no tampering of the classical communication is allowed. These give rise to different sets of possible output states.

[3] As noted earlier, in Ref. [66], the trace norm appearing in the security definition is not divided by 2. In contrast, the typical security definition [64, 65] includes the explicit factor of 1/2. The definition used in Ref. [66] is deliberate and well motivated within that work; we stress that the difference amounts only to an overall factor of 2 in the security parameter.

observe that the definition depends on the set of possible output states $\mathcal{W}(\mathcal{P}_{\mathrm{QKD}})$, which in turn depends on the authentication setting under consideration. Under the assumption of honest authentication (and appropriate protocol design), asymmetric aborts cannot occur. Throughout this chapter, we adopt the convention that the ideal and real states of various kinds are related analogously to Eq. (8.7); that is, the ideal state is obtained by applying the map $\mathcal{R}_{\mathrm{ideal}}$ to the corresponding real state.

8.2 Model and Reduction Statement

We will now specify various protocols, various assumptions on authentication and the classical communication model, and state our reduction theorem.

8.2.1 Authenticated Classical Communication Model

We will now explain the authenticated classical communications model we assume for the practical authentication setting. We stress that this model still contains idealized properties, in the sense that Eve has zero probability of faking messages without the authentication aborting. However, it is practical in the sense that it accounts for timing tampering and one-sided aborts. Moreover, we believe that an $\varepsilon_{\mathrm{auth}}$-close construction of such a channel is achievable within a composable framework (see Section 8.2.2 later for further discussion).

We begin by introducing notation to describe the sending and receiving of classical messages between Alice and Bob, which are mediated by Eve. For each message, we associate a register label from both the sender's and receiver's perspectives, and a global time (see Fig. 8.1). We emphasize that no assumptions are made about the alignment between the sender's and receiver's message ordering; these may differ in the presence of an active adversary. Moreover, we do not assume that Alice and Bob share synchronized clocks, nor do they need to record the timing of messages during the protocol. The times introduced here are used only for the purpose of theoretical analysis and refer to the global time when these events occur.

- **Alice sending:** Alice sends messages in registers $C^{(i)}_{A\to E}$, where the index i denotes the ordering of messages from her perspective, i.e, in the order she sends them. We let $t^{(i)}_{A\to E}$ denote the time at which this message leaves Alice.

- **Alice receiving:** Alice receives messages $C^{(i)}_{E\to A}$, where the index i denotes the ordering of messages from her perspective, i.e, in the order she receives them. We let $t^{(i)}_{E\to A}$ denote the time at which this message is received by Alice.
- **Bob sending:** Bob sends messages in registers $C^{(i)}_{B\to E}$, where the index i denotes the ordering of messages from Bob's perspective, i.e, in the order he sends them. We let $t^{(i)}_{B\to E}$ denote the time at which this message leaves Bob.
- **Bob receiving:** Bob receives messages $C^{(i)}_{E\to B}$, where the index i denotes the ordering of messages from his perspective, i.e, in the order he receives them. We let $t^{(i)}_{E\to B}$ denote the time at which this message is received by Bob.

Thus, each sent (received) message is indexed from the sender's (receiver's) point of view, and the time values reflect the true time at which these events occur (which are not known to Alice and Bob). We will modify this setting later in Section 8.4.

We assume that the classical authenticated channel between the two honest parties has the following properties (see Fig. 8.1):

1. **Timing:** If the ith message is received *before* the ith message was sent, then the received message is the special symbol `auth-abort`. Formally,

$$\begin{aligned} t^{(i)}_{A\to E} > t^{(i)}_{E\to B} \quad &\implies \quad C^{(i)}_{E\to B} \text{ stores } \texttt{auth-abort}, \quad \forall i. \\ t^{(i)}_{B\to E} > t^{(i)}_{E\to A} \quad &\implies \quad C^{(i)}_{E\to A} \text{ stores } \texttt{auth-abort}, \quad \forall i. \end{aligned} \tag{8.9}$$

   We refer to the case where $t^{(i)}_{B\to E} \leq t^{(i)}_{E\to A}$ and $t^{(i)}_{A\to E} \leq t^{(i)}_{E\to B}$ holds for all i as "relative time ordering being preserved".

2. **Modifying messages:** If ith message is received *after* the ith message was sent, then the received message is either a copy of the sent message or it is an `auth-abort`. Formally,

$$\begin{aligned} t^{(i)}_{A\to E} \leq t^{(i)}_{E\to B} \quad &\implies \quad \text{Either } C^{(i)}_{E\to B} \text{ and } C^{(i)}_{A\to E} \text{ store identical messages,} \\ &\qquad\quad \text{or } C^{(i)}_{E\to B} \text{ stores } \texttt{auth-abort}, \quad \forall i. \\ t^{(i)}_{B\to E} \leq t^{(i)}_{E\to A} \quad &\implies \quad \text{Either } C^{(i)}_{E\to A} \text{ and } C^{(i)}_{B\to E} \text{ store identical messages,} \\ &\qquad\quad \text{or } C^{(i)}_{E\to A} \text{ stores } \texttt{auth-abort}, \quad \forall i. \end{aligned} \tag{8.10}$$

   We assume if Eve attempts to block messages for longer than some preselected finite duration, then this results in the "received message" being an `auth-abort` (which

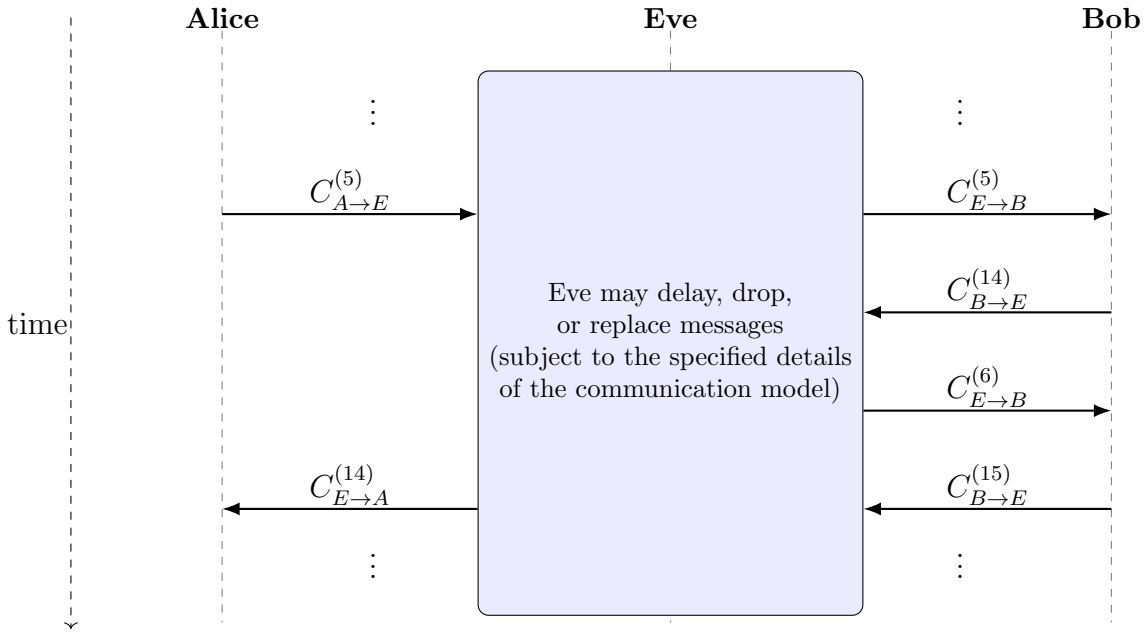


Figure 8.1: The practical authenticated classical communication model used in this chapter. Messages pass through Eve, who may delay, drop, or substitute them with `auth-abort`, subject to the constraints described in Section 8.2.1. Time flows from top to bottom in the figure, which illustrates an example scenario: in earlier parts of the protocol (not shown in the figure), 4 messages have been sent from Alice to Bob, and 13 messages from Bob to Alice. Eve does not interfere with Alice's 5th message to Bob. However, she chooses to delay Bob's 14th message. (Presumably, Alice does not send a new message during this period because she is waiting to receive one.) During the delay, Eve receives Bob's 15th message and also delivers the 6th message to Bob. According to our communication model, this implies that $C^{(6)}_{E\to B}$ must be `auth-abort`, since it was received before Alice sent her 6th message.

can be implemented simply by having the receiving party record `auth-abort` after that duration has elapsed).

For a given QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$, we denote the set of output states possible in the above model for authenticated classical communication via $\mathcal{W}^{\mathrm{real}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}})$. In the honest authentication setting, we assume that Eve is not allowed to perform any operation that

can results in an `auth-abort`. That is, we are guaranteed to have:

$$\begin{aligned} &t^{(i)}_{A\to E} \leq t^{(i)}_{E\to B} && \forall i \\ &t^{(i)}_{B\to E} \leq t^{(i)}_{E\to A} && \forall i \\ &C^{(i)}_{E\to B} \text{ and } C^{(i)}_{A\to E} \text{ store identical messages} && \forall i \\ &C^{(i)}_{E\to A} \text{ and } C^{(i)}_{B\to E} \text{ store identical messages} && \forall i \end{aligned} \tag{8.11}$$

We denote the set of output states possible under this setting via $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$.

8.2.2 Implementing the authenticated communication model

We note that there exist implementations of authenticated classical channels that closely approximate the functionality described by our model. One such implementation involves Alice and Bob sharing a pool of pre-distributed keys, which are used to authenticate each classical message using a message authentication scheme. As messages are sent and received, the parties iterate through their sending and receiving key pools. For example, they may employ Wegman–Carter authentication [161], potentially with key recycling, as discussed in Ref. [150].

In such a setup, assuming the authentication keys remain secret, any attempt by Eve to modify a message will result in an invalid authentication tag with high probability, which causes the receiver to interpret the message as an `auth-abort`. Moreover, if Eve attempts to deliver a message to the receiver *before* the corresponding message has been sent, she will not have access to a valid message–tag pair. In this case as well, the receiver will reject the message as invalid (with high probability) and interpret it as `auth-abort`. The same holds if e.g. a pair of messages are swapped, since both messages would then result in `auth-abort`s (with high probability). Note that in this description, there is no requirement for Alice and Bob to include the message index as a part of the message.

In practice, however, no implementation can perfectly realize the idealized model. There is always a small probability that Eve successfully forges a valid tag for a modified message. To account for this, we could proceed in either of two ways. First, we could track this probability explicitly throughout our entire analysis, i.e. noting at every step that there is some small probability of Eve forging the message without being detected, and writing the proof such that this event is explicitly tracked and accounted for. Alternatively, we could just perform our analysis entirely under the idealized model, and then rely on a separate proof that the implemented authentication protocol is a composably $\varepsilon_{\text{auth}}$-secure construction (in

some composable security framework) of the authenticated channel described above - given these, one can invoke composability to lift the security claims based entirely on the ideal case to the real implemented scenario. In this chapter, our analysis will be based on the latter approach, i.e. we assume the parties have access to the authenticated channel with the functionality described earlier as a starting resource.

We acknowledge however that to our knowledge, the existing literature on composable security currently does not contain an explicit construction of that resource [150, 65, 67]; still, we believe such a construction to be achievable via similar arguments as in Ref. [150], and leave it as a point to be resolved in future work. In fact, if one disregards the technicalities introduced by message timing, the construction of a multi-use authenticated channel with one-sided aborts has already been demonstrated in Ref. [65].

8.2.3 Authentication Post-Processing Protocol (APP)

Recall our setting, where we have a core QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$, followed by an Authentication Post-Processing protocol $\mathcal{P}_{\mathrm{APP}}$. We refer to the resulting combined protocol as $\mathcal{P}_{\mathrm{QKD}} = \mathcal{P}_{\mathrm{APP}} \circ \widetilde{\mathcal{P}}_{\mathrm{QKD}}$. Our goal is to reduce the security of the combined protocol $\mathcal{P}_{\mathrm{QKD}}$ (in the practical authentication setting) to the security of the core QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$ alone (in the honest authentication setting). To achieve this, we design the Authentication Post-Processing protocol $\mathcal{P}_{\mathrm{APP}}$ such that

- both parties abort whenever any message during the core QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$ results in an `auth-abort`,
- it commutes with the map $\mathcal{R}_{\mathrm{ideal}}$.

These properties are crucial in our proof of the reduction in Section 8.3. We will now specify the Authentication Post-Processing protocol.

Let $\rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}$ denote the final state obtained after the execution of the core QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$, where $\boldsymbol{C}_{\mathbf{fin}} = \boldsymbol{C}_{\boldsymbol{A}\to\boldsymbol{E}}\boldsymbol{C}_{\boldsymbol{E}\to\boldsymbol{B}}\boldsymbol{C}_{\boldsymbol{B}\to\boldsymbol{E}}\boldsymbol{C}_{\boldsymbol{E}\to\boldsymbol{A}}$ collects all classical communication that occurred during the core protocol, and $\boldsymbol{E}_{\mathbf{fin}}$ denotes all of Eve's side information, which may include a copy of the classical communication. During the authentication post-processing phase, Alice and Bob start with the state $\rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}$, perform some classical operations and communicate using registers $\boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{A}\to\boldsymbol{E}}, \boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{E}\to\boldsymbol{B}}, \boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{B}\to\boldsymbol{E}}, \boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{E}\to\boldsymbol{A}}$ (see Fig. 8.2).

Protocol 5 (AuthPP Protocol)**.** Starts with state $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}$. Classical communication is undertaken in the registers $\boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{A}\to\boldsymbol{E}}, \boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{E}\to\boldsymbol{B}}, \boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{B}\to\boldsymbol{E}}, \boldsymbol{C}^{\mathbf{auth}}_{\boldsymbol{E}\to\boldsymbol{A}}$.

APP 1 Alice checks whether any of her received messages in $\boldsymbol{C}_{\boldsymbol{E}\to\boldsymbol{A}}$ is a `auth-abort`. If she finds one, she replaces K_A with $\perp$.

APP 2 Bob checks whether any of his received messages in $\boldsymbol{C}_{\boldsymbol{E}\to\boldsymbol{B}}$ is an `auth-abort`. If he finds one, he replaces K_B with $\perp$.

APP 3 Bob computes l'_B from K_B. If it is non-zero, he sends a preliminary `accept` message to Alice. Otherwise, he sends an `abort` message to Alice.

APP 4 Alice computes l'_A from K_A. If it is non-zero, *and* she receives an `accept` message from Bob, she sends her final `accept` message to Bob. Else she sends `abort` message to Bob.

APP 5 If Alice sent `accept` message, she does nothing. If she sent `abort` message, she replaces her key registers with $\perp$.

APP 6 If Bob receives an `accept` message from Alice, he does nothing. If Bob receives either a `auth-abort` or an `abort` message, he replaces his key register K_B with $\perp$. We let l_B denote the final key length stored in K_B.

Mathematically, the above protocols can be described as follows:

1. In APP 1 and APP 2, Alice and Bob simply replace their key registers with $\perp$s if they received an `auth-abort` during the prior protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. This is described by a map $\mathcal{E}^{\text{repl}}_{\text{auth}} \in \text{CPTP}(\boldsymbol{C}'_{\mathbf{fin}} K_A K_B, \boldsymbol{C}'_{\mathbf{fin}} K_A K_B)$ (see Remark 8.2.1).
2. In APP 3 and APP 4, Alice and Bob first compute the key lengths l'_A, l'_B stored in their key registers K_A, K_B respectively at that point in time. Based on these values, they engage in two rounds of communications. For a given value of l'_A, l'_B, this can be described as a map (influenced by Eve) $\mathcal{E}^{(l'_A,l'_B)}_{\text{comm}} \in \text{CPTP}(\boldsymbol{E}_{\mathbf{fin}}, \boldsymbol{E}'_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}})$. The overall map is given by $\mathcal{E}_{\text{comm}} \in \text{CPTP}(K_A K_B \boldsymbol{E}_{\mathbf{fin}}, K_A K_B \boldsymbol{E}'_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}})$. Note that $\boldsymbol{C}_{\mathbf{auth}}$ here contains separate messages that were sent and received, since Eve may attack this communication in any manner she desires, potentially modifying her quantum side-information as well [4].

[4]Some messages are still yet to be sent or received; however, for notational simplicity we let the map act on the entirety of $\boldsymbol{C}_{\mathbf{auth}}$, with the understanding that it leaves registers meant to store future messages unchanged.

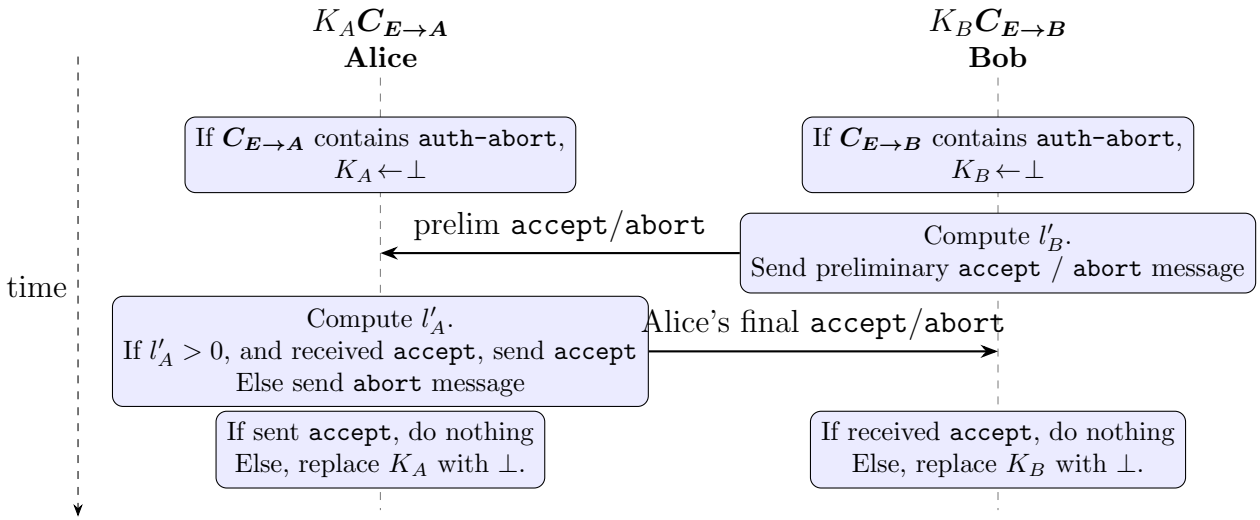


Figure 8.2: Schematic of AuthPP Protocol described in Section 8.2.3. Alice and Bob first update their key registers based on whether they received an `auth-abort` in any of the prior communication. They then communicate their tentatively `accept` / `abort` decisions. They then perform a final update operation on their key registers depending on their final `accept` / `abort` decision.

3. In APP 5 and APP 6, Alice and Bob use the result of the communication in the previous step $\boldsymbol{C}_{\mathbf{auth}}$ to determine their final `accept` / `abort` status. This is described as a map $\mathcal{E}_{\text{update}} \in \text{CPTP}(K_A K_B \boldsymbol{C}_{\mathbf{auth}}, K_A K_B \boldsymbol{C}_{\mathbf{auth}})$

The final output state is denoted by $\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} = \mathcal{E}_{\text{update}} \circ \mathcal{E}_{\text{comm}} \circ \mathcal{E}^{\text{repl}}_{\text{auth}} \left(\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}\right)$, where $\boldsymbol{C}'_{\mathbf{fin}} = \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}}$, where add a superscript 'final' to the state to denote that this is the final output.

Remark 8.2.1. *Note that the first two steps in the above protocol serve to ensure that if any classical communication resulted in an* ***auth-abort****, then the receiving party stores a $\perp$ in the key register. In practice, one can simply enforce this property by appropriate design of the QKD protocol, i.e, by ensuring that the QKD protocol itself stores $\perp$ in the key register whenever* ***auth-abort*** *is received. In such cases, we can omit APP 1 and APP 2 from the authentication post-processing steps, as is done in Ref. [3]. Here we wish to prove a statement that is agnostic to the nature of the QKD protocol implemented. Hence we include APP 1 and APP 2 as explicit steps.*

8.2.4 Reduction Statement

We are now ready to state the theorem that reduces the security analysis of QKD protocols to the setting in which authentication behaves honestly.

Theorem 8.2.1 (Reduction of QKD security analysis to the honest authentication setting)**.** *Let $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$ be an arbitrary QKD protocol. Let $\mathcal{P}_{\mathrm{APP}}$ be the AuthPP Protocol described in Section 8.2.3, executed after the core QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$. Let $\mathcal{P}_{\mathrm{QKD}} = \mathcal{P}_{\mathrm{APP}} \circ \widetilde{\mathcal{P}}_{\mathrm{QKD}}$ denote the resulting QKD protocol. Let $\mathcal{W}^{\mathrm{hon}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}})$ denote the set of possible output states of $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$ in the honest authentication setting (see Section 8.2.1). Let $\mathcal{W}^{\mathrm{real}}_{\mathrm{auth}}(\mathcal{P}_{\mathrm{QKD}})$ denote the set of possible output states of $\mathcal{P}_{\mathrm{QKD}}$ in the practical authentication setting (see Section 8.2.1). Then, the $\varepsilon^{\mathrm{secure}}$-security for all output states in $\mathcal{W}^{\mathrm{hon}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}})$ implies $\varepsilon^{\mathrm{secure}}$-security for all output states[5] in $\mathcal{W}^{\mathrm{real}}_{\mathrm{auth}}(\mathcal{P}_{\mathrm{QKD}})$. That is,*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\mathrm{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\mathrm{ideal,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\mathrm{secure}} \qquad \forall \rho^{\mathrm{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\mathrm{hon}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}}) \\
&\qquad\qquad\qquad\qquad \Downarrow \\
&\frac{1}{2}\left\|\rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\mathrm{ideal}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\mathrm{secure}} \qquad \forall \rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \in \mathcal{W}^{\mathrm{real}}_{\mathrm{auth}}(\mathcal{P}_{\mathrm{QKD}}).
\end{aligned} \tag{8.12}$$

Proof Idea. The detailed proof of this theorem is presented in Section 8.3. We define an event $\Omega_{\text{auth-hon}}$, corresponding to the case where no `auth-aborts` are received during the execution of the core protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$. Under the communication model from Section 8.2.1, any attempt by Eve to tamper with the message content or disturb the relative timing of messages leads to an `auth-abort`. Thus, if we consider states partial on $\Omega_{\text{auth-hon}}$, we may assume that the authentication behaves honestly. (Recall that the state partial on $\Omega_{\text{auth-hon}}$ refers to the state that is conditioned on the event $\Omega_{\text{auth-hon}}$, but which is not re-normalized after the conditioning).

Since $\mathcal{P}_{\mathrm{APP}}$ ensures that both parties abort whenever an `auth-abort` is received, it suffices to upper bound the trace distance from Definition 8.1.1 for the output state of $\mathcal{W}^{\mathrm{real}}_{\mathrm{auth}}(\mathcal{P}_{\mathrm{QKD}})$ partial on $\Omega_{\text{auth-hon}}$. This is because if $\Omega_{\text{auth-hon}}$ does not occur, then both parties abort and the trace distance is zero by definition (see Lemma 8.3.1).

[5] Note that any scenario in which Eve chooses to ignore or forget part of the public classical communication can be treated as one where she first records all communication and then traces out whatever she wishes at the end of the QKD protocol. Moreover, since QKD security analysis already allows Eve to retain all public communication, keeping the public communication register explicit and accessible to her is without loss of generality.

Next, we observe that $\mathcal{P}_{\text{APP}}$ commutes with the ideal map $\mathcal{R}_{\text{ideal}}$. We use this to show that, it is sufficient to prove security for all states in $\mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial on the event $\Omega_{\text{auth-hon}}$ (see Lemma 8.3.2). The final step is showing that it then suffices to prove the security of the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$ in the honest authentication setting. This is shown in Lemmas 8.3.3 to 8.3.5.

Remark 8.2.2. *Theorem 8.2.1 is quite general and serves as a bridge between the standard QKD security analyses performed under the assumption of honest authentication and the more realistic setting where the authentication channel may be actively attacked—both in terms of message content and timing. Furthermore, we emphasize that it is entirely independent of the specific details of the QKD protocol being implemented, whether it is device-dependent or device-independent, prepare-and-measure or entanglement-based, etc.*

8.3 Proof of the Reduction Theorem 8.2.1

In this section, we will provide a rigorous proof of Theorem 8.2.1.

8.3.1 Proving that `auth-abort` in the core QKD protocol results in both parties aborting

We start by proving the following lemma, which states that if either Alice or Bob received an `auth-abort` in $\boldsymbol{C}_{\mathbf{fin}}$ during the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$, then both parties will abort during authentication postprocessing. We use $\Omega_{\text{auth-hon}}$ to denote the event that neither Alice nor Bob receive an `auth-abort` in $\boldsymbol{C}_{\mathbf{fin}}$ during $\widetilde{\mathcal{P}}_{\text{QKD}}$, and write $\Omega^{\text{C}}_{\text{auth-hon}}$ for its complement.

Lemma 8.3.1. *Let $\Omega_{\text{auth-hon}}$ be the event where neither Alice nor Bob receive an `auth-abort` in $\boldsymbol{C}_{\mathbf{fin}}$ during $\widetilde{\mathcal{P}}_{\text{QKD}}$, and let $\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}}$ denote the final output state at the end of the full QKD protocol $\mathcal{P}_{\text{QKD}}$. Then the following equality holds*

$$\mathcal{R}_{\text{ideal}}\left[\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}|\Omega^{\text{C}}_{\text{auth-hon}}}\right] =: \rho^{\text{ideal,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}|\Omega^{\text{C}}_{\text{auth-hon}}} = \rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}|\Omega^{\text{C}}_{\text{auth-hon}}}. \tag{8.13}$$

Therefore,

$$\frac{1}{2}\left\|\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\text{ideal,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}}\right\|_1 = \frac{1}{2}\left\|\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \tag{8.14}$$

Proof. The proof of Eq. (8.13) follows straightforwardly from the structure of the AuthPP Protocol by considering the state $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\text{fin}} \boldsymbol{E}_{\text{fin}} | \Omega^{\text{C}}_{\text{auth-hon}}}$ and tracking it throughout the protocol.

Let us suppose that Alice receives at least one `auth-abort`. Then, APP 1 replaces K_A with $\perp$, and Alice announces `abort` to Bob in APP 4. Bob either receives an `abort` or `auth-abort`, and in either case, replaces his K_B register with $\perp$ in APP 6. The final output key length for both parties is 0.

Similarly, let us suppose that Bob receives at least one `auth-abort`. Then, APP 2 replaces K_B with $\perp$, and Bob sends an `abort` message to Alice in APP 3. This leads to Alice sending an `abort` message to Bob in APP 4 and replacing her key register K_A with $\perp$ in APP 5. Thus, the final output key length for both parties is 0.

The required Eq. (8.13) follows by noting that $\mathcal{R}_{\text{ideal}}$ acts as identity when $l_A = l_B = 0$. Finally, Eq. (8.14) follows from Eq. (8.13) via

$$\begin{aligned}\frac{1}{2}\left\|\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}}}\right\|_1 &= \frac{1}{2}\left\|\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}} \wedge \Omega_{\text{auth-hon}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}} \wedge \Omega_{\text{auth-hon}}}\right\|_1 \\ &+ \frac{1}{2}\left\|\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}} \wedge \Omega^{\text{C}}_{\text{auth-hon}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}} \wedge \Omega^{\text{C}}_{\text{auth-hon}}}\right\|_1 \\ &= \frac{1}{2}\left\|\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}} \wedge \Omega_{\text{auth-hon}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\text{fin}} \boldsymbol{E}'_{\text{fin}} \wedge \Omega_{\text{auth-hon}}}\right\|_1\end{aligned} \tag{8.15}$$

where the first equality follows from the fact that the states conditioned on $\Omega_{\text{auth-hon}}$ and $\Omega^{\text{C}}_{\text{auth-hon}}$ live on orthogonal spaces, and the final equality follows from Eq. (8.13). □

8.3.2 Reducing to security before authentication post-processing

From Eq. (8.13) we see that we only need to prove security for output states of $\mathcal{P}_{\text{QKD}}$ partial on $\Omega_{\text{auth-hon}}$. We would like to reduce the analysis to output states of $\widetilde{\mathcal{P}}_{\text{QKD}}$ partial on $\Omega_{\text{auth-hon}}$. We will show in Lemma 8.3.2 (see also Fig. 8.3) that, conditioned on $\Omega_{\text{auth-hon}}$, the final real and ideal output states (at the end of $\mathcal{P}_{\text{QKD}}$) can be obtained by the action of $\mathcal{E}_{\text{update}} \circ \mathcal{E}_{\text{comm}} \circ \mathcal{E}^{\text{repl}}_{\text{auth}}$ on the real and ideal states at the end of the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. Using the fact that the one-norm is non-increasing under CPTP maps, we can thus instead focus on the distance between the real and ideal output states *before* the authentication post-processing. This distance will then be related to the usual security guarantee obtained under the assumption that authentication behaves honestly.

Lemma 8.3.2 (Commutation of $\mathcal{R}_{\text{ideal}}$ and AuthPP Protocol)**.** *Let $\Omega_{\text{auth-hon}}$ denote the event where neither Alice nor Bob received an* `auth-abort` *in $\boldsymbol{C}_{\mathbf{fin}}$ during the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. Let $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}}$ denote the real state at the end of the core QKD protocol conditioned on $\Omega_{\text{auth-hon}}$. Let the following states denote its evolution through AuthPP Protocol,*

$$\begin{aligned}
\rho^{\text{real,repl}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{E}^{\text{repl}}_{\text{auth}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{E}_{\text{comm}} \left[\rho^{\text{real,repl}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{E}_{\text{update}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right].
\end{aligned} \tag{8.16}$$

Define the corresponding ideal states by the action of the map $\mathcal{R}_{\text{ideal}}$ on the real states, i.e

$$\begin{aligned}
\rho^{\text{ideal}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{ideal,repl}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,repl}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{ideal,comm}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right].
\end{aligned} \tag{8.17}$$

Then, the ideal states defined above are the same as those obtained by evolving $\rho^{\text{ideal}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}}$ through the AuthPP Protocol, i.e,

$$\begin{aligned}
\rho^{\text{ideal,repl}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &= \mathcal{E}^{\text{repl}}_{\text{auth}} \left[\rho^{\text{ideal}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{ideal,comm}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &= \mathcal{E}_{\text{comm}} \left[\rho^{\text{ideal,repl}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right], \\
\rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} &= \mathcal{E}_{\text{update}} \left[\rho^{\text{ideal,comm}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}} \boldsymbol{E}_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right].
\end{aligned} \tag{8.18}$$

Note that this lemma also holds when conditioning on $\Omega^{\text{C}}_{\text{auth-hon}}$ instead of $\Omega_{\text{auth-hon}}$. However, the proof in that case is considerably more cumbersome, and we do not require it here. Recall that $\boldsymbol{C}'_{\mathbf{fin}} = \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{C}_{\mathbf{auth}}$.

Proof. The proof consists of some straightforward though fairly cumbersome algebra. We wish to show that the three vertical arrows on the right hand side of Fig. 8.3 are satisfied. We also note that none of the maps in $\mathcal{P}_{\text{APP}}$ ever affect the register $\boldsymbol{C}_{\mathbf{fin}}$ (they only read from the register), thus the event $\Omega_{\text{auth-hon}}$ can be defined at the start, and is "preserved" throughout the evolution of the real or ideal state.

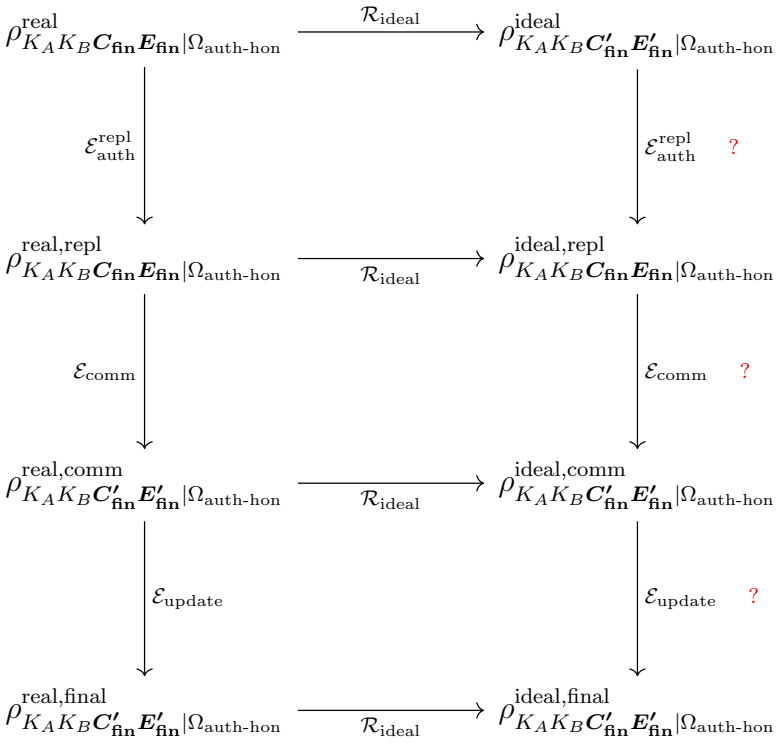


Figure 8.3: A diagram illustrating transformations between real and ideal states evolving through the AuthPP Protocol. The '?' indicates the transformations that must be shown to be true in Lemma 8.3.2. The states go through the map $\mathcal{E}^{\text{repl}}_{\text{auth}} \in \text{CPTP}(K_AK_B\boldsymbol{C}_{\mathbf{fin}}, K_AK_B\boldsymbol{C}_{\mathbf{fin}})$ that replaces the key registers depending on $\boldsymbol{C}_{\mathbf{fin}}$. They then go through some communication steps given by $\mathcal{E}_{\text{comm}} \in \text{CPTP}(K_AK_B\boldsymbol{E}_{\mathbf{fin}}, K_AK_B\boldsymbol{E}'_{\mathbf{fin}}\boldsymbol{C}_{\mathbf{auth}})$ (influenced by Eve). Finally, Alice and Bob perform the final updates to their key registers described by $\mathcal{E}_{\text{update}} \in \text{CPTP}(K_AK_B\boldsymbol{C}_{\mathbf{auth}}, K_AK_B\boldsymbol{C}_{\mathbf{auth}})$.

First arrow: For the first vertical arrow, we simply note that if $\Omega_{\text{auth-hon}}$ occurs, then the map $\mathcal{E}^{\text{repl}}_{\text{auth}}$ acts identically on the input state. Thus,

$$\mathcal{E}^{\text{repl}}_{\text{auth}} \circ \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}|\Omega_{\text{auth-hon}}}\right] = \mathcal{R}_{\text{ideal}} \circ \mathcal{E}^{\text{repl}}_{\text{auth}} \left[\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}|\Omega_{\text{auth-hon}}}\right] \tag{8.19}$$

is trivially satisfied.

Second arrow: For the second vertical arrow, we note that the $\mathcal{E}_{\text{comm}}$ first looks at the key lengths stored in Alice and Bob's registers, and then simply makes some announcements (and implements Eve's attacks). The $\mathcal{R}_{\text{ideal}}$ map also simply replaces the key registers based on the key lengths. Neither maps affects the key lengths stored in K_A, K_B. Let $\Pi^{l'_A,l'_B}_{K_AK_B} \in \text{CPTP}(K_AK_B, K_AK_B)$ denote the map that projects onto the subspace where the key registers store keys of lengths l'_A, l'_B. Then, since Alice and Bob's announcements only depend on the length of their key registers l'_A, l'_B, $\mathcal{E}_{\text{comm}}$ has the following structure:

$$\mathcal{E}_{\text{comm}} = \sum_{l'_A,l'_B} \Pi^{l'_A,l'_B}_{K_AK_B} \otimes \mathcal{E}^{(l'_A,l'_B)}_{\text{comm}}, \tag{8.20}$$

where $\mathcal{E}^{(l'_A,l'_B)}_{\text{comm}} \in \text{CPTP}(\boldsymbol{C_{\text{fin}}E_{\text{fin}}}, \boldsymbol{C_{\text{fin}}C_{\text{auth}}E'_{\text{fin}}})$ [6], and does not act on the K_AK_B registers. Moreover, the $\mathcal{R}_{\text{ideal}}$ map also has a similar structure (Eq. (8.6)), namely

$$\mathcal{R}_{\text{ideal}} = \bigoplus_{l'_A,l'_B} \mathcal{R}^{(l'_A,l'_B)}_{\text{ideal}}, \qquad \text{where } \mathcal{R}^{(l'_A,l'_B)}_{\text{ideal}} \in \text{CPTP}(K_A^{l'_A}K_B^{l'_B}, K_A^{l'_A}K_B^{l'_B}). \tag{8.21}$$

Then, we note that

$$\begin{aligned}
\mathcal{E}_{\text{comm}} \circ \mathcal{R}_{\text{ideal}} &= \sum_{l'_A,l'_B} \Pi^{l'_A,l'_B}_{K_AK_B} \circ \mathcal{R}^{(l'_A,l'_B)}_{\text{ideal}} \otimes \mathcal{E}^{(l'_A,l'_B)}_{\text{comm}} \\
&= \sum_{l'_A,l'_B} \mathcal{R}^{(l'_A,l'_B)}_{\text{ideal}} \circ \Pi^{l'_A,l'_B}_{K_AK_B} \otimes \mathcal{E}^{(l'_A,l'_B)}_{\text{comm}} \\
&= \mathcal{R}_{\text{ideal}} \circ \mathcal{E}_{\text{comm}},
\end{aligned} \tag{8.22}$$

where all the equalities follow from the definition of the maps. The required claim then follows from Eq. (8.22).

Third arrow: For the third vertical arrow, we use the fact that $\mathcal{E}_{\text{update}}$ simply reads from the $\boldsymbol{C_{\text{auth}}}$ register and performs operations on the K_A, K_B registers. Its operations depend on the values observed in the $\boldsymbol{C_{\text{auth}}}$ register. To proceed we will require some additional notation.

Let us use $\Omega^{\text{fin-dec}}_{(i,j)}$, where i, j can either be $\top$ or $\perp$ to denote the final accept or abort decisions (and communication) undertaken by Alice and Bob as follows:

[6] It actually leaves the $\boldsymbol{C_{\text{fin}}}$ register untouched.

- If $i = \top$, Alice does nothing in APP 5. This corresponds to Alice sending a final `accept` message in APP 4.
- If $i = \bot$, Alice replaces the key register with the $\bot$ value in APP 5. This corresponds to Alice sending a final `abort` message in APP 4.
- If $j = \top$, Bob does nothing in APP 6. This corresponds to him receiving an `accept` message from Alice in APP 3.
- If $j = \bot$, Bob replaces his key register $\bot$ in APP 6. This corresponds to him receiving either an `abort` or `auth-abort` message from Alice in APP 3.

The $\mathcal{R}_{\text{ideal}}$ map also performs operations on the $K_A K_B$ register, and its operations only depend on the lengths of the strings stored in K_A, K_B. Recall from Section 8.2.3 that we use l'_A, l'_B to denote these lengths before the update operation, and l_A, l_B to denote these lengths after the update operation.

Let us first consider the scenario where we first apply $\mathcal{E}_{\text{update}}$ and then $\mathcal{R}_{\text{ideal}}$. Thus, we will focus first on the state $\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C'_{\text{fin}}} \boldsymbol{E'_{\text{fin}}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B}}$. This state is a mixture of the following states which correspond to various final accept or abort decisions:

$$\begin{aligned}\Big\{ &\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C'_{\text{fin}}} \boldsymbol{E'_{\text{fin}}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B} \wedge \Omega^{\text{fin-dec}}_{(\top,\top)}}, \\ &\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C'_{\text{fin}}} \boldsymbol{E'_{\text{fin}}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B} \wedge \Omega^{\text{fin-dec}}_{(\bot,\bot)}}, \\ &\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C'_{\text{fin}}} \boldsymbol{E'_{\text{fin}}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B} \wedge \Omega^{\text{fin-dec}}_{(\top,\bot)}}, \\ &\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C'_{\text{fin}}} \boldsymbol{E'_{\text{fin}}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B} \wedge \Omega^{\text{fin-dec}}_{(\bot,\top)}} \Big\}.\end{aligned} \tag{8.23}$$

(Note that for the AuthPP Protocol considered in this chapter, we can never have the $\Omega^{\text{fin-dec}}_{(\bot,\top)}$ occur. However, we leave it in our analysis to enable this proof to be easily adapted to variations of AuthPP Protocol). From the actions of the update map (see APP 5 and APP 6), it is straightforward to verify that

$$\mathcal{E}_{\text{update}} \circ \mathcal{R}_{\text{ideal}}[\cdot] = \mathcal{R}_{\text{ideal}} \circ \mathcal{E}_{\text{update}}[\cdot] \qquad \text{where } \cdot \text{ is any state from Eq. (8.23).} \tag{8.24}$$

That is, the required commutation holds conditioned on any combination of final `accept`/`abort` outcomes. This implies

$$\mathcal{E}_{\text{update}} \circ \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B}} \right] = \mathcal{R}_{\text{ideal}} \circ \mathcal{E}_{\text{update}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}} \wedge \Omega_{l'_A, l'_B}} \right] \tag{8.25}$$

holds $\forall l'_A, l'_B$. Since the above equation holds for all values of the intermediate key lengths l'_A, l'_B, we have the required claim:

$$\mathcal{E}_{\text{update}} \circ \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right] = \mathcal{R}_{\text{ideal}} \circ \mathcal{E}_{\text{update}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega_{\text{auth-hon}}} \right]. \tag{8.26}$$

Thus, the stated Lemma follows from Eqs. (8.19), (8.22) and (8.26). This concludes the proof. □

This commuting property allows us to focus on the distance between the real and ideal states *before* AuthPP Protocol, rather than after. This can be formalized using the following corollary.

Corollary 8.3.1. *Let $\widetilde{\mathcal{P}}_{\text{QKD}}$, $\mathcal{P}_{\text{APP}}$, and $\mathcal{P}_{\text{QKD}}$ be protocols such that the overall QKD protocol is given by $\mathcal{P}_{\text{QKD}} = \mathcal{P}_{\text{APP}} \circ \widetilde{\mathcal{P}}_{\text{QKD}}$, where $\mathcal{P}_{\text{APP}}$ denotes a post-processing routine executed after the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. Assume that classical communication in the practical and honest setting behaves as specified in Section 8.2.1, and suppose that $\mathcal{P}_{\text{APP}}$ is as described in AuthPP Protocol. That is, consider the same setup as in Theorem 8.2.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial on the event $\Omega_{\text{auth-hon}}$, implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}})$. That is*

$$\begin{aligned} \frac{1}{2} \left\| \rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}} \right\|_1 &\leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\ &\Downarrow \\ \frac{1}{2} \left\| \rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \right\|_1 &\leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}}) \end{aligned} \tag{8.27}$$

Proof. For any output state $\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}})$ of the full QKD protocol, consider the corresponding state $\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ obtained at the end of the core QKD

protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. Then, we have

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\text{ideal,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}}\right\|_1 \\
&= \frac{1}{2}\left\|\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \\
&= \frac{1}{2}\left\|\mathcal{E}_{\text{update}}\circ\mathcal{E}_{\text{comm}}\circ\mathcal{E}^{\text{repl}}_{\text{auth}}\left[\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right]\right\|_1 \\
&\leq \frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1
\end{aligned} \tag{8.28}$$

where we use Lemma 8.3.1 for the first line, Lemma 8.3.2 for the second line, and the fact that the one-norm cannot increase under the action of CPTP maps for the final line. This suffices to prove the required claim. □

Thus, Corollary 8.3.1 allows us to restrict our attention to bounding

$$\frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \tag{8.29}$$

which is the distance between the real and ideal states after the core QKD protocol (partial on the event $\Omega_{\text{auth-hon}}$).

8.3.3 Reducing to scenario where authentication satisfies honest behaviour

The task now is to show that if the QKD protocol is analyzed under the assumption that authentication follows honest behaviour, then this analysis applies to output state (partial on $\Omega_{\text{auth-hon}}$) in the setting where authentication is not assumed to be honest. Under the communication model defined in Section 8.2.1, the event $\Omega_{\text{auth-hon}}$ coincides with the event that authentication behaved honestly. Indeed, any attempt to tamper with the contents of a message or violate the temporal ordering of messages triggers an `auth-abort` (i.e., $\Omega^{\text{C}}_{\text{auth-hon}}$). Thus, it is natural to relate the two scenarios.

While this may initially seem straightforward, making the connection formal is non-trivial. One might intuitively expect that conditioning on $\Omega_{\text{auth-hon}}$ should allow us to restrict attention to the honest-authentication setting. However, this naive reasoning fails upon realizing that the set of operations available to Eve in the real setting is strictly *larger*

than that in the honest authentication setting.[7] Consequently, the set of possible output states in the practical authentication setting $\mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ is strictly *larger* than the set of possible output states in the honest authentication setting $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ (even if we consider partial states on $\Omega_{\text{auth-hon}}$). To circumvent this problem, we introduce a *virtual authentication setting* (i.e, a new set of assumptions describing a virtual authentication scenario) which acts as a bridge that allows us to relate the two settings. This technical step is essential for our reduction argument that follows. Thus, the series of reductions that we build is (informally) described by:

$$\mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}}) \xrightarrow{\textit{Lemma 8.3.1}} \mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}})_{\wedge\Omega_{\text{auth-hon}}} \xrightarrow{\textit{Corollary 8.3.1}} \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})_{\wedge\Omega_{\text{auth-hon}}} \xrightarrow{\textit{Lemma 8.3.3}}$$
$$\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})_{\wedge\Omega_{\text{auth-hon}}} \xrightarrow{\textit{Lemma 8.3.4}} \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \xrightarrow{\textit{Lemma 8.3.5}} \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}), \tag{8.30}$$

where the set of output states in the virtual setting is denoted using $\mathcal{W}^{\text{virt}}$ and described shortly.

Describing the virtual authentication setting correct messages

In the virtual authentication setting, Eve still has the ability to implement any attack she wants on the classical channel; in particular, she controls the message timings $t^{(i)}_{E\to A}, t^{(i)}_{E\to B}$ and the contents of $C^{(i)}_{E\to A}, C^{(i)}_{E\to B}$. Thus, the set of possible operations she can do is *exactly the same* as in the practical authentication setting. However, the virtual setting is designed such that it is equivalent to the practical authentication setting whenever event $\Omega_{\text{auth-hon}}$ occurs, through the use of special registers $\widetilde{\boldsymbol{C}}$. The virtual authentication setting is described as follows:

1. Eve's attack results in the registers $\boldsymbol{C_{A\to E}}, \boldsymbol{C_{E\to A}}, \boldsymbol{C_{B\to E}}, \boldsymbol{C_{E\to B}}$ being sent and received in the exact same way as the practical authentication setting (see Section 8.2.1). As before, each party labels their outgoing (incoming) messages according to the order in which the messages are sent (received).

2. **Timing:** If the ith message is received *before* the ith message was sent, the receiving party gets the correct message in additional registers $\widetilde{\boldsymbol{C}}$, at some time after the

[7] For example, consider an operation in which Eve - perhaps probabilistically, or via a unitary interaction between her quantum side information and the classical signals - preemptively sends messages to one party in order to induce that party to advance to the next stage of the protocol earlier than intended. Such an operation is simply not *allowed* in the honest authentication setting, therefore the resulting output state cannot be identified in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$.

message was sent. Stated formally:

$$\begin{aligned} t^{(i)}_{A\to E} > t^{(i)}_{E\to B} \quad &\implies \text{Bob receives correct message in } \widetilde{C}^{(i)}_{E\to B} \text{ at time after } t^{(i)}_{A\to E}, \quad \forall i. \\ t^{(i)}_{B\to E} > t^{(i)}_{E\to A} \quad &\implies \text{Alice receives correct message in } \widetilde{C}^{(i)}_{E\to A} \text{ at time after } t^{(i)}_{B\to E}, \quad \forall i. \end{aligned} \tag{8.31}$$

3. **Modifying messages:** If ith message is received *after* the ith message was sent, then the receiving party gets the correct message in additional registers $\widetilde{\boldsymbol{C}}$, at the same time as the actual message is received. Stated formally:

$$\begin{aligned} t^{(i)}_{A\to E} \leq t^{(i)}_{E\to B} \quad &\implies \quad \text{Bob receives the correct message in } \widetilde{C}^{(i)}_{E\to B} \text{ at time } t^{(i)}_{E\to B}, \quad \forall i. \\ t^{(i)}_{B\to E} \leq t^{(i)}_{E\to A} \quad &\implies \quad \text{Alice receives the correct message in } \widetilde{C}^{(i)}_{E\to A} \text{ at time } t^{(i)}_{E\to A}, \quad \forall i. \end{aligned} \tag{8.32}$$

4. Alice and Bob use the registers $\widetilde{\boldsymbol{C}}_{\boldsymbol{E\to A}}, \widetilde{\boldsymbol{C}}_{\boldsymbol{E\to B}}$ for the received message, and implement decisions based on the correct copies they receive. They entirely ignore the messages received in $\boldsymbol{C}_{\boldsymbol{E\to A}}, \boldsymbol{C}_{\boldsymbol{E\to B}}$.

We use $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ to denote the set of output states that can be obtained in the virtual setting for the given protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. We will now prove a series of lemmas that reduce $\varepsilon^{\text{secure}}$-security statement we wish to prove (Eq. (8.29)) to $\varepsilon^{\text{secure}}$-security of all states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$. We remark that, strictly speaking, the protocols in the virtual setting differ slightly from those in the practical authentication setting, as they make use of distinct classical communication registers (the virtual setting uses the corresponding magic registers). However, since these registers are equivalent by construction, and Alice and Bob perform the same operations based on the received communication in both the practical and virtual authentication settings, we do not label these protocols differently across the two.

Reducing security statements

We first reduce the security analysis to states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial on $\Omega_{\text{auth-hon}}$.

Lemma 8.3.3. *Consider the same setup as in Theorem 8.2.1 and Corollary 8.3.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial on $\Omega_{\text{auth-hon}}$, implies $\varepsilon^{\text{secure}}$-*

security for all output states in $\mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ *partial on* $\Omega_{\text{auth-hon}}$*. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \Downarrow \\
&\frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})
\end{aligned} \tag{8.33}$$

Proof. Fix any attack by Eve, and consider the corresponding state $\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$:

$$\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}} = \rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} + \rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega^{\text{C}}_{\text{auth-hon}}}. \tag{8.34}$$

For the same attack, consider the corresponding state $\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ in the virtual setting:

$$\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} = \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} + \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega^{\text{C}}_{\text{auth-hon}}}. \tag{8.35}$$

Recall that the virtual setting is the one where the correct messages are received by both parties in the registers $\widetilde{\boldsymbol{C}}$, and Alice and Bob use these values in the protocol. In the event $\Omega_{\text{auth-hon}}$, the actual messages (received in $\boldsymbol{C}_{\mathbf{fin}}$) are exactly the same as the correct messages received in $\widetilde{\boldsymbol{C}}$, and are received at exactly the same time as the correct messages in $\widetilde{\boldsymbol{C}}$. Thus, these two registers are equivalent, and lead to Alice and Bob performing the same operations at all times (conditioned on the event $\Omega_{\text{auth-hon}}$). Thus, we have

$$\begin{aligned}
\text{Tr}_{\widetilde{\boldsymbol{C}}}\left[\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right] &= \rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} \\
\text{Tr}_{\widetilde{\boldsymbol{C}}}\left[\rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right] &= \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}
\end{aligned} \tag{8.36}$$

where the second equality follows from the first equality, and the fact that $\mathcal{R}_{\text{ideal}}$ does not act on $\widetilde{\boldsymbol{C}}$. With these two equalities, we obtain the desired claim by using the fact that the one-norm decreases under the action of CPTP maps, as follows:

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \\
&= \frac{1}{2}\left\|\text{Tr}_{\widetilde{\boldsymbol{C}}}\left[\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right]\right\|_1 \\
&\leq \frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1
\end{aligned} \tag{8.37}$$

The required claim follows from noting that the above inequality is true for all states $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$. In fact, the inequality above can actually be tightened to an equality, since $\widetilde{\boldsymbol{C}}$ is simply a copy of the messages in $\boldsymbol{C}_{\mathbf{fin}}$ (although the weaker inequality already suffices for our purposes).

□

The following lemma reduces the security analysis to states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ (without needing to consider partial states on event $\Omega_{\text{auth-hon}}$).

Lemma 8.3.4. *Consider the same setup as in Theorem 8.2.1 and Corollary 8.3.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$, implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\mathcal{P}_{\text{QKD}})$, subnormalized conditioned on the event $\Omega_{\text{auth-hon}}$. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad\qquad\qquad \Downarrow \\
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})
\end{aligned} \tag{8.38}$$

Proof. For any state $\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ we have

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}}\right\|_1 \\
&\leq \frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega_{\text{auth-hon}}}\right\|_1 \\
&+ \frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega^{\text{C}}_{\text{auth-hon}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}} \wedge \Omega^{\text{C}}_{\text{auth-hon}}}\right\|_1 \\
&= \frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1
\end{aligned} \tag{8.39}$$

where the first inequality follows from the fact that we add positive terms to the right hand side of the inequality, and the final equality follows from the fact that the states conditioned on $\Omega_{\text{auth-hon}}$ and $\Omega^{\text{C}}_{\text{auth-hon}}$ have support on orthogonal spaces. □

The following lemma reduces the security analysis to states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$.

Lemma 8.3.5. *Consider the same setup as in Theorem 8.2.1 and Corollary 8.3.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad\qquad\qquad \Downarrow \\
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})
\end{aligned} \tag{8.40}$$

The idea behind the proof is based on the intuition that, in the virtual setting, the registers $\widetilde{\boldsymbol{C}}$ capture the communication that would occur in the honest model, and Alice and Bob use these registers for determining their actions. Consequently, the actual received messages are irrelevant — in fact, we can even assume that they are never delivered.

Proof. Consider any state $\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$, and fix the corresponding attack strategy by Eve. From our construction of the virtual authentication setting, this implies that messages in $\widetilde{\boldsymbol{C}}$ are always correct and are received some time after being sent. Messages in $\boldsymbol{C}_{\mathbf{fin}}$ may include `auth-aborts` and timing irregularities, but they are not used by Alice or Bob in the protocol at all.

Next, consider the related attack strategy in the honest authentication setting, which we construct from the attack strategy in the virtual setting. Here Eve creates a copy of every message sent out from Alice's or Bob's laboratory. Each message is correctly delivered to the receiving party (according to the timing specified by $\widetilde{\boldsymbol{C}}$). Instead of attacking those messages, Eve performs her attack from the virtual setting on the *copy* of the messages sent out, and does not forward the resulting (potentially tampered message) to the receiving party (see Fig. 8.4). Let the resulting state be $\rho^{\text{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$. Then, we have the following equality with a slight abuse of notation:

$$\rho^{\text{real,virt}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \widetilde{\boldsymbol{C}} \boldsymbol{E}_{\mathbf{fin}}} = \rho^{\text{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}, \tag{8.41}$$

where $\boldsymbol{C}_{\mathbf{fin}}$ and $\boldsymbol{E}_{\mathbf{fin}}$ on the left-hand side (which store the outcome of Eve's attack) are identified with $\boldsymbol{E}_{\mathbf{fin}}$ on the right-hand side (where Eve implements the same attack on a copy of the classical messages and does not forward the resulting message to Bob), and $\widetilde{\boldsymbol{C}}$ on the left-hand side (which contains the correctly delivered, correctly timed messages) is identified with $\boldsymbol{C}_{\mathbf{fin}}$ on the right-hand side (the honest setting, where correct messages are received at the correct times).

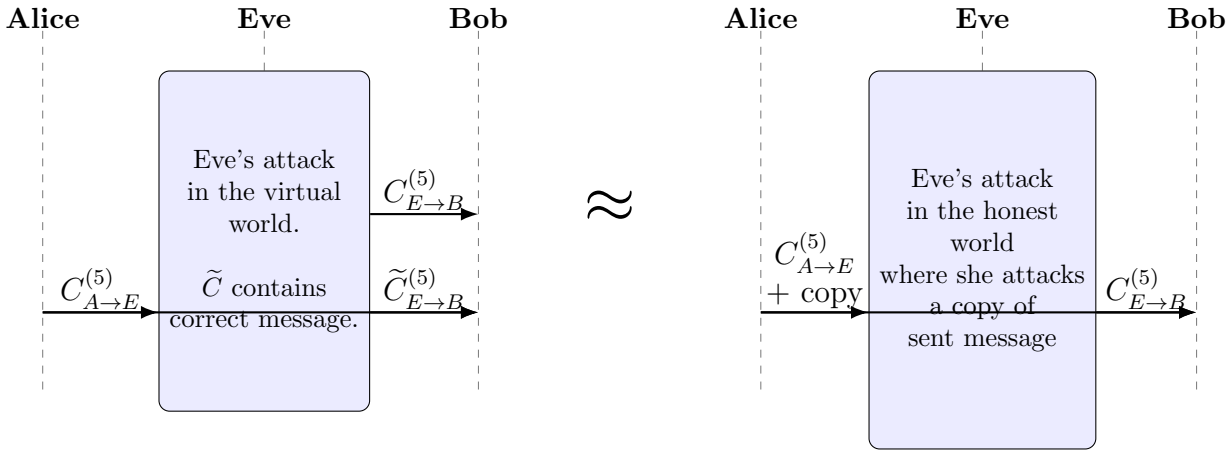


Figure 8.4: For every operation that Eve performs in the virtual authentication setting, one can construct an equivalent operation in the honest authentication setting, where Eve creates a copy of each sent message and performs her original operation on this copy. She does not forward the result of her attack on the copy to the receiver; instead, she forwards the original, unmodified message to the receiving party.

From these properties, we have

$$\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\text{fin}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\text{fin}}}\right\|_1 = \frac{1}{2}\left\|\rho^{\text{real,hon}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\boldsymbol{E}_{\text{fin}}} - \rho^{\text{ideal,hon}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\boldsymbol{E}_{\text{fin}}}\right\|_1. \tag{8.42}$$

This proves the required statement: if the right-hand side is upper bounded by $\varepsilon^{\text{secure}}$ for all states $\rho^{\text{real,hon}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\boldsymbol{E}_{\text{fin}}} \in \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$, then the same bound holds for the left-hand side for all states $\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\text{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$. This concludes the proof. □

Thus, combining all these reductions, we obtain the required statement which we restate below:

Theorem 8.2.1 (Reduction of QKD security analysis to the honest authentication setting)**.** *Let $\widetilde{\mathcal{P}}_{\text{QKD}}$ be an arbitrary QKD protocol. Let $\mathcal{P}_{\text{APP}}$ be the AuthPP Protocol described in Section 8.2.3, executed after the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. Let $\mathcal{P}_{\text{QKD}} = \mathcal{P}_{\text{APP}} \circ \widetilde{\mathcal{P}}_{\text{QKD}}$ denote the resulting QKD protocol. Let $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ denote the set of possible output states of $\widetilde{\mathcal{P}}_{\text{QKD}}$ in the honest authentication setting (see Section 8.2.1). Let $\mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}})$ denote the set of possible output states of $\mathcal{P}_{\text{QKD}}$ in the practical authentication setting (see Section 8.2.1). Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ implies*

$\varepsilon^{\text{secure}}$-*security for all output states*[8] *in* $\mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}})$. *That is,*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,hon}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\boldsymbol{E}_{\text{fin}}} - \rho^{\text{ideal,hon}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\boldsymbol{E}_{\text{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,hon}}_{K_AK_B\boldsymbol{C}_{\text{fin}}\boldsymbol{E}_{\text{fin}}} \in \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad\qquad\qquad \Downarrow \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (8.12) \\
&\frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}'_{\text{fin}}\boldsymbol{E}'_{\text{fin}}} - \rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}'_{\text{fin}}\boldsymbol{E}'_{\text{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real}}_{K_AK_B\boldsymbol{C}'_{\text{fin}}\boldsymbol{E}'_{\text{fin}}} \in \mathcal{W}^{\text{real}}_{\text{auth}}(\mathcal{P}_{\text{QKD}}).
\end{aligned}$$

Proof. The proof follows from Corollary 8.3.1 and Lemmas 8.3.3 to 8.3.5. □

8.4 Delayed Authentication

The protocols considered so far utilize an authenticated classical channel for every message sent and received, as described in Section 8.2.1. However, the number of bits required to authenticate an n-bit message with information-theoretic security increases with n (albeit only logarithmically) [161, 151]. Consequently, it is more efficient (in terms of authentication key consumption) to batch multiple messages together before authenticating them.

In this section, we consider a modified version of the previously studied scenario, in which the authenticated classical channel is used only twice - once by each party - to authenticate the entire transcript of classical communication. For this section, we assume that Alice and Bob have synchronized clocks. We emphasize that this assumption is made only for this section and is necessary to ensure that Alice and Bob can compare transcripts along with their associated timestamps. We again let $\widetilde{\mathcal{P}}_{\text{QKD}}$ denote a generic QKD protocol. However, we now analyze the security of a setting where all communication during $\widetilde{\mathcal{P}}_{\text{QKD}}$ takes place over an insecure, unauthenticated classical channel. In this case, Eve is free to replace any message or arbitrarily modify its timing, and the delivery restrictions described in Section 8.2.1 no longer apply.

We then introduce a delayed Authentication Post-Processing Protocol, denoted by $\mathcal{P}^{\text{del}}_{\text{APP}}$, described in Section 8.4.1. In this step, Alice and Bob exchange their entire communication transcripts (along with timestamps) over an authenticated channel and verify their consistency. The restrictions described in Section 8.2.1 apply to these messages.

[8] Note that any scenario in which Eve chooses to ignore or forget part of the public classical communication can be treated as one where she first records all communication and then traces out whatever she wishes at the end of the QKD protocol. Moreover, since QKD security analysis already allows Eve to retain all public communication, keeping the public communication register explicit and accessible to her is without loss of generality.

If the transcripts match[9] - i.e., if they confirm that they received the correct messages at the appropriate times - they proceed; otherwise, they abort the protocol.

With these modifications, we are able to establish an analogue of Theorem 8.2.1, stated in Theorem 8.4.1. The proof follows via analogous steps to that of Theorem 8.2.1. We note that the idea of delayed authentication has been explored in the context of QKD in several prior works [163, 162]. However, these studies typically focus on estimating authentication costs or perform the security analysis only for specific QKD protocols.

For ease of explanation and to maintain intuitive correspondence with earlier sections, we make a slight abuse of notation in this section. In particular, the real output states are denoted using the same symbols as before ($\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\text{fin}} \boldsymbol{E}_{\text{fin}}}$), but they now correspond to a different setting $\mathcal{W}^{\text{real}}_{\text{del-auth}}(\mathcal{P}_{\text{QKD}})$ (described in greater detail in the following subsections). The honest and virtual settings, however, are defined exactly as before.

8.4.1 Delayed Authentication Post-Processing Protocol (del-APP)

As before, let $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\text{fin}} \boldsymbol{E}_{\text{fin}}}$ denote the final state obtained after the execution of the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$, where $\boldsymbol{C}_{\text{fin}} = \boldsymbol{C}_{\boldsymbol{A}\to\boldsymbol{E}} \boldsymbol{C}_{\boldsymbol{E}\to\boldsymbol{B}} \boldsymbol{C}_{\boldsymbol{B}\to\boldsymbol{E}} \boldsymbol{C}_{\boldsymbol{E}\to\boldsymbol{A}}$ collects all classical communication that occurred during the core protocol, and $\boldsymbol{E}_{\text{fin}}$ denotes all of Eve's side information, which may include a copy of the classical communication. Recall our notation: Alice sends (receives) her ith message in the register $C^{(i)}_{A\to E}$ ($C^{(i)}_{E\to A}$) at time $t^{(i)}_{A\to E}$ ($t^{(i)}_{E\to A}$) with Bob's messages and timings defined analogously. During the authentication post-processing phase, Alice and Bob start with the state $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\text{fin}} \boldsymbol{E}_{\text{fin}}}$ and perform the following actions (see Fig. 8.5).

Protocol 6 (del-AuthPP Protocol)**.** Starts with the state $\rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\text{fin}} \boldsymbol{E}_{\text{fin}}}$. Classical communication is undertaken in the registers $\boldsymbol{C}^{\text{auth}}_{\boldsymbol{A}\to\boldsymbol{E}}, \boldsymbol{C}^{\text{auth}}_{\boldsymbol{E}\to\boldsymbol{B}}, \boldsymbol{C}^{\text{auth}}_{\boldsymbol{B}\to\boldsymbol{E}}, \boldsymbol{C}^{\text{auth}}_{\boldsymbol{E}\to\boldsymbol{A}}$.

dAPP 1 Alice prepares a transcript $\mathcal{T}_A$ describing the messages she sent and received during $\widetilde{\mathcal{P}}_{\text{QKD}}$, and their timings. That is, she prepares

$$\mathcal{T}_A = \left(\left\{ \left(C^{(i)}_{A\to E}, t^{(i)}_{A\to E} \right) \right\}_i, \left\{ \left(C^{(j)}_{E\to A}, t^{(j)}_{E\to A} \right) \right\}_j \right).$$

She sends $\mathcal{T}_A$ to Bob by making one use of the authenticated classical channel.

[9] They don't need to match literally, since the time stamps will be different. But the messages need to match, and the timings must satisfy certain time-ordering.

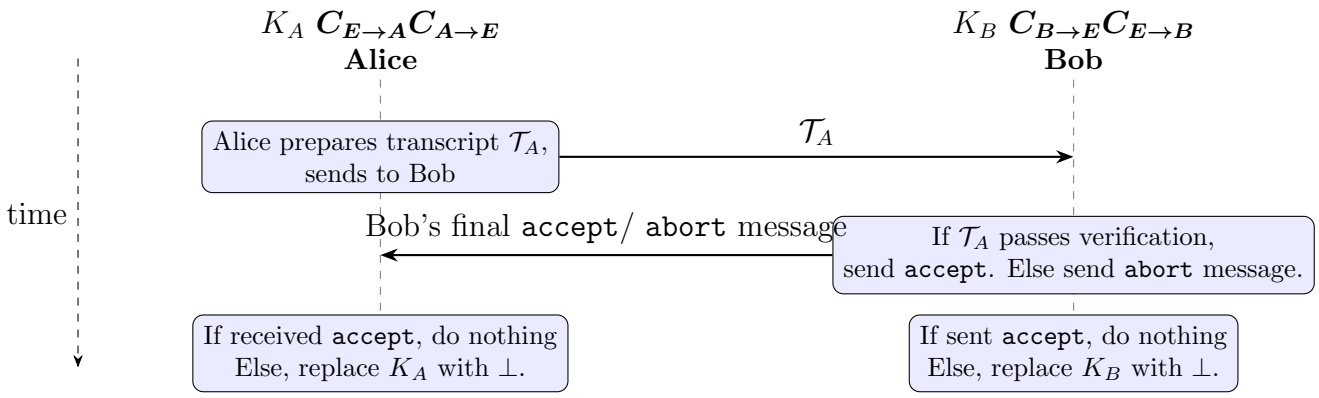


Figure 8.5: Schematic of del-AuthPP Protocol described in Section 8.4.1. Alice and Bob first communicate and verify transcripts. If transcripts matches, they accept the protocol. Else, they abort the protocol and replace their key registers with $\perp$s.

dAPP 2 If Bob receives an `auth-abort`, he sends an `abort` message to Alice. Otherwise, he checks whether the received transcript matches his own. That is, he verifies that messages were received after they were sent, and that the message contents matched. Formally he checks whether:

$$\begin{aligned} t^{(i)}_{A\to E} &\leq t^{(i)}_{E\to B} && \forall i, \\ t^{(i)}_{B\to E} &\leq t^{(i)}_{E\to A} && \forall i, \\ C^{(i)}_{A\to E} \text{ and } C^{(i)}_{E\to B} &\text{ contain identical messages} && \forall i, \\ C^{(i)}_{E\to A} \text{ and } C^{(i)}_{B\to E} &\text{ contain identical messages} && \forall i. \end{aligned} \tag{8.43}$$

If verification passes, he sends an `accept` message; otherwise, he sends an `abort` message.

dAPP 3 If Bob sends an `accept` message, he does nothing. If he sends an `abort` message, he replaces K_B with $\perp$. We denote by l_B the final key length stored in K_B.

dAPP 4 If Alice receives an `accept` message, she does nothing. If Alice receives either an `auth-abort` or an `abort` message, she replaces her key register K_A with $\perp$. We denote by l_A the final key length stored in K_A.

Mathematically, the above protocols can be described as follows:

1. In dAPP 1 and dAPP 2, Alice and Bob engage in two rounds of communication. This can be described by a map (influenced by Eve) $\mathcal{E}^{\text{del}}_{\text{comm}} \in \text{CPTP}(\boldsymbol{C_{\text{fin}}E_{\text{fin}}}, \boldsymbol{C'_{\text{fin}}E'_{\text{fin}}})$.

2. In dAPP 3 and dAPP 4, Alice and Bob use the result of the communication in the previous step $\boldsymbol{C_{\text{auth}}}$ to determine their final `accept` / `abort` status. This is described as a map $\mathcal{E}^{\text{del}}_{\text{update}} \in \text{CPTP}(K_A K_B \boldsymbol{C_{\text{auth}}}, K_A K_B \boldsymbol{C_{\text{auth}}})$

The final output state is denoted by $\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C'_{\text{fin}}E'_{\text{fin}}}} = \mathcal{E}^{\text{del}}_{\text{update}} \circ \mathcal{E}^{\text{del}}_{\text{comm}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{C_{\text{fin}}E_{\text{fin}}}}\right]$, where $\boldsymbol{C'_{\text{fin}}} = \boldsymbol{C_{\text{fin}}C_{\text{auth}}}$.

Notice that the structure of this protocol closely mirrors that of AuthPP Protocol, except that the first two steps of AuthPP Protocol are omitted here. This alignment ensures that the ensuing proofs proceed in essentially the same way.

Remark 8.4.1. *Notice that in this setting, there are only two uses of the authenticated classical channel. Consequently, the amount of secret key required for authentication is significantly lower than what was considered previously in this work. However, Alice and Bob must now store all messages sent and received (along with their corresponding timestamps) until the very end of the protocol, in order to compare and match their transcripts. This, in turn, reduces the benefits of on-the-fly announcements [7, Remark 3.1], which allow Alice and Bob to perform public announcements on-the-fly and save classical memory and storage requirements. Nevertheless, one can still envision a use case where on-the-fly announcements are performed along with delayed authentication to enable Alice and Bob to begin their classical processing (such as sifting) earlier, while still retaining the necessary information in memory for transcript comparison at a later stage. Alternatively, one can accept the requirement for larger classical memory (and not implement on-the-fly announcements), in order to save authentication keys. Finally, note that Alice and Bob need only store sufficient information to recover the ordering of all messages; the precise timestamps are not necessary. This can simplify the storage requirements further.*

8.4.2 Reduction Statement

We are interested in the security analysis of $\mathcal{P}^{\text{del}}_{\text{QKD}} = \mathcal{P}^{\text{del}}_{\text{APP}} \circ \widetilde{\mathcal{P}}_{\text{QKD}}$. Let us denote the set of output states that are possible when we use insecure, unauthenticated communication during $\widetilde{\mathcal{P}}_{\text{QKD}}$ and authenticated communication during $\mathcal{P}^{\text{del}}_{\text{APP}}$ as $\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\mathcal{P}^{\text{del}}_{\text{QKD}})$. The analogous result to Theorem 8.2.1 for the delayed authentication setting can now be stated and proved in an analogous manner.

Theorem 8.4.1 (Reduction of QKD security analysis to the honest authentication setting with delayed authentication)**.** *Let $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$ be an arbitrary QKD protocol. Let $\mathcal{P}^{\mathrm{del}}_{\mathrm{APP}}$ be the del-AuthPP Protocol described in Section 8.4.1, executed after the core QKD protocol $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$. Let $\mathcal{P}^{\mathrm{del}}_{\mathrm{QKD}} = \mathcal{P}^{\mathrm{del}}_{\mathrm{APP}} \circ \widetilde{\mathcal{P}}_{\mathrm{QKD}}$ denote the resulting QKD protocol. Let $\mathcal{W}^{\mathrm{real}}_{\mathrm{del-auth}}(\mathcal{P}_{\mathrm{QKD}})$ denote the set of output states in the delayed authentication setting, where communication during $\widetilde{\mathcal{P}}_{\mathrm{QKD}}$ is not authenticated while communication during $\mathcal{P}^{\mathrm{del}}_{\mathrm{APP}}$ is authenticated (see Section 8.2.1). Let $\mathcal{W}^{\mathrm{hon}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}})$ denote the set of output states in the honest authentication setting (see Section 8.2.1). Then, the $\varepsilon^{\mathrm{secure}}$-security for all output states in $\mathcal{W}^{\mathrm{hon}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}})$ implies $\varepsilon^{\mathrm{secure}}$-security for all output states in $\mathcal{W}^{\mathrm{real}}_{\mathrm{del-auth}}(\mathcal{P}^{\mathrm{del}}_{\mathrm{QKD}})$. That is,*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\mathrm{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\mathrm{ideal,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\mathrm{secure}} \qquad \forall \rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\mathrm{hon}}_{\mathrm{auth}}(\widetilde{\mathcal{P}}_{\mathrm{QKD}}) \\
&\qquad\qquad\qquad\qquad \Downarrow \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (8.44) \\
&\frac{1}{2}\left\|\rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\mathrm{ideal}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\mathrm{secure}} \qquad \forall \rho^{\mathrm{real}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \in \mathcal{W}^{\mathrm{real}}_{\mathrm{del-auth}}(\mathcal{P}^{\mathrm{del}}_{\mathrm{QKD}}).
\end{aligned}$$

The proof is stated in Chapter D.

8.5 Summary and Outlook

In this chapter, we addressed the problem of analyzing QKD protocols in the practical authentication setting, where authentication may result in asymmetric aborts and message timing can be modified. This setting necessitates a modification of the standard QKD security definition and, crucially, renders nearly all existing analyses, which are undertaken in the honest authentication setting, invalid under practical authentication assumptions.

By introducing an authentication post-processing protocol, we demonstrated that the security of a complete QKD protocol (including the authentication post-processing) in the practical authentication setting can be reduced to that of the core QKD protocol in the honest authentication setting. The latter is the setting overwhelmingly considered in existing QKD security proofs. Hence, our results retroactively lift the security of such prior analyses to the practical authentication setting. Moreover, our construction is fully general—it applies to any QKD protocol and is equally suitable for device-dependent, measurement-device-independent[10] (MDI), and device-independent (DI) protocols, whether of the prepare-and-measure or entanglement-based type. We also presented two variants of

[10]Such protocols also involve public announcements made by an untrusted third party. We emphasize that our analysis applies only to the communication between Alice and Bob themselves; it does not address

this construction: one in which all communication is authenticated, and another where only the final two messages are authenticated, thereby reducing the consumption of authentication keys.

In this chapter, our perspective was that Eve's attack together with the protocol description jointly determine a single channel mapping input states to output states. Looking ahead, an important next step is to formalize the new security definition and the practical authenticated channel within a composable security framework. Achieving this will likely require employing models such as causal boxes [164] or related formalisms that explicitly capture the causal and temporal structure of classical communication.

how to handle announcements originating from an external third party. Typically in MDI protocols, Alice and Bob need to achieve consensus on the third party's announcements — while our result does not directly address those announcements, it does show that Alice and Bob can rely on the honest-authentication scenario for communication between themselves, in order to achieve such consensus.

Chapter 9

Summary and Outlook

As promised in Chapter 1, this thesis set out to present *rigorous* security proofs for *practical* quantum key distribution protocols using a *variety* of proof techniques.

We encountered fully rigorous security proofs, most notably in Chapter 7, where we proved the security of a highly general QKD protocol with a strong emphasis on precision, explicit assumptions, and mathematical clarity. We also explored a wide range of proof techniques, including IID collective attack analyses (Chapter 4), postselection based uplifts to coherent attacks (Chapter 5), entropic uncertainty relations (Chapter 6), and MEAT-based methods (Chapter 7). In every case, the analysis was applied to one of the most practically relevant QKD protocols: decoy-state BB84.

Beyond serving as a unifying exposition of major proof techniques, this thesis makes several concrete contributions to the security analysis of QKD. In particular, Chapter 5 revamps the postselection technique introduced in Ref. [36], placing it on a more rigorous mathematical footing and ensuring its applicability to realistic optical implementations of QKD. In Chapter 4, we developed a security proof for variable-length QKD protocols, filling a gap in the existing literature. In Chapter 6, we resolved a nearly two decades old open problem concerning basis-efficiency mismatch in phase error based security proofs, thereby allowing these methods to be applied to practical prepare-and-measure scenarios. This has now been extended to address additional scenarios, such as passive setups and correlated imperfections [83], and combined with analyses of source imperfections [80]. In Chapter 7, we presented a remarkably general and modular security analysis of practical QKD protocols using MEAT. Our analysis there can be straightforwardly applied to other QKD protocols beyond decoy-state BB84, and can be extended to include device imperfections and side-channel attacks as well. Therefore, it is meant to serve as the foundation for certification

efforts for QKD. Finally, in Chapter 8, we looked at some standard (unrealistic) assumptions commonly made about authentication in typical QKD security proofs, and showed that these assumptions can be relaxed to realistic ones with a minor protocol modification.

Comparing proof techniques: At this point, a natural question arises: which proof technique is best?

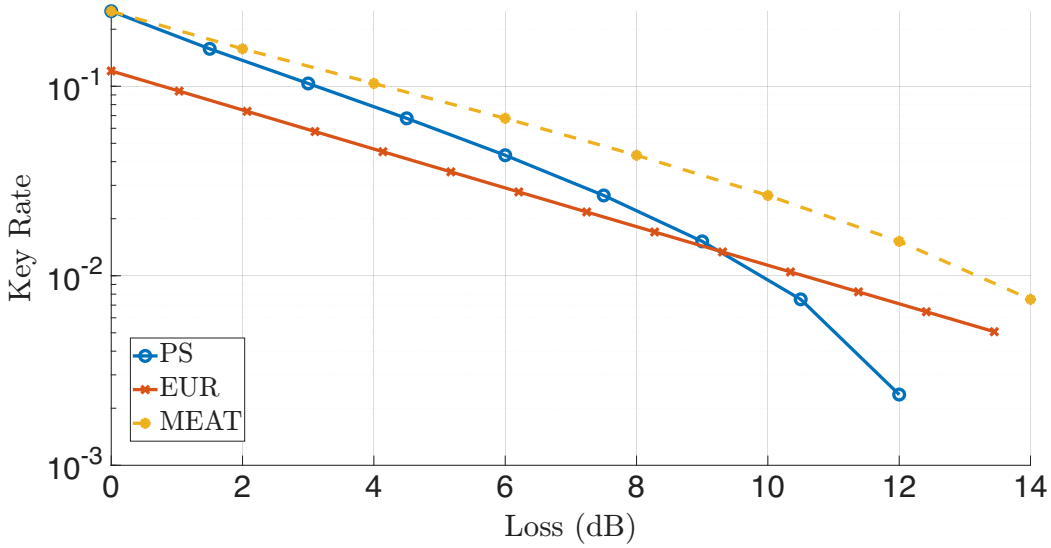


Figure 9.1: Key rate for the variable-length decoy-state BB84 protocol plotted as a function of loss, comparing the different proof techniques presented in this thesis. Note that the protocols are not strictly identical across techniques, due to differences inherent to the respective proof methods. For MEAT, the protocol is as described in Section 7.5. The PS protocol is identical to the MEAT protocol, except that it does not allow on-the-fly announcements. For EUR, the protocol follows Section 6.6. Such comparison plots, over a wider range of parameters, were first presented in Refs. [12, 9]; the present figure is generated using code based on Ref. [9] (MEAT), Ref. [2] (EUR) and Ref. [6] (PS), which we duly acknowledge. In particular, Refs. [12, 9] should be cited for all results pertaining to the numerical comparison of key rates between these proof techniques.

In earlier chapters, we highlighted significant drawbacks of both postselection-based and phase error rate-based approaches. In particular, the postselection technique appears fundamentally difficult to extend to scenarios involving on-the-fly announcements and correlated imperfections. Phase error-based methods, on the other hand, suffer from a notable lack of modularity. (See also [7, Section 7] for a comparison between proof

techniques). In the opinion of this author, MEAT does not suffer from comparably fundamental limitations, and is the "correct" way to approach the security analysis of QKD protocols. Moreover, MEAT yields competitive key rates [9], (see Fig. 9.1). That said, MEAT is a relatively recent development and has not yet been explored to the same depth as more established techniques. Nevertheless, this author remain confident that it represents, overall, the most robust and conceptually apt approach to QKD security proofs currently available.

Future work: While this thesis presents one highly rigorous security analysis for a practical protocol, it does not currently accommodate device imperfections into that analysis. The next major challenge in QKD lies in the systematic integration of imperfections and side-channel attacks into security analyses, with the aim of producing security proofs that apply directly to implemented systems. While many isolated results addressing individual imperfections exist—and while recent work has begun to combine several of these effects—a complete and unified treatment of all relevant imperfections and side channels for a given physical setup remains a formidable open problem. It is my hope that the methods developed in this thesis, and in particular those presented in Chapter 7, will serve as a foundation for future efforts to further close the gap between theoretical security proofs and real-world QKD systems.

Thank you for reading this thesis. Should you notice any shortcomings, I hope you can find solace in the following universal truth:

> Papers and theses are never finished, only abandoned.
>
> Norbert Lütkenhaus (original source unknown)

References

[1] Devashish Tupkary, Ernest Y.-Z. Tan, and Norbert Lütkenhaus. Security proof for variable-length quantum key distribution. *Physical Review Research*, 6(2):023002, April 2024. doi:10.1103/PhysRevResearch.6.023002.

[2] Devashish Tupkary, Shlok Nahar, Pulkit Sinha, and Norbert Lütkenhaus. Phase error rate estimation in QKD with imperfect detectors. *Quantum*, 9:1937, December 2025. doi:10.22331/q-2025-12-11-1937.

[3] Devashish Tupkary, Shlok Nahar, Amir Arqand, Ernest Y. Z. Tan, and Norbert Lütkenhaus. A rigorous and complete security proof of decoy-state BB84 quantum key distribution, 2026. URL: https://arxiv.org/abs/2601.18035, arXiv:2601.18035.

[4] Devashish Tupkary, Shlok Nahar, and Ernest Y. Z. Tan. Authentication in security proofs for quantum key distribution, 2026. URL: https://arxiv.org/abs/2601.17960, arXiv:2601.17960.

[5] Shlok Nahar, Devashish Tupkary, Yuming Zhao, Norbert Lütkenhaus, and Ernest Y.-Z. Tan. Postselection Technique for Optical Quantum Key Distribution with Improved de Finetti Reductions. *PRX Quantum*, 5(4):040315, October 2024. doi:10.1103/PRXQuantum.5.040315.

[6] Lars Kamin, Devashish Tupkary, and Norbert Lütkenhaus. Improved finite-size effects in quantum key distribution with applications to decoy-state protocols. *Phys. Rev. Res.*, 8:013332, Mar 2026. URL: https://link.aps.org/doi/10.1103/48xf-my6t, doi:10.1103/48xf-my6t.

[7] Devashish Tupkary, Ernest Y. Z. Tan, Shlok Nahar, Lars Kamin, and Norbert Lütkenhaus. Qkd security proofs for decoy-state bb84: protocol variations, proof techniques, gaps and limitations, 2025. URL: https://arxiv.org/abs/2502.10340, arXiv:2502.10340.

[8] John Burniston, Wenyuan Wang, Lars Kamin, Jie Lin, Patrick Coles, Eric Metodiev, Ian George, Nicky Kai Hong Li, Kun Fang, Max Chemtov, Yanbao Zhang, Christopher Böhm, Adam Winick, Thomas van Himbeeck, Scott Johnstun, Shlok Nahar, Devashish Tupkary, Shihong Pan, Zhiyao Wang, Aodhan Corrigan, Florian Kanitschar, Laura Gracie, Shouzhen Gu, Natansh Mathur, Twesh Upadhyaya, and Norbert Lutkenhaus. Open QKD Security: Version 2.1.0, December 2024. doi:10.5281/zenodo.14262569.

[9] Lars Kamin, John Burniston, and Ernest Y.-Z. Tan. Rényi security framework against coherent attacks applied to decoy-state QKD, April 2025. arXiv:2504.12248 [quant-ph]. URL: http://arxiv.org/abs/2504.12248, doi:10.48550/arXiv.2504.12248.

[10] Norbert Lütkenhaus. Lecture notes on QKD.

[11] Amir Arqand and Ernest Y. Z. Tan. Marginal-constrained entropy accumulation theorem, 2025. URL: https://arxiv.org/abs/2502.02563, arXiv:2502.02563.

[12] Lars Kamin. *From Asymptotic to Finite-Size Security in Decoy-State Quantum Key Distribution*. PhD thesis, University of Waterloo, 2026. URL: https://uwspace.uwaterloo.ca/items/48bd4a40-69d8-4342-bfcc-50fc5d0b67ca.

[13] Red Hat. A brief history of cryptography, 2023. [Accessed 25-12-2025]. URL: https://www.redhat.com/en/blog/brief-history-cryptography.

[14] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949. doi:10.1002/j.1538-7305.1949.tb00928.x.

[15] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi:10.1109/TIT.1976.1055638.

[16] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978. doi:10.1145/359340.359342.

[17] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman Te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul Leyland, Joël Marchand, François Morain, Alec Muffett, Chris Putnam, Craig Putnam, and Paul Zimmermann. Factorization of a 512-bit rsa modulus. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'00, page 1–18, Berlin, Heidelberg, 2000. Springer-Verlag. URL: https://doi.org/10.1007/3-540-45539-6_1.

[18] National Institute of Standards and Technology. Advanced encryption standard (aes). Technical Report FIPS PUB 197, National Institute of Standards and Technology, Washington, DC, 2001. Accessed: 2026-04-07. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[19] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. URL: http://dx.doi.org/10.1137/S0097539795293172, doi:10.1137/s0097539795293172.

[20] National Institute of Standards and Technology. Nist releases first 3 finalized post-quantum encryption standards, 2024. [Accessed 25-12-2025]. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[21] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 560, pages 175–179, Bangalore, India, 1984. IEEE. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025, doi:10.1016/j.tcs.2014.05.025.

[22] Renato Renner and Ramona Wolf. The debate over qkd: A rebuttal to the nsa's objections, 2023. URL: https://arxiv.org/abs/2307.15116, arXiv:2307.15116.

[23] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. *The Case for Quantum Key Distribution*, page 283–296. Springer Berlin Heidelberg, 2010. URL: http://dx.doi.org/10.1007/978-3-642-11731-2_35, doi:10.1007/978-3-642-11731-2_35.

[24] ANSSI, BSI, NLNCSA, Swedish National Communications Security Authority, and Swedish Armed Forces. Position paper on quantum key distribution. Technical report, ANSSI, BSI, NLNCSA, Swedish NCSA, January 2024. [Accessed 07-04-2026]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf.

[25] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, September 2017. URL: http://dx.doi.org/10.1038/nature23461, doi:10.1038/nature23461.

[26] National Security Agency. Quantum key distribution (qkd) and quantum cryptography (qc), 2023. [Accessed 25-12-2025]. URL: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[27] European Telecommunications Standards Institute (ETSI). Post quantum computing impact on ict systems; recommendations on business continuity and algorithm selection. ETSI EG 203 310 V1.0.0 (Final draft) EG 203 310, ETSI, Apr 2016. Guide (CYBER); Post Quantum Computing Impact on ICT Systems. URL: https://www.etsi.org/deliver/etsi_eg/203300_203399/203310/01.00.00_50/eg_203310v010000m.pdf.

[28] Lawrence M. Ioannou and Michele Mosca. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 255–274, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. doi:10.1007/978-3-642-25405-5_17.

[29] Dominique Unruh. Everlasting multi-party computation. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, pages 380–397, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. doi:10.1007/978-3-642-40084-1_22.

[30] Michele Mosca, Douglas Stebila, and Berkant Ustaoğlu. Quantum key distribution in the classical authenticated key exchange framework. In Philippe Gaborit, editor, *Post-Quantum Cryptography*, pages 136–154, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. doi:10.1007/978-3-642-38616-9_9.

[31] Michele Mosca and Marco Piani. Quantum Threat Timeline Report 2024 - Global Risk Institute — globalriskinstitute.org. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/, 2024. [Accessed 20-12-2025].

[32] Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.*, 95:045006, Dec 2023. URL: https://link.aps.org/doi/10.1103/RevModPhys.95.045006, doi:10.1103/RevModPhys.95.045006.

[33] Akihiro Mizutani, Toshihiko Sasaki, and Go Kato. Protocol-level description and self-contained security proof of decoy-state BB84 QKD protocol, 2025. URL: https://arxiv.org/abs/2504.20417, arXiv:2504.20417.

[34] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, July 2017. doi:10.22331/q-2017-07-14-14.

[35] Toyohiro Tsurumaru. Leftover Hashing From Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution. *IEEE*

Transactions on Information Theory, 66(6):3465–3484, June 2020. doi:10.1109/TIT.2020.2969656.

[36] Matthias Christandl, Robert König, and Renato Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Physical Review Letters*, 102(2):020504, January 2009. doi:10.1103/PhysRevLett.102.020504.

[37] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, USA, 1st edition, 2018. URL: https://cs.uwaterloo.ca/~watrous/TQI/.

[38] Marco Tomamichel. *Quantum Information Processing with Finite Resources*, volume 5 of *SpringerBriefs in Mathematical Physics*. Springer International Publishing, Cham, 2016. doi:10.1007/978-3-319-21891-5.

[39] C.A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, May 1999. URL: http://dx.doi.org/10.1109/18.761271, doi:10.1109/18.761271.

[40] Frédéric Dupuis. Privacy Amplification and Decoupling Without Smoothing. *IEEE Transactions on Information Theory*, 69(12):7784–7792, December 2023. doi:10.1109/TIT.2023.3301812.

[41] Frédéric Dupuis, Omar Fawzi, and Renato Renner. Entropy Accumulation. *Communications in Mathematical Physics*, 379(3):867–913, November 2020. doi:10.1007/s00220-020-03839-5.

[42] Rupert L. Frank and Elliott H. Lieb. Monotonicity of a relative Rényi entropy. *Journal of Mathematical Physics*, 54(12), 2013. URL: http://dx.doi.org/10.1063/1.4838835, doi:10.1063/1.4838835.

[43] Felix Leditzky, Mark M. Wilde, and Nilanjana Datta. Strong converse theorems using Rényi entropies. *J. Math. Phys.*, 57(8):082202, August 2016. doi:10.1063/1.4960099.

[44] Marco Tomamichel and Renato Renner. Uncertainty Relation for Smooth Entropies. *Physical Review Letters*, 106(11):110506, March 2011. doi:10.1103/PhysRevLett.106.110506.

[45] Christopher C Gerry and Peter L Knight. *Introductory quantum optics*. Cambridge University Press, Cambridge, England, 2 edition, November 2023.

[46] Yishay Mansour, Noam Nisan, and Prasoon Tiwari. The computational complexity of universal hashing. *Theoretical Computer Science*, 107(1):121–133, 1993. URL: https://www.sciencedirect.com/science/article/pii/030439759390257T, doi:10.1016/0304-3975(93)90257-T.

[47] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77, July 2018. doi:10.22331/q-2018-07-26-77.

[48] Hao Hu, Jiyoung Im, Jie Lin, Norbert Lütkenhaus, and Henry Wolkowicz. Robust interior point method for quantum key distribution rate computation. *Quantum*, 6:792, 2022. URL: https://quantum-journal.org/papers/q-2022-09-08-792/.

[49] Mariana Navarro, Andrés González Lorente, Pablo V. Parellada, Carlos Pascual-García, and Mateus Araújo. Finite-size quantum key distribution rates from rényi entropies using conic optimization, 2025. URL: https://arxiv.org/abs/2511.10584, arXiv:2511.10584.

[50] Kerry He, James Saunderson, and Hamza Fawzi. Qics: Quantum information conic solver. *arXiv preprint arXiv:2410.17803*, 2024. URL: https://arxiv.org/abs/2410.17803.

[51] Andrés González Lorente, Pablo V Parellada, Miguel Castillo-Celeita, and Mateus Araújo. Quantum key distribution rates from non-symmetric conic optimization. *Quantum*, 9:1657, 2025. URL: https://quantum-journal.org/papers/q-2025-03-10-1657/.

[52] Rebecca RB Chung, Nelly HY Ng, and Yu Cai. Generalized numerical framework for improved finite-sized key rates with rényi entropy. *Physical Review A*, 112(1):012612, 2025. URL: https://journals-aps-org.proxy.lib.uwaterloo.ca/pra/abstract/10.1103/tyts-8v8j.

[53] Gereon Koßmann and René Schwonnek. Optimising the relative entropy under semidefinite constraints. *npj Quantum Information*, 12(1), January 2026. URL: http://dx.doi.org/10.1038/s41534-026-01184-4, doi:10.1038/s41534-026-01184-4.

[54] Yukun Wang, Ignatius William Primaatmaja, Emilien Lavie, Antonios Varvitsiotis, and Charles Ci Wen Lim. Characterising the correlations of prepare-and-measure quantum networks. *npj Quantum Information*, 5(1):17, 2019. URL: https://www.nature.com/articles/s41534-019-0133-3.

[55] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503, March 2012. arXiv:1109.1473, doi:10.1103/PhysRevLett.108.130503.

[56] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, February 1992. doi:10.1103/PhysRevLett.68.557.

[57] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as a Precondition for Secure Quantum Key Distribution. *Physical Review Letters*, 92(21):217903, May 2004. doi:10.1103/PhysRevLett.92.217903.

[58] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices, September 2004. arXiv:quant-ph/0212066, doi:10.48550/arXiv.quant-ph/0212066.

[59] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Physical Review A*, 78(3):032302, September 2008. doi:10.1103/PhysRevA.78.032302.

[60] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing Models for Optical Measurements in Quantum Communication. *Physical Review Letters*, 101(9):093601, August 2008. doi:10.1103/PhysRevLett.101.093601.

[61] Toyohiro Tsurumaru. Squash operator and symmetry. *Physical Review A*, 81(1):012328, January 2010. doi:10.1103/PhysRevA.81.012328.

[62] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. Romero Alvarez, T. Moroder, and N. Lütkenhaus. Squashing model for detectors and applications to quantum-key-distribution protocols. *Physical Review A*, 89(1):012325, January 2014. doi:10.1103/PhysRevA.89.012325.

[63] Yanbao Zhang, Patrick J. Coles, Adam Winick, Jie Lin, and Norbert Lütkenhaus. Security proof of practical quantum key distribution with detection-efficiency mismatch. *Physical Review Research*, 3(1):013076, January 2021. doi:10.1103/PhysRevResearch.3.013076.

[64] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution, 2005. URL: https://arxiv.org/abs/quant-ph/0409078, doi:10.1007/978-3-540-30576-7_21.

[65] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94(2):025008, June 2022. doi:10.1103/RevModPhys.94.025008.

[66] Carla Ferradini, Martin Sandfuchs, Ramona Wolf, and Renato Renner. Defining security in quantum key distribution, 2025. URL: https://arxiv.org/abs/2509.13405, arXiv:2509.13405.

[67] Anne Broadbent and Martti Karvonen. Categorical composable cryptography: extended version. *Logical Methods in Computer Science*, Volume 19, Issue 4, December 2023. URL: http://dx.doi.org/10.46298/lmcs-19(4:30)2023, doi:10.46298/lmcs-19(4:30)2023.

[68] Gonzalo Arrazola. Quantum quotes, 2014. [Accessed 07-02-2026]. URL: https://qonaom.wordpress.com/2014/06/30/quantum-quotes/.

[69] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5), August 2003. URL: http://dx.doi.org/10.1103/PhysRevLett.91.057901, doi:10.1103/physrevlett.91.057901.

[70] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005. URL: https://link.aps.org/doi/10.1103/PhysRevLett.94.230504, doi:10.1103/PhysRevLett.94.230504.

[71] Xiang-Bin Wang. Beating the PNS attack in practical quantum cryptography. *Physical Review Letters*, 94(23):230503, June 2005. arXiv:quant-ph/0410075. URL: http://arxiv.org/abs/quant-ph/0410075, doi:10.1103/PhysRevLett.94.230503.

[72] Norbert Lütkenhaus. Estimates for practical quantum cryptography. *Physical Review A*, 59(5):3301–3319, May 1999. URL: http://dx.doi.org/10.1103/PhysRevA.59.3301, doi:10.1103/physreva.59.3301.

[73] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, January 1992. URL: http://dx.doi.org/10.1007/BF00191318, doi:10.1007/bf00191318.

[74] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330–1333, August 2000. URL: http://dx.doi.org/10.1103/PhysRevLett.85.1330, doi:10.1103/physrevlett.85.1330.

[75] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5), April 2000. URL: http://dx.doi.org/10.1103/PhysRevA.61.052304, doi:10.1103/physreva.61.052304.

[76] Hugo Krawczyk. LFSR-based Hashing and Authentication. In Yvo G. Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, pages 129–139, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg. URL: https://link.springer.com/chapter/10.1007/3-540-48658-5_15, doi:10.1007/3-540-48658-5_15.

[77] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 844–850, October 2022. doi:10.1109/FOCS54457.2022.00085.

[78] Shlok Nahar, Devashish Tupkary, and Norbert Lütkenhaus. Imperfect detectors for adversarial tasks with applications to quantum key distribution. *Quantum*, 10:2044, March 2026. URL: http://dx.doi.org/10.22331/q-2026-03-24-2044, doi:10.22331/q-2026-03-24-2044.

[79] Shlok Nahar, Twesh Upadhyaya, and Norbert Lütkenhaus. Imperfect phase randomization and generalized decoy-state quantum key distribution. *Physical Review Applied*, 20(6):064031, December 2023. doi:10.1103/PhysRevApplied.20.064031.

[80] Guillermo Currás-Lorenzo, Margarida Pereira, Shlok Nahar, and Devashish Tupkary. Security of quantum key distribution with source and detector imperfections through phase-error estimation, 2025. URL: https://arxiv.org/abs/2507.03549, arXiv:2507.03549.

[81] Chi-Hang Fred Fung, H. F. Chau, and Hoi-Kwong Lo. Universal squash model for optical communications using linear optics and threshold detectors. *Physical Review A*, 84(2):020303, August 2011. doi:10.1103/PhysRevA.84.020303.

[82] Twesh Upadhyaya, Thomas Van Himbeeck, Jie Lin, and Norbert Lütkenhaus. Dimension Reduction in Quantum Key Distribution for Continuous- and Discrete-Variable Protocols. *PRX Quantum*, 2(2):020325, May 2021. doi:10.1103/PRXQuantum.2.020325.

[83] Zhiyao Wang, Devashish Tupkary, and Shlok Nahar. Phase error estimation for passive detection setups with imperfections and memory effects, 2025. URL: https://arxiv.org/abs/2508.21486.

[84] Frédéric Dupuis and Omar Fawzi. Entropy Accumulation With Improved Second-Order Term. *IEEE Transactions on Information Theory*, 65(11):7596–7612, November 2019. doi:10.1109/TIT.2019.2929564.

[85] Tony Metger and Renato Renner. Security of quantum key distribution from generalised entropy accumulation. *Nature Communications*, 14(1):5272, August 2023. doi:10.1038/s41467-023-40920-8.

[86] Amir Arqand, Thomas A. Hahn, and Ernest Y.-Z. Tan. Generalized Rényi entropy accumulation theorem and generalized quantum probability estimation, May 2024. arXiv:2405.05912, doi:10.48550/arXiv.2405.05912.

[87] Thomas van Himbeeck and Peter Brown. Tight and general finite-size security of quantum key distribution. In preparation, presented at QCrypt 2023.

[88] Omar Fawzi, Jan Kochanowski, Cambyse Rouzé, and Thomas Van Himbeeck. Additivity and chain rules for quantum entropies via multi-index Schatten norms, 2025. URL: https://arxiv.org/abs/2502.01611, arXiv:2502.01611.

[89] Masato Koashi. Simple security proof of quantum key distribution via uncertainty principle, May 2005. arXiv:quant-ph/0505108, doi:10.48550/arXiv.quant-ph/0505108.

[90] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, April 2009. doi:10.1088/1367-2630/11/4/045018.

[91] Peter W. Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2):441–444, July 2000. doi:10.1103/PhysRevLett.85.441.

[92] D. Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, February 2003. doi:10.1109/TIT.2002.807289.

[93] Ian George, Jie Lin, and Norbert Lütkenhaus. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Physical Review Research*, 3(1):013274, March 2021. doi:10.1103/PhysRevResearch.3.013274.

[94] Darius Bunandar, Luke CG Govia, Hari Krovi, and Dirk Englund. Numerical finite-key analysis of quantum key distribution. *npj Quantum Information*, 6(1):104, 2020. doi:10.1038/s41534-020-00322-w.

[95] Renato Renner. *Security of Quantum Key Distribution*. Doctoral Thesis, ETH Zurich, 2005. doi:10.3929/ethz-a-005115027.

[96] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. Finite-key analysis on the 1-decoy state QKD protocol, April 2018. arXiv:1801.03443, doi:10.1063/1.5023340.

[97] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Physical Review A*, 89(2):022307, February 2014. doi:10.1103/PhysRevA.89.022307.

[98] Jerome Wiesemann, Jan Krause, Devashish Tupkary, Norbert Lütkenhaus, Davide Rusca, and Nino Walenta. A consolidated and accessible security proof for finite-size decoy-state quantum key distribution. *Quantum*, 10:2037, March 2026. URL: http://dx.doi.org/10.22331/q-2026-03-23-2037, doi:10.22331/q-2026-03-23-2037.

[99] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, February 2013. doi:10.1088/1367-2630/15/2/023006.

[100] Daniele Dequal, Luis Trigo Vidarte, Victor Roman Rodriguez, Giuseppe Vallone, Paolo Villoresi, Anthony Leverrier, and Eleni Diamanti. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Information*, 7(1):1–10, January 2021. doi:10.1038/s41534-020-00336-4.

[101] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, September 2017. doi:10.1038/nature23655.

[102] Phuc V. Trinh, Alberto Carrasco-Casado, Hideki Takenaka, Mikio Fujiwara, Mitsuo Kitamura, Masahide Sasaki, and Morio Toyoshima. Statistical verifications and deep-learning predictions for satellite-to-ground quantum atmospheric channels. *Communications Physics*, 5(1):1–18, September 2022. doi:10.1038/s42005-022-01002-1.

[103] Jasminder S. Sidhu, Thomas Brougham, Duncan McArthur, Roberto G. Pousa, and Daniel K. L. Oi. Finite key effects in satellite quantum key distribution. *npj Quantum Information*, 8(1):1–11, February 2022. doi:10.1038/s41534-022-00525-3.

[104] Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Wei Chen, Yong-Gang Zhu, Pavel V. Morozov, Alexander V. Divochiy, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. Twin-field quantum key distribution over 830-km fibre. *Nature Photonics*, 16(2):154–161, January 2022. URL: http://dx.doi.org/10.1038/s41566-021-00928-2, doi:10.1038/s41566-021-00928-2.

[105] Cecilia Clivati, Alice Meda, Simone Donadello, Salvatore Virzì, Marco Genovese, Filippo Levi, Alberto Mura, Mirko Pittaluga, Zhiliang Yuan, Andrew J. Shields, Marco Lucamarini, Ivo Pietro Degiovanni, and Davide Calonico. Coherent phase transfer for real-world twin-field quantum key distribution. *Nature Communications*, 13(1), January 2022. URL: http://dx.doi.org/10.1038/s41467-021-27808-1, doi:10.1038/s41467-021-27808-1.

[106] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields. Stability of high bit rate quantum key distribution on installed fiber. *Optics Express*, 20(15):16339, July 2012. URL: http://dx.doi.org/10.1364/OE.20.016339, doi:10.1364/oe.20.016339.

[107] Masahito Hayashi and Toyohiro Tsurumaru. Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, 14(9):093014, September 2012. doi:10.1088/1367-2630/14/9/093014.

[108] Shun Kawakami. *Security of Quantum Key Distribution with Weak Coherent Pulses*. PhD thesis, University of Tokyo, 2018. URL: https://repository.dl.itc.u-tokyo.ac.jp/records/50621.

[109] Guillermo Currás-Lorenzo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi. Tight finite-key security for twin-field quantum key distribution. *npj Quantum Information*, 7(1):1–9, February 2021. doi:10.1038/s41534-020-00345-3.

[110] C. Radhakrishna Rao, Gábor J. Székely, and Alfréd Rényi Institute of Mathematics, editors. *Statistics for the 21st Century: Methodologies for Applications of the Future*. Number v. 161 in Statistics, Textbooks and Monographs. Marcel Dekker, New York, 2000.

[111] C. J. Clopper and E. S. Pearson. The Use of Confidence or Fiducial Limits Illustrated in the Case of the Binomial. *Biometrika*, 26(4):404–413, 1934. arXiv:2331986, doi:10.2307/2331986.

[112] Renner, Renato. Simplifying information-theoretic arguments by post-selection, 2010. URL: http://hdl.handle.net/20.500.11850/29085, doi:10.3929/ETHZ-B-000029085.

[113] Paula Belzig. Studying stabilizer de finetti theorems and possible applications in quantum information processing, 2024. arXiv:2403.10592.

[114] Rotem Arnon-Friedman and Renato Renner. de Finetti reductions for correlations. *Journal of Mathematical Physics*, 56(5):052203, May 2015. arXiv:1308.0312 [quant-ph]. URL: http://arxiv.org/abs/1308.0312, doi:10.1063/1.4921341.

[115] Omar Fawzi and Renato Renner. Quantum Conditional Mutual Information and Approximate Markov Chains. *Communications in Mathematical Physics*, 340(2):575–611, December 2015. URL: http://link.springer.com/10.1007/s00220-015-2466-x, doi:10.1007/s00220-015-2466-x.

[116] Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner. Impossibility of Growing Quantum Bit Commitments. *Physical Review Letters*, 107(9):090502, August 2011. URL: https://link.aps.org/doi/10.1103/PhysRevLett.107.090502.

[117] Lars Kamin, Amir Arqand, Ian George, Norbert Lütkenhaus, and Ernest Y.-Z. Tan. Finite-size analysis of prepare-and-measure and decoy-state quantum key distribution via entropy accumulation, Jun 2025. URL: https://link.aps.org/doi/10.1103/PRXQuantum.6.020342, doi:10.1103/PRXQuantum.6.020342.

[118] Zhen Zhang, Qi Zhao, Mohsen Razavi, and Xiongfeng Ma. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Physical Review A*, 95(1):012333, January 2017. doi:10.1103/PhysRevA.95.012333.

[119] Shlok Nahar. *A proof-technique-independent framework for detector imperfections in QKD*. PhD thesis, University of Waterloo, 2025. URL: https://uwspace.uwaterloo.ca/items/ff6bda01-eefc-4bd7-bc1c-6207afd36142.

[120] Cong Jiang, Xiao-Long Hu, Zong-Wen Yu, Hai Xu, and Xiang-Bin Wang. Side-channel-secure quantum key distribution with state-dependent correlated errors and trojan-horse attack. *Opt. Express*, 33(25):51715–51729, Dec 2025. URL: https://opg.optica.org/oe/abstract.cfm?URI=oe-33-25-51715, doi:10.1364/OE.576910.

[121] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical review letters*, 90(16):167904, 2003. URL: https://journals-aps-org.proxy.lib.uwaterloo.ca/prl/abstract/10.1103/PhysRevLett.90.167904.

[122] Takaya Matsuura, Shinichiro Yamano, Yui Kuramochi, Toshihiko Sasaki, and Masato Koashi. Asymptotically tight security analysis of quantum key distribution based on universal source compression, 2025. URL: https://arxiv.org/abs/2504.07356, arXiv:2504.07356.

[123] Yang-Guang Shan, Zhen-Qiang Yin, Shuang Wang, Wei Chen, De-Yong He, Guang-Can Guo, and Zheng-Fu Han. Improved finite-key analysis for side-channel-secure quantum key distribution with de finetti reduction. *Physica Scripta*, 100(11):115117, nov 2025. doi:10.1088/1402-4896/ae1fbb.

[124] Ken-ichiro Yoshino, Mikio Fujiwara, Kensuke Nakata, Tatsuya Sumiya, Toshihiko Sasaki, Masahiro Takeoka, Masahide Sasaki, Akio Tajima, Masato Koashi, and Akihisa Tomita. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Information*, 4(1), February 2018. URL: http://dx.doi.org/10.1038/s41534-017-0057-8, doi:10.1038/s41534-017-0057-8.

[125] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1):634, January 2012. doi:10.1038/ncomms1631.

[126] Margarida Pereira, Guillermo Currás-Lorenzo, Álvaro Navarrete, Akihiro Mizutani, Go Kato, Marcos Curty, and Kiyoshi Tamaki. Modified BB84 quantum key distribution protocol robust to source imperfections. *Physical Review Research*, 5(2):023065, April 2023. doi:10.1103/PhysRevResearch.5.023065.

[127] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Physical Review A*, 90(5):052314, November 2014. doi:10.1103/PhysRevA.90.052314.

[128] Víctor Zapatero, Álvaro Navarrete, and Marcos Curty. Implementation security in quantum key distribution. *Advanced Quantum Technologies*, 8(2):2300380, 2025. URL: https://advanced.onlinelibrary.wiley.com/doi/abs/10.1002/qute.202300380, arXiv:https://advanced.onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202300380, doi:10.1002/qute.202300380.

[129] Guillermo Currás-Lorenzo, Margarida Pereira, Go Kato, Marcos Curty, and Kiyoshi Tamaki. Security of high-speed quantum key distribution with imperfect sources. *arXiv preprint arXiv:2305.05930*, 2023. URL: https://arxiv.org/abs/2305.05930.

[130] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2(1):349, June 2011. doi:10.1038/ncomms1348.

[131] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, August 2006. arXiv:quant-ph/0511032, doi:10.1103/PhysRevA.74.022313.

[132] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, October 2010. doi:10.1038/nphoton.2010.214.

[133] Shihan Sajeed, Poompong Chaiwongkhot, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Physical Review A*, 91(6):062301, June 2015. arXiv:1502.02785, doi:10.1103/PhysRevA.91.062301.

[134] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Info. Comput.*, 7(1):73–82, January 2007. URL: https://arxiv.org/abs/quant-ph/0512080, arXiv:quant-ph/0512080.

[135] L. Lydersen and J. Skaar. Security of quantum key distribution with bit and basis dependent detector flaws. *Quantum Info. Comput.*, 2010. URL: https://arxiv.org/abs/0807.0767, arXiv:0807.0767, doi:10.48550/ARXIV.0807.0767.

[136] Øystein Marøy, Lars Lydersen, and Johannes Skaar. Security of quantum key distribution with arbitrary individual imperfections. *Physical Review A*, 82(3), September 2010. URL: https://link.aps.org/doi/10.1103/PhysRevA.82.032337, doi:10.1103/PhysRevA.82.032337.

[137] Anton Trushechkin. Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case. *Quantum*, 6:771, July 2022. doi:10.22331/q-2022-07-22-771.

[138] M. K. Bochkov and A. S. Trushechkin. Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds. *Physical Review A*, 99(3):032308, March 2019. doi:10.1103/PhysRevA.99.032308.

[139] Federico Grasselli, Giovanni Chesi, Nathan Walk, Hermann Kampermann, Adam Widomski, Maciej Ogrodnik, Michał Karpiński, Chiara Macchiavello, Dagmar Bruß, and Nikolai Wyderka. Quantum key distribution with basis-dependent detection probability. *Phys. Rev. Appl.*, 23:044011, Apr 2025. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.23.044011, doi:10.1103/PhysRevApplied.23.044011.

[140] Alessandro Marcomini, Akihiro Mizutani, Fadri Grünenfelder, Marcos Curty, and Kiyoshi Tamaki. Loss-tolerant quantum key distribution with detection efficiency mismatch. *Quantum Science and Technology*, 10(3):035002, apr 2025. doi:10.1088/2058-9565/adc8cc.

[141] Chi-Hang Fred Fung, Kiyoshi Tamaki, Bing Qi, Hoi-Kwong Lo, and Xiongfeng Ma. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Information and Computation*, 9:131–165, October 2009. arXiv:0802.3788, doi:10.26421/QIC9.1-2-8.

[142] Agnes Ferenczi and Norbert Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Physical Review A*, 85(5):052310, May 2012. doi:10.1103/PhysRevA.85.052310.

[143] R. J. Serfling. Probability Inequalities for the Sum in Sampling without Replacement. *The Annals of Statistics*, 2(1):39–48, January 1974. doi:10.1214/aos/1176342611.

[144] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1), July 2005. URL: http://dx.doi.org/10.1103/PhysRevA.72.012326, doi:10.1103/physreva.72.012326.

[145] Masahito Hayashi and Ryota Nakayama. Security analysis of the decoy method with the Bennett–Brassard 1984 protocol for finite key lengths. *New Journal of Physics*, 16(6):063009, June 2014. doi:10.1088/1367-2630/16/6/063009.

[146] Markus Rau, Tobias Vogl, Giacomo Corrielli, Gwenaelle Vest, Lukas Fuchs, Sebastian Nauerth, and Harald Weinfurter. Spatial mode side channels in free-space qkd implementations. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):187–191, 2015. doi:10.1109/JSTQE.2014.2372008.

[147] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2), February 2006. URL: http://dx.doi.org/10.1103/PhysRevA.73.022320, doi:10.1103/physreva.73.022320.

[148] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2(1), June 2011. URL: http://dx.doi.org/10.1038/ncomms1348, doi:10.1038/ncomms1348.

[149] Guillermo Currás-Lorenzo, Margarida Pereira, Kiyoshi Tamaki, and Marcos Curty. Rigorous phase-error-estimation security framework for qkd with correlated sources, 2026. URL: https://arxiv.org/abs/2601.08417, arXiv:2601.08417.

[150] Christopher Portmann. Key Recycling in Authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, July 2014. doi:10.1109/TIT.2014.2317312.

[151] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau. Practical issues in quantum-key-distribution postprocessing. *Physical Review A*, 81(1):012318, January 2010. doi:10.1103/PhysRevA.81.012318.

[152] Valerio Scarani and Renato Renner. Security Bounds for Quantum Cryptography with Finite Resources. In Yasuhito Kawano and Michele Mosca, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 83–95, Berlin, Heidelberg, 2008. Springer. doi:10.1007/978-3-540-89304-2_8.

[153] Masahito Hayashi. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Physical Review A*, 76(1):012329, July 2007. doi:10.1103/PhysRevA.76.012329.

[154] Raymond Y Q Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024, apr 2009. doi:10.1088/1367-2630/11/4/045024.

[155] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5(1), April 2014. URL: http://dx.doi.org/10.1038/ncomms4732, doi:10.1038/ncomms4732.

[156] Te Sun Han and M. Hoshi. Interval algorithm for random number generation. *IEEE Transactions on Information Theory*, 43(2):599–611, 1997. doi:10.1109/18.556116.

[157] Peter J. Brown, Sammy Ragy, and Roger Colbeck. A Framework for Quantum-Secure Device-Independent Randomness Expansion. *IEEE Transactions on Information Theory*, 66(5):2964–2987, 2020. doi:10.1109/TIT.2019.2960252.

[158] Yanbao Zhang, Honghao Fu, and Emanuel Knill. Efficient randomness certification by quantum probability estimation. *Phys. Rev. Res.*, 2:013016, Jan 2020. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.2.013016, doi:10.1103/PhysRevResearch.2.013016.

[159] Mateus Araújo, Marcus Huber, Miguel Navascués, Matej Pivoluska, and Armin Tavakoli. Quantum key distribution rates from semidefinite programming. *Quantum*, 7:1019, 2023. URL: https://quantum-journal.org/papers/q-2023-05-24-1019/.

[160] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018–3021, October 1998. URL: http://dx.doi.org/10.1103/PhysRevLett.81.3018, doi:10.1103/physrevlett.81.3018.

[161] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, June 1981. doi:10.1016/0022-0000(81)90033-7.

[162] Evgeniy O. Kiktenko, Aleksei O. Malyshev, Maxim A. Gavreev, Anton A. Bozhedarov, Nikolay O. Pozhar, Maxim N. Anufriev, and Aleksey K. Fedorov. Lightweight Authentication for Quantum Key Distribution. *IEEE Transactions on Information Theory*, 66(10):6354–6368, October 2020. doi:10.1109/TIT.2020.2989459.

[163] Wen Yu Kon, Jefferson Chu, Kevin Han Yong Loh, Obada Alia, Omar Amer, Marco Pistoia, Kaushik Chakraborty, and Charles Lim. Quantum authenticated key expansion with key recycling, 2024. URL: https://arxiv.org/abs/2409.16540, arXiv:2409.16540.

[164] Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner, and Björn Tackmann. Causal Boxes: Quantum Information-Processing Systems Closed Under Composition. *IEEE Transactions on Information Theory*, 63(5):3277–3305, May 2017. doi:10.1109/TIT.2017.2676805.

[165] Marco Tomamichel. A Framework for Non-Asymptotic Quantum Information Theory, July 2013. arXiv:1203.2142, doi:10.48550/arXiv.1203.2142.

[166] Wassily Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, 58(301):13–30, March 1963. doi:10.1080/01621459.1963.10500830.

APPENDICES

Appendix A

Variable-length input to privacy amplification

We will now provide proof of the statements from Section 4.6.

Lemma 4.6.1. *Let $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$ be a state classical in $\mathbf{SC}$ (where the $\mathbf{S}$ register takes values in $\{0,1\}^{\leq n}$), with the property that conditioned on each possible value $\bar{c}$ on the $\mathbf{C}$ register, the resulting distribution on $\mathbf{S}$ is only supported on values in $\{0,1\}^{k_{\bar{c}}}$ for some constant $k_{\bar{c}} \in \mathbb{N}$. Note that $\mathbf{C}$ is a classical register which can be store arbitrary values for the purposes of this lemma. Let $\rho_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}}$ be the state obtained from $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$ by first computing the number of bits $\mathrm{len}(\mathbf{S})$ in the $\mathbf{S}$ register, then implementing a universal$_2$ hashing procedure from $\mathrm{len}(\mathbf{S})$ bits to ℓ_{fixed} bits (in other words, the procedure described in Case 3 of Section 4.6.1). Then for any event Ω on the classical register $\mathbf{C}$, we have (for $\rho^{(\mathrm{ideal})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}} := \frac{\mathbb{I}_{K_A}}{|K_A|} \otimes \rho_{\mathbf{C}\hat{\boldsymbol{E}}}$):*

$$\begin{aligned}
&\Pr(\Omega)\frac{1}{2}\left\|\rho_{K_A\mathbf{C}\hat{\boldsymbol{E}}|\Omega} - \rho^{(\mathrm{ideal})}_{K_A\mathbf{C}\hat{\boldsymbol{E}}|\Omega}\right\|_1 \\
&\leq \Pr(\Omega)2^{-\left(\frac{\alpha-1}{\alpha}\right)\left(\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho|\Omega}-\ell_{\mathrm{fixed}}+2\right)} \\
&\leq 2^{-\left(\frac{\alpha-1}{\alpha}\right)\left(\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}-\ell_{\mathrm{fixed}}+2\right)}
\end{aligned} \tag{4.62}$$

Proof. As explained in Section 4.6.2, the hashing procedure described above can be thought of as *first* randomly sampling $f_i \in \mathcal{F}_{\mathrm{hash}}(i, \ell_{\mathrm{fixed}})$ for every i, and then computing $f_{\mathrm{len}(\mathbf{S})}(\mathbf{S})$. However, as noted in that section, this process is not a valid universal$_2$ hashing procedure from $\{0,1\}^{\leq n}$ to ℓ_{fixed} bits.

Consider instead the following virtual hashing process, based on new hash families [1] $\mathcal{F}^{\text{virt}}_{\text{hash}}(i, \ell_{\text{fixed}}) \coloneqq \mathcal{F}_{\text{hash}}(i, \ell_{\text{fixed}}) \times \{0,1\}^{\ell_{\text{fixed}}}$ (for every i). This virtual process first randomly samples $(f_i, u_i) \in \mathcal{F}^{\text{virt}}_{\text{hash}}(i\ell_{\text{fixed}},)$ for every i, i.e. f_i is sampled from the same universal$_2$ hash family $\mathcal{F}_{\text{hash}}(i, \ell_{\text{fixed}})$ as before, and u_i is a random ℓ_{fixed}-bit string. It then computes $f_{\text{len}(\mathbf{S})}(\mathbf{S}) \oplus u_{\text{len}(\mathbf{S})}$ as its hash output. Now, this virtual hashing procedure *is* a valid universal$_2$ hashing procedure from $\{0,1\}^{\leq n}$ to ℓ_{fixed} bits, because each hash family $\mathcal{F}^{\text{virt}}_{\text{hash}}(i, \ell_{\text{fixed}})$ is universal$_2$ *and* satisfies the "uniform output" property (Eq. (4.61)).

Denote the output state of the virtual process (acting on $\rho_{\mathbf{SC}\hat{\boldsymbol{E}}}$) as $\rho^{(\text{virtual})}_{K_A\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}}$ [2], where H_{PA} stores the description of the hash function chosen in the virtual process (in particular, all the values (f_i, u_i) from the virtual process). Let us analogously define $\rho^{(\text{ideal,virtual})}_{K_A\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}} \coloneqq \frac{\mathbb{I}_{K_A}}{|K_A|} \otimes \rho^{(\text{virtual})}_{\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}}$.

Now, we construct a CPTP map $\mathcal{E} : K_A\mathbf{C}\hat{\boldsymbol{E}} \to K_A\mathbf{C}\hat{\boldsymbol{E}}$ that will map the virtual output states to the actual output states. This map $\mathcal{E}$ does the following operations:

1. Look at $\mathbf{C}$ and determine the corresponding value $k_{\bar{C}}$ (as defined in the conditions of this lemma)[3], to be used in the subsequent steps.
2. Look at H_{PA} and determine $u_{k_{\bar{C}}}$, to be used in the subsequent steps.
3. Replace K_A with $K_A \oplus u_{k_{\bar{C}}}$ (essentially removing the XOR that was applied during the hashing procedure).
4. Partial trace on the H_{PA} register, on everything except the $f_{k_{\bar{C}}}$ information.

It is straightforward to verify that this map $\mathcal{E}$ indeed satisfies

$$\begin{aligned} \mathcal{E}\left(\rho^{(\text{virtual})}_{K_A\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}}\right) &= \rho_{K_A\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}}, \\ \mathcal{E}\left(\rho^{(\text{ideal,virtual})}_{K_A\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}}\right) &= \rho^{(\text{ideal})}_{\mathbf{C}H_{\text{PA}}\hat{\boldsymbol{E}}}, \end{aligned} \tag{A.1}$$

and analogously for the above states conditioned on the event Ω (since $\mathcal{E}$ does not disturb the register $\mathbf{C}$).

[1] This specification of $\mathcal{F}^{\text{virt}}_{\text{hash}}(i, \ell_{\text{fixed}})$ is not technically a set of *functions*, since each element of $\mathcal{F}^{\text{virt}}_{\text{hash}}(i, \ell_{\text{fixed}})$ is instead a tuple where the second term is an ℓ_{fixed}-bit string. However, each such element uniquely specifies a function in a simple manner that we shall shortly specify.

[2] The "virtual" notation here has nothing to with the virtual states and worlds introduced in Chapter 7.

[3] $\mathcal{E}$ cannot "directly" compute len($\mathbf{S}$) because the register $\mathbf{S}$ is no longer present in the states it acts on.

Therefore, we have

$$\begin{aligned}
&\Pr(\Omega)\frac{1}{2}\left\|\rho_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}|\Omega} - \rho^{(\mathrm{ideal})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}|\Omega}\right\|_1 \\
&= \Pr(\Omega)\frac{1}{2}\left\|\mathcal{E}\left(\rho^{(\mathrm{virtual})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}|\Omega} - \rho^{(\mathrm{ideal,virtual})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}|\Omega}\right)\right\|_1 \\
&\leq \Pr(\Omega)\frac{1}{2}\left\|\rho^{(\mathrm{virtual})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}|\Omega} - \rho^{(\mathrm{ideal,virtual})}_{K_A\mathbf{C}H_{\mathrm{PA}}\hat{\boldsymbol{E}}|\Omega}\right\|_1 \\
&\leq \Pr(\Omega)2^{-\left(\frac{\alpha-1}{\alpha}\right)\left(\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho|\Omega} - \ell_{\mathrm{fixed}} + 2\right)} \\
&\leq 2^{-\left(\frac{\alpha-1}{\alpha}\right)\left(\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho} - \ell_{\mathrm{fixed}} + 2\right)}
\end{aligned} \tag{A.2}$$

where we used the fact that CPTP maps cannot increase trace norm in the third inequality, and Leftover Hashing Lemma for Rényi entropies (Lemma 3.5.1) for the fourth inequality, and Lemma 2.2.3 for the final inequality. □

Lemma 4.6.2. *Suppose $\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}, \rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}$ are states that are classical in $\mathbf{C}$, and related to each other as follows: letting $R_{\bar{c}}$ be a register containing the support of the conditional state $\rho_{R|\mathbf{C}=\bar{c}}$, there exist isometries $V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}}$ such that*[4]

$$\begin{aligned}
&V\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}V^{\dagger} = \rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}, \text{ where} \\
&V \coloneqq \sum_{\bar{c}} V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}} \otimes |\bar{c}\rangle\langle\bar{c}|_{\mathbf{C}}\,.
\end{aligned} \tag{4.63}$$

Then we have

$$\widetilde{H}^{\uparrow}_{\alpha}(\mathbf{S}|\mathbf{C}\hat{\boldsymbol{E}})_{\rho} = \widetilde{H}^{\uparrow}_{\alpha}(R|\mathbf{C}\hat{\boldsymbol{E}})_{\rho}. \tag{4.64}$$

Proof. We intuitively expect Eq. (4.64) to be true, since Eq. (4.63) essentially states that $\mathbf{C}$ can be used to isometrically convert R to $\mathbf{S}$. To formalize this, we first note that each isometry $V^{(\bar{c})}_{R_{\bar{c}}\to\mathbf{S}}$ can always be extended to an isometry $V^{(\bar{c})}_{R\to\mathbf{S}}$, i.e. where the domain is the full Hilbert space of R (padding the output space $\mathbf{S}$ with extra dimensions if $\dim(R) > \dim(\mathbf{S})$). Furthermore, Eq. (4.63) still holds with V defined in terms of these new isometries instead, i.e. we have

$$\begin{aligned}
&V\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}V^{\dagger} = \rho_{\mathbf{S}\mathbf{C}\hat{\boldsymbol{E}}}, \text{ where} \\
&V \coloneqq \sum_{\bar{c}} V^{(\bar{c})}_{R\to\mathbf{S}} \otimes |\bar{c}\rangle\langle\bar{c}|_{\mathbf{C}}\,.
\end{aligned} \tag{A.3}$$

[4]Eq. (4.63) is a well-defined expression despite the fact that V is not defined on all of $R\mathbf{C}$, because $\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}$ is only supported on the subspace on which V is defined.

(It does not matter how we chose the extensions, since $\rho_{R\mathbf{C}\hat{\boldsymbol{E}}}$ is only supported on a subspace that is unaffected by these choices of extensions.)

Furthermore, letting $\mathbf{C}_c$ be a copy of the register $\mathbf{C}$, using [41, Lemma B.7] we have

$$\begin{aligned} H_\alpha(\mathbf{S}\mathbf{C}_c|\mathbf{C}E)_\rho &= H_\alpha(\mathbf{S}|\mathbf{C}E)_\rho, \\ H_\alpha(R\mathbf{C}_c|\mathbf{C}E)_\rho &= H_\alpha(R|\mathbf{C}E)_\rho, \end{aligned} \tag{A.4}$$

Thus, it is enough to show that $H_\alpha(\mathbf{S}\mathbf{C}_c|\mathbf{C}E)_\rho = H_\alpha(R\mathbf{C}_c|\mathbf{C}E)_\rho$. This follows from Eq. (A.3), and the fact that the Rényi entropy is invariant under isometries on the first subsystem (Lemma 7.2.2 with $f = 0$), since by defining the isometry $\widetilde{V}_{R\mathbf{C}_c\to\mathbf{S}\mathbf{C}_c} \coloneqq \sum_{\bar{c}} V^{(\bar{c})}_{R\to\mathbf{S}} \otimes |\bar{c}\rangle\langle\bar{c}|_{\mathbf{C}_c}$ we have

$$\widetilde{V}\rho_{R\mathbf{C}_c\mathbf{C}E}\widetilde{V}^\dagger = \rho_{\mathbf{S}\mathbf{C}_c\mathbf{C}E}. \tag{A.5}$$

which concludes the proof[5]. □

[5]An alternative proof would be to instead use [38, Proposition 5.1] to split the conditional entropies into terms conditioned on each value of $\mathbf{C}$, and note that the equality holds for each term by invariance of Rényi entropy under isometries on the first subsystem.

Appendix B

Proofs of statements for the postselection technique

In this appendix, we will provide proofs of various statements utilized in Chapter 5.

Lemma 5.2.1 (Satisfying permutation invariance)**.** *Consider the QKD protocol* $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell)}, \sigma_A\}$ *where* $\mathcal{E}_{\mathrm{QKD}}^{(\ell)} \in \mathrm{CPTP}(A_1^n B_1^n, K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}})$ *is the QKD protocol map describing QKD Protocol. Define a new protocol map* $\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}$ *by first applying a uniformly random permutation to the systems* $A_1^n B_1^n$*, announcing the permutation in a classical register* C_{perm}*, and then applying* $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$*. Explicitly,*

$$\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}(\cdot) = \mathcal{E}_{\mathrm{QKD}}^{(\ell)} \circ \left(\sum_{\pi \in S_n^{\mathrm{perm}}} \frac{1}{n!} P_\pi^{n,d_A d_B}(\cdot) P_\pi^{n,d_A d_B \dagger} \otimes |\pi\rangle\langle\pi|_{C_{\mathrm{perm}}} \right). \tag{5.11}$$

Then the following statements hold:

1. *The protocol* $\{\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}, \sigma_A\}$ *describes QKD Protocol with the optional permutation step applied to the* X_1^n, Y_1^n *registers, where the applied permutation is announced in the (additional) register* C_{perm}*, which is made available to Eve.*

2. *The difference between the real and ideal protocols,*

$$\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})} - \mathrm{Tr}_{K_B} \circ \mathcal{R}_{\mathrm{ideal}} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})},$$

   is permutation invariant according to Definition 5.1.2.

Proof. The first part of the lemma follows from the fact that, in Generic QKD Protocol, the state preparation and measurement procedures are identical in each round. After applying the source-replacement scheme and obtaining the effective protocol map $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$, Alice and Bob perform the same measurements in every round. Since the measurements are the same in each round, the permutation π may equivalently be applied and announced either to the post-measurement classical registers $X_1^n Y_1^n$ or to the pre-measurement quantum systems $A_1^n B_1^n$.

For the second part, observe that the difference between the real and ideal protocols can be written as

$$\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})} - \mathrm{Tr}_{K_B} \circ \mathcal{R}_{\mathrm{ideal}} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})} = \mathcal{F} \circ \sum_{\pi \in S_n^{\mathrm{perm}}} \frac{1}{n!} \mathcal{W}_\pi \otimes |\pi\rangle\langle\pi|_{C_{\mathrm{perm}}} , \tag{B.1}$$

where $\mathcal{W}_\pi$ denotes the action of the permutation π on the systems $A_1^n B_1^n$.

To prove permutation invariance, consider any permutation $\pi' \in S_n^{\mathrm{perm}}$ and define a map $G_{\pi'}$ that replaces the classical register $|\pi\rangle\langle\pi|_{C_{\mathrm{perm}}}$ by $|\pi \circ \pi'\rangle\langle\pi \circ \pi'|_{C_{\mathrm{perm}}}$. Then

$$\begin{aligned} G_{\pi'} \circ \left(\mathcal{F} \circ \sum_{\pi \in S_n^{\mathrm{perm}}} \mathcal{W}_\pi \otimes |\pi\rangle\langle\pi|_{C_{\mathrm{perm}}} \right) \circ \mathcal{W}_{\pi'} &= G_{\pi'} \circ \left(\mathcal{F} \circ \sum_{\pi \in S_n^{\mathrm{perm}}} \frac{1}{n!} \mathcal{W}_{\pi \circ \pi'} \otimes |\pi\rangle\langle\pi|_{C_{\mathrm{perm}}} \right) \\ &= \mathcal{F} \circ \sum_{\pi \in S_n^{\mathrm{perm}}} \frac{1}{n!} \mathcal{W}_{\pi \circ \pi'} \otimes |\pi \circ \pi'\rangle\langle\pi \circ \pi'|_{C_{\mathrm{perm}}} \\ &= \mathcal{F} \circ \sum_{\pi \in S_n^{\mathrm{perm}}} \frac{1}{n!} \mathcal{W}_\pi \otimes |\pi\rangle\langle\pi|_{C_{\mathrm{perm}}} , \end{aligned} \tag{B.2}$$

where the first two equalities follow from the definitions of $\mathcal{W}_{\pi'}$ and $G_{\pi'}$, and the final equality follows by a simple relabeling of the permutation variable in the summation. This establishes permutation invariance. □

Lemma 5.2.2. *Let $\{\sigma_A, \mathcal{E}_{\mathrm{QKD}}^{(\ell)}\}$ be a QKD protocol, and let $\{\sigma_A, \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}\}$ be a related QKD protocol in which the maps are related by a random permutation (Eq. (5.11)). Then,*

$$\begin{aligned} &\frac{1}{2} \left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm}),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 \\ &= \frac{1}{2} \left\| \left(\left(\mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell)} - \mathrm{Tr}_{K_B} \circ \mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}} \right) \otimes \mathrm{id}_{E_1^n} \right) \left[\rho_{ABE}^{\otimes n} \right] \right\|_1 . \end{aligned} \tag{5.12}$$

That is, security against IID collective attacks for $\mathcal{E}_{\mathrm{QKD}}^{(\ell)}$ implies security against IID collective attacks for $\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}$.

Proof. The claim follows by straightforward algebra. Let $\mathcal{W}_\pi$ denote the permutation π acting on the A and B systems. Then

$$\begin{aligned}
&\frac{1}{2}\left\|\left(\left(\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}-\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm}),\mathrm{ideal}}\right)\otimes\mathrm{id}_{E_1^n}\right)\left[\rho_{ABE}^{\otimes n}\right]\right\|_1 \\
&=\sum_{\pi\in S_n^{\mathrm{perm}}}\frac{1}{n!}\frac{1}{2}\left\|\left(\left(\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm})}-\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell,\mathrm{perm}),\mathrm{ideal}}\right)\otimes\mathrm{id}_{E_1^n}\right)\circ\mathcal{W}_\pi\left[\rho_{ABE}^{\otimes n}\otimes|\pi\rangle\langle\pi|_{C_{\mathrm{perm}}}\right]\right\|_1 \\
&=\frac{1}{2}\left\|\left(\left(\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell)}-\mathrm{Tr}_{K_B}\circ\mathcal{E}_{\mathrm{QKD}}^{(\ell),\mathrm{ideal}}\right)\otimes\mathrm{id}_{E_1^n}\right)\left[\rho_{ABE}^{\otimes n}\right]\right\|_1,
\end{aligned} \tag{B.3}$$

where the final equality follows from the fact that $\rho_{ABE}^{\otimes n}$ is invariant under permutations of the A and B systems. □

Lemma 5.2.3. *Let $\mathcal{F},\mathcal{F}'\in\mathrm{T}(A_1^nB_1^n,K)$ be linear maps such that $\mathcal{F}-\mathcal{F}'$ is a permutation-invariant linear map. Let $\rho_{A_1^nB_1^nR''}\in\mathrm{Pos}(A^nB^nR'')$ be any extension of $\rho_{A_1^nB_1^n}$. Then the state $\bar{\rho}_{A_1^nB_1^n}=\frac{1}{n!}\sum_{\pi\in S_n^{\mathrm{perm}}}\mathcal{W}_\pi(\rho_{A_1^nB_1^n})$ is permutation-invariant, and for any purification $\bar{\rho}_{A_1^nB_1^nR'}$ of that state, we have*

$$\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\otimes\mathrm{id}_{R''}\right)\left(\rho_{A_1^nB_1^nR''}\right)\right\|_1\leq\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\otimes\mathrm{id}_{R'}\right)\left(\bar{\rho}_{A_1^nB_1^nR'}\right)\right\|_1. \tag{5.13}$$

Proof. Construct

$$\bar{\rho}_{A_1^nB_1^nR''\widetilde{R}}=\frac{1}{n!}\sum_{\pi\in S_n^{\mathrm{perm}}}\left(\mathcal{W}_\pi\otimes\mathbb{I}_{R''}\right)\left(\rho_{A_1^nB_1^nR''}\right)\otimes|\pi\rangle\langle\pi|_{\widetilde{R}} \tag{B.4}$$

as an extension of $\bar{\rho}_{A_1^nB_1^n}$. Therefore, there exists $\Phi\in\mathrm{CPTP}(R',R''\widetilde{R})$ such that $\left(\mathrm{id}_{A_1^nB_1^n}\otimes\Phi\right)\left(\bar{\rho}_{A_1^nB_1^nR'}\right)=\bar{\rho}_{A_1^nB_1^nR''\widetilde{R}}$. Since trace norm cannot increase under CPTNI maps, we have

$$\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\otimes\mathrm{id}_{R''\widetilde{R}}\right)\left(\bar{\rho}_{A_1^nB_1^nR''\widetilde{R}}\right)\right\|_1\leq\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\otimes\mathrm{id}_{R'}\right)\left(\bar{\rho}_{A_1^nB_1^nR'}\right)\right\|_1. \tag{B.5}$$

Next, making use of the permutation-invariance of $\mathcal{F}-\mathcal{F}'$, we have

$$\begin{aligned}
\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\otimes\mathrm{id}_{R''}\right)\left(\rho_{A_1^nB_1^nR''}\right)\right\|_1&=\frac{1}{n!}\sum_{\pi\in S_n^{\mathrm{perm}}}\frac{1}{2}\left\|\left(G_\pi\circ(\mathcal{F}-\mathcal{F}')\circ\mathcal{W}_\pi\otimes\mathrm{id}_{R''}\right)\left(\rho_{A_1^nB_1^nR''}\right)\right\|_1 \\
&\leq\frac{1}{n!}\sum_{\pi\in S_n^{\mathrm{perm}}}\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\circ\mathcal{W}_\pi\otimes\mathrm{id}_{R''}\right)\left(\rho_{A_1^nB_1^nR''}\right)\right\|_1 \\
&=\frac{1}{2}\left\|\left((\mathcal{F}-\mathcal{F}')\otimes\mathrm{id}_{R''\widetilde{R}}\right)\left(\bar{\rho}_{A_1^nB_1^nR''\widetilde{R}}\right)\right\|_1,
\end{aligned} \tag{B.6}$$

where the inequality again follows from the fact that CPTNI maps cannot increase trace norm, and the final inequality follows from the fact that the states $((\mathcal{F}-\mathcal{F}')\circ\mathcal{W}_\pi\otimes \mathrm{id}_{R''})\left(\rho_{A_1^nB_1^nR''}\right)$ are orthogonal for different π. Putting Eqs. (B.5) and (B.6) together, we get the desired result. □

Lemma 5.2.4. *Let $\rho_{A_1^nB_1^n}\in \mathrm{Pos}(A_1^nB_1^n)$ and $\tau_{A_1^nB_1^n}\in \mathrm{Pos}(A_1^nB_1^n)$ be such that $\rho_{A_1^nB_1^n}\leq g_{n,x}\tau_{A_1^nB_1^n}$ for some $g_{n,x}>0$. Let $\rho_{A_1^nB_1^nR'}$ be any extension of $\rho_{A_1^nB_1^n}$, and let $\tau_{A_1^nB_1^nR}$ be any purification of $\tau_{A_1^nB_1^n}$. Then for any two maps $\mathcal{F},\mathcal{F}'\in \mathrm{T}(A_1^nB_1^n,K)$,*

$$\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'})\left(\rho_{A_1^nB_1^nR'}\right)\right\|_1\leq g_{n,x}\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R})\left(\tau_{A_1^nB_1^nR}\right)\right\|_1 \tag{5.14}$$

Proof. Let us consider $\rho_{A_1^nB_1^n},\tau_{A_1^nB_1^n}$ to have trace 1; the extension to positive operators follows naturally. Since $\rho_{A_1^nB_1^n}\leq g_{n,x}\tau_{A_1^nB_1^n}$, there exists a $\omega_{A_1^nB_1^n}\in \mathrm{S}_=(A_1^nB_1^n)$ such that $\rho_{A_1^nB_1^n}+(g_{n,x}-1)\omega_{A_1^nB_1^n}=g_{n,x}\tau_{A_1^nB_1^n}$. One can then construct an extension of of $\tau_{A_1^nB_1^n}$ as,

$$\tau_{A_1^nB_1^nR'M}=\frac{1}{g_{n,x}}\rho_{A_1^nB_1^nR'}\otimes|0\rangle\langle 0|_M+\left(1-\frac{1}{g_{n,x}}\right)\omega_{A_1^nB_1^nR'}\otimes|1\rangle\langle 1|_M\,. \tag{B.7}$$

Since the map $(\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'M}$ acts identically on M, the two terms above are orthogonal before and after the action of the map. Therefore,

$$\begin{aligned}\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'M})\left(\tau_{A_1^nB_1^nR'M}\right)\right\|_1 &= \frac{1}{g_{n,x}}\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'M})\left(\rho_{A_1^nB_1^nR'}\otimes|0\rangle\langle 0|\right)\right\|_1\\ &\quad+\left(1-\frac{1}{g_{n,x}}\right)\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'M})\left(\omega_{A_1^nB_1^nR'}\otimes|1\rangle\langle 1|\right)\right\|_1\\ &\geq \frac{1}{g_{n,x}}\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'})\left(\rho_{A_1^nB_1^nR'}\right)\right\|_1\end{aligned} \tag{B.8}$$

Finally, for any purification $\tau_{A_1^nB_1^nR}$ of $\tau_{A_1^nB_1^n}$, and extension $\tau_{A_1^nB_1^nR'M}$ of $\tau_{A_1^nB_1^n}$, there exists a CPTP map $\Phi\in \mathrm{CPTP}(R,R'M)$ such that $\left(\mathrm{id}_{A_1^nB_1^n}\otimes\Phi\right)\left(\tau_{A_1^nB_1^nR}\right)=\tau_{A_1^nB_1^nR'M}$ (Lemma 2.1.1). Therefore,

$$\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R})\left(\tau_{A_1^nB_1^nR}\right)\right\|_1\geq\frac{1}{2}\left\|((\mathcal{F}-\mathcal{F}')\otimes \mathrm{id}_{R'M})\left(\tau_{A_1^nB_1^nR'M}\right)\right\|_1 \tag{B.9}$$

follows from the fact that CPTP maps cannot increase trace norm. Putting Eq. (B.8) and (B.9) together, the desired result is obtained. □

Appendix C

Proofs of statements for EUR analysis

In this chapter, we will provide the proof of various statements utilized in Chapter 6.

C.1 Variable-length security

We start with the proof of the following theorem, which is suitable for EUR based analysis.

Theorem 6.1.1 (Variable-length security for EUR based methods)**.** *In QKD Protocol, let $\Omega(\vec{p})$ denote a well-defined event on the state $\rho_{\mathbf{SS}_B\widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}}}$ just before privacy amplification. Therefore, $\Omega(\hat{c}_1^n, \vec{p})$ denotes well-defined events, where $\hat{c}_1^n$ denotes the value of the public announcement register $\widehat{C}_1^n$ in the protocol, and $\vec{p}$ denotes values that are not directly observed in the protocol. For every value of $\hat{c}_1^n$, let $\mathcal{V}(\hat{c}_1^n)$ be a set of possible values of $\vec{p}$.*

Let $\zeta(\hat{c}_1^n, \vec{p}) \in [0, 1)$ be such that the following bound on the smooth min entropy of the preamplification string holds,

$$H_{\min}^{\sqrt{\zeta(\hat{c}_1^n, \vec{p})}}(\mathbf{S}|\widehat{C}_1^n \hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n, \vec{p})} \geq \beta(\hat{c}_1^n) \qquad \forall \hat{c}_1^n, \forall \vec{p} \in \mathcal{V}(\hat{c}_1^n). \tag{6.1}$$

where the smoothing parameters $\zeta(\hat{c}_1^n, \vec{p})$ satisfy

$$\sum_{\hat{c}_1^n} \sum_{\vec{p} \in \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p}))\zeta_{(\hat{c}_1^n, \vec{p})} + \sum_{\hat{c}_1^n} \sum_{\vec{p} \notin \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p})) \leq \varepsilon_{\mathrm{AT}}^2. \tag{6.2}$$

Let the output key length be given by

$$\ell(\hat{c}_1^n) \coloneqq \max\left\{\left\lfloor \beta(\hat{c}_1^n) - \lambda_{\mathrm{EC}}(\hat{c}_1^n) - 2\log\left(\frac{1}{\varepsilon_{\mathrm{PA}}}\right) - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil + 2\right\rfloor, 0\right\}. \tag{6.3}$$

Then QKD Protocol is $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EV}})$*-secure.*

Proof. Again, the proof of correctness follows from Lemma 3.4.1, and thus we are only required to show the $(2\varepsilon_{\mathrm{AT}} + \varepsilon_{\mathrm{PA}})$-secrecy of the protocol. Recall that the QKD Protocol is such that it produces an output key of length $\ell(\hat{c}_1^n)$, and uses an error-correction protocol with number of possible transcripts given by $2^{\lambda_{\mathrm{EC}}(\hat{c}_1^n)}$, when the event $\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}$ occurs. Otherwise the protocol produces a key of length 0. Thus, we are required to obtain an upper bound on

$$\begin{aligned}\Delta = &\sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \Pr(\Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}) \times \\ &\frac{1}{2}\left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n) \wedge \Omega_{\mathrm{EV}}} \right\|_1\end{aligned} \tag{C.1}$$

where we have used our trick of noting that the states conditioned on different $\Omega(\hat{c}_1^n)$ have orthogonal support.[1]. Using the triangle inequality, and expanding in terms of the unobserved events $\vec{p}$, we obtain

$$\begin{aligned}\Delta \leq &\sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p}} \Pr(\Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}) \times \\ &\frac{1}{2}\left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} \right\|_1 \\ &= \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \in \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}) \times \\ &\frac{1}{2}\left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} \right\|_1 \\ &+ \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \notin \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}) \times \\ &\frac{1}{2}\left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} \right\|_1\end{aligned} \tag{C.2}$$

[1]Regardless, the above expression is certainly larger than the expression we seek to bound for the secrecy requirement, via the triangle inequality

where we have simply grouped the sum over $\vec{p}$ into two different terms. The first contribution

can be bounded as follows:

$$\Delta_1 \coloneqq \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p})\wedge\Omega_{\mathrm{EV}}) \tag{C.3}$$
$$\times\,\frac{1}{2}\left\|\rho_{K_A\widehat{C}_1^n C_{\mathrm{EC}}C_{\mathrm{EV}}H_{\mathrm{PA}}H_{\mathrm{EV}}\hat{\boldsymbol{E}}|\Omega(\hat{c}_1^n,\vec{p})\wedge\Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A\widehat{C}_1^n C_{\mathrm{EC}}C_{\mathrm{EV}}H_{\mathrm{PA}}H_{\mathrm{EV}}\hat{\boldsymbol{E}}|\Omega(\hat{c}_1^n,\vec{p})\wedge\Omega_{\mathrm{EV}}}\right\|_1$$
$$\le \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p})) \tag{C.4}$$
$$\times\left(2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\zeta(\hat{c}_1^n,\vec{p})}}(\mathbf{S}|\widehat{C}_1^n C_{\mathrm{EC}}C_{\mathrm{EV}}H_{\mathrm{EV}}\hat{\boldsymbol{E}})_{(\rho|\Omega(\hat{c}_1^n,\vec{p}))\wedge\Omega_{\mathrm{EV}}}-\ell(\hat{c}_1^n)+2\right)}+2\sqrt{\zeta(\hat{c}_1^n,\vec{p})}\right)$$
$$\le \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p})) \tag{C.5}$$
$$\times\left(2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\zeta(\hat{c}_1^n,\vec{p})}}(\mathbf{S}|\widehat{C}_1^n H_{\mathrm{EV}}\hat{\boldsymbol{E}})_{(\rho|\Omega(\hat{c}_1^n,\vec{p}))\wedge\Omega_{\mathrm{EV}}}-\lambda_{\mathrm{EC}}(\hat{c}_1^n)-\left\lceil\log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil-\ell(\hat{c}_1^n)+2\right)}+2\sqrt{\zeta(\hat{c}_1^n,\vec{p})}\right)$$
$$\le \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p})) \tag{C.6}$$
$$\times\left(2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\zeta(\hat{c}_1^n,\vec{p})}}(\mathbf{S}|\widehat{C}_1^n H_{\mathrm{EV}}\hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n,\vec{p})}-\lambda_{\mathrm{EC}}(\hat{c}_1^n)-\left\lceil\log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil-\ell(\hat{c}_1^n)+2\right)}+2\sqrt{\zeta(\hat{c}_1^n,\vec{p})}\right)$$
$$= \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p})) \tag{C.7}$$
$$\times\left(2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\zeta(\hat{c}_1^n,\vec{p})}}(\mathbf{S}|\widehat{C}_1^n\hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n,\vec{p})}-\lambda_{\mathrm{EC}}(\hat{c}_1^n)-\left\lceil\log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil-\ell(\hat{c}_1^n)+2\right)}+2\sqrt{\zeta(\hat{c}_1^n,\vec{p})}\right)$$
$$= \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p})) \tag{C.8}$$
$$\times\left(2^{-\frac{1}{2}\left(H_{\min}^{\sqrt{\zeta(\hat{c}_1^n,\vec{p})}}(\mathbf{S}|\widehat{C}_1^n H_{\mathrm{EV}}\hat{\boldsymbol{E}})_{\rho|\Omega(\hat{c}_1^n,\vec{p})}-\beta(\hat{c}_1^n)+2\log\frac{1}{\varepsilon_{\mathrm{PA}}}\right)}+2\sqrt{\zeta(\hat{c}_1^n,\vec{p})}\right)$$
$$\le \sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p}))\left(\varepsilon_{\mathrm{PA}}+2\sqrt{\zeta(\hat{c}_1^n,\vec{p})}\right) \tag{C.9}$$
$$\le \varepsilon_{\mathrm{PA}} + 2\sqrt{\sum_{\hat{c}_1^n:\,\ell(\hat{c}_1^n)>0}\sum_{\vec{p}\in\mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n,\vec{p}))\,\zeta(\hat{c}_1^n,\vec{p})}. \tag{C.10}$$

In Eq. (C.3), we explicitly rewrite the contribution Δ_1 as a weighted sum of trace distances conditioned on the events $\Omega(\hat{c}_1^n, \vec{p})$ and Ω_{EV}. The bound in Eq. (C.4) follows from applying the Leftover Hashing Lemma (Lemma 3.5.1) to the resulting *subnormalized* state, where the smoothing parameter depends on the conditioning event.[2] In Eq. (C.5), we apply Lemma 2.2.4 to remove the classical registers corresponding to error correction and error verification. Since the state is already conditioned on Ω_{EV}, the one bit verification response from Bob takes a deterministic value and therefore does not contribute to the entropy loss. The partial conditioning on Ω_{EV} is removed in Eq. (C.6) using Lemma 2.2.9. In Eq. (C.7) we remove the H_{EV} register without penalty, since it is completely independent of the rest of the registers (by applying data processing Lemma 2.2.10 in both directions). In Eq. (C.8), we substitute the definition of the key length $\ell(\hat{c}_1^n)$, and in Eq. (C.9) we invoke the assumed lower bound involving $\beta(\hat{c}_1^n)$ from the theorem statement. Finally, Eq. (C.10) follows from the fact that the probabilities $\Pr(\Omega(\hat{c}_1^n, \vec{p}))$ sum to at most one, together with the concavity of the square root function and Jensen's inequality, which allows the sum to be pulled inside the square root

To bound the remaining remaining term is a lot more straightforward:

$$\begin{aligned}
\Delta_2 \coloneqq & \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \notin \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}) \times \\
& \frac{1}{2} \left\| \rho_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} - \rho^{\mathrm{ideal}}_{K_A \widehat{C}_1^n C_{\mathrm{EC}} C_{\mathrm{EV}} H_{\mathrm{PA}} H_{\mathrm{EV}} \hat{\boldsymbol{E}} | \Omega(\hat{c}_1^n, \vec{p}) \wedge \Omega_{\mathrm{EV}}} \right\|_1 \\
& \leq \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \notin \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p}))
\end{aligned} \tag{C.11}$$

We can now simply combine the two bounds, and obtain

$$\begin{aligned}
\Delta &\leq \Delta_1 + \Delta_2 \\
&\leq \varepsilon_{\mathrm{PA}} + 2 \sqrt{\sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \in \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p})) \zeta(\hat{c}_1^n, \vec{p})} + \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \notin \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p})) \\
&\leq \varepsilon_{\mathrm{PA}} + 2 \sqrt{\sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \in \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p})) \zeta(\hat{c}_1^n, \vec{p}) + \sum_{\hat{c}_1^n : \ell(\hat{c}_1^n) > 0} \sum_{\vec{p} \notin \mathcal{V}(\hat{c}_1^n)} \Pr(\Omega(\hat{c}_1^n, \vec{p}))} \\
&\leq \varepsilon_{\mathrm{PA}} + 2\varepsilon_{\mathrm{AT}}.
\end{aligned} \tag{C.12}$$

[2] Here we point out a technical subtlety concerning the choice of smoothing parameter for subnormalized states. Namely, that the smoothing parameter for smooth min entropy of the state $\rho_{\wedge\Omega}$ must be smaller than $\sqrt{\Pr(\Omega)_\rho}$. In the above analysis, if this condition is not satisfied then the required bound follows trivially. Hence, the assumption that $\sqrt{\zeta(\hat{c}_1^n, \vec{p})} \leq \Pr(\Omega_{\mathrm{EV}} | \Omega(\hat{c}_1^n, \vec{p}))_\rho$.

Here we use the fact that $2\sqrt{a}+b \leq 2\sqrt{a+b}$ for $0 \leq a, b, a+b \leq 1$ in the third line, and the stated condition from the theorem for the final line. □

Remark C.1.1. *Note that the critical step here was using the concavity of the square root function to see that a bound on the average failure probability of the phase error estimation procedure is enough to prove security. This is the same fundamental trick used by Ref. [107, 108, 109]. Our presentation here is in the EUR framework, where this manifests in the deliberate choice of our smoothing parameter in the first part of the proof.*

Remark C.1.2. *Notice that in the variable-length protocol for which we proved security, the number of bits on which privacy amplification is applied is variable. It depends on the number of key generation rounds obtained in each protocol run. Some subtle issues regarding two-universal hashing on a variable-length input register were pointed out and addressed in Section 4.6. In particular, it was noted that first looking at the number of bits in the raw key, and then choosing an appropriate two-universal hashing procedure for that many input bits,* does not produce a valid two-universal hashing procedure on the input space of variable-length bit strings. *Due to this, the Leftover Hashing Lemma cannot be straightforwardly applied to such a scenario. However, this issue was addressed by showing that when the locations of the discard rounds are publicly announced, the theoretical analyses of scenarios where the rounds are actually discarded, vs mapped to special symbols such as* 0 *or* $\perp$ *(where leftover-hashing lemma can be applied), are equivalent Lemmas 4.6.1 and 4.6.2. Due to this equivalence, the PA procedure described above can be applied in QKD protocols.*

It is interesting to note that these issues are completely avoided by the above proof, in a very different manner than Section 4.6. This is because in this proof, we always apply the Leftover Hashing Lemma on a state conditioned on the specific length of the raw key register (Eq. (6.14)). Therefore, the Leftover Hashing Lemma can be applied in a straightforward manner, and there are no issues is choosing the hashing family based on the specific length of the raw key register. In other words, the PA procedure described above is valid for this proof. In a similar sense, the variable-length security proof from Chapter 4 critically relied on a technical Lemma 2.2.7, that necessitated the use of Rényi entropies instead of smooth min entropy in that analysis. However, the variable-length proof presented above takes a different approach, and does not impose the same requirements on the behavior of smooth min entropy. Again, this is due to the use of Eq. (6.14). Later, in Chapter 7 we will see an analysis using Rényi entropies that is much simpler than the one presented in Chapter 4.

C.2 Technical Statements

We first prove the two-step measurement lemma which was utilized extensively in Chapter 6 to reformulate the measurement process of the QKD protocol.

Lemma 6.3.1 (Filtering POVMs)**.** *Let $\{\Gamma_k | k \in \mathcal{A}\}$ be a POVM on a register Q, and let $\{\mathcal{A}_i\}_{i \in \mathcal{P}_\mathcal{A}}$ be a partition of $\mathcal{A}$, and let $\rho \in \mathrm{S}_=(Q)$ be a state. The classical register storing the measurement outcomes when ρ is measured using $\{\Gamma_k\}_{k \in \mathcal{A}}$ is given by*

$$\rho_{\text{final}} \coloneqq \sum_{k \in \mathcal{A}} \mathrm{Tr}(\Gamma_k \rho) \left|k\right\rangle\!\left\langle k\right| . \tag{6.15}$$

This measurement procedure is equivalent (in the sense of being the same quantum to classical channel) to the following two-step measurement procedure: First doing a coarse-grained "filtering" measurement of i, using POVM $\{\tilde{F}_i\}_{i \in \mathcal{P}_\mathcal{A}}$, where

$$\begin{aligned} \tilde{F}_i &\coloneqq \sum_{j \in \mathcal{A}_i} \Gamma_j, \qquad \textit{leading to the post-measurement state} \\ \rho'_{\text{intermediate}} &= \sum_{i \in \mathcal{P}_\mathcal{A}} \sqrt{\tilde{F}_i} \rho \sqrt{\tilde{F}_i}^\dagger \otimes \left|i\right\rangle\!\left\langle i\right| . \end{aligned} \tag{6.16}$$

Upon obtaining outcome i in the first step, measuring using POVM $\{G_k\}_{k \in \mathcal{A}_i}$ where

$$\begin{aligned} G_k &\coloneqq \sqrt{\tilde{F}_i}^+ \Gamma_k \sqrt{\tilde{F}_i}^+ + P_k \qquad \textit{leading to the post-measurement classical state} \\ \rho'_{\text{final}} &= \sum_{i \in \mathcal{P}_\mathcal{A}} \sum_{k \in \mathcal{A}_i} \mathrm{Tr}\left(G_k \sqrt{\tilde{F}_i} \rho \sqrt{\tilde{F}_i} \right) \left|k\right\rangle\!\left\langle k\right| , \end{aligned} \tag{6.17}$$

where F^+ denotes the pseudo-inverse of F, and P_k are any positive operators satisfying $\sum_{k \in \mathcal{A}_i} P_k = \mathbb{I} - \Pi_{\tilde{F}_i}$, where $\Pi_{\tilde{F}_i}$ denotes the projector onto the support of $\tilde{F}_i$.

Proof. Observe that $\{\tilde{F}_i | i \in \mathcal{P}_\mathcal{A}\}$ is a valid set of POVMs by construction. Moreover, $\{G_k | k \in \mathcal{A}_i\}$ is a valid set of POVMs for each i, also by construction. Thus we only need to show that $\rho_{\text{final}} = \rho'_{\text{final}}$. Using the cyclicity of trace in Eq. (6.17), it suffices to prove

$$\sqrt{\tilde{F}_i} G_k \sqrt{\tilde{F}_i} = \Gamma_k \quad \forall i \in \mathcal{P}_\mathcal{A}, \forall k \in \mathcal{A}_i. \tag{C.13}$$

Substituting the expression for F_k into the above equation, we obtain

$$\begin{aligned}\sqrt{\tilde{F}_i}G_k\sqrt{\tilde{F}_i} &= \sqrt{\tilde{F}_i}\left(\sqrt{\tilde{F}_i}^{+}\Gamma_k\sqrt{\tilde{F}_i}^{+} + P_k\right)\sqrt{\tilde{F}_i} \\ &= \sqrt{\tilde{F}_i}\left(\sqrt{\tilde{F}_i}^{+}\Gamma_k\sqrt{\tilde{F}_i}^{+}\right)\sqrt{\tilde{F}_i} \\ &= \Pi_{\tilde{F}_i}\Gamma_k\Pi_{\tilde{F}_i} \\ &= \Gamma_k,\end{aligned} \tag{C.14}$$

where the second equality follows from the fact that P_k and $\tilde{F}_i$ have orthogonal supports, and the final equality uses the fact that the support for $\tilde{F}_i$ is larger than the support for Γ_k for $k \in \mathcal{A}_i$. This concludes the proof. □

We will now turn our attention to technical statements needed to replace the smooth max entropy term (of two classical strings) with a suitable function of the error rate between those two strings.

Lemma C.2.1 ([34, Lemma 7])**.** *Let $\rho_{CQ} \in S_{\leq}(CQ)$ be classical in C, and let Ω be any event on C such that $\Pr(\Omega)_\rho \leq \varepsilon$. Then there exists a sub-normalized state $\tilde{\rho}_{CQ} \in S_{\leq}(CQ)$ with $\Pr(\Omega)_{\tilde{\rho}} = 0$, and $P(\rho, \tilde{\rho}) \leq \sqrt{\varepsilon}$, where P denotes the purified distance (see Definition 2.1.11).*

We use the above lemma in the proof of the following statement. The following statement allows us to replace the smooth max entropy term in the EUR statement with our bound on the phase error rate. The proof is basically the same as the proof of [34, Proposition 8].

Lemma C.2.2. *Let $\rho \in S_{\leq}(XY)$ where X, Y store n-bit strings, and let $\boldsymbol{e}_{XY}$ denote the error rate in these strings. Let Ω be any event such that $\boldsymbol{e}_{XY} > e_{max}$, and let $\Pr(\Omega)_\rho \leq \kappa$. For any $e_{max} < 1/2$, we have*

$$H_{\max}^{\sqrt{\kappa}}(X|Y)_\rho \leq nh(e_{max}) \tag{C.15}$$

Proof. By Lemma C.2.1, there exists a state $\tilde{\rho}_{XY}$ such that $\Pr(\Omega)_{\tilde{\rho}} = 0$ and $P(\rho, \tilde{\rho}) \leq \sqrt{\kappa}$.

Therefore we have

$$\begin{aligned} H_{\max}^{\sqrt{\kappa}}(X|Y)_\rho &\leq H_{\max}(X|Y)_{\tilde{\rho}} \\ &= \log\left(\sum_{y\in\{0,1\}^n} \Pr(Y=y)_{\tilde{\rho}} 2^{H_{\max}(X|Y)_{\tilde{\rho}|Y=y}}\right) \\ &\leq \max_{y\in\{0,1\}^n} H_{\max}(X|Y)_{\tilde{\rho}|Y=y} \\ &= \max_{y\in\{0,1\}^n} \log\left|\left\{x\in\{0,1\}^n : \Pr(X=x\wedge Y=y)_{\tilde{\rho}} > 0\right\}\right| \\ &\leq \log\left(\sum_{k=0}^{ne_{\max}} \binom{n}{k}\right), \\ &\leq \log\left(2^{nh(e_{\max})}\right) \end{aligned} \tag{C.16}$$

where we used the definition of the smooth max entropy in the first inequality, and [165, Sec. 4.3.2] for the second equality. The third inequality and the fourth equality follow from the definitions. The fifth inequality follows from the fact that the state $\tilde{\rho}$ is guaranteed to have $\leq ne_{\max}$ errors, while the final inequality follows from the suitable bound on the sum of binomial coefficients. □

C.3 Sampling

In this section, we prove the technical statements needed to prove our sampling bounds.

C.3.1 Random Sampling

We start with the usual Serfling [143] statement in the following lemma. The following lemma is obtained from [34, Eq. 74, Lemma 6]

Lemma C.3.1 (Serfling)**.** *Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_{m+n}$ be bit-valued random variables. Let $\boldsymbol{J}_m$ denote the choice of a uniformly random subset of m positions, out of $m+n$ positions. Then,*

$$\begin{aligned} \Pr\left(\sum_{i\notin\boldsymbol{J}_m} \frac{\boldsymbol{X}_i}{n} \geq \sum_{i\in\boldsymbol{J}_m} \frac{\boldsymbol{X}_i}{m} + \gamma_{serf}\right) &\leq e^{-2\gamma_{serf}^2 f_{\text{serf}}(m,n)}, \\ f_{\text{serf}}(m,n) &:= \frac{nm^2}{(n+m)(m+1)}. \end{aligned} \tag{C.17}$$

Serfling basically states that if one chooses a random set of positions, then the fraction of 1s in those positions gives us a good estimate of the fraction of 1s in the remaining positions. However, observe that the sampling procedure in the protocol from Sections 6.3.3 and 6.4.4 does not actually choose a random subset of fixed-length for testing. Instead, the protocol decides to map each conclusive round to test or key in an IID manner. Therefore, the application of the Serfling bound is not straightforward. In the following lemma, we show how the Serfling bound can still be rigorously used.

Lemma 6.3.2 (Serfling with IID sampling)**.** *Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_n$ be bit-valued random variables. Suppose each position i is mapped to the "test set" ($i \in \boldsymbol{J}_t$) with probability p_t, and the "key set" ($i \in \boldsymbol{J}_k$) with probability p_k. Let $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$ be the event that exactly n_{X} positions are mapped to test, and exactly n_{K} positions are mapped to key. Then, conditioned on the event $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$, the following statement is true:*

$$\Pr\left(\sum_{i\in\boldsymbol{J}_k}\frac{\boldsymbol{X}_i}{n_{\mathsf{K}}} \geq \sum_{i\in\boldsymbol{J}_t}\frac{\boldsymbol{X}_i}{n_{\mathsf{X}}} + \gamma_{\mathrm{serf}}\right)_{|\Omega(n_{\mathsf{X}},n_{\mathsf{K}})} \leq e^{-2\gamma_{\mathrm{serf}}^2 f_{\mathrm{serf}}(n_{\mathsf{X}},n_{\mathsf{K}})}, \tag{6.19}$$

$$f_{\mathrm{serf}}(n_{\mathsf{X}}, n_{\mathsf{K}}) \coloneqq \frac{n_{\mathsf{K}} n_{\mathsf{X}}^2}{(n_{\mathsf{K}} + n_{\mathsf{X}})(n_{\mathsf{X}} + 1)}.$$

Proof. Since the sampling procedure randomly assigns each bit to test or key (or does nothing with them if $p_t + p_k < 1$), Lemma C.3.1 cannot be directly applied. However, consider what happens if we condition on the event $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$. Then, for a given set of positions that form the $n_{\mathsf{X}} + n_{\mathsf{K}}$ positions selected for test or key, it is the case that each set of n_{X} positions is equally likely. Therefore, the above sampling procedure is exactly equivalent to:

1. First determining the event $\Omega(n_{\mathsf{X}}, n_{\mathsf{K}})$ by sampling from *some* probability distribution.
2. Pick some $n_{\mathsf{X}} + n_{\mathsf{K}}$ positions at random.
3. Then determining the exact positions of the n_{X} test rounds, by choosing a random subset of fixed-size n_{X} out of these $n_{\mathsf{X}} + n_{\mathsf{K}}$ positions.

The necessary claim follows by applying Lemma C.3.1 for step 3 of the above procedure. □

C.3.2 Sampling with imperfect detectors

We now turn our attention to proving Lemma 6.4.1, which is the main statement utilized in extending the EUR approach to imperfect detectors in Section 6.4. We start by proving Lemmas C.3.2 and 6.4.2 which we use later in the proof of Lemma C.3.3.

Recall our notation: If $\rho_{Q^n} \in S{=}(Q^{\otimes n})$ is an arbitrary state, and $\{P_1, P_2, \ldots, P_m\}$ is a set of POVM elements, then we let $\boldsymbol{N}_{P_i}$ denote the classical random variable corresponding to the number of measurement outcomes corresponding to P_i when the state ρ_{Q^n} is measured. Moreover, let $\boldsymbol{D}_P$ denote the classical random variable that describes the measurement outcomes when each subsystem of ρ is measured using $\{P_1, P_2, \ldots, P_m\}$. We use $S \sim \boldsymbol{D}_P$ to denote the statement S is sampled from $\boldsymbol{D}_P$.

Lemma C.3.2. *Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I - P\}$ and $\{P', I - P'\}$ be two sets of POVM elements such that $P \leq P'$. Then, for any e, it is the case that*

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) \leq \Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e\right) \tag{C.18}$$

Proof. We will describe a procedure to generate random strings S, S' such that $S \sim \boldsymbol{D}_P, S' \sim \boldsymbol{D}'_P$. Consider the POVM $\{P, P' - P, I - P'\}$, and let T be the classical string taking values in $\{0, 1, 2\}^n$ which stores the measurement outcomes when measured using this POVM. Then, S, S' can be obtained by first obtaining T, followed by the following remapping

$$(S_i, S'_i) = \begin{cases} (1,1) & T_i = 0 \\ (0,1) & T_i = 1 \\ (0,0) & T_i = 2 \end{cases}$$

where i denotes the position in the string. The required claim follows from the observation that the above procedure maps more S'_i to 1 than S_i. Thus,

$$\Pr(w(\boldsymbol{S}') \geq w(\boldsymbol{S})) \geq 0 \implies \Pr(w(\boldsymbol{S}') > ne) \geq \Pr(w(\boldsymbol{S}) \geq ne) \tag{C.19}$$

where w denotes the hamming weight of the string (sum of each element of the string). The necessary statement follows after noting that $w(S) \sim \boldsymbol{N}_P$ and $w(S') \sim \boldsymbol{N}_{P'}$ (which can be argued rigorously using the two-step measurement Lemma 6.3.1). □

Remark C.3.1. *Note a conceptual subtlety in the above proof: The procedure used to generate S, S' in the above proof has some joint probability distribution associated to it. This means that (S, S') is a well-defined random variable. However, one cannot talk about*

the joint probability distribution of two different sets of measurement on the same quantum state. This subtle issue is avoided by noting that we are only interested in making statements on the marginal probability distribution of S and S', and how they relate to one another. And it is indeed true that these distributions satisfy $S \sim \boldsymbol{D}_P$ and $S' \sim \boldsymbol{D}_{P'}$, which is enough to prove our claim. The fact that S, S' has some joint distribution associated with it is immaterial.

Lemma 6.4.2 (Small POVM measurement)**.** *Let $\rho_{Q^n} \in \mathrm{S}_=(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I - P\}$ be a POVM such that $\|P\|_\infty \leq \delta$. Then*

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq \delta + c\right) \leq F_{\mathrm{bin}}(n, \delta, c) \coloneqq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}, \tag{6.37}$$

where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathbb{I} - P\}$.

Proof. Since $\|P\|_\infty \leq \delta$, we have $P \leq \delta I$. By Lemma C.3.2, we have

$$\Pr\left(\frac{\boldsymbol{N}_P}{n} \geq \delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_{\delta I}}{n} \geq \delta + c\right) \tag{C.20}$$

Observe that measurement using $\{\delta I, (1-\delta) I\}$ is equivalent to Bernoulli sampling. Thus $\boldsymbol{N}_{\delta I}$ obeys the binomial distribution. Therefore,

$$\Pr\left(\frac{\boldsymbol{N}_{\delta I}}{n} \geq \delta + c\right) \leq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}. \tag{C.21}$$

□

Lemma C.3.3. *Let $\rho_{Q^n} \in S_\circ(Q^{\otimes n})$ be an arbitrary state. Let $\{P, I - P\}$ and $\{P', I - P'\}$ be two sets of POVM elements. Suppose there exists a $0 \leq \tilde{P} \leq I$ such that $P \leq \tilde{P}, P' \leq \tilde{P}$, and $\left\|\tilde{P} - P\right\|_\infty \leq \delta$. Then*

$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + (\delta + c)\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F_{\mathrm{bin}}(n, \delta, c), \tag{C.22}$$

where $F_{\mathrm{bin}}(n, \delta, c)$ was defined in Lemma 6.4.2.

Proof. We will describe a process to generate $S \sim \boldsymbol{D}_P$ and $\tilde{S} \sim \boldsymbol{D}_{\tilde{P}}$, in a similar manner as in the proof of Lemma C.3.2. In particular, let T be the random variable taking values in $\{0,1,2\}^n$ that stores the measurement outcomes of $\{P, \tilde{P} - P, I - \tilde{P}\}$ measurements. We generate $S, \tilde{S}$ by first obtaining T, followed by the following remapping

$$(S_i, \tilde{S}_i) = \begin{cases} (1,1) & T_i = 0 \\ (0,1) & T_i = 1 \\ (0,0) & T_i = 2. \end{cases}$$

Then,

$$\begin{aligned} \Pr(\boldsymbol{N}_{\tilde{P}} \geq ne + n(\delta + c)) &= \Pr\Big(w(\tilde{\boldsymbol{S}}) \geq ne + n(\delta + c)\Big) \\ &= \Pr\Big(w(\tilde{\boldsymbol{S}}) \geq ne + n(\delta + c) \cap w(\boldsymbol{S}) \geq ne\Big) \\ &+ \Pr\Big(w(\tilde{\boldsymbol{S}}) \geq ne + n(\delta + c) \cap w(\boldsymbol{S}) < ne\Big) \\ &\leq \Pr(w(\boldsymbol{S}) \geq ne) + \Pr\Big(w(\tilde{\boldsymbol{S}}) - w(\boldsymbol{S}) \geq n(\delta + c)\Big) \\ &= \Pr(\boldsymbol{N}_P \geq ne) + \Pr\big(\boldsymbol{N}_{\tilde{P}-P} \geq n(\delta + c)\big) \\ &\leq \Pr(\boldsymbol{N}_P \geq ne) + F_{\text{bin}}(n, \delta, c). \end{aligned} \tag{C.23}$$

where we used Lemma 6.4.2 in the final inequality, the fact that $w(S) \sim \boldsymbol{N}_P$ and $w(\tilde{S}) - w(S) = w(\tilde{S} - S) \sim \boldsymbol{N}_{\tilde{P}-P}$ ($\tilde{S}_i - S_i = 1$ if and only if $T_i = 1$) for the penultimate inequality, and basic properties of probabilities for the remaining steps. Next, we replace the $\tilde{P}$ with P' using Lemma C.3.2 and $\tilde{P} \geq P'$, and obtain

$$\Pr(\boldsymbol{N}_{P'} \geq ne + n(\delta + c)) \leq \Pr(\boldsymbol{N}_{\tilde{P}} \geq ne + n(\delta + c)). \tag{C.24}$$

The proof follows after noting that Eqs. (C.23) and (C.24) $\implies$ Eq. (C.22). □

Lemma C.3.3 above requires an explicit construction of a $\tilde{P}$ satisfying the necessary requirements. However, this requirement can be removed, and we obtain a sightly worse result with greater generality below.

Lemma 6.4.1 (Similar measurements lead to similar observed frequencies)**.** *Let $\rho_{Q^n} \in \mathrm{S}_{=}(Q^{\otimes n})$ be an arbitrary state. Let $\{P, \mathbb{I} - P\}$ and $\{P', \mathbb{I} - P'\}$ be two sets of POVM elements, such that $\|P' - P\|_\infty \leq \delta$. Then,*

$$\Pr\left(\frac{\boldsymbol{N}_{P'}}{n} \geq e + 2\delta + c\right) \leq \Pr\left(\frac{\boldsymbol{N}_P}{n} \geq e\right) + F_{\text{bin}}(n, 2\delta, c), \tag{6.32}$$

for $e \in [0,1]$, where $\boldsymbol{N}_P$ is the number of P-outcomes when each subsystem of ρ_{Q^n} is measured using POVM $\{P, \mathbb{I} - P\}$, and

$$F_{\text{bin}}(n, \delta, c) \coloneqq \sum_{i=n(\delta+c)}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i}. \tag{6.33}$$

Proof. Let $G' = (1-\delta)P'$, and $G = (1-\delta)P$. Using $0 \leq G \leq P$ and Lemma C.3.2, we obtain

$$\Pr(\boldsymbol{N}_G \geq ne) \leq \Pr(\boldsymbol{N}_P \geq ne). \tag{C.25}$$

Using $0 \leq G' + \delta I \leq I$, $G' + \delta I \geq G$, $\|G' + \delta I - G\|_\infty \leq \delta + \delta(1-\delta) \leq 2\delta$, and Eq. (C.23), we obtain

$$\Pr(\boldsymbol{N}_{G'+\delta I} \geq ne + n(2\delta + c)) \leq \Pr(\boldsymbol{N}_G \geq ne) + F_{\text{bin}}(n, 2\delta, c), \tag{C.26}$$

Finally, using $G' + \delta I \geq P'$, and Lemma C.3.2, we obtain

$$\Pr(\boldsymbol{N}_{P'} \geq ne + n(2\delta + c)) \leq \Pr(\boldsymbol{N}_{G'+\delta I} \geq ne + n(2\delta + c)). \tag{C.27}$$

The proof follows from the observation that Eqs. (C.25) to (C.27) $\implies$ Eq. (6.32). □

Remark C.3.2. *The statements above are written for a measurement procedure where the same POVM is used to measure each round of the state. However the proofs do not actually use this fact. The same proofs are valid even if the measurement for each round is done using a different POVM element (as long it satisfies the required bounds on the ∞-norm). The proofs are identical, and the statements are stated formally in [2, Appendix C3].*

C.4 Combining bounds

In this section, we will combine Eqs. (6.28), (6.31), (6.36) and (6.39) and obtain Eq. (6.40). This process is simply some cumbersome algebra and the use of the union bound for probabilities.

Combining Eqs. (6.28) and (6.31), we obtain

$$
\begin{aligned}
&\Pr\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{XX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\
&= \Pr\Big(\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{XX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\Big) \bigcap \big(\tilde{\boldsymbol{e}}^{\text{obs}}_{\mathbf{XX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}}\big)\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\
&+ \Pr\Big(\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{XX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\Big) \bigcap \big(\tilde{\boldsymbol{e}}^{\text{obs}}_{\mathbf{XX}} < \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}}\big)\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\
&\leq \Pr\big(\tilde{\boldsymbol{e}}^{\text{obs}}_{\mathbf{XX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}}\big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} + \Pr\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{XX}} \geq \tilde{\boldsymbol{e}}^{\text{obs}}_{\mathbf{XX}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\
&\leq \varepsilon^2_{\text{AT-a}}.
\end{aligned}
\tag{C.28}
$$

We will now combine Eqs. (C.28) and (6.36). To do so we will additionally need to condition on $e^{\text{obs}}_{\mathsf{X}}$. However, note that Eq. (6.36) remains true with this additional conditioning (because $e^{\text{obs}}_{\mathsf{X}}$ is observed on a different set of rounds). Thus we obtain

$$
\begin{aligned}
&\Pr\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{ZX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\text{bin}}(\tilde{n}_{\mathsf{K}}, \delta_1)\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} \\
&= \sum_{e^{\text{obs}}_{\mathsf{X}}} \Pr\big(\Omega(e^{\text{obs}}_{\mathsf{X}})|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\big) \Pr\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{ZX}} \geq e^{\text{obs}}_{\mathsf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma^{\varepsilon_{\text{AT-b}}}_{\text{bin}}(\tilde{n}_{\mathsf{K}}, \delta_1)\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}},e^{\text{obs}}_{\mathsf{X}})} \\
&\leq \sum_{e^{\text{obs}}_{\mathsf{X}}} \Pr\big(\Omega(e^{\text{obs}}_{\mathsf{X}})|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\big) \Pr\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{XX}} \geq e^{\text{obs}}_{\mathsf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}},e^{\text{obs}}_{\mathsf{X}})} + \frac{\varepsilon^2_{\text{AT-b}}}{2} \\
&= \Pr\Big(\tilde{\boldsymbol{e}}^{\text{key}}_{\mathbf{XX}} \geq \boldsymbol{e}^{\mathbf{obs}}_{\mathbf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})\Big)_{|\Omega(\tilde{n}_{\mathsf{X}},\tilde{n}_{\mathsf{K}})} + \frac{\varepsilon^2_{\text{AT-b}}}{2} \\
&\leq \varepsilon^2_{\text{AT-a}} + \varepsilon^2_{\text{AT-b}}.
\end{aligned}
\tag{C.29}
$$

where the first equality follows from the definition of conditional probability. The second inequality is obtained by setting $e = e^{\text{obs}}_{\mathsf{X}} + \gamma^{\varepsilon_{\text{AT-a}}}_{\text{serf}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})$ in Eq. (6.36), the third equality follows from the definition of probability and the final inequality follows from Eq. (C.28)

Combing Eqs. (C.29) and (6.39), we obtain

$$
\begin{aligned}
&\Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \frac{\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}} + \gamma_{\mathrm{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_{\mathsf{K}}, \delta_1)}{(1 - \delta_2 - \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_{\mathsf{K}}, \delta_2))}\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} \\
&= \Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \frac{\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}} + \gamma_{\mathrm{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_{\mathsf{K}}, \delta_1)}{1 - \delta_2 - \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_{\mathsf{K}}, \delta_2)}\right. \\
&\qquad \left.\bigcap \left(\tilde{\boldsymbol{e}}_{\mathsf{ZX}}^{\mathrm{key}} \leq \boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}\left(1 - \delta_2 - \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_{\mathsf{K}}, \delta_2)\right)\right)\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} \\
&\Pr\left(\boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}} \geq \frac{\boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}} + \gamma_{\mathrm{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_{\mathsf{K}}, \delta_1)}{1 - \delta_2 - \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_{\mathsf{K}}, \delta_2)}\right. \\
&\qquad \left.\bigcap \left(\tilde{\boldsymbol{e}}_{\mathsf{ZX}}^{\mathrm{key}} > \boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}\left(1 - \delta_2 - \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_{\mathsf{K}}, \delta_2)\right)\right)\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} = \\
&\leq \Pr\left(\tilde{\boldsymbol{e}}_{\mathsf{ZX}}^{\mathrm{key}} \leq \boldsymbol{e}_{\mathsf{X}}^{\mathbf{key}}(1 - \delta_2 - \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-c}}}(\tilde{n}_{\mathsf{K}}, \delta_2))\right)_{|\Omega(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}})} \\
&+ \Pr\left(\tilde{\boldsymbol{e}}_{\mathsf{ZX}}^{\mathrm{key}} \geq \boldsymbol{e}_{\mathsf{X}}^{\mathbf{obs}} + \gamma_{\mathrm{serf}}^{\varepsilon_{\text{AT-a}}}(\tilde{n}_{\mathsf{X}}, \tilde{n}_{\mathsf{K}}) + \delta_1 + \gamma_{\mathrm{bin}}^{\varepsilon_{\text{AT-b}}}(\tilde{n}_{\mathsf{K}}, \delta_1)\right) \leq \varepsilon_{\text{AT-a}}^2 + \varepsilon_{\text{AT-b}}^2 + \varepsilon_{\text{AT-c}}^2,
\end{aligned}
$$

which is the required result.

C.5 Decoy Analysis

In this section, we perform the decoy analysis from Chapter 6. Let O denote a specific outcome of a given round, and let n_O denote the number of rounds that resulted in the outcome O. For instance, it could denote that both Alice and Bob measured in the X basis and obtained a detection (in which case $n_O = n_{\mathsf{X}}$). We will perform a general decoy analysis for any outcome O. Let n_{O,μ_k} denote the number of rounds that resulted in the outcome O where Alice used intensity μ_k. We have access to this information during the protocol. Let $n_{O,m}$ denote the number of rounds that resulted in the outcome O where Alice prepared a state of m photons. We wish to obtain bounds on $n_{O,m}$ using n_{O,μ_k}.

In practice, Alice first chooses an intensity μ_k of the pulse, which then determines the photon number m of the pulse, via the Poissonian distribution, independently for each round. Thus we have

$$
p_{m|\mu_k} = e^{-\mu_k}\frac{\mu_k^m}{m!}. \tag{C.30}
$$

The probability of m-photons being emitted, can be obtained via

$$\tau_m = \sum_{\mu_k} p_{\mu_k} p_{m|\mu_k} = \sum_{\mu_k} p_{\mu_k} e^{-\mu_k} \frac{\mu_k^m}{m!}. \tag{C.31}$$

Now, without loss of generality, we can view Alice as *first* choosing the photon number m, and *then* choosing a intensity setting μ_k with probability given by

$$p_{\mu_k|m} = p_{\mu_k} p_{m|\mu_k} / \tau_m. \tag{C.32}$$

This is the fundamental idea used by [97, 145, 155]. In this case, due to the fact that each signal is mapped to an intensity independently of other signals, one can apply the Hoeffdings inequality to these independent events, and obtain

$$\Pr\left(\left| \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}} \right| \geq \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2} \ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2} \right)} \right) \leq \varepsilon_{\text{AT-d}}^2. \tag{C.33}$$

Remark C.5.1. *The application of Hoeffdings inequality here is subtle, and is made rigorous in Lemmas C.5.1 and C.5.2 in Section C.5.2 (see also Ref. [155]). Note that in general, the photon numbers of every pulse in the protocol are chosen independently, since Alice chooses intensity independently for each pulse. However, here we are interested in photon numbers corresponding to rounds that led to a specific outcome O. Since we postselect pulses based on the outcome, we can no longer claim that the photon numbers of these pulses (pulses that led to outcome O) are sampled independently, or that intensities of these pulses are chosen independently. This is because they now depend on Eve's attack. Rather, Lemmas C.5.1 and C.5.2 rely on exploiting the fact that conditioned on any fixed sequence of photon numbers of the pulses, the intensities are chosen independently of one another. One can therefore apply Hoeffdings inequality. Then, since the resulting statements holds for any fixed sequence of photon numbers, the conditioning on this event can be removed.*

We can now combine Eq. (C.33) for all intensities μ_k using the union bounds for probabilities ($\Pr(\Omega_1 \wedge \Omega_2) \geq 1 - \Pr(\Omega_1^c) - \Pr(\Omega_2^c)$). Reformulating the expressions, we obtain

$$\Pr\left(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2} \ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2} \right)} \leq \sum_{m=0}^{\infty} p_{\mu_k|m} \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}} \leq \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} + \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2} \ln\left(\frac{2}{\varepsilon_{\text{AT-d}}^2} \right)} \quad \forall k \in \{1,2,3\} \right)$$
$$\geq 1 - 3\varepsilon_{\text{AT-d}}^2. \tag{C.34}$$

To obtain Eq. (6.45), we will apply decoy analysis (Eq. (C.34)) for three separate events: conclusive Z basis rounds selected for key generation (denoted by K), conclusive X basis rounds (denoted by X), and conclusive X basis rounds leading to an error (denoted by $X_{\neq}$). Then, Eq. (C.34) can be applied these events (again using the union bound for probabilities) to obtain:

$$\Pr\left(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} - \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)} \leq \sum_{m=0}^{\infty} p_{\mu_k|m}\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{m}} \leq \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} + \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)} \right.$$
$$\left. \forall k \in \{1,2,3\}, \quad \forall O \in \{X_{\neq}, X, K\}\right) \geq 1 - 9\varepsilon^2_{\text{AT-d}}. \tag{C.35}$$

Let $\mathcal{S}_{\text{constraints}}$ denote the set of inequalities inside the probability in the above expressions. Therefore we have $\Pr(\mathcal{S}_{\text{constraints}}) \geq 1 - 9\varepsilon^2_{\text{AT-d}}$.

C.5.1 Bounds on zero and one photon statistics

For any event $O \in \{X, X_{\neq}, K\}$, the relevant bounds on the zero-photon and single-photon components can be obtained by algebraic manipulation of the expressions in $\mathcal{S}_{\text{constraints}}$. In general, any method for bounding the relevant zero-photon and single-photon components using $\mathcal{S}_{\text{constraints}}$ suffices. In this work, we follow exactly the steps taken by Ref. [97, Appendix A] to obtain these bounds. Thus, we only write the final expressions here. We define

$$\boldsymbol{n}^{\pm}_{\boldsymbol{O},\boldsymbol{\mu_k}} \coloneqq \frac{e^{\mu_k}}{p_{\mu_k}}\left(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu_k}} \pm \sqrt{\frac{\boldsymbol{n}_{\boldsymbol{O}}}{2}\ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)}\right) \tag{C.36}$$

The lower bound on the zero-photon component is given by [97, Eq. 2]

$$\mathcal{S}_{\text{constraints}} \implies \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{0}} \geq \mathcal{B}^{\text{decoy}}_{\text{min}-0}(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}}) \coloneqq \tau_0 \frac{\mu_2 \boldsymbol{n}^{-}_{\boldsymbol{O},\boldsymbol{\mu_3}} - \mu_3 \boldsymbol{n}^{+}_{\boldsymbol{O},\boldsymbol{\mu_2}}}{\mu_2 - \mu_3}. \tag{C.37}$$

The lower bound on the one-photon component is given by [97, Eq. 3]

$$\mathcal{S}_{\text{constraints}} \implies \boldsymbol{n}_{\boldsymbol{O},\boldsymbol{1}} \geq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}}) \coloneqq \left(\frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3) - \mu_2^2 + \mu_3^2}\right) \times$$
$$\left(\boldsymbol{n}^{-}_{\boldsymbol{O},\boldsymbol{\mu_2}} - \boldsymbol{n}^{+}_{\boldsymbol{O},\boldsymbol{\mu_3}} - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2}\left(\boldsymbol{n}^{+}_{\boldsymbol{O},\boldsymbol{\mu_1}} - \mathcal{B}^{\text{decoy}}_{\text{min}-0}(\boldsymbol{n}_{\boldsymbol{O},\boldsymbol{\mu}_{\vec{\boldsymbol{k}}}})/\tau_0\right)\right). \tag{C.38}$$

The upper bound on the one-photon component is given by [97, Eq. 4]

$$\mathcal{S}_{\text{constraints}} \implies \boldsymbol{n_{O,1}} \leq \mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n_{O,\mu_{\vec{k}}}}) \coloneqq \tau_1 \frac{\boldsymbol{n^{+}_{O,\mu_2}} - \boldsymbol{n^{-}_{O,\mu_3}}}{\mu_2 - \mu_3}. \tag{C.39}$$

Since $\Pr(\mathcal{S}_{\text{constraints}}) \geq 1 - 9\varepsilon^2_{\text{AT-d}}$, and Eqs. (C.37) to (C.39) follow from the expressions in $\mathcal{S}_{\text{constraints}}$, we obtain

$$\Pr\left(e^{\text{obs}}_{\mathbf{X},\mathbf{1}} \geq \frac{\mathcal{B}^{\text{decoy}}_{\text{max}-1}(\boldsymbol{n_{\mathbf{X}\neq,\mu_{\vec{k}}}})}{\mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{\mathbf{X},\mu_{\vec{k}}}})} \quad \vee \quad \boldsymbol{n_{\mathbf{X},1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{\mathbf{X},\mu_{\vec{k}}}}) \quad \vee \quad \boldsymbol{n_{\mathbf{K},1}} \leq \mathcal{B}^{\text{decoy}}_{\text{min}-1}(\boldsymbol{n_{\mathbf{K},\mu_{\vec{k}}}})\right) \leq 9\varepsilon^2_{\text{AT-d}} \tag{C.40}$$

C.5.2 Rigorous use of Hoeffdings

In this section, we will rigorously justify the application of Hoeffdings concentration inequality [166] in the decoy analysis of this work. To do so, we will first state the following general lemma.

Lemma C.5.1. *Let $\boldsymbol{X}_1 \dots \boldsymbol{X}_n$ be random variables. Let X_i be a specific value taken by the random variable $\boldsymbol{X}_i$. For each i, a new random variable $\boldsymbol{Y}_i$ is generated from X_i via the probability distribution $\Pr(\boldsymbol{Y}_i|X_i)$. Then*

$$\Pr\left(\left|\sum_i (\boldsymbol{Y}_i)_{|\Omega(X_1\dots X_{n_O})} - \mathrm{E}\left(\sum_i (\boldsymbol{Y}_i)_{|\Omega(X_1\dots X_{n_O})}\right)\right| \geq t\right) \leq 2\exp\left\{\frac{-2t^2}{\sum_i (b_i - a_i)^2}\right\} \tag{C.41}$$

where $[a_i, b_i]$ denotes the range of $\boldsymbol{Y}_i$, and E denotes the expectation value. (Note that we do not require the $\boldsymbol{X}_i$s to be independent random variables, nor do we require the $\boldsymbol{Y}_i$s to be independent random variables).

Proof. Fix a specific sequence $X_1 \dots X_n$ of values taken by the random variables $\boldsymbol{X}_i$s. The variables $\boldsymbol{Y}_i$, conditioned on this specific input $X_1 \dots X_n$, are then *independent* random variables (since they are generated by $\Pr(\boldsymbol{Y}_i|X_i)$). Thus, Hoeffding's inequality applies.

□

The above lemma is utilized to perform decoy analysis in the following lemma.

Lemma C.5.2. *In the decoy-state QKD protocol of Section 6.5, fix an outcome O, and intensity μ_k. Then, we have*

$$\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m}\boldsymbol{n_{O,m}}\right| \geq \sqrt{\frac{\boldsymbol{n_O}}{2}\ln\left(\frac{2}{\varepsilon_{AT\text{-}d}^2}\right)}\right) \leq \varepsilon_{AT\text{-}d}^2. \tag{C.42}$$

Proof. Consider all the rounds where O is observed. Condition on the event that n_O such rounds are observed. Let $X_1 \dots X_{n_O}$ be the sequence of photon numbers of Alice's signals corresponding to these rounds. Condition further on the event that a specific sequence $X_1 \dots X_{n_O}$ is observed.

Fix an intensity μ_k of interest. Define $\boldsymbol{Y}_i$ as

$$\boldsymbol{Y}_i \coloneqq \begin{cases} 1 & \text{if intensity } \mu_k \text{ is assigned to the } i\text{th round} \\ 0 & \text{if intensity } \mu_k \text{ is not assigned to the } i\text{th round.} \end{cases} \tag{C.43}$$

Since the intensity of each round is chosen from a probability distribution that only depends on the photon number of each round, each $\boldsymbol{Y}_i$ is generated independently via $\Pr(\boldsymbol{Y}_i|X_i)$. By the construction of $\boldsymbol{Y}_i$s, $\sum_i \boldsymbol{Y}_i = \boldsymbol{n_{O,\mu_k}}$. By the construction of X_is, $|\{i|X_i = m\}| = n_{O,m}$. Then $\mathrm{E}\left(\sum_i(\boldsymbol{Y}_i|X_i)\right) = \sum_{m=0}^{\infty} p_{\mu_k|m} n_{O,m}$. Applying Lemma C.5.1, we directly obtain

$$\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} n_{O,m}\right| \geq t\right)_{|\Omega(X_1 \dots X_{n_O}, n_O)} \leq 2\exp\left\{\frac{-2t^2}{n_O}\right\}. \tag{C.44}$$

The above statement is valid for all $X_1 \dots X_{n_O}$ compatible with $n_O, n_{O,\vec{m}}$. We now obtain a statement that only conditions on n_O via

$$\begin{aligned}
&\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m}\boldsymbol{n_{O,m}}\right| \geq t\right)_{|\Omega(n_O)} \\
&= \sum_{X_1 \dots X_{n_O}} \Pr(\Omega(X_1 \dots X_{n_O})|\Omega(n_O)) \Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} n_{O,m}\right| \geq t\right)_{|\Omega(X_1 \dots X_{n_O}, n_O)} \\
&\leq \sum_{X_1 \dots X_{n_O}} \Pr(\Omega(X_1 \dots X_{n_O})|\Omega(n_O)) 2\exp\left\{\frac{-2t^2}{n_O}\right\} \\
&= 2\exp\left\{\frac{-2t^2}{n_O}\right\}.
\end{aligned} \tag{C.45}$$

Setting $t = \sqrt{\frac{n_O}{2} \ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)}$, we obtain

$$\Pr\left(\left|\boldsymbol{n_{O,\mu_k}} - \sum_{m=0}^{\infty} p_{\mu_k|m} \boldsymbol{n_{O,m}}\right| \geq \sqrt{\frac{n_O}{2} \ln\left(\frac{2}{\varepsilon^2_{\text{AT-d}}}\right)}\right)_{|\Omega(n_O)} \leq \varepsilon^2_{\text{AT-d}}, \tag{C.46}$$

which directly implies the required statement.

□

Appendix D

Proofs of statements related to delayed Authentication

In this chapter, we prove Theorem 8.4.1, using an approach that very closely mirrors the approach taken the prove Theorem 8.2.1. To prove this result, we begin by defining the event $\Omega_{\text{dauth-hon}}$ as the event in which Alice's transcript $\mathcal{T}_A$ is such that it satisfies the verification conditions. (Note that this refers to the actual transcript itself, not to whether Bob successfully receives it). Thus, $\Omega_{\text{dauth-hon}}$ is already determined by the time $\widetilde{\mathcal{P}}_{\text{QKD}}$ concludes. Intuitively, conditioned on the event $\Omega_{\text{dauth-hon}}$, we may assume that authentication behaved honestly during the execution of $\widetilde{\mathcal{P}}_{\text{QKD}}$. Analogous to Lemma 8.3.1, we prove the following lemma, which states that if $\Omega_{\text{dauth-hon}}$ does not occur, then both parties abort.

Lemma D.0.1. *Let $\Omega_{\text{dauth-hon}}$ be the event that Alice's transcript $\mathcal{T}_A$ is such that it satisfies the verification conditions, and let $\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}}$ denote the final output state at the end of the full QKD protocol $\mathcal{P}_{\text{QKD}}$. Then the following equality holds*

$$\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega^{\text{C}}_{\text{dauth-hon}}} = \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} | \Omega^{\text{C}}_{\text{dauth-hon}}} \right]. \tag{D.1}$$

Therefore,

$$\frac{1}{2} \left\| \rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \right\|_1 = \frac{1}{2} \left\| \rho^{\text{real,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} \wedge \Omega_{\text{dauth-hon}}} - \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}} \wedge \Omega_{\text{dauth-hon}}} \right\|_1 \tag{D.2}$$

Proof. The proof follows in a similar manner as the proof of Lemma 8.3.1, by noting that del-AuthPP Protocol ensures that both parties abort when $\Omega^{\text{C}}_{\text{dauth-hon}}$ occurs. □

Analogous to Lemma 8.3.2, we now show that conditioned on the event $\Omega_{\text{dauth-hon}}$, the final real and ideal output states (at the end of $\mathcal{P}^{\text{del}}_{\text{QKD}}$) can be obtained by the action of $\mathcal{E}^{\text{del}}_{\text{update}} \circ \mathcal{E}^{\text{del}}_{\text{comm}}$ on the real and ideal states the end of the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$.

Lemma D.0.2 (Commutation of $\mathcal{R}_{\text{ideal}}$ and del-AuthPP Protocol)**.** *Let $\Omega_{\text{dauth-hon}}$ be the event in which Alice's transcript $\mathcal{T}_A$ is such that it satisfies the verification conditions. Let $\rho^{\text{real}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}}$ denote the real state at the end of the core QKD protocol conditioned on $\Omega_{\text{dauth-hon}}$. Let the following states denote its evolution through del-AuthPP Protocol:*

$$\begin{aligned} \rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &:= \mathcal{E}^{\text{del}}_{\text{comm}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right], \\ \rho^{\text{real,final}}_{K_A K_B \boldsymbol{C'_{\text{fin}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &:= \mathcal{E}^{\text{del}}_{\text{update}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right]. \end{aligned} \tag{D.3}$$

Define the corresponding ideal states by the action of the map $\mathcal{R}_{\text{ideal}}$ on the real states, i.e

$$\begin{aligned} \rho^{\text{ideal}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right], \\ \rho^{\text{ideal,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right], \\ \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C'_{\text{fin}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &:= \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,final}}_{K_A K_B \boldsymbol{C'_{\text{fin}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right]. \end{aligned} \tag{D.4}$$

Then, the ideal states defined above are the same as those obtained by evolving $\rho^{\text{ideal}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}}$ through the del-AuthPP Protocol, i.e,

$$\begin{aligned} \rho^{\text{ideal,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &= \mathcal{E}^{\text{del}}_{\text{comm}} \left[\rho^{\text{ideal}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right], \\ \rho^{\text{ideal,final}}_{K_A K_B \boldsymbol{C'_{\text{fin}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} &= \mathcal{E}^{\text{del}}_{\text{update}} \left[\rho^{\text{ideal,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right]. \end{aligned} \tag{D.5}$$

Proof. The fact that

$$\mathcal{E}^{\text{del}}_{\text{comm}} \circ \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right] = \mathcal{R}_{\text{ideal}} \circ \mathcal{E}^{\text{del}}_{\text{comm}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} E_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right] \tag{D.6}$$

follows from the fact that $\mathcal{E}^{\text{del}}_{\text{comm}} \in \text{CPTP}(\boldsymbol{C_{\text{fin}} E_{\text{fin}}}, \boldsymbol{C'_{\text{fin}} E'_{\text{fin}}})$ and $\mathcal{R}_{\text{ideal}} \in \text{CPTP}(K_A K_B, K_A K_B)$: they act on disjoint registers. (This is analogous to the commutation corresponding to the second arrow in the proof of Lemma 8.3.2).

The fact that

$$\mathcal{E}^{\text{del}}_{\text{update}} \circ \mathcal{R}_{\text{ideal}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right] = \mathcal{R}_{\text{ideal}} \circ \mathcal{E}^{\text{del}}_{\text{update}} \left[\rho^{\text{real,comm}}_{K_A K_B \boldsymbol{C_{\text{fin}} C_{\text{auth}} E'_{\text{fin}}} | \Omega_{\text{dauth-hon}}} \right] \tag{D.7}$$

follows from analogous arguments to the commutation corresponding to the third arrow in the proof of Lemma 8.3.2. In particular, we consider each possible combination of final accept / abort decisions, and find that the required commutation holds for all of them. □

Using these results, we obtain the following corollary which is analogous to Corollary 8.3.1.

Corollary D.0.1. *Consider the same setting as in Theorem 8.4.1. The $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial on $\Omega_{\text{dauth-hon}}$, implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\mathcal{P}^{\text{del}}_{\text{QKD}})$. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}}-\rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}}\right\|_1\leq\varepsilon^{\text{secure}} \qquad \forall\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}}\in\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})\\
&\qquad\qquad\Downarrow\\
&\frac{1}{2}\left\|\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}}-\rho^{\text{ideal,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}}\right\|_1\leq\varepsilon^{\text{secure}} \qquad \forall\rho^{\text{real,final}}_{K_AK_B\boldsymbol{C}'_{\mathbf{fin}}\boldsymbol{E}'_{\mathbf{fin}}}\in\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\mathcal{P}^{\text{del}}_{\text{QKD}})
\end{aligned} \tag{D.8}$$

Proof. The claim follows from Lemmas D.0.1 and D.0.2 using arguments identical to those used in the proof of Corollary 8.3.1. □

We then construct the virtual authentication setting in exactly the same manner as before (see Section 8.3.3). In the virtual setting, Eve can do any operation she wants on the classical messages, and the correct messages are delivered at correct timings in the special registers $\widetilde{\boldsymbol{C}}$. Moreover, Alice and Bob use these special registers for further steps in the QKD protocol. We then obtain the following lemma. (Note that *technically*, this virtual setting differs slightly from the one considered in Section 8.3.3, as the classical communication here is unauthenticated. However, this technical distinction does not affect the proof steps or underlying logic.)

Lemma D.0.3. *Consider the same setup as in Theorem 8.4.1 and Corollary D.0.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial on $\Omega_{\text{dauth-hon}}$, implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ partial $\Omega_{\text{dauth-hon}}$. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}}-\rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}}\right\|_1\leq\varepsilon^{\text{secure}} \qquad \forall\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}}\in\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})\\
&\qquad\qquad\Downarrow\\
&\frac{1}{2}\left\|\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}}-\rho^{\text{ideal}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}}\right\|_1\leq\varepsilon^{\text{secure}} \qquad \forall\rho^{\text{real}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}}\in\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})
\end{aligned} \tag{D.9}$$

Proof. The claim follows by arguments identical to those used in the proof of Lemma 8.3.3. □

The following lemma reduces the security analysis to states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$.

Lemma D.0.4. *Consider the same setup as in Theorem 8.4.1 and Corollary D.0.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$, implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\mathcal{P}_{\text{QKD}})$ partial on $\Omega_{\text{dauth-hon}}$. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad \Downarrow \\
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{dauth-hon}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}\wedge\Omega_{\text{auth-hon}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})
\end{aligned} \tag{D.10}$$

Proof. The claim follows by arguments identical to those used in the proof of Lemma 8.3.4. □

The following lemma reduces the security analysis to states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$.

Lemma D.0.5. *Consider the same setup as in Theorem 8.4.1 and Corollary D.0.1. Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})$. That is*

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,hon}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,hon}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad \Downarrow \\
&\frac{1}{2}\left\|\rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real,virt}}_{K_AK_B\boldsymbol{C}_{\mathbf{fin}}\widetilde{\boldsymbol{C}}\boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{virt}}(\widetilde{\mathcal{P}}_{\text{QKD}})
\end{aligned} \tag{D.11}$$

Proof. The claim follows by arguments identical to those used in the proof of Lemma 8.3.5. □

Bringing it all together, we obtain the proof of the required reduction statement.

Theorem 8.4.1 (Reduction of QKD security analysis to the honest authentication setting with delayed authentication)**.** *Let $\widetilde{\mathcal{P}}_{\text{QKD}}$ be an arbitrary QKD protocol. Let $\mathcal{P}^{\text{del}}_{\text{APP}}$ be the del-AuthPP Protocol described in Section 8.4.1, executed after the core QKD protocol $\widetilde{\mathcal{P}}_{\text{QKD}}$. Let $\mathcal{P}^{\text{del}}_{\text{QKD}} = \mathcal{P}^{\text{del}}_{\text{APP}} \circ \widetilde{\mathcal{P}}_{\text{QKD}}$ denote the resulting QKD protocol. Let $\mathcal{W}^{\text{real}}_{\text{del}-\text{auth}}(\mathcal{P}_{\text{QKD}})$ denote the set of output states in the delayed authentication setting, where communication during $\widetilde{\mathcal{P}}_{\text{QKD}}$ is not authenticated while communication during $\mathcal{P}^{\text{del}}_{\text{APP}}$ is authenticated (see*

Section 8.2.1). Let $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ denote the set of output states in the honest authentication setting (see Section 8.2.1). Then, the $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}})$ implies $\varepsilon^{\text{secure}}$-security for all output states in $\mathcal{W}^{\text{real}}_{\text{del-auth}}(\mathcal{P}^{\text{del}}_{\text{QKD}})$. That is,

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{\text{real,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} - \rho^{\text{ideal,hon}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real}}_{K_A K_B \boldsymbol{C}_{\mathbf{fin}} \boldsymbol{E}_{\mathbf{fin}}} \in \mathcal{W}^{\text{hon}}_{\text{auth}}(\widetilde{\mathcal{P}}_{\text{QKD}}) \\
&\qquad\qquad\qquad\qquad \Downarrow \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (8.44) \\
&\frac{1}{2}\left\|\rho^{\text{real}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}}\right\|_1 \leq \varepsilon^{\text{secure}} \qquad \forall \rho^{\text{real}}_{K_A K_B \boldsymbol{C}'_{\mathbf{fin}} \boldsymbol{E}'_{\mathbf{fin}}} \in \mathcal{W}^{\text{real}}_{\text{del-auth}}(\mathcal{P}^{\text{del}}_{\text{QKD}}).
\end{aligned}$$

Proof. The proof follows from Corollary D.0.1 and Lemmas D.0.3 to D.0.5. □

Appendix E

Miscellaneous

This appendix collects various results and observations from across the thesis.

E.1 Proof of the Correctness and Secrecy Decomposition of the Security Definition (Section 3.1.2)

Lemma 3.1.1. *(Correctness and Secrecy imply Security) A QKD protocol that is $\varepsilon^{\text{secret}}$-secret, and $\varepsilon^{\text{correct}}$-correct, is $(\varepsilon^{\text{secret}} + \varepsilon^{\text{correct}})$-secure.*

Proof. The proof is just simple algebra, and can be found in many works [95, 65]. For a version explicitly written for variable-length protocols, see [1, Lemma 11]. We include it here for the sake of completeness.

Consider the same setting as in Definitions 3.1.1 and 3.1.2, where $\mathcal{W}(\mathcal{P}_{\text{QKD}})$ denotes the set of all possible output states for the given protocol, and let $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$ denote the output state, and let $\Omega_{\text{len}=l}$ denote the event that a final key of length l is produced. Fix the real output state $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}}$. Let us write

$$\begin{aligned}
\rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} &= \sum_{k_A,k_B \in \{0,1\}^l} \Pr(k_A, k_B|\Omega_{\text{len}=l})\, |k_A, k_B\rangle\langle k_A, k_B|_{K_A K_B} \otimes \rho^{(k_A,k_B)}_{\boldsymbol{E}|\Omega_{\text{len}=l}} \\
\rho^{\text{correct}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} &= \sum_{k_A,k_B \in \{0,1\}^l} \Pr(k_A, k_B|\Omega_{\text{len}=l})\, |k_A, k_A\rangle\langle k_A, k_A|_{K_A K_B} \otimes \rho^{(k_A,k_B)}_{\boldsymbol{E}|\Omega_{\text{len}=l}} \\
\rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} &= \sum_{k_A \in \{0,1\}^l} \frac{1}{2^k}\, |k_A, k_A\rangle\langle k_A, k_A|_{K_A K_B} \otimes \rho^{\text{real}}_{\boldsymbol{E}|\Omega_{\text{len}=l}},
\end{aligned} \tag{E.1}$$

where the ideal output state written above can be easily verified to be the output of the $\mathcal{R}_{\text{ideal}}$ acting on the real output state. Here the states $\rho^{(k_A,k_B)}_{\boldsymbol{E}|\Omega_{\text{len}=l}}$ are simply Eve's conditional states when the key registers hold keys k_A, k_B respectively, each of length l. The states labeled "correct" are obtained by simply replacing Bob's key with Alice's key in the real output state. Then, using the triangle inequality, the trace distance from the security condition can be upper bounded as

$$\begin{aligned}
&\sum_l \Pr(\Omega_{\text{len}=l}) \frac{1}{2} \left\| \rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} \right\|_1 \\
&\leq \sum_l \Pr(\Omega_{\text{len}=l}) \frac{1}{2} \left\| \rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} - \rho^{\text{correct}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} \right\|_1 \\
&+ \sum_l \Pr(\Omega_{\text{len}=l}) \frac{1}{2} \left\| \rho^{\text{correct}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} \right\|_1
\end{aligned} \tag{E.2}$$

The first term in Eq. (E.2) can be upper bounded by the correctness condition as follows:

$$\begin{aligned}
&\sum_l \Pr(\Omega_{\text{len}=l}) \frac{1}{2} \left\| \rho^{\text{real}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} - \rho^{\text{correct}}_{K_A K_B \boldsymbol{E}|\Omega_{\text{len}=l}} \right\|_1 \\
&\leq \sum_l \Pr(\Omega_{\text{len}=l}) \sum_{k_A,k_B \in \{0,1\}^l} \Pr(k_A, k_B | \Omega_{\text{len}=l}) \\
&\times \frac{1}{2} \left\| |k_A, k_B\rangle\langle k_A, k_B|_{K_A K_B} \otimes \rho^{(k_A,k_B)}_{\boldsymbol{E}|\Omega_{\text{len}=l}} - |k_A, k_A\rangle\langle k_A, k_A|_{K_A K_B} \otimes \rho^{(k_A,k_B)}_{\boldsymbol{E}|\Omega_{\text{len}=l}} \right\|_1 \\
&\leq \sum_l \Pr(\Omega_{\text{len}=l}) \sum_{k_A,k_B \in \{0,1\}^l, k_A \neq k_B} \Pr(k_A, k_B | \Omega_{\text{len}=l}) \\
&= \Pr(K_A \neq K_B) \leq \varepsilon^{\text{correct}},
\end{aligned} \tag{E.3}$$

where we apply the triangle inequality for the first inequality. In the second inequality, we replace the one-norm with 0 when $k_A = k_B$ and with 2 otherwise. The equality in the final line then follows from basic properties of probability, and the final inequality follows form $\varepsilon^{\text{correct}}$-correctness of the protocol

The second term in Eq. (E.2) is identical to the left-hand-side Eq. (3.8), since $K_A = K_B$ and hence K_B can be traced out without affecting the one-norm. Thus, upper bounding it by $\varepsilon^{\text{secret}}$ is identical to the secrecy requirement.

Thus, we have shown that for all $\rho^{\text{real}}_{K_A K_B \boldsymbol{E}} \in \mathcal{W}(\mathcal{P}_{\text{QKD}})$,

$$\frac{1}{2} \left\| \rho^{\text{real}}_{K_A K_B \boldsymbol{E}} - \rho^{\text{ideal}}_{K_A K_B \boldsymbol{E}} \right\|_1 \leq \varepsilon^{\text{correct}} + \varepsilon^{\text{secret}}, \tag{E.4}$$

which is identical to the required security statement. This concludes the proof. □

E.2 Explanation of Decoy-State Plots from Section 4.5

To perform finite-size security proof for decoy-state protocols against IID collective attacks using Ref. [6], we perform the following steps.

- We use the tagging source map from Section 3.6.2 and instead consider a protocol in which Alice emits the tagged states defined in Eq. (3.32), which we recall here for convenience:

$$(\xi_{(a,\mu,z)})_{A'} = \sum_{N=0}^{N_{\text{ph}}} p_\mu^{\text{poiss}}(N) \, |N\rangle\langle N|_a + \left(1 - \sum_{N=0}^{N_{\text{ph}}} p_\mu^{\text{poiss}}(N)\right) |a,\mu\rangle\langle a,\mu| \, . \tag{E.5}$$

  where $p_\mu^{\text{poiss}}(N) \coloneqq e^{-\mu}\frac{\mu^N}{N!}$ is the poissonian distribution. Source maps are required when we apply the postselection technique in Chapter 5; we defer a rigorous justification for their use to that discussion.

- Second, we employ the source-replacement scheme. The block-diagonal structure of the states allows us to write the following shared state:

$$\sigma_{\bar{A}\hat{A}} = \sum_{N=0}^{N_{\text{ph}}} \Pr(N) \, |N\rangle\langle N|_{\hat{A}} \otimes \sigma_A^{(N)} + \Pr(\text{flag}) \, |\text{flag}\rangle\langle\text{flag}|_{\hat{A}} \otimes \sigma_A^{(\text{flag})}, \tag{E.6}$$

  where $\Pr(N)$ denotes the probability that Alice emits an N-photon pulse, and $\sigma_A^{(N)}$ is the source-replaced state corresponding to that emission event. We set $N = \text{flag}$ when Alice emits a pulse containing more than N_{ph} photons, which, after the application of the source map, manifests as the output of a classical flag.

- In fact, we can treat the protocol as one where Alice first decides to prepare an N-photon pulse according to some known probability distribution, *then* samples the encoding choice a, prepares and sends that state, and *only afterward* assigns the pulse a particular intensity μ or a $\texttt{test}, \texttt{gen}$ label. We use y to denote Bob's outcome. Alice assigns her labels using the distribution

$$\Pr(\texttt{test}, \mu | a, y) = \Pr(\texttt{test}, \mu | a) = \Pr(\texttt{test}, \mu, a) / \Pr(a). \tag{E.7}$$

  where the first equality follows from the fact that Alice decides the $\texttt{test}, \texttt{gen}$ label. Thus, we have

$$\mathbf{F}^{\text{obs}}_{a,\mu,\texttt{test},y} \approx \Pr(a, \mu, \texttt{test}, y) = \Pr(\texttt{test}, \mu | a, y) \operatorname{Tr}[\Gamma_{a,y}\rho] \tag{E.8}$$

where $\Gamma_{a,y}$ the POVM corresponding to Alice sending state a, and Bob measuring outcome y.[1]

- We then turn to the decoy-state analysis. For the time being, we fix a true state ρ_{AB} describing Eve's attack, and let y denote Bob's measurement outcome (Recall that Alice's label for her state $x = (a, \mu, z)$). Alice's setting choice is specified by (a, μ). We define

$$\widehat{Y}_N^{y|a} \coloneqq \Pr(y|a, N, \texttt{test})_\rho = \Pr(y|a, N, \texttt{test}, \mu)_\rho, \qquad \forall N \in \{0, \ldots, N_{\text{ph}}\}, N = \text{flag} \tag{E.9}$$

and obtain

$$\begin{aligned} \Pr(y|a, \mu, \texttt{test}) &= \sum_{N=0}^{N_{\text{ph}}} \Pr(N|a, \mu, \texttt{test}) \Pr(y|a, N, \mu, \texttt{test}) \\ &\quad + \Pr(\text{flag}|a, \mu, \texttt{test}) \Pr(y|a, \text{flag}, \mu, \texttt{test}) \\ &= \sum_{N=0}^{N_{\text{ph}}} \Pr(N|a, \mu, \texttt{test}) \widehat{Y}_N^{y|a} + \Pr(\text{flag}|a, \mu, \texttt{test}) \widehat{Y}_{\text{flag}}^{y|a}, \end{aligned} \tag{E.10}$$

which holds for all intensities μ. This system of linear equations can be solved via linear programming by imposing the bounds $0 \leq \widehat{Y}_N^{y|a}, \widehat{Y}_{\text{flag}}^{y|a} \leq 1$, provided that the quantities $\Pr(y|a, \mu, \texttt{test})$ are accessible. Note that the remaining terms $\Pr(N|a, \mu, \texttt{test}), \Pr(\text{flag}|a, \mu, \texttt{test})$ are known exactly.

- Finally, the probabilities $\Pr(y|a, \mu, \texttt{test})$ are related to the observed frequencies of the announcements $\mathbf{F}_k^{\text{obs}}$, including their worst-case values as obtained from the set constructions introduced earlier. In particular, we have

$$F_{(a,\mu,\texttt{test},y)} \approx \Pr(y|a, \mu, \texttt{test}) \Pr(a, \mu, \texttt{test}). \tag{E.11}$$

Putting everything together yields the following key-rate formula. Two remarks are in order. First, the decoy-state analysis in Ref. [6] is carried out without the use of source maps, but it can be straightforwardly adapted to incorporate them. In any case, the analysis without source maps provides a valid lower bound on the one that includes source maps.[2] Second, Ref. [6] also derives an improved second-order correction term, which we do not include here. Subject to these modifications, we obtain the following theorem.

[1] In this case, the $\texttt{test}, \texttt{gen}$ flags do not appear in the source-replacement scheme directly, but instead appear as classical postprocessing by Alice. Both perspectives are equivalent.

[2] The differences arise from a modified treatment of terms corresponding to pulses containing more than N_{ph} photons. Since such events occur with very small probability, their impact on the key rate is negligible.

Corollary E.2.1. *(Variable-length Decoy-state BB84 [6]) Consider the variable-length decoy-state BB84 variant of the Generic QKD Protocol as specified in Section 3.3, with the confidence set $\mathcal{V}(\mathbf{F}^{\mathrm{obs}})$ (which depends on $\varepsilon_{\mathrm{AT}}$) as constructed in Lemma 4.3.2. Then this variable-length deocy-state BB84 protocol is $(\varepsilon_{\mathrm{AT}}+\varepsilon_{\mathrm{PA}}+\varepsilon_{\mathrm{EV}})$-secure against IID collective attacks, as long as the $\ell(\mathbf{F}^{\mathrm{obs}})$ satisfies*[3]

$$\begin{aligned}
\ell(\mathbf{F}^{\mathrm{obs}}) \leq \Bigg\lfloor & n \inf_{\nu^{(1)}\in\Sigma^{(1)}(\mathbf{F}^{\mathrm{obs}})} \Pr(N=1) H(S|\widehat{C}E)_{\nu^{(1)}} - n(\alpha-1)\log^2(1+2\dim(S)) - \lambda_{\mathrm{EC}}^{\mathrm{fixed}} \\
& - \left\lceil \log\left(\frac{1}{\varepsilon_{\mathrm{EV}}}\right)\right\rceil - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{\mathrm{PA}}}\right) + 2 \Bigg\rfloor, \\
\Sigma^{(1)}(\mathbf{F}^{\mathrm{obs}}) \coloneqq \big\{ & \mathcal{G}[\omega_{ABE}^{(1)}] \;\mid\; \omega_A^{(1)} \in \mathrm{S}_{=}(AB), \omega_A^{(1)} = \sigma_A^{(1)}, \\
& \Pr(a,\mathtt{test}|N=1)\widetilde{Y}^{y|a}_{N=1,L} \leq \Pr(\mathtt{test}|a,N=1)\operatorname{Tr}\left[\Gamma_k \omega_{AB}^{(1)}\right] \leq \Pr(a,\mathtt{test}|N=1)\widetilde{Y}^{y|a}_{N=1,L}\big\}
\end{aligned} \tag{E.12}$$

where $\alpha \in (1, 1+1/\log(1+2\dim(S)))$, and $\widetilde{Y}^{y|a}_{N,L}, \widetilde{Y}^{y|a}_{N,L}$ are given by

$$\begin{aligned}
& \widehat{Y}^{y|a}_{N,L} \coloneqq \min_{\{\widehat{\mathbf{Y}}_m\}_m} \widehat{Y}^{y|a}_m, \qquad \widehat{Y}^{y|a}_{N,L} \coloneqq \min_{\{\widehat{\mathbf{Y}}_m\}_m} Y_N^{y|a} \\
s.t. \; & \frac{\mathbf{F}^{\mathrm{obs}}_{(a,\mu,\mathtt{test},y)} - \kappa^{\mathrm{var,L}}_{(a,\mu,\mathtt{test},y)}}{\Pr(a,\mu,\mathtt{test})} \leq \sum_{m=1}^{N_{\mathrm{ph}}} p_\mu^{\mathrm{poiss}}(m)\widehat{Y}_m^{y|a} + \left(1 - \sum_{m=0}^{N_{\mathrm{ph}}} p_\mu^{\mathrm{poiss}}(m)\right)\widehat{Y}^{y|a}_{\mathrm{flag}}, \\
& \frac{\mathbf{F}^{\mathrm{obs}}_{(a,\mu,\mathtt{test},y)} + \kappa^{\mathrm{var,L}}_{(a,\mu,\mathtt{test},y)}}{\Pr(a,\mu,\mathtt{test})} \geq \sum_{m=1}^{N_{\mathrm{ph}}} p_\mu^{\mathrm{poiss}}(m)\widehat{Y}_m^{y|a} + \left(1 - \sum_{m=0}^{N_{\mathrm{ph}}} p_\mu^{\mathrm{poiss}}(m)\right)\widehat{Y}^{y|a}_{\mathrm{flag}}, \\
& \forall (a,\mu,\mathtt{test},y) \in \widehat{\mathcal{C}}_{\mathrm{test}}, \\
& 0 \leq Y_m^{y|a} \leq 1 \; \forall m \in \{1,\ldots,N_{\mathrm{ph}},\mathrm{flag}\}.
\end{aligned} \tag{E.13}$$

[3] See Ref. [6] for an analysis that improves the second term in the key rate expression to $n_{\mathrm{sift}}(\alpha-1)\log^2(1+2\dim(S))$, where n_{sift} denotes the number of key generation rounds that are not discarded and are actually used for key generation. This refinement effectively increases the key rate in the high-loss regime, where most rounds are discarded, while yielding only a negligible improvement in low-loss regimes, since this term is already small compared to the leading-order contribution. Both fixed-length and variable-length results can be obtained using this improved bound, but we do not pursue this here.