A proof-technique-independent framework for detector imperfections in QKD

by

Shlok Nahar

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, 2025

© Shlok Nahar 2025

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:	Dagmar Bruß Professor, Dept. of Theoretical Physics, Heinrich-Heine-Universität Düsseldorf
Supervisor:	Norbert Lütkenhaus Professor, Dept. of Physics, University of Waterloo
Internal Member:	Alan Jamison Assistant Professor, Dept. of Physics, University of Waterloo
Internal-External Member:	Ashwin Nayak Professor, Dept. of Combinatorics and Optimization, University of Waterloo
Other Member(s):	Thomas Jennewein Associate Professor, Dept. of Physics, 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 this 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 primarily based on the following published articles and preprints completed under the supervision of Norbert Lütkenhaus. Each work was primarily led by its corresponding first author, who carried out the majority of the research. This thesis presents the parts of these works to which I contributed substantially.

[A] **Shlok Nahar**, Devashish Tupkary and Norbert Lütkenhaus, PRX Quantum 5, 040315 (2024)

[B] Devashish Tupkary, **Shlok Nahar**, Pulkit Sinha and Norbert Lütkenhaus, Quantum 9, 1937 (2025)

[C] **Shlok Nahar**, Devashish Tupkary and Norbert Lütkenhaus, arXiv:2503.06328

See Section 1.1 for detailed explanations about how materials from these papers are used in this thesis.

Abstract

The security of Quantum Key Distribution (QKD) protocols is theoretically established using idealised device models. However, the physical implementations upon which practical security relies inevitably deviate from these ideals. This thesis develops a rigorous and versatile framework to address a subclass of such deviations: detector imperfections.

This framework, termed 'noise channels', is independent of security proof technique. This approach recasts imperfections as a quantum channel preceding an idealised measurement process. By granting the eavesdropper control over this channel, the security analysis is simplified to an ideal scenario, with the effects of the imperfections mathematically contained within a well-defined parameter. The utility and versatility of the framework are demonstrated through applying it to the postselection technique, and for phase error estimation. The application to phase error estimation is an improvement over past analyses which either assumed qubit detection setups, IID attacks, or required hardware modifications. We observe a remarkably high tolerance to imperfections when using the postselection technique.

Finally, we extend the framework to address cross-round correlations, providing a methodology to prove security against detector memory effects such as afterpulsing and dead times. This work thus establishes a structured and powerful toolkit for analysing detector imperfections in practical QKD systems, unifying their treatment across different security proof techniques and advancing the development of robust implementation security.

Acknowledgements

First and foremost, I would like to express my deepest appreciation to my supervisor, Prof. Norbert Lütkenhaus. His generosity with time, patience through my missteps, and the rare balance of independence and guidance have shaped me into a more careful and confident researcher than I imagined I could become.

I am indebted to the OQCT group for a supportive and lively research environment with many interesting discussions. Special thanks to Devashish Tupkary, with whom I had the pleasure of working with for most of my PhD; working together has been an integral part of my research experience. I also thank Amir Arqand for teaching me much of what I know about EAT-based proofs. I thank Lars Kamin for multiple discussions about quantum optics, and for bearing with my Beamer shenanigans. I thank John Burniston for helpful comments about my code. I would like to thank Prof. Ernest Tan for his steady guidance, incisive questions, and many whiteboard discussions that sharpened this work. I also thank Zhiyao Wang, Aodhan Corrigan, and Shihong Pan for teaching me as much about mentorship as I hope I taught them — and for being a pleasure to mentor. A special thanks to Shihong Pan as well for providing parts of the code that was used to produce some of the plots in this thesis.

I also thank Norbert for organising the security-proof workshop, which enabled many fruitful discussions and introduced me to many interesting people whom I also gratefully acknowledge for their illuminating discussions: Prof. Masato Koashi, Fred Fung, Dr. Momtchil Peev, Prof. Gláucia Murta, Margarida Pereira, Guillermo Currás-Lorenzo, Victor Zapatero, Prof. Peter Brown, Ashutosh Marwah and Toyohiro Tsurumaru. Many parts of this thesis can be traced back to conversations with them. I owe a particular debt to Takaya Matsuura for teaching me much of what I know about phase error correction-based proofs, and to Yuming Zhao for teaching me much of what I know of de Finetti theorems and Schur-Weyl duality. I thank Florian Kanitschar and Ian George for multiple interesting discussions.

Many thanks to Zhiyao Wang, Aodhan Corrigan, Jerome Wiesemann, Margarida Pereira, Guillermo Currás-Lorenzo, Amir Arqand, Devashish Tupkary and Matej Pivoluska for carefully reading drafts and offering thoughtful feedback that strengthened the presentation and arguments. I would also like to thank Akash Patel for the silly Easter egg included in this thesis.

I also thank Prof. Michael Reimer, Sayan Gangopadhyaya, and Matteo Pennacchietti, with whom I had the pleasure of collaborating on an experimental project that sharpened my understanding of real-world constraints.

I am grateful to my examiners for their time and feedback, and to my past committee members, Agata Branczyk and Prof. Michele Mosca, whose feedback on earlier presentations and research influenced several choices in the structure and exposition of this thesis.

I also thank the broader IQC community that has made me a better scientist in countless ways. Special thanks to Sanchit Srivastava for being my willing "guinea pig" for many practice talks, and Arsalan Motamedi and Amolak Kalra for discussions that pushed me to think beyond my immediate area and connect ideas across subfields.

I would like to thank John Donohue for helping me learn to explain advanced concepts to a lay audience in a way that is accessible, yet accurate. Watching him present was always inspiring and mesmerising. I would also like to thank Michele Roche for reliably and efficiently handling the cumbersome logistics that allowed me to focus on research.

Finally, my deepest thanks go to my friends, family and partner, Shreya for their unwavering support and encouragement. Nothing I have accomplished would have been possible without their patience, love, and belief.

Table of Contents

Examining Committee ii

Author's Declaration iii

Statement of Contributions iv

Abstract v

Acknowledgements vi

List of Figures xiii

List of Tables xvi

1 Introduction 1

1.1 Contributions and structure of the thesis 3

2 Preliminaries 5

2.1 Quantum information 5

2.1.1 States and Hilbert spaces 5

2.1.2 Composite systems and registers 6

2.1.3 Quantum processes: channels and measurements 7

2.1.4 State and channel distinguishability 7

2.2 Quantum optics . . . 8
2.2.1 Quantising classical electromagnetic fields . . . 8
2.2.2 Coherent states . . . 8
2.2.3 Beam splitters . . . 9
2.2.4 Threshold detectors . . . 10
2.2.5 Dark counts . . . 10
2.2.6 Detector loss . . . 12
2.2.7 Multimode detection setups . . . 13
2.3 Concentration inequalities . . . 14
2.3.1 Binomial distribution . . . 15
2.3.2 Hoeffding's inequality . . . 17
2.3.3 Serfling's inequality . . . 18

3 A toolbox for the theoretical analysis of practical QKD protocols 20
3.1 Protocol description . . . 20
3.2 Security definition . . . 23
3.3 Source-replacement scheme . . . 25
3.4 Simplifying analysis of practical devices . . . 28
3.4.1 Abstract reduction argument . . . 28
3.4.2 Source maps . . . 30
3.4.3 Squashing maps . . . 33
3.4.4 Extension to infinite-dimensions . . . 41

4 Noise channels in QKD 43
4.1 Generic constructions of noise channels . . . 43
4.2 Construction of noise channel for loss and dark counts for generic detection setups . . . 48
4.2.1 Noise channel for dark counts . . . 48

4.2.2 Noise channel for loss . . . 51
4.3 Multimode extensions . . . 54
4.4 Concluding remarks . . . 55

5 Postselection technique for optical QKD protocols 57
5.1 Motivating de Finetti reductions . . . 58
5.2 Choice of de Finetti reduction for QKD . . . 59
5.3 Imperfect detection setups . . . 62
5.4 Decoy-state protocols . . . 67
5.4.1 Construction of shield system for decoy-state protocols . . . 68
5.4.2 IID decoy-state analysis for tagged sources . . . 70
5.5 Concrete application . . . 72
5.5.1 Recipe for application . . . 72
5.5.2 Optical setup . . . 73
5.5.3 Tagging . . . 74
5.5.4 Applying the WPFSS . . . 75
5.5.5 Application of noise channels . . . 78
5.5.6 Results . . . 81
5.6 Concluding remarks . . . 84

6 Phase error rate estimation with imperfect detectors 87
6.1 Phase errors and secrecy . . . 88
6.2 Phase error estimation with no basis-efficiency mismatch . . . 90
6.3 Phase error estimation with basis-efficiency mismatch . . . 92
6.3.1 Equivalent protocol . . . 92
6.3.2 Sampling strategy . . . 94
6.4 Phase error estimation with noise channels . . . 96
6.4.1 Application of noise channel . . . 103

6.4.2 Comparison with sampling bound . . . 108
6.4.3 Finite-size plots . . . 109
6.5 Concluding Remarks . . . 110

7 Security against correlated imperfections **113**
7.1 Reduction to finite correlation length . . . 114
7.2 Protocol modification . . . 116
7.3 Correlated noise channel . . . 117
7.4 Future directions . . . 121

8 Conclusion and outlook **123**

References **126**

APPENDICES **138**

A Extension to infinite-dimensions **139**

B Noise Channel constructions **143**

C Improved de Finetti reductions **150**
C.1 Generic improvement . . . 151
C.2 Improvements with symmetries . . . 152
C.2.1 Improvement for IID-block-diagonal states . . . 153
C.2.2 Improvement for IID symmetries . . . 154
C.3 Proofs of technical statements . . . 156
C.3.1 Toolkit from representation theory . . . 156
C.3.2 Proofs . . . 158

D Computing deviation metrics for phase error estimation **168**

D.1 Deviation metrics for sampling strategy in Section 6.3 168

D.1.1 Computing POVMs 170

D.1.2 Computing δ_1 171

D.1.3 Computing δ_2 173

D.2 Bounding number of flags for phase error estimation with noise channel . . 173

D.2.1 Bounding deviation from ideality 174

D.2.2 Bounding minimum eigenvalue 175

List of Figures

2.1 Schematic of a generic beam splitter. The input modes are labelled 1 and 2, while the output modes are labelled 3 and 4. ([1, Fig. 2.2]) 10

3.1 The imperfect source can always be replaced by the perfect source in security proofs if they are related via a source map since the imperfect source gives Eve more power. ([1, Fig. 2.1]) 30

3.2 The imperfect POVM $\vec{\Gamma}$ can be modelled as a squashing map Λ followed by a perfect POVM $\vec{F}$. Giving the squashing map Λ to Eve lets us restrict our analysis to the perfect POVM $\vec{F}$. ([2, Fig. 2]) 31

3.3 Trivial squashing map that always exists. 36

3.4 Flag-state squashing map (adapted from [3, Fig. 2]). 37

4.1 Constructive description of the noise channel. With probability q, the noise channel measures and converts the input state into a flag state. The output flag state is depicted by dashed lines. 45

4.2 A set of equivalences (as quantum-to-classical measurement channels) of detection setups to consider dark counts and loss as part of the noise channel, using the flag-state squasher. 49

5.1 A set of equivalences (as quantum-to-classical measurement channels) of detection setups to use Theorems 4.3 and 4.4 with the postselection technique. Here, $\mathcal{P}'_{\text{cg}}$ represents the classical post-processing carried out in the protocol, $\mathcal{P}^{\mathbf{d_B}}$ is the dark count post-processing, $\mathcal{P}_{\text{cg}}$ is the coarse-graining required for the WPFSS Λ_{WPFSS}, and $\mathcal{P}_{\text{dc}}$ is the post-processing fixed by Eq. (5.10). In the figure, olive post-processing maps represent free choices that can be made to make equivalences (ii) and (v) hold. Orange post-processing maps represent stochastic processes fixed by equivalences (i) and (iii). 64

5.2 Schematics of the implementation of the three-state protocol as in [4]. The numbers below the beam splitters reflect their transmissivity. IM and VA refer to intensity modulator and variable attenuator respectively. 74

5.3 Simplifying the description of the detection setup with lossy detectors. . . 76

5.4 Simplifying the description of the detection setup with lossy detectors. . . 77

5.5 Plots demonstrating the performance of the postselection technique for the three-state protocol, and highlighting the importance of our improvements. 83

5.6 Plots demonstrating the effect of imperfections on the key rate. Our security analysis is minimally affected by detector imperfections. We observe non-zero key rates for imperfection values upto 51%, though we only plot the key rates upto imperfection values upto 30%. 85

6.1 Flowchart depicting the phase error estimation strategy. The testing and key generation rounds go through an additional second step filtering measurement that depends on the basis used, which typically results in a few rounds being discarded, before undergoing the final measurement. The basis used in these measurements in indicated in each box, and indicates the basis used by both Alice and Bob. The dotted arrows and boxes represent virtual measurements that do not actually happen in the real protocol. Connections between the error rates in different boxes are highlighted using curved arrows. 93

6.2 Flowchart depicting the equivalent protocol using the noise channel. Each round is first processed by a noise channel, which flags it with probability $q_{>0}$. The remaining non-flag rounds (in the 'preserved subspace') are then acted on by a basis-independent filter so that their error rates in the test and key generation rounds can be related via Serfling's inequality. The error rates in the flag space cannot be related to each other, and must be accounted for (as in Lemma 6.1). 97

6.3 The noise channel from Fig. 6.2 can be moved to after the basis choice to construct another equivalent protocol useful for bounding the number of flags in the key generation and test rounds. 105

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 $N_{\text{tot}} = 10^{12}$ number of total signals sent, for various values of Δ_η, Δ_{dc}. Colours encode the extent of characterisation Δ_η, Δ_{dc}, while line styles distinguish the method (dashed: noise channel approach; solid: sampling strategy). We find that the noise channel method to treat basis-efficiency mismatch results in better key rates. 111

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_{tot}), for $\Delta_\eta = \Delta_{\text{dc}} = 0.05$. Colours encode the total number of signals, while line styles distinguish the method (dashed: noise channel approach; solid: sampling strategy). 112

7.1 Illustration of the noise channel construction which determines whether a round will be rejected or not. The rounds that are not rejected are only measured using a photon-number measurement, which determines the detect vs no-detect outcome. This photon-number measurement does not change the measurement statistics, as the POVM is block-diagonal. The rounds that are rejected have their entire measurements completed in order to determine the detection event. ([5, Fig. 8]) 119

B.1 Constructive description of the noise channel. Each line corresponds to a subspace of the input Hilbert space associated with the block-diagonal decomposition of the POVM elements. The dashed lines refer to classical states. 144

B.2 Constructive description of the noise channel. Each line corresponds to a subspace of the input Hilbert space associated with the block-diagonal decomposition of the POVM elements. The dashed lines refer to classical states. 149

List of Tables

3.1 Examples of squashing maps, with brief description of their application and limitations. 35

5.1 de Finetti reductions and their applicability to QKD protocols with penalty parameter x in $g_{n,x} = \binom{n+x-1}{x-1}$. Our work derives de Finetti reductions with the smallest penalty, without sacrificing applicability. 61

5.2 Simulation parameters used for secret key rate plots. We do not optimise all the values. 82

6.1 Notation for random variables used in the phase error estimation. 100

8.1 Comparison of the two security analyses with noise channels. 124

Chapter 1

Introduction

> "Just because you're paranoid doesn't mean they aren't after you."
>
> - Joseph Heller, *Catch-22*

Quantum Key Distribution (QKD) is a maturing technology used to share a secret key between two parties, Alice and Bob, secure against any eavesdropper, Eve. Since its initial conception in 1984 with the Bennet-Brassard BB84 [6] protocol, QKD has progressed from theoretical foundations to experimental implementations.

On the theoretical side, a central part of this progress has been the development of distinct security proof techniques. These different proof techniques are [1]:

1. **Phase error correction**-based proofs [7]. These proofs connect the security of the protocol to the success probability of a virtual quantum error correction procedure designed to correct 'phase errors' — errors in the conjugate basis to that used for key generation.

2. Proofs [8] based on the **entropic uncertainty relation (EUR)** [9]. These proofs use an entropic version of the Heisenberg uncertainty principle which limits the Eve's information about the secret key based on Bob's 'phase' error rate in the conjugate basis.

[1] See [2, Section 6] for a more detailed summary of the different proof techniques. See also [2, Section 7] for a comparison.

3. The **postselection technique** [10, 11]. These proofs reduce the security analysis against arbitrary attacks to the more tractable problem of security against independent and identically distributed (IID) attacks, albeit at the cost of a dimensional penalty to the key rate.

4. **Entropy Accumulation Theorem (EAT)**-based proofs [12, 13, 14], which use entropic chain rules to provide bounds on the total entropy accumulated over all rounds in terms of single-round quantities.

Functionally, the EUR- and phase error correction-based proofs both hinge on the task of bounding the phase error rate. This shared dependency leads to them often being categorised together as phase error estimation-based proof techniques.

Each of these security proof techniques possesses its own distinct set of advantages and challenges. While recent advances [14] in EAT-based proofs currently position it as a leading candidate for constructing robust, high-rate security proofs. Nevertheless, a central premise of this thesis is that there is enduring value in a holistic approach that encompasses all proof techniques. Each proof technique has its own particular strengths; a problem that is analytically cumbersome in one may be straightforward in another. By studying a variety of proof techniques, we can identify and transfer powerful methods between them, thereby enabling more rapid and comprehensive advancements than would be possible by focusing on a single technique in isolation.

This theoretical richness, however, confronts a fundamental challenge: experimental implementations often deviate from the idealised device models assumed in security proofs. As we near the commercial deployment of QKD protocols, it is of increasing importance to perform more refined analyses that take into account such experimental imperfections. For example, devices cannot be perfectly characterised, and thus the theoretical analysis must account for cases involving only partial models. Moreover, the adversary might even have some limited control over the devices. This has led to growing attention to addressing imperfections in QKD security proofs; both for realistic sources [15, 16, 17], and for realistic detection setups [18, 19, 20, 21, 22].

While this body of work constitutes a tremendous amount of progress towards the implementation security of QKD protocols, it is primarily restricted to the entropic uncertainty relation (EUR)- and phase-error correction-based proofs. On the other hand, work [23, 24] addressing imperfections compatible with entropy accumulation theorem-based proofs either assume qubit sources [23], or require bounds on quantities that cannot be easily related to physical device parameters [24].[2] Thus, it is important to develop meth-

[2] See recent work [17] for a notable exception.

ods that are more broadly applicable, both across proof techniques within QKD as well as for applications outside QKD.

In this work, we focus primarily on the treatment of detector imperfections by developing a proof technique-independent framework. We demonstrate its utility through several applications. We apply noise channels to the postselection technique and for phase error estimation, highlighting the unique subtleties and limitations that arise in each case. We also comment on the applicability of our framework to EAT-based proofs. This includes an increased applicability to imperfect detection setups with active basis choice. Notably, this solution is achieved by adapting an insight from phase error estimation, highlighting the utility of the holistic approach to studying different proof techniques.Finally, we extend the framework to address the challenging problem of detector memory effects, such as afterpulsing. While our initial analysis of this problem was guided by methods developed for phase error estimation proofs, the resulting formalism for correlated imperfections is itself proof technique-independent, further demonstrating the utility of studying different proof techniques.

1.1 Contributions and structure of the thesis

The remainder of this thesis is structured as follows:

- Chapter 2 provides a brief background of concepts in quantum information theory, quantum optics and concentration inequalities. This chapter is meant more as a reference and to set up notation, and can be skipped till referred to in other chapters.

- Chapter 3 provides the required QKD-specific background required for the rest of the thesis. This chapter contains an assortment of tools that are required for the analysis of practical QKD protocols. Many of these tools are existing results, though this chapter presents them with a new proof technique-independent perspective. This perspective along with some of the tools described in the chapter are contributions made in our work [11, 25]. This chapter sets the context for the rest of the work.

- Chapter 4 formally develops the noise channel formalism. We provide generic constructions for modelling imperfections and detail the specific channels for dark counts and detector loss. This is based on our work in Ref. [26].

- In Chapter 5, we first extend the applicability of the postselection technique to optical prepare and measure protocols. We also improve on the dimensional-dependent

penalty incurred when applying the postselection technique. Finally, we apply the noise channel formalism to the postselection technique. The core improvements to the proof technique are from our work in Ref. [11], while the application of the noise channel to the postselection technique is described in our work in Ref. [26]. Some refinements to this application are influenced by ideas in our work in Ref. [21].

- Chapter 6 addresses the task of phase error estimation with imperfect detectors. We present two methods to achieve this task, and contrast them. The first method is based on developing a robust sampling strategy, and is based on our work in Ref. [5]. The second method is an application of the noise channel formalism to this problem. Some refinements of the noise channel method, similar to those in Chapter 5, are influenced by ideas in our work in Ref. [21].

- Chapter 7 addresses the security of detection setups with memory effects such as dead times and afterpulsing. This treatment requires a protocol modification that discards rounds following a detection event. This is an extension of ideas in our work [5, 26].

All the code used to generate the plots in this thesis was produced using the Open QKD Security package [27], and can be found at https://openqkdsecurity.wordpress.com/repositories-for-publications/

Chapter 2

Preliminaries

> "The sciences do not try to explain, they hardly even try to interpret, they mainly make models."
>
> - John von Neumann

In this chapter, we introduce the preliminaries required to read the rest of the thesis.

2.1 Quantum information

For an axiomatic and pedagogical introduction to quantum information, we refer the interested reader to [1, Section 2.1]. Here, we briefly state the key definitions, and set up notation to be used in the rest of this work.

2.1.1 States and Hilbert spaces

A quantum mechanical system is described by an associated complex Hilbert space, denoted by $\mathcal{H}$. We restrict our attention to the set of linear operators $\mathrm{L}(\mathcal{H})$ on this space. We denote the set of positive semidefinite operators on $\mathcal{H}$ as $\mathrm{Pos}(\mathcal{H})$.

The state of a system is described by a density operator ρ which is a positive semidefinite operator with unit trace. Formally, the set of all valid density operators on $\mathcal{H}$, which we

denote by $\mathrm{S}_\circ(\mathcal{H})$, is the subset of $\mathrm{Pos}(\mathcal{H})$ constrained by the trace condition:

$$\mathrm{S}_\circ(\mathcal{H}) := \{\rho \in \mathrm{Pos}(\mathcal{H}) \mid \mathrm{Tr}[\rho] = 1\}. \tag{2.1}$$

A state is termed pure if it is a rank-one projector $|\psi\rangle\langle\psi|$ for some state vector $|\psi\rangle \in \mathcal{H}$. Otherwise, the state is mixed.

2.1.2 Composite systems and registers

When considering multiple quantum systems, the total system is described by the tensor product of the individual Hilbert spaces. To distinguish these subsystems, we assign each a label, referred to as a register.

Notational aside 2.1. For notational conciseness, we will frequently use the register label (e.g., A) to denote its associated Hilbert space ($\mathcal{H}_A$) when the meaning is unambiguous. Consequently, notations such as $\mathrm{S}_\circ(A)$ and $\mathrm{Pos}(A)$ should be understood as $\mathrm{S}_\circ(\mathcal{H}_A)$ and $\mathrm{Pos}(\mathcal{H}_A)$, respectively.

Given registers A and A', a state of the composite system is an operator $\rho_{AA'} \in \mathrm{S}_\circ(AA')$ on the space $\mathcal{H}_A \otimes \mathcal{H}_{A'}$. The state of a subsystem is recovered by taking the partial trace over all other registers; for instance, $\rho_A = \mathrm{Tr}_{A'}[\rho_{AA'}]$.

Notational aside 2.2. We refer to n copies of the same register A as $A^n = A_1 \dots A_n$. Further, we denote a subset of these registers as $A_j^l = A_j \dots A_l$, where $j < l$.

We sometimes distinguish between two types of registers. A quantum register is one whose state can be any valid density operator on its associated Hilbert space. In contrast, a classical register is a special case, constrained to hold only states that are diagonal in a particular, fixed basis $|i\rangle$. A state ρ_F in a classical register is thus always of the form

$$\rho_C = \sum_i p_i |i\rangle\langle i|,$$

where $\{p_i\}$ is a probability distribution.

Any mixed state ρ_A on a register A can be viewed as the partial trace of a larger pure state $|\rho\rangle\langle\rho|_{AE}$ on a composite system $\mathcal{H}_A \otimes \mathcal{H}_E$. The auxiliary register E is known as the

purifying system. The dimension of the purifying register needs to be at least as large as the rank of the mixed state ρ_A, and the pure state is unique upto isometries on the purifying register.

2.1.3 Quantum processes: channels and measurements

The most general physical processes are described by quantum channels. A quantum channel is a completely positive and trace-preserving (CPTP) linear map Φ that takes density operators on an input space to density operators on an output space. We denote the set of such channels from A to B as $\mathcal{C}(A, B)$.

A measurement (also called POVM) is a set of positive semidefinite operators $\{\Gamma_i\}$ that sum to the identity, $\sum_i \Gamma_i = \mathbb{I}$. The probability of obtaining outcome i when measuring a state ρ is given by the Born rule, $p(i) = \mathrm{Tr}[\Gamma_i \rho]$. We can formalise the measurement process itself as a specific type of channel, a measurement channel, which maps a quantum state to a classical register holding the outcome: $\mathcal{M}[\rho] = \sum_i \mathrm{Tr}[\Gamma_i \rho] |i\rangle\langle i|$. To represent an entire measurement compactly, we will often group the POVM elements into a vector, denoted as $\vec{\Gamma}$.

For every channel $\Phi \in \mathcal{C}(A, B)$, one can define its adjoint $\Phi^\dagger$ acting from $\mathrm{L}(B)$ to $\mathrm{L}(A)$, defined by the relation $\mathrm{Tr}[\Gamma \Phi(\rho)] = \mathrm{Tr}\left[\Phi^\dagger(\Gamma)\rho\right]$, for all linear operators $\rho \in \mathrm{L}(A)$ and $\Gamma \in \mathrm{L}(B)$. The adjoint of a channel is completely positive and unital, as can be derived from the defining relation stated above. Intuitively channels can be thought of as maps from states to states, the adjoint of channels can be thought of as maps from POVMs to POVMs.

2.1.4 State and channel distinguishability

We quantify the difference between operators via Schatten norms. In particular the difference between quantum states, is typically quantified via the 1-norm, and the difference between POVM elements is typically quantified via the ∞-norm. The difference between channels is defined via the diamond norm, also known as the completely bounded trace norm. Given two channels $\Phi, \Psi \in \mathcal{C}(A, B)$ their diamond norm is defined as

$$\|\Phi - \Psi\|_\diamond \coloneqq \max_{\substack{X \in \mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_A) \\ \|X\|_1 \leq 1}} \|(\Phi - \Psi) \otimes \mathrm{id}_A[X]\|_1.$$

2.2 Quantum optics

In what follows, we provide a number of dry facts and set up the notation and language that is used in a variety of places in this work. For a more pedagogical and comprehensive introduction to quantum optics, see for e.g. Refs. [28, 29, 30].

2.2.1 Quantising classical electromagnetic fields

In classical optics, an electromagnetic field can be decomposed into a set of orthogonal modes, most conveniently labelled by their wave vector k (and polarisation, which we suppress for notational simplicity). Each such mode carries an associated frequency $\omega(k)$[1] and behaves like an independent degree of freedom. Quantisation promotes the classical field amplitudes of these modes to operators.[2] The resulting creation and annihilation operators, $a_k^\dagger$ and a_k, satisfy the canonical commutation relations $[a_k, a_{k'}^\dagger] = \delta_{k,k'}$. The Hilbert space associated with a single mode k is spanned by the number states, or Fock states, $\{|n\rangle_k\}_{n\in\mathbb{N}_0}$, which are acted on by the creation and annihilation operators as

$$\begin{aligned} a_k^\dagger |n\rangle_k &= \sqrt{n+1}\,|n+1\rangle_k \\ a_k |n\rangle_k &= \sqrt{n}\,|n-1\rangle_k\,. \end{aligned}$$

Physically, $|n\rangle_k$ represents n photons in mode k. When multiple modes are present, the full Hilbert space is the tensor product of the single-mode spaces. Thus, the basis states for a d distinct modes can be expressed as

$$\{|\vec{n}\rangle\}_{\vec{n}\in\mathbb{N}_0^d} \coloneqq \{|n_1,\ldots,n_d\rangle\}_{n_1,\ldots,n_d\in\mathbb{N}_0},$$

where $|\vec{n}\rangle$ represents the state with n_i photons in the i^{th} mode.

2.2.2 Coherent states

An important, widely used class of states are *coherent states*. These are eigenstates of the annihilation operator

$$a_k |\alpha\rangle_k = \alpha\,|\alpha\rangle_k \tag{2.2}$$

[1] Note that the magnitude of the wave vector along with the speed of light determine the frequency.

[2] While this might seem somewhat ad hoc at first, it can also be understood by promoting all *observables*, such as the electromagnetic fields, to operators, similar to the quantisation of position and momentum in Newtonian mechanics.

where the complex eigenvalue α is called the amplitude of the coherent state.[3] The set of coherent states $\{|\alpha\rangle_k\}_{\alpha\in\mathbb{C}}$ form an overcomplete basis for the Hilbert space. We can write the coherent state in the Fock basis as

$$|\alpha\rangle_k = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle_k . \tag{2.3}$$

The *phase* and *intensity* of a coherent state $|\alpha\rangle$, correspond to the phase θ of the complex number $\alpha = \sqrt{\mu}e^{i\theta}$, and the square of its amplitude $\mu = |\alpha|^2$ respectively. We call a mixture of coherent states with a fixed intensity but uniformly random phase, a completely phase-randomised or fully phase-randomised coherent state given by

$$\rho_{\mathrm{PR}}^{\mu} = \frac{1}{2\pi} \int_0^{2\pi} d\theta \left|\sqrt{\mu}e^{i\theta}\right\rangle\!\left\langle\sqrt{\mu}e^{i\theta}\right|_k \tag{2.4}$$

$$= \sum_{n=0}^{\infty} p_\mu(n) |n\rangle\langle n|_k , \tag{2.5}$$

where p_μ is a Poisson distribution with mean μ.

2.2.3 Beam splitters

A beam splitter is an optical device with two input ports and two output ports. Classically, it combines the incoming light fields through interference, redistributing the light into the two output beams according to its reflectivity and transmissivity. Quantum mechanically, it acts similarly — but on the mode operators as depicted in Fig. 2.1 [1, Fig. 2.2]. The beam splitter generically transforms the input modes a_1, a_2 to the output modes a_3, a_4 as $a_3 = \sqrt{t}a_1 + e^{i\phi}\sqrt{r}a_2$ and $a_4 = \sqrt{t}a_2 - e^{-i\phi}\sqrt{r}a_1$ where r and t are the reflectivity and transmissivity of the beam splitter respectively with $r + t = 1$, and ϕ is the phase shift caused by the reflection. For simplicity, we will always assume that $\phi = \pi$.

Note that a more nuanced multi-modal model of the beam-splitter would include a potentially different set of reflectivity r, transmissivity t and phase shift ϕ for different sets of input frequency and polarisation modes.

[3] The coherent state $|0\rangle_k$ corresponds exactly to the Fock state $|0\rangle_k$ saving us from some ambiguity, though this is not the case for the coherent state $|1\rangle_k$, and so on.

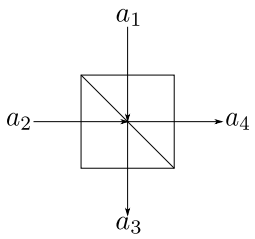


Figure 2.1: Schematic of a generic beam splitter. The input modes are labelled 1 and 2, while the output modes are labelled 3 and 4. ([1, Fig. 2.2])

2.2.4 Threshold detectors

Threshold detectors are devices that ideally 'click' in the presence of incident photons, and don't click in the absence of incident photons. Mathematically, threshold detectors can be described by a two-element POVM $\{\Gamma_{\text{click}}, \Gamma_{\text{no-click}}\}$, where $\Gamma_{\text{no-click}} \coloneqq |0\rangle\langle 0|$, and $\Gamma_{\text{click}} = \mathbb{I} - |0\rangle\langle 0|$.

We primarily consider two deviations from ideality in this work:

1. Dark count: A click outcome in the absence of incident photons.
2. Detector loss: A no-click outcome in the presence of incident photons.

2.2.5 Dark counts

Dark counts are clicks that are registered by a detector in the absence of any incident photons. There are, broadly speaking, two mechanisms that explain this phenomenon. Firstly, threshold detectors sometimes have dark counts as a result of thermal noise, where thermally generated carriers or quantum tunnelling of electrons can cause spurious detections [31]. This results in dark counts that are independent of any other click events. Secondly, after a click event, some[4] threshold detectors sometimes have trapped charges that are released at a later time causing additional click events, commonly called afterpulsing [32].

Independent dark counts

The independent dark counts can be modelled as a classical post-processing being applied to the measurement outcomes of a detector without dark counts. Specifically, consider a

[4]Specifically, single-photon avalanche diode detectors, in which a single absorbed photon releases charge carriers that trigger a large avalanche current, producing a detectable electrical pulse.

threshold detector with dark count rate d_B having POVM $\{\Gamma^{d_B}_{\text{no-click}}, \Gamma^{d_B}_{\text{click}}\}$ corresponding to no-click and click events respectively. This can be written in terms of the POVM $\{\Gamma_{\text{no-click}}, \Gamma_{\text{click}}\}$ of a threshold detector without dark counts as

$$\begin{aligned} \Gamma^{d_B}_{\text{no-click}} &= (1-d_B)\Gamma_{\text{no-click}} \\ \Gamma^{d_B}_{\text{click}} &= \Gamma_{\text{click}} + d_B\Gamma_{\text{no-click}}. \end{aligned} \tag{2.6}$$

Equation (2.6) can be more concisely written as

$$\vec{\Gamma}_{d_B} = \mathcal{P}^{d_B}\vec{\Gamma}, \tag{2.7}$$

where $\mathcal{P}^{d_B} = \begin{pmatrix} 1-d_B & 0 \\ d_B & 1 \end{pmatrix}$ is a stochastic matrix that describes the classical post-processing, and $\vec{\Gamma} = \begin{pmatrix} \Gamma_{\text{no-click}} \\ \Gamma_{\text{click}} \end{pmatrix}$.

Notational aside 2.3 (Dark count probabilities?)**.** Dark count rates are usually reported as the number of spurious click outcomes per unit time in the absence of incident photons. If the detector integrates over a fixed time window in each round, the dark count rate can be converted into a per-round probability of a click. Accordingly, we adopt this abstraction and speak of the dark count rate as the probability of a click in each round.

Similarly, for a more general detection setup with k threshold detectors, we can write the post-processing map acting on all 2^k click patterns based on the dark count rates $\mathbf{d_B} = (d_1, d_2, \cdots, d_k)$ as $\mathcal{P}^{\mathbf{d_B}}$. While the exact structure of $\mathcal{P}^{\mathbf{d_B}}$ is not important, we shall comment on the relevant properties of $\mathcal{P}^{\mathbf{d_B}}$ where applicable.

Notational aside 2.4 (Elements of postprocessing matrix)**.** In this work, we will refer to the (i, j) element of a post-processing matrix $\mathcal{P}$ as $\mathcal{P}_{i|j}$ to represent the probability of outcome (alternately, click pattern) i given outcome (alternately, click pattern) j.

Afterpulsing

Afterpulsing can be modelled as an increased dark count rate in the rounds immediately following a detection event, persisting for a finite number of rounds. In reality, however,

trapped charge carriers can be released at arbitrarily long timescales, so the effect never vanishes entirely. Instead, its probability decays exponentially and becomes negligible after sufficiently long delays. Such vanishingly small deviations from ideality can, in principle, be treated rigorously using the methods of [33, Section 3.3], as discussed in Section 7.1.

2.2.6 Detector loss

Detector loss captures the fact that a photon incident on a detector does not always result in a registered click. It is useful to distinguish two sources of detector loss. Independent loss, arising from the detector's non-unital efficiency and independent of previous detections. Loss that occurs because the detector requires a recovery period after a click, during which it cannot register further events (known as dead time).

Detector efficiency

A typical single-mode quantum optical model for detection efficiency uses the single-photon detection efficiency η, which represents the probability of the detector registering a click for each incident photon. This can also be represented as a beam splitter with transmission amplitude coefficient $\sqrt{\eta}$, followed by a lossless detector. A more complete multimode model can be developed by allowing for a different efficiencies for different input modes.

A simple special case of the single-mode model that we use in the proof of Theorem 4.4 is that of a lossy detector with no dark counts, where the input has *no more than a single photon*. In this case, the loss can be represented as a classical post-processing analogous to Eq. (2.7)

$$\vec{\Gamma}_\eta = \mathcal{P}^\eta \vec{\Gamma}, \tag{2.8}$$

where $\mathcal{P}^\eta = \begin{pmatrix} 1 & 1-\eta \\ 0 & \eta \end{pmatrix}$, and $\vec{\Gamma} = \begin{pmatrix} \Gamma_{\text{no-click}} \\ \Gamma_{\text{click}} \end{pmatrix}$. Similarly, for a more general detection setup with k threshold detectors, we can write the post-processing map $\mathcal{P}^{\boldsymbol{\eta}}$ acting on all 2^k click patterns based on the loss of each detector $\boldsymbol{\eta} = (\eta_1, \eta_2, \cdots, \eta_k)$. Note once again that this post-processing map is valid for detectors without dark counts, with an input with no more than a single photon. We stress that at no point in this work do we assume that our detectors only allow for a single photon input; we simply detailed the model in the single-photon subspace.

Notational aside 2.5 (Postprocessing matrix ordered by number of clicks)**.** Throughout this work, we use post-processing matrices to describe detection setups involving multiple detectors. The rows and columns of these matrices are ordered by increasing numbers of detection events.

Dead times

Dead time can be modelled as a period of reduced sensitivity immediately following a detection event, during which the detector efficiency is reduced, and which lasts for a finite number of rounds. This recovery time can be gradual rather than abrupt: its efficiency might increase continuously with time and never truly attain a sharp cutoff [34]. However, the residual inefficiency at long delays is typically negligible, and can in principle be treated rigorously using the methods of [33, Section 3.3], as discussed in Section 7.1.

2.2.7 Multimode detection setups

Thus far, we have described optical components in the single-mode picture. Extending these models to multiple modes is, in principle, straightforward: each component can be expressed as a direct sum of its single-mode description, acting independently on each mode. However, this naive approach quickly encounters a subtlety: there is no guarantee that different components diagonalise in the same mode basis. For example, a beam splitter may act diagonally in the frequency basis, while a time-gated detector is naturally described in the time domain, so their mode decompositions need not coincide. The challenge, therefore, is to construct models that faithfully capture the joint action of such components when their 'preferred' mode decompositions do not align.

While a complete treatment of these multimode models is essential for cryptographic applications such as QKD, this is outside the scope of this work. For concreteness, we focus on a simple independent multimode model in which the preferred mode bases of all optical components coincide. This situation might arise, for example, in a time-domain description, where detectors are time-gated and beam splitters are taken to act independently on each temporal mode. Formally this means that each POVM element decomposes as

$$\Gamma_i = \bigoplus_k \Gamma_{i,k}, \tag{2.9}$$

where each block POVM $\Gamma_{i,k}$ represents the single-mode POVM with parameters corresponding to mode k. The block-diagonal structure reflects our assumption that different

spatio-temporal modes (e.g. times of arrival or frequencies) are treated as independent, without coherent coupling. This already covers known attacks such as the time-shift attack.[5]

A more realistic multimode model has been studied in [18, Section 3], where the core assumption is that all the optical components act on the information-carrying mode (e.g. polarisation) independently of the auxiliary modes (e.g. frequency, time-of-arrival and incidence angle of the input beam). A full description of the latter model requires detailed experimental characterisation [18, Section 3.1]. Nevertheless, we expect that, given such a characterisation, the methods developed in this work could be extended to accommodate the more general multimode setting.

2.3 Concentration inequalities

In quantum information theory (and in classical probability theory), one frequently seeks to make rigorous statements about the properties of an $n-$partite quantum system based on measurements made on k subsystems. For instance, one might want to quantify how likely it is that the observed statistics on the k subsystems deviate from the statistics on the remaining $n-k$ subsystems. This is precisely the role of concentration inequalities: they bound the probability bounds of such a "bad" event occurring.

More formally, given n random variables $\mathbf{Z}_1, \ldots, \mathbf{Z}_n$, define $\mathbf{S}_n \coloneqq \sum_i \mathbf{Z}_i$. Intuitively, we would expect that the random variable $\mathbf{S}_n$ cannot be much lower than its expected value $\mathbb{E}(\mathbf{S}_n)$. A concentration inequality would then be an upper bound on the probability of this "bad" event $\Omega_{\text{bad}} \coloneqq \{\vec{z} \mid \sum_{i=1}^{n} z_i < \mathbb{E}(\mathbf{S}_n) - n\gamma\}$ occurring

$$\Pr\left[\vec{\mathbf{Z}} \in \Omega_{\text{bad}}\right] \coloneqq \Pr\left[\mathbf{S}_n < \mathbb{E}(\mathbf{S}_n) - n\gamma\right] \leq \varepsilon(\gamma, n). \tag{2.10}$$

[5] A more detailed discussion is as follows: the independent multimode model assumes no coupling between any pair of spatio-temporal modes during measurement. This allows an adversary to exploit auxiliary degrees of freedom such as time-of-arrival, frequency, or incidence angle, provided that each choice corresponds to a definite mode and no coherent superpositions are used. Even with this limitation, the model captures a wide range of classical side-channel attacks. For example, the time-shift attack [35, 36] fits naturally within this model, since it corresponds to Eve selecting different arrival times to exploit efficiency mismatch in gated detectors. Similarly, other strategies such as modifying the detector temperature are also covered.

Notational aside 2.6. For our purposes its often more useful to think of ε as a fixed quantity, and define γ to be function of ε and n. Thus, we use the notation $\underline{\gamma}(\varepsilon, n)$ to indicate this. In this context, for conciseness, we write Eq. (2.10) as $\mathbf{S}_n \underset{\varepsilon}{\geq} \mathbb{E}(\mathbf{S}_n) - n\underline{\gamma}(\varepsilon, n)$, which is to be read as $\mathbf{S}_n \geq \mathbb{E}(\mathbf{S}_n) - n\underline{\gamma}(\varepsilon, n)$ except with probability ε. Similarly, we can define $\overline{\gamma}(\varepsilon, n)$ such that $\mathbf{S}_n \underset{\varepsilon}{\leq} \mathbb{E}(\mathbf{S}_n) + n\overline{\gamma}(\varepsilon, n)$ can be read as $\mathbf{S}_n \leq \mathbb{E}(\mathbf{S}_n) + n\overline{\gamma}(\varepsilon, n)$ except with probability ε.

We abbreviate the notation $\mathbf{Z} \underset{0}{\leq} r$ as simply $\mathbf{Z} \leq r$, where it is obvious from context.

In a quantum information context, we consider the random variables that arise as outcomes of measurements. To this end, we consider an n round quantum state $\rho_{A^n} \in \mathrm{S}_\circ(A^n)$. We have n single-round measurements, $\{\Gamma_j^{(i)}\}_{j=1}^d \subset \mathrm{Pos}(A)$. The state after measurement is given by the classical state

$$\begin{aligned}\rho_{Z^n} &= \sum_{z_1,\ldots,z_n \in [d]} \mathrm{Tr}\left[\Gamma_{z_1}^{(1)} \otimes \cdots \otimes \Gamma_{z_n}^{(n)}\ \rho_{A^n}\right] |z_1 \ldots z_n\rangle\langle z_1 \ldots z_n| \\ &=: \sum_{\vec{z} \in [d]^n} \mathrm{Tr}\left[\Gamma_{\vec{z}}\ \rho_{A^n}\right] |\vec{z}\rangle\langle\vec{z}|\,.\end{aligned}$$

Thus, the outcome of each measurement $\{\Gamma_j^{(i)}\}_{j=1}^d$ is a random variable $\mathbf{Z}_i$ where the joint distribution of $\mathbf{Z}_1, \ldots, \mathbf{Z}_n$ is given by ρ_{Z^n}. Now, the probability of the bad event Ω_{bad} can be equivalently described in this language as

$$\Pr\left[\vec{\mathbf{Z}} \in \Omega_{\mathrm{bad}}\right] = \mathrm{Tr}\left[\Gamma_{\vec{z} \in \Omega_{\mathrm{bad}}}\ \rho_{A^n}\right] := \sum_{\vec{z} \in \Omega_{\mathrm{bad}}} \mathrm{Tr}\left[\Gamma_{\vec{z}}\ \rho_{A^n}\right]. \tag{2.11}$$

We sometimes refer to $\Gamma_{\vec{z} \in \Omega_{\mathrm{bad}}}$ as the "failure" POVM element, since it represents the event that the lower bound has failed.

We now give some examples of concentration inequalities that shall be used in this thesis.

2.3.1 Binomial distribution

The prototypical example of a binomial distribution is that of n flips of a biased coin where the probability of heads is p. Here, we model the coin flips as n IID random variables $\mathbf{Z}_i$

which take value 1 if the outcome of the coin is heads, and 0 if it is tails. The probability of obtaining exactly l heads is $\binom{n}{l}p^l(1-p)^{n-l}$. Thus, the probability of getting at most l heads is $\sum_{j=0}^{l}\binom{n}{j}p^j(1-p)^{n-j}$. Thus, we obtain the concentration inequality,

$$\Pr\left[\mathbf{S}_n < \mathbb{E}(\mathbf{S}_n) - n\gamma_{\text{binom}}\right] = \Pr\left[\mathbf{S}_n < np - n\gamma_{\text{binom}}\right] \leq \sum_{j=0}^{\lfloor np - n\gamma_{\text{binom}}\rfloor} \binom{n}{j} p^j (1-p)^{n-j}. \tag{2.12}$$

In a quantum information context, the binomial distribution arises as the outcome of an n round IID state $\rho^{\otimes n}$ acted on by a two-outcome IID measurement $\{\Gamma_0, \Gamma_1\}$ in each round. Now, when using this inequalities in QKD we would typically not know the value of p, as the state ρ is unknown (and the output of the adversary's attack). In this case, the n rounds are broken up into a k round test set, and an $n-k$ round key generation set. Then the concentration inequality can be used with the observations in the k test rounds to estimate the value of p.

Notational aside 2.7. We use the notation $\vec{\mathbf{Z}}_{\text{test}} \coloneqq \{\mathbf{Z}_i |\ i \text{ is a test round}\}$ to denote the random variables $\mathbf{Z}_i$ in the test set, and similarly $\vec{\mathbf{Z}}_{\text{key}}$ to denote the random variables in the key generation set. For binomial random variables, we we use the notation $\left|\vec{\mathbf{Z}}_{\text{test}}\right| \coloneqq \sum_{i \text{ is a test round}} \mathbf{Z}_i$, and similarly for key generation rounds.

Alternately, the concentration inequality can be used twice, with a union bound to bound the deviation in the number of 1s in the test set from the number of 1s in the key generation set. For example, we can obtain an upper bound on the number of 1s in the key generation set as follows

$$\begin{aligned}
&\left|\vec{\mathbf{Z}}_{\text{test}}\right| \underset{\varepsilon_1}{\geq} kp - k\underline{\gamma_{\text{binom}}}(\varepsilon_1, k) \\
&\left|\vec{\mathbf{Z}}_{\text{key}}\right| \underset{\varepsilon_2}{\leq} (n-k)p + (n-k)\overline{\gamma_{\text{binom}}}(\varepsilon_2, n-k) \\
\implies &\left|\vec{\mathbf{Z}}_{\text{key}}\right| \underset{\varepsilon_1+\varepsilon_2}{\leq} \frac{n-k}{k}\left|\vec{\mathbf{Z}}_{\text{test}}\right| + (n-k)\left(\underline{\gamma_{\text{binom}}}(\varepsilon_1, k) + \overline{\gamma_{\text{binom}}}(\varepsilon_2, n-k)\right).
\end{aligned} \tag{2.13}$$

The failure event in this case can be defined as $\Omega_{\text{bad}} \coloneqq \{\vec{z} \mid |\vec{z}_{\text{key}}| > \frac{n-k}{k}|\vec{z}_{\text{test}}| + (n-k)\left(\underline{\gamma_{\text{binom}}}(\varepsilon_1, k) + \overline{\gamma_{\text{binom}}}(\varepsilon_2, n-k)\right)\}$.

Although the functions $\underline{\gamma_{\text{binom}}}$ and $\overline{\gamma_{\text{binom}}}$ are well-studied and can be numerically computed, there is no analytical expression for them. Thus, sometimes Hoeffding's inequality is used for this analysis instead, as described below.

2.3.2 Hoeffding's inequality

Hoeffding's inequality [37, Theorem 2] is a more general concentration inequality, and can be used for n independent (but not identical) random variables $\mathbf{Z}_1, \ldots, \mathbf{Z}_n$ which take values in some bounded range $a_i \leq \mathbf{Z}_i \leq b_i$. The concentration inequality can be expressed as

$$\mathbf{S}_n \underset{\varepsilon}{\geq} \mathbb{E}[\mathbf{S}_n] - n\underline{\gamma_{\text{hoeff}}}(\varepsilon, n), \quad \text{where}$$

$$\underline{\gamma_{\text{hoeff}}}(\varepsilon, n) \coloneqq \sqrt{\frac{1}{2n^2} \sum_{i=1}^{n} (b_i - a_i)^2 \ln\left(\frac{1}{\varepsilon}\right)},$$

and similarly for the upper bound, where $\overline{\gamma_{\text{hoeff}}} = \underline{\gamma_{\text{hoeff}}} =: \gamma_{\text{hoeff}}$.

Hoeffding's inequality can also be used for IID binomial random variables, where $a_i = 0$ and $b_i = 1$ for all i. Thus, $\underline{\gamma_{\text{binom}}} \leq \gamma_{\text{hoeff}}$, and $\overline{\gamma_{\text{binom}}} \leq \gamma_{\text{hoeff}}$. This introduces some looseness, but yields a simple closed-form expression in the analysis which might be simpler.[6]

Similar to the binomial distribution, Hoeffding's inequality can be used in quantum information on the outcome of n independent measurements on an n round tensor product (but not necessarily IID) state.

For another application of Hoeffding's inequality, consider the following scenario. Let $\vec{z}$ be an n-bit string. We "test" the bit as follows. Each round we pick an index j to be included in the test set Ω_{test} uniformly at random. The value of the bit at index j is a random variable (where the randomness is over the choice of index) which we call $\mathbf{Z}_i$ for round i of the test. Note that since each round we pick the index independently of the indices picked in other rounds, $\mathbf{Z}_1, \ldots, \mathbf{Z}_k$ form a set of k IID random variables. Further, note that the expectation value of each $\mathbf{Z}_i$ is the fraction of 1s in the string. Thus, Hoeffding's inequality[7] can be used to bound the Hamming weight[8] of the entire string $\vec{z}$ in terms of the Hamming weight of the test string.

[6] Sharper closed-form bounds are also available; see, for instance, [38] for an exposition of such tail bounds.

[7] The results discussed in Section 2.3.1 can also be used here since the $\mathbf{Z}_i$ are IID binomial random variables.

[8] This is the number of 1s ($|\vec{z}|$) in the string.

This scenario of sampling with replacement is not directly applicable to our work. Instead, it is more typical to consider a scenario where each index is picked ensuring that no index is picked twice, also referred to as sampling without replacement. For instance, consider an n round state $\rho_{A^n} \in \mathrm{S}_\circ(A^n)$, measured by an IID 2-outcome POVM $\{\Gamma_1, \Gamma_2\}$. In a QKD protocol such a state is the output of the adversary Eve's attack, and so we typically cannot assume that the state is IID or in a tensor product. The outcome of this measurement is a bit string. We can randomly pick a subset of size k to test on. The values of the bits in this subset are the values of the random variables $\mathbf{Z}_1, \ldots, \mathbf{Z}_k$. Note that these random variables are not independent, but the bounds obtained from sampling with replacement (such as Hoeffding's inequality) hold even if we sample without replacement [37, Theorem 4].

Remark 2.1 (Hoeffding not tight)**.** *For sampling without replacement, one might expect that as $k \to n$, the test set is representative of the entire set, and so the probability of deviation should go to 0. However, this is not the case when we use Hoeffding's inequality which only depends on the size of the test set, and not the size of the entire string. Serfling's inequality [39] is a sharpening of Hoeffding's inequality, though it too does not satisfy this property.*

2.3.3 Serfling's inequality

We first state the original form of Serfling's inequality for sampling without replacement.

Lemma 2.1 (Serfling [39, Corollary 1.1])**.** *Consider an n bit string where μ is the fraction of 1s in the string. Let $\mathbf{Z}_1, \ldots, \mathbf{Z}_k$ be the random variables corresponding to the value of bits in a randomly picked subset of size k. Then*

$$\sum_{i=1}^{k} \mathbf{Z}_i \underset{\varepsilon}{\leq} k\mu + k\gamma_{\mathrm{serf}}(\varepsilon, k, n), \quad \textit{where}$$

$$\gamma_{\mathrm{serf}}(\varepsilon, k, n) \coloneqq \sqrt{\frac{1 - \frac{k-1}{n}}{2k} \ln\left(\frac{1}{\varepsilon}\right)}.$$

Recall that the random variables $\mathbf{Z}_1, \ldots, \mathbf{Z}_k$ need not be independent or identical. Further, note the improvement over Hoeffding's inequality: $\gamma_{\mathrm{hoeff}}(\varepsilon, k) = \sqrt{\frac{1}{2k} \ln\left(\frac{1}{\varepsilon}\right)}$.

As already discussed in this section, we often wish to find the deviation of the fraction of 1s in the test set, from the fraction of 1s in the rest of the string. We will derive this from Lemma 2.1, closely follow the description in [40, Supplementary Note 2].

First, we define $\mathbf{S}_{\text{test}} = \sum_{i=1}^{k} \mathbf{Z}_i$, and $\mathbf{S}_{\text{key}} = \sum_{i=k+1}^{n} \mathbf{Z}_i$. We wish to find $\overline{\gamma_{\text{serf}}}(\varepsilon, k, n)$ such that

$$\frac{1}{n-k}\mathbf{S}_{\text{key}} \underset{\varepsilon}{\leq} \frac{1}{k}\mathbf{S}_{\text{test}} + \overline{\gamma_{\text{serf}}}(\varepsilon, k, n). \tag{2.14}$$

Note that $\mathbf{S}_{\text{test}} + \mathbf{S}_{\text{key}} = n\mu$, so that Eq. (2.14) can be rewritten as

$$\frac{1}{n-k}\mathbf{S}_{\text{key}} \underset{\varepsilon}{\leq} \mu + \frac{k}{n}\overline{\gamma_{\text{serf}}}(\varepsilon, k, n).$$

Now we directly use Lemma 2.1 to obtain

$$\overline{\gamma_{\text{serf}}}(\varepsilon, k, n) = \frac{n}{k}\sqrt{\frac{1 - \frac{n-k-1}{n}}{2(n-k)} \ln\left(\frac{1}{\varepsilon}\right)}. \tag{2.15}$$

An important property of $\overline{\gamma_{\text{serf}}}(\varepsilon, k, n)$ that we shall make use of in Chapter 6 is that $\overline{\gamma_{\text{serf}}}(\varepsilon, k-x, n-x)$ is a monotonically increasing function of $x \in [0, k)$. This can be seen as follows. First, we rewrite Eq. (2.15) as

$$\overline{\gamma_{\text{serf}}}(\varepsilon, k, n) = \frac{1}{k}\sqrt{\frac{n(k+1)}{2(n-k)} \ln\left(\frac{1}{\varepsilon}\right)}, \tag{2.16}$$

so that

$$\overline{\gamma_{\text{serf}}}(\varepsilon, k-x, n-x) = \sqrt{\frac{n-x}{k-x} \cdot \frac{k+1-x}{k-x} \cdot \frac{1}{2(n-k)} \ln\left(\frac{1}{\varepsilon}\right)},$$

where monotonicity can be established from noting that $\frac{a-x}{b-x}$ is a monotonically increasing function of $x \in [0, b)$ when $b < a$. Further, $\overline{\gamma_{\text{serf}}}(\varepsilon, k, n)$ is a monotonically decreasing function of n, as can be readily verified from Eq. (2.16).

Chapter 3

A toolbox for the theoretical analysis of practical QKD protocols

> "Remember that all models are wrong; the practical question is how wrong do they have to be to not be useful."
>
> — George E. P. Box

This chapter introduces the theoretical 'toolbox' required for the analysis of practical QKD protocols. The tools presented here provide methods to reduce complex, imperfect physical systems to simpler, idealised models amenable to security analysis. Specifically, we will formalise QKD security definitions and then introduce two reduction techniques: source maps for handling imperfect state preparations, and squashing maps for imperfect detection setups.

3.1 Protocol description

QKD is a quantum information processing task where two parties, Alice and Bob attempt to share a random bit string in the presence of a malicious eavesdropper, Eve. The resources assumed available to Alice and Bob for this purpose are

- a source of **private classical randomness**,

- an **insecure quantum channel** between Alice and Bob which Eve has full control over, and
- multiple uses of a **classical authenticated channel**. Here, a classical authenticated channel is a classical channel between Alice and Bob which Eve can read, but not modify.[1]

The main subtleties in this work, however, will arise not from the communication resources themselves, but from the details of how quantum states are prepared and detected. Depending on the arrangement of source and receiver modules involved, QKD protocols are typically grouped into three broad types:

- Prepare-and-measure (PM) protocols: Alice prepares states which are transmitted to Bob over the (insecure) quantum channel, who then performs the measurement.
- Entanglement-based (EB) protocols: Eve prepares and sends states to both Alice and Bob, who perform the measurements.
- Measurement-device–independent (MDI) protocols: Both Alice and Bob prepare states and send them to Eve, who performs the measurement.

Here, we explicitly consider PM QKD protocols as they contain both a trusted source description and a trusted receiver module description[2], though much of our analysis is applicable to all three types of QKD protocols.

We now outline the steps in a generic (fixed length)[3] PM protocol.

1. **Signal Preparation:** Alice randomly prepares one of a set of quantum states $\{\rho_i\}_{i=1}^{d_{\mathrm{A}}}$ each with probability $\{p_i\}_{i=1}^{d_{\mathrm{A}}}$. Sometimes Alice's state preparation is described by more than one parameter (for example, intensity and polarisation of coherent state prepared). We refer to her choice of state prepared i as her setting choice.

[1] Strictly speaking, one can only implement [41, 42] a weaker version of authentication, i.e., a classical channel that either transmits the same output as the input, *or* outputs a flag declaring that the transmission has failed/aborted. While care must be taken to analyse the security of QKD protocols that use this weaker resource, much of the analysis remains exactly the same if one aborts the QKD protocol whenever authentication aborts. Thus, in the interest of pedagogy, we make the common assumption of access to the stronger authenticated classical channel which never aborts.

[2] By "trusted" we mean that a quantum mechanical description of the device is fixed and not under adversarial control, though small deviations from this are tolerated when modelling imperfections.

[3] More commonly used protocols are generally "variable length" protocols, where the key length is decided based on the measured test data. However, for our work this distinction is not important, and we present the more pedagogically accessible fixed length variant.

2. **Measurement:** Bob measures the states that he receives by a n_{B}-outcome POVM $\{\Gamma_j\}_{j=1}^{n_{\mathrm{B}}}$ and records the outcome from each round.

After repeating the above steps n times, we proceed to the next part of the protocol.

3. **Announcements:** Alice and Bob make announcements over the authenticated classical channel. Importantly, in our work we restrict our attention to protocols where all announcements are made only after Alice and Bob complete all their signal preparation and measurement steps.

4. **Parameter estimation:**[4] Alice and Bob randomly choose a subset of the rounds for testing. They announce their measurement outcomes on this subset of rounds, and decide whether to accept or abort the protocol based on their announcements. We denote the event that they accept the protocol as Ω_{acc}.

5. **Sifting:** Alice and Bob sift the data based on the announcements made i.e. based on the announcements, they choose a subset of protocol rounds to keep and discard the rest. This is also referred to as post-selection[5].

6. **Key Map:** Alice[6] uses her signal state data as well as the announcements to map it into a key string. This is called the raw key.

7. **Error Correction:** Alice and Bob perform error correction, which results in Bob outputting a guess of Alice's raw key.

8. **Privacy Amplification:** Alice and Bob produce their final secret key of predetermined length[7] l by applying a common (communicated over the authenticated classical channel) two-universal hash function on the raw key.

Alice, Bob and Eve's state at the end of the QKD protocol is given by $\rho_{K_A K_B E_{\mathrm{fin}}}$, where E_{fin} includes all classical communication during the protocol.

[4] This is sometimes more accurately (for fixed length protocols) referred to as acceptance testing.

[5] Not to be confused with the postselection technique; a common QKD security proof approach which we discuss in Chapter 5.

[6] Bob could also perform the key map. This is called reverse reconciliation. In that case Alice and Bob's roles in the next steps are reversed.

[7] See previous footnote about variable length protocols.

3.2 Security definition

The most important criterion for a security definition to satisfy is that it is composably secure, i.e., the keys generated from a QKD protocol can safely be used as part of a larger cryptographic protocol [43, 44]. Such a definition is formalised [45, 46, 47, 48, 49, 50] by quantifying how indistinguishable the real implementation of a QKD protocol is from an idealized resource that either outputs a uniformly random and identical secret key to Alice and Bob, or aborts. The indistinguishability is measured [51, 52] by the trace distance[8] between the real output state $\rho_{K_A K_B E_{\text{fin}}}$ and the corresponding ideal state, and a protocol is called ε-secure if this distance is at most ε:

Definition 3.1 (Security definition)**.** Let $\varepsilon \in [0,1]$ be the security parameter, and let $\rho_{K_A K_B E_{\text{fin}}}$ be Alice, Bob and Eve's state output at the end of the QKD protocol, where E_{fin} includes all classical communication during the protocol. Such a protocol is said to be an *ε-secure QKD protocol* if

$$\Pr[\Omega_{\text{acc}}] \left\| \rho_{K_A K_B E_{\text{fin}}|\Omega_{\text{acc}}} - \sum_{k\in\{0,1\}^l} \frac{1}{2^l} |kk\rangle\langle kk|_{K_A K_B} \otimes \rho_{E_{\text{fin}}|\Omega_{\text{acc}}} \right\|_1 \leq \varepsilon. \tag{3.1}$$

A simple application of the triangle inequality allows us to decompose the security statement into two conditions [51]:

(i) correctness, requiring Alice and Bob's keys to agree, and

(ii) secrecy, requiring the key to be uniform and independent of Eve's system.

Correctness only depends on Alice and Bob's honest behaviour and is thus generally easier to prove. On the other hand, secrecy requires a careful consideration of Eve's attack. Thus, we restrict our attention to proving secrecy:

Definition 3.2. Let $\varepsilon_{\text{sec}} \in [0,1]$ be the secrecy parameter, and let $\rho_{K_A E_{\text{fin}}}$ be Alice and Eve's state output at the end of the QKD protocol, where E_{fin} includes all classical communication during the protocol. Such a protocol is said to be an *ε_{sec}-secret QKD protocol*

[8] Strictly speaking, all the composability proofs assume that the QKD protocol can be modelled as a channel that outputs Alice, Bob and Eve's joint quantum state at the end. More realistic models of QKD protocols, such as quantum combs [53] or causal boxes [54], take into account the interactive nature of the protocol.

if

$$\Pr[\Omega_{\text{acc}}] \left\| \rho_{K_A E_{\text{fin}}|\Omega_{\text{acc}}} - \sum_{k\in\{0,1\}^l} \frac{1}{2^l} |k\rangle\langle k|_{K_A} \otimes \rho_{E_{\text{fin}}|\Omega_{\text{acc}}} \right\|_1 \leq \varepsilon_{\text{sec}}. \tag{3.2}$$

The secrecy definition above is stated entirely in terms of the output state of the QKD protocol, without reference to the process itself. For our purposes, however, it is more useful to make the QKD protocol an explicit part of the definition. We therefore restate the secrecy criterion below.

First note that Alice's random state preparation described in protocol step 1 can be equivalently represented by a preparation of the classical-quantum state $\rho^{\text{prep}}_{AA'} = \sum_i^{d_A} p_i |i\rangle\langle i|_A \otimes \rho_i$, followed by a measurement of the A register in the computational basis. Next, instead of preparing and measuring such a state in each round, we model the protocol as preparing $(\rho^{\text{prep}}_{AA'})^{\otimes n}$ at the start of the protocol, and then measuring Alice's registers A^n round by round. Alice's measurements commute with Eve's attacks as they act on different subsystems. Thus, without loss of generality, we can assume that Eve attacks the A' subsystem at the very start of the protocol (before Alice's measurements).

Thus, the output state of the QKD protocol can be described as

$$\rho_{K_A E_{\text{fin}}} = \mathcal{E}^{(l)}_{\text{QKD}} \circ \mathcal{A}\left[(\rho^{\text{prep}}_{AA'})^{\otimes n}\right],$$

where $\mathcal{A} \in \mathcal{C}\left(A'^n, B^n E^n\right)$ represents Eve's attack, and $\mathcal{E}^{(l)}_{\text{QKD}} \in \mathcal{C}\left(A^n B^n E^n, K_A E_{\text{fin}}\right)$ represents the rest of the QKD protocol (including Alice's computational basis measurements) and acts as the identity on Eve's subsystems E^n. Similarly, the ideal state can be described as

$$\mathcal{E}^{(l),\text{ideal}}_{\text{QKD}} \circ \mathcal{A}\left[(\rho^{\text{prep}}_{AA'})^{\otimes n}\right],$$

where $\mathcal{E}^{(l),\text{ideal}}_{\text{QKD}}$ is a channel which first performs $\mathcal{E}^{(l)}_{\text{QKD}}$, and then replaces the key register with $\sum_{k\in\{0,1\}^l} \frac{1}{2^l} |k\rangle\langle k|_{K_A}$ if the protocol accepts. With this reformulation, we can equivalently restate the secrecy criterion.

Notational aside 3.1 (QKD protocol)**.** We will represent a QKD protocol by the tuple $\{\mathcal{E}^{(l)}_{\text{QKD}}, (\rho^{\text{prep}}_{AA'})^{\otimes n}\}$, as this fully characterises the trusted portion of the protocol. When the details of the state preparation are unimportant, we will represent the protocol

simply by $\mathcal{E}^{(l)}_{\mathrm{QKD}}$.

Definition 3.3 (Secrecy)**.** Let $\varepsilon_{\mathrm{sec}} \in [0,1]$ be the secrecy parameter, and let $\{\mathcal{E}^{(l)}_{\mathrm{QKD}}, (\rho^{\mathrm{prep}}_{AA'})^{\otimes n}\}$ be a QKD protocol. Such a protocol is said to be an $\varepsilon_{\mathrm{sec}}$-*secret QKD protocol* if

$$\sup_{\mathcal{A}\in\mathcal{C}(A'^n,B^nE^n)} \left\| \left(\mathcal{E}^{(l)}_{\mathrm{QKD}} - \mathcal{E}^{(l),\mathrm{ideal}}_{\mathrm{QKD}}\right) \circ \mathcal{A}\left[(\rho^{\mathrm{prep}}_{AA'})^{\otimes n}\right] \right\|_1 \leq \varepsilon_{\mathrm{sec}}. \tag{3.3}$$

The supremum in the definition reflects the fact that $\varepsilon_{\mathrm{sec}}$-secrecy must hold against *all* attacks $\mathcal{A} \in \mathcal{C}(A'^n, B^nE^n)$. We might sometimes want to restrict the supremum to a subset $\mathbb{A} \subset \mathcal{C}(A'^n, B^nE^n)$. We say that the QKD protocol is then $\varepsilon_{\mathrm{sec}}$-*secret against* $\mathbb{A}$.

Technical aside 3.1 (What is A?)**.** Note that the secrecy definition Definition 3.3 can be used for PM, EB and MDI QKD protocols, where the roles of A and A' depend on the setting. For EB QKD protocols, the register A is register. For MDI QKD protocols, A consists of classical registers for Alice and Bob, while A' consists of the quantum states they prepare.

Protocol	$(A,\ A')$
PM	(Alice's classical choice, Alice'squantum states)
EB	(Trivial, Eve's information prior to QKD protocol)
MDI	(Alice+Bob classical registers, their quantum states)

3.3 Source-replacement scheme

QKD security proofs often contain a simplifying step where Eve is assumed to hold a purification $\rho_{A^nB^nE^n}$ of Alice and Bob's joint state after her attack $\mathcal{A}$. Note that such a purification implicitly includes a purification of Alice's initially prepared state $(\rho^{\mathrm{prep}}_{AA'})^{\otimes n}$. In particular, $\rho_{A^nB^nE^n}$ includes a purification of the classical, private A register. Thus, naively using these proof techniques would directly reveal Alice's choices to Eve, making secrecy impossible. In addition to this, if Alice prepares mixed states $\{\rho_i\}_{i=1}^{d_{\mathrm{A}}}$, Eve would be given a purification of this as well, which introduces looseness in the analysis. To address this issue, we employ the source-replacement scheme [55, 56, 57] and shield systems [58] to restate the QKD protocol as one where Alice's initial state preparation is pure.

Lemma 3.1 (Shield system)**.** *Let* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right\}$ *be a QKD protocol, where Alice's state preparation* $\rho_{AA'}^{\mathrm{prep}} = \sum_{i=1}^{d_{\mathrm{A}}} p(i) \left|i\right\rangle\!\left\langle i\right|_A \otimes \rho_i$*. Let* $\left\{\mathcal{E}_{\mathrm{QKD-shield}}^{(l)}, (\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right\}$ *be another QKD protocol differing only in Alice's state preparation*

$$\rho_{AA_SA'}^{\mathrm{prep}} = \sum_{i=1}^{d_A} p(i) \left|i\right\rangle\!\left\langle i\right|_A \otimes \left|\rho_i\right\rangle\!\left\langle \rho_i\right|_{A_SA'}, \tag{3.4}$$

and that A_S *(termed the* shield system*) is not sent to Bob and is traced out by Alice. Here,* $|\rho_i\rangle$ *is a purification of Alice's signal state* $\rho_i = \mathrm{Tr}_{A_S}\left[|\rho_i\rangle\!\langle\rho_i|\right]$*. Then, the* $\varepsilon_{\mathrm{sec}}$*-secrecy of* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right\}$ *is equivalent to the* $\varepsilon_{\mathrm{sec}}$*-secrecy of* $\left\{\mathcal{E}_{\mathrm{QKD-shield}}^{(l)}, (\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right\}$*.*

Proof. Since the QKD protocol $\left\{\mathcal{E}_{\mathrm{QKD-shield}}^{(l)}, (\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right\}$ traces out the shield system A_S^n, we may write $\mathcal{E}_{\mathrm{QKD-shield}}^{(l)} = \mathcal{E}_{\mathrm{QKD}}^{(l)} \circ \mathrm{Tr}_{A_S^n}$, and $\mathcal{E}_{\mathrm{QKD-shield}}^{(l),\mathrm{ideal}} = \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \circ \mathrm{Tr}_{A_S^n}$. Thus, for any attack $\mathcal{A}$,

$$\begin{aligned}\left\|\left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}\right) \circ \mathcal{A}\left[(\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right]\right\|_1 &= \left\|\left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}\right) \circ \mathcal{A} \circ \mathrm{Tr}_{A_S^n}\left[(\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right]\right\|_1 \\ &= \left\|\left(\mathcal{E}_{\mathrm{QKD-shield}}^{(l)} - \mathcal{E}_{\mathrm{QKD-shield}}^{(l),\mathrm{ideal}}\right) \circ \mathcal{A}\left[(\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right]\right\|_1,\end{aligned}$$

where the last equality follows since Eve's attack does not act on the shield system A_S^n. Taking the supremum over all attacks $\mathcal{A}$ establishes the claim. □

Lemma 3.2 (Source-replacement scheme)**.** *Let* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right\}$ *be a QKD protocol where Alice's state preparation* $\rho_{AA_SA'}^{\mathrm{prep}} = \sum_{i=1}^{d_A} p(i) \left|i\right\rangle\!\left\langle i\right|_A \otimes \left|\rho_i\right\rangle\!\left\langle \rho_i\right|_{A_SA'}$*, and where* $\mathcal{E}_{\mathrm{QKD}}^{(l)}$ *measures Alice's register* A *in the computational basis at the start of each round. Let* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, \rho_{AA_SA'}^{\otimes n}\right\}$ *be another QKD protocol differing only in Alice's (pure) state preparation*

$$\rho_{AA_SA'} = \sum_{i,j=1}^{d_A} \sqrt{p(i)p(j)} \left|i\right\rangle\!\left\langle j\right|_A \otimes \left|\rho_i\right\rangle\!\left\langle \rho_j\right|_{A_SA'}. \tag{3.5}$$

Then, the $\varepsilon_{\mathrm{sec}}$*-secrecy of* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n}\right\}$ *is equivalent to the* $\varepsilon_{\mathrm{sec}}$*-secrecy of* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, \rho_{AA_SA'}^{\otimes n}\right\}$*.*

Proof. Let $\Psi_{\mathrm{meas}} \in \mathcal{C}(A, A)$ be the measurement channel with Kraus operators $\{|i\rangle\langle i|_A\}_{i=1}^{d_{\mathrm{A}}}$. Since $\mathcal{E}_{\mathrm{QKD}}^{(l)}$ measures Alice's register A in the computational basis, $\mathcal{E}_{\mathrm{QKD}}^{(l)} = \mathcal{E}_{\mathrm{QKD}}^{(l)} \circ \Psi_{\mathrm{meas}}^{\otimes n}$ and $\mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} = \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \circ \Psi_{\mathrm{meas}}^{\otimes n}$. Then, for any attack $\mathcal{A}$,

$$\begin{aligned}
\left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \right) \circ \mathcal{A} \left[(\rho_{AA_SA'})^{\otimes n} \right] \right\|_1 &= \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \right) \circ \mathcal{A} \circ \Psi_{\mathrm{meas}}^{\otimes n} \left[(\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n} \right] \right\|_1 \\
&= \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \right) \circ \Psi_{\mathrm{meas}}^{\otimes n} \circ \mathcal{A} \left[(\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n} \right] \right\|_1 \\
&= \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \right) \circ \mathcal{A} \left[(\rho_{AA_SA'}^{\mathrm{prep}})^{\otimes n} \right] \right\|_1,
\end{aligned}$$

where the first equality follows from the definition of the state preparation $\Psi_{\mathrm{meas}}[\rho_{AA_SA'}] = \rho_{AA_SA'}^{\mathrm{prep}}$, and the second last equality follows since Eve's attack does not Alice's register A^n. Taking the supremum over all attacks $\mathcal{A}$ establishes the claim. □

Using Lemmas 3.1 and 3.2 it suffices to prove security only for a source-replaced protocol where Alice's initial state preparation $\rho_{AA_SA'}^{\otimes n}$ is pure. Consequently, the common simplification that Eve holds a purification of Alice and Bob's joint state introduces no looseness in the analysis.

Remark 3.1. *[Secrecy with respect to state after Eve's attack] After applying the source-replacement scheme, the $\varepsilon_{\mathrm{sec}}$-secrecy condition can be equivalently described in terms of the state $\rho_{A^nA_S^nB^nE^n}$ after Eve's attack by identifying $\rho_{A^nA_S^nB^nE^n} = \mathcal{A}\left[\rho_{AA_SA'}^{\otimes n}\right]$ in the above formulae:*

$$\sup_{\substack{\rho_{A^nA_S^nB^nE^n} \in \mathrm{S}_\circ\left(A^nA_S^nB^nE^n\right) \\ \mathrm{Tr}_{B^nE^n}\left[\rho_{A^nA_S^nB^nE^n}\right] = \mathrm{Tr}_{A'^n}\left[(\rho_{AA_SA'})^{\otimes n}\right]}} \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \right) \left[\rho_{A^nA_S^nB^nE^n} \right] \right\|_1 \leq \varepsilon_{\mathrm{sec}}, \tag{3.6}$$

where the constraint $\mathrm{Tr}_{B^nE^n}\left[\rho_{A^nA_S^nB^nE^n}\right] = \mathrm{Tr}_{A'^n}\left[(\rho_{AA_SA'})^{\otimes n}\right]$ represents that Eve's attack $\mathcal{A}$ does not act on Alice's secret and shield systems AA_S. Moreover, since the trace norm is monotonically decreasing under channels, the supremum in Eq. (3.6) can equivalently be written in terms of $\rho_{A^nA_S^nB^n}$ as

$$\sup_{\substack{\rho_{A^nA_S^nB^n} \in \mathrm{S}_\circ\left(A^nA_S^nB^n\right) \\ \mathrm{Tr}_{B^n}\left[\rho_{A^nA_S^nB^n}\right] = \mathrm{Tr}_{A'^n}\left[(\rho_{AA_SA'})^{\otimes n}\right]}} \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}} \right) \left[\rho_{A^nA_S^nB^nE^n} \right] \right\|_1 \leq \varepsilon_{\mathrm{sec}}, \tag{3.7}$$

with $\rho_{A^nA_S^nB^nE^n}$ taken to be any purification of $\rho_{A^nA_S^nB^n}$.

Notational aside 3.2 (Fixed marginal constraint)**.** We refer to the constraint $\mathrm{Tr}_{B^n}\left[\rho_{A^nB^n}\right] = \mathrm{Tr}_{A'^n}\left[(\rho_{AA_SA'})^{\otimes n}\right]$ as the *fixed marginal constraint*. Note that in the source-replacement picture, the QKD protocol can be equivalently specified by the tuple $\left\{\mathcal{E}^{(l)}_{\mathrm{QKD}}, \mathrm{Tr}_{A'}\left[\rho_{AA_SA'}\right]\right\}$ as the fixed marginal constraint contains all the information about the state preparation. Further, for brevity, we omit the shield system A_S from the notation whenever it plays no role in the argument. In this case, the shield system A_S can be understood to be a part of Alice's register A.

Technical aside 3.2 (Intermediate source-replacement schemes)**.** In Lemma 3.2 we have considered two extreme cases — a pure, entangled state preparation $\rho_{AA_SA'}$, and the separable state $\rho^{\mathrm{prep}}_{AA_SA'}$. However, note that the essential requirement on the states to prove the equivalence stated in Lemma 3.2 was that $\Psi_{\mathrm{meas}}[\rho_{AA_SA'}] = \rho^{\mathrm{prep}}_{AA_SA'}$. Thus, any state $\rho^{\mathrm{int}}_{AA_SA'}$ such that $\Psi_{\mathrm{meas}}[\rho^{\mathrm{int}}_{AA_SA'}] = \rho^{\mathrm{prep}}_{AA_SA'}$ may be employed in the security analysis. Such intermediate states are potentially useful in analysing protocols where Alice's signal states $\{\rho_i\}_{i=1}^{d_{\mathrm{A}}}$ are not known exactly.

3.4 Simplifying analysis of practical devices

Lemmas 3.1 and 3.2 are sufficient to analyse the security of idealised qubit protocols. However, current implementations of QKD protocols typically use quantum optical setups, which deviate significantly from the qubit assumption. In particular, these optical systems are infinite-dimensional, leading to technical complications and making numerical analysis more challenging. With this motivation in mind, we now introduce some general tools to simplify the analysis of QKD protocols. These tools are, in fact, broadly applicable, so we first present the general structure of the argument in an abstract setting before specialising to QKD.

3.4.1 Abstract reduction argument

We consider a generic two-party adversarial setting in which the trusted operations are Alice's preparation of one of a set of states $\vec{\rho}$ and Bob's measurement with a POVM $\vec{\Gamma}$, while the adversary Eve is allowed to apply an arbitrary channel $\mathcal{A}$ between them. Within this setting, we consider "imperfect" state preparation and measurement. Here, an

"imperfect" (or real) device denotes the target model of interest, whereas a "perfect" (or virtual) device denotes an idealised abstraction that is tractable for theoretical analysis.

The performance for such a protocol is quantified by a cost function $f(\mathcal{A}|\vec{\rho},\vec{\Gamma})$, which evaluates the effect of Eve's attack $\mathcal{A}$ given Alice and Bob's trusted preparation $\vec{\rho}$ and measurement $\vec{\Gamma}$. This cost function is required to be small for all possible attacks $\mathcal{A}$. For instance, in QKD, such a cost function is instantiated by the secrecy definition Definition 3.3. As might be expected from the protocol structure, the cost function satisfies the property

$$f\left(\mathcal{A} \mid \Psi\left[\vec{\rho}\right], \Lambda^{\dagger}\left[\vec{\Gamma}\right]\right) = f\left(\Lambda \circ \mathcal{A} \circ \Psi \mid \vec{\tau}, \vec{\Gamma}\right), \tag{3.8}$$

for all channels Ψ, Λ.

This already suggests the form of the reduction, where the analysis of imperfect state preparation $\vec{\rho}$ can be reduced to the analysis of the perfect state preparation $\vec{\tau}$ whenever there exists a channel Ψ — called a *source map* — such that $\rho_i = \Psi[\tau_i]$ for all i. Similarly, the analysis of an imperfect measurement $\vec{\Gamma}$ can be reduced to the analysis of the perfect measurement $\vec{F}$ whenever there exists a channel Λ — called a *squashing map* — such that $\Gamma_j = \Lambda^{\dagger}[F_j]$ for all j. An intuitive explanation of this fact is depicted in Fig. 3.1 [1, Fig. 2.1] and Fig. 3.2 [2, Fig. 2]. We justify this more formally below.

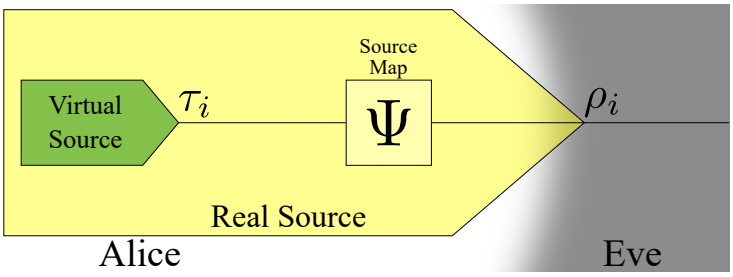
Theorem 3.1. *(Informal) Let $\vec{\rho} \subset \mathrm{S}_{\circ}(A)$ and $\vec{\Gamma} \subset \mathrm{Pos}(B)$ be the imperfect state preparation and measurement for an adversarial protocol. Let there exist a source map $\Psi \in \mathcal{C}(R, A)$ and perfect state preparation $\vec{\tau} \subset \mathrm{S}_{\circ}(R)$ such that $\rho_i = \Psi[\tau_i]$ for all i, and let there exist a squashing map $\Lambda \in \mathcal{C}(B, Q)$ and perfect measurement $\vec{F} \in \mathrm{Pos}(Q)$ such that $\Gamma_j = \Lambda^{\dagger}[F_j]$ for all j. Then for any subset (of attack channels) $\mathbb{A} \supset \Psi \circ \mathcal{C}(A, B) \circ \Lambda$,*

$$\sup_{\mathcal{A} \in \mathcal{C}(A,B)} f(\mathcal{A}|\vec{\rho},\vec{\Gamma}) \leq \sup_{\mathcal{A} \in \mathbb{A}} f(\mathcal{A}|\vec{\tau},\vec{F}), \tag{3.9}$$

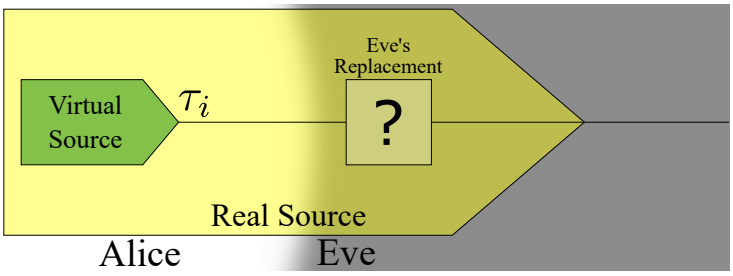
for any cost function f satisfying Eq. (3.8).

Proof. The proof is straightforward:

$$\begin{aligned}
\sup_{\mathcal{A} \in \mathcal{C}(A,B)} f(\mathcal{A}|\vec{\rho},\vec{\Gamma}) &= \sup_{\mathcal{A} \in \mathcal{C}(A,B)} f(\mathcal{A}|\Psi[\vec{\tau}],\Lambda^{\dagger}[\vec{F}]) \\
&= \sup_{\mathcal{A} \in \mathcal{C}(A,B)} f(\Lambda \circ \mathcal{A} \circ \Psi|\vec{\tau},\vec{F}) \\
&\leq \sup_{\mathcal{A} \in \mathbb{A}} f(\mathcal{A}|\vec{\tau},\vec{F}),
\end{aligned}$$



(a) We can model the real source as a virtual source followed by a source map since they both have the exact same output.



(b) Once we give Eve control of the source map, she can perform any physical operation on the output of the virtual source, including the source map Ψ if reproducing the real state is beneficial to her.

Figure 3.1: The imperfect source can always be replaced by the perfect source in security proofs if they are related via a source map since the imperfect source gives Eve more power. ([1, Fig. 2.1])

where the first equality follows from the squashing and source map conditions, the second equality follows from the structure of the two-party protocol as stated in Eq. (3.8), and the last inequality follows from the attack set condition $\mathbb{A} \supset \Psi \circ \mathcal{C}(A, B) \circ \Lambda$. □

Remark 3.2. *The set $\mathbb{A}$ can always be chosen to be $\mathcal{C}(R, Q)$ as the composition of channels is a channel.*

We will now specialise this argument to QKD, and give some useful examples. First, we detail source maps.

3.4.2 Source maps

We first state the formal statement of source maps before giving a common example useful for the analysis of decoy-state protocols [59, 60, 61].

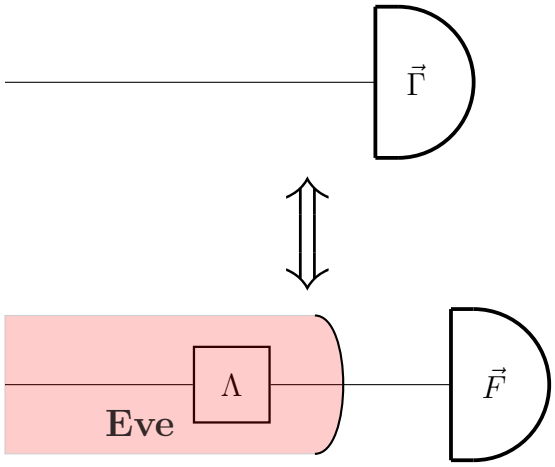


Figure 3.2: The imperfect POVM $\vec{\Gamma}$ can be modelled as a squashing map Λ followed by a perfect POVM $\vec{F}$. Giving the squashing map Λ to Eve lets us restrict our analysis to the perfect POVM $\vec{F}$. ([2, Fig. 2])

Corollary 3.1 (Source Maps)**.** *Let* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right\}$ *be a QKD protocol where Alice's state preparation is given by* $\rho_{AA'}^{\mathrm{prep}} = \sum_{i=1}^{d_{\mathrm{A}}} p(i) \left|i\right\rangle\!\left\langle i\right|_A \otimes \rho_i$*. Suppose there exists a source map* $\Psi \in \mathcal{C}(A'', A')$ *and a set of virtual states* $\{\tau_i\}_{i=1}^{d_{\mathrm{A}}} \subset \mathrm{S}_\circ(A')$ *such that* $\rho_i = \Psi[\tau_i]$ *for all* i*. Consider the corresponding virtual protocol* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\tau_{AA''}^{\mathrm{prep}})^{\otimes n}\right\}$ *where* $\tau_{AA''}^{\mathrm{prep}} = \sum_{i=1}^{d_{\mathrm{A}}} p(i) \left|i\right\rangle\!\left\langle i\right|_A \otimes \tau_i$*. Then, the* $\varepsilon_{\mathrm{sec}}$*-secrecy of* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\tau_{AA''}^{\mathrm{prep}})^{\otimes n}\right\}$ *implies the* $\varepsilon_{\mathrm{sec}}$*-secrecy of* $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right\}$.

Proof. The proof is a special case of the proof of Theorem 3.1 as follows. The source map relation $\rho_i = \Psi[\tau_i]$ for all i, implies that

$$\rho_{AA'}^{\mathrm{prep}} \;=\; (\mathrm{id}_{A^n} \otimes \Psi^{\otimes n})[\tau_{AA''}^{\mathrm{prep}}].$$

Thus,

$$\sup_{\mathcal{A} \in \mathcal{C}(A'^n, B^n E^n)} \left\| (\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}) \circ \mathcal{A}\left[(\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right] \right\|_1 \tag{3.10}$$

$$= \sup_{\mathcal{A} \in \mathcal{C}(A'^n, B^n E^n)} \left\| (\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}) \circ \mathcal{A} \circ \Psi^{\otimes n}\left[(\tau_{AA''}^{\mathrm{prep}})^{\otimes n}\right] \right\|_1$$

$$\leq \sup_{\mathcal{A}' \in \mathcal{C}(A''^n, B^n E^n)} \left\| (\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}) \circ \mathcal{A}'\left[(\tau_{AA''}^{\mathrm{prep}})^{\otimes n}\right] \right\|_1. \tag{3.11}$$

This chain of equations upper bounds the secrecy of $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right\}$ (Eq. (3.10)) with the secrecy of $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\tau_{AA''}^{\mathrm{prep}})^{\otimes n}\right\}$ (Eq. (3.11)), hence establishing the claim. □

Remark 3.3 (Correlated Source Maps)**.** *The proof straightforwardly extends to the case where the imperfect state preparation is not IID, even if we require the perfect states to be IID. In that case the required source map $\Psi \in \mathcal{C}\left(A''^n, A'^n\right)$ must act jointly across n rounds in a non-IID manner.*

As already noted, the real state preparation $\rho_{AA'}^{\mathrm{prep}}$ is fixed by the implementation. By contrast, the choice of virtual state preparation $\tau_{AA''}^{\mathrm{prep}}$ is a degree of freedom in the theoretical analysis, provided one can establish the existence of a suitable source map. In practice, such existence is typically demonstrated by giving an explicit construction of the source map.

An important example of source maps called tagging [62] is useful for the analysis of fully-phase randomised coherent states. In this case, the imperfection is the fact that the real states

$$\rho_{a,\mu} = \bigoplus_{m=0}^{\infty} p(m|\mu)\rho_{a,m} \in \mathrm{S}_{\circ}\left(\bigoplus_{m=0}^{\infty} \mathcal{H}_m\right) \tag{3.12}$$

are infinite-dimensional. In this case, finite-dimensional "tagged states" [62] can be constructed, where the space with photon number greater than N_{ph} is tagged as follows:

$$\tau_{a,\mu} = \bigoplus_{m=0}^{N_{\mathrm{ph}}} p(m|\mu)\rho_{a,m} + \left(1 - \sum_{m=0}^{N_{\mathrm{ph}}} p(m|\mu)\right) |a,\mu\rangle\langle a,\mu|\,, \tag{3.13}$$

where $\{|a,\mu\rangle\}_{a,\mu}$ form an orthonormal basis for a space orthogonal to $\bigoplus_{m=0}^{N_{\mathrm{ph}}} \mathcal{H}_m$. We state this formally below.

Lemma 3.3 (Tagged laser source)**.** *Let $\rho_{a,\mu} = \bigoplus_{m=0}^{\infty} p(m|\mu)\rho_{a,m} \in \mathrm{S}_{\circ}(\bigoplus_{m=0}^{\infty} \mathcal{H}_m)$ be the real state prepared by Alice corresponding to setting choice a, μ. Given $N_{\mathrm{ph}} \in \mathbb{N}$, let the virtual state prepared by Alice be*

$$\tau_{a,\mu} = \bigoplus_{m=0}^{N_{\mathrm{ph}}} p(m|\mu)\rho_{a,m} + \left(1 - \sum_{m=0}^{N_{\mathrm{ph}}} p(m|\mu)\right) |a,\mu\rangle\langle a,\mu|\,, \tag{3.14}$$

where $\{|a,\mu\rangle\}_{a,\mu}$ form an orthonormal basis for a space orthogonal to $\bigoplus_{m=0}^{N_{\mathrm{ph}}} \mathcal{H}_m$. Then there exists a channel Ψ_{tag} such that $\Psi_{\mathrm{tag}}[\tau_{a,\mu}] = \rho_{a,\mu}$ for all setting choices a, μ.

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

$$\frac{1}{\left(1-\sum_{m=0}^{N_{\text{ph}}} p(m|\mu)\right)} \bigoplus_{m=N_{\text{ph}}+1}^{\infty} p(m|\mu)\rho_{a,m};$$

and that acts as the identity on $\mathrm{L}\left(\bigoplus_{m=0}^{N_{\text{ph}}} \mathcal{H}_m\right)$. It is then straightforward to verify that $\Psi_{\text{tag}}[\tau_{a,\mu}] = \rho_{a,\mu}$. □

We explain the utility of tagging in more detail in Chapter 5. Source maps have also been used to address imperfect phase-randomisation [63], and to construct QKD protocols that are robust to side-channel attacks [64], and thus is a powerful tool to prove security of realistic QKD protocols. We now describe the application of squashing maps.

3.4.3 Squashing maps

The conceptual idea of squashing maps [65, 66, 67, 68], illustrated in Fig. 3.2, has been around for quite some time, and several variants have since been proposed. It is useful to distinguish between two distinct ways in which squashing maps can be applied in security proofs:

- **Part of security proof.** One can carry out most of the analysis using the real measurement and apply a squashing argument only at a later stage to simplify a specific part of the proof. This makes the reduction closely tied to specific proof techniques, limiting its general applicability. For example, the universal squasher [69] is a robust variant of the idea that is tied to phase-error–based approaches [7, 9], with no evident pathway to generalisation. Similarly, the dimension-reduction method [70] improves the numerical tractability of key-rate optimisations, but it can only be employed in proof techniques where the analysis easily reduces to a single-round numerical optimisation problem.

- **Security-definition reduction.** Alternatively, one can incorporate the squashing reduction directly into the security definition, so that the entire analysis is phrased in terms of the perfect measurement. This has the advantage that the reduction itself is independent of the proof technique being used.[9] This is the perspective we adopt in what follows.

[9]Strictly speaking, different proof techniques may require different choices of "perfect" settings, in the sense of what is deemed theoretically tractable. Thus there is some dependence on the proof technique in identifying the perfect model, but once fixed, the squashing reduction itself is technique-independent.

The following corollary formalises the reduction we will use.

Corollary 3.2 (Squashing)**.** *Let $\mathcal{E}^{(l)}_{\mathrm{QKD}}$ be a QKD protocol where Bob's measurement is described by the POVM $\{\Gamma_i\}_{i=1}^{n_{\mathrm{meas}}} \subset \mathrm{Pos}(B)$, and let $\mathcal{E}^{(l)}_{\mathrm{QKD-Sq}}$ be an otherwise identical protocol where Bob's measurement is described by the POVM $\{F_i\}_{i=1}^{n_{\mathrm{meas}}} \subset \mathcal{B}(Q)$. If there exists a channel $\Lambda \in \mathcal{C}(B, Q)$ such that $\Gamma_i = \Lambda^\dagger[F_i]$ for all i, and a set $\mathbb{A} \supset \Lambda^{\otimes n} \circ \mathcal{C}(A'^n, B^n E^n)$, then the $\varepsilon_{\mathrm{sec}}$-secrecy of $\mathcal{E}^{(l)}_{\mathrm{QKD-Sq}}$ against $\mathbb{A}$ implies the $\varepsilon_{\mathrm{sec}}$-secrecy of $\mathcal{E}^{(l)}_{\mathrm{QKD}}$.*

Proof. The proof is a special case of the proof of Theorem 3.1 as follows. The squashing condition $\Gamma_i = \Lambda^\dagger[F_i]$ implies that Bob's measurement in $\mathcal{E}^{(l)}_{\mathrm{QKD}}$ can be simulated by first applying Λ and then measuring with $\{F_i\}_{i=1}^{n_{\mathrm{meas}}}$, i.e.

$$\mathcal{E}^{(l)}_{\mathrm{QKD}} \;=\; \mathcal{E}^{(l)}_{\mathrm{QKD-Sq}} \circ \Lambda^{\otimes n}.$$

Hence, for any input state preparation $\rho^{\mathrm{prep}}_{AA'} \in \mathrm{S}_\circ(AA')$,

$$\sup_{\mathcal{A} \in \mathcal{C}(A'^n, B^n E^n)} \left\| (\mathcal{E}^{(l)}_{\mathrm{QKD}} - \mathcal{E}^{(l),\mathrm{ideal}}_{\mathrm{QKD}}) \circ \mathcal{A}\left[(\rho^{\mathrm{prep}}_{AA'})^{\otimes n}\right] \right\|_1 \tag{3.15}$$

$$= \sup_{\mathcal{A} \in \mathcal{C}(A'^n, B^n E^n)} \left\| (\mathcal{E}^{(l)}_{\mathrm{QKD-Sq}} - \mathcal{E}^{(l),\mathrm{ideal}}_{\mathrm{QKD-Sq}}) \circ (\Lambda^{\otimes n} \circ \mathcal{A})\left[(\rho^{\mathrm{prep}}_{AA'})^{\otimes n}\right] \right\|_1$$

$$\leq \sup_{\mathcal{A}' \in \mathbb{A}} \left\| (\mathcal{E}^{(l)}_{\mathrm{QKD-Sq}} - \mathcal{E}^{(l),\mathrm{ideal}}_{\mathrm{QKD-Sq}}) \circ \mathcal{A}'\left[(\rho^{\mathrm{prep}}_{AA'})^{\otimes n}\right] \right\|_1. \tag{3.16}$$

Thus, we have shown that the secrecy of $\mathcal{E}^{(l)}_{\mathrm{QKD}}$ (Eq. (3.15)) is upper bounded by the secrecy of $\mathcal{E}^{(l)}_{\mathrm{QKD-Sq}}$ (Eq. (3.16)). □

Remark 3.4 (Correlated Squashers)**.** *As in Remark 3.3, this proof extends to the case where the imperfect measurement is not IID, even if the perfect measurement is taken to be IID. In that case the required squashing map $\Lambda \in \mathcal{C}(B^n, Q^n)$ must act jointly across n rounds in a non-IID manner.*

Notational aside 3.3 (Squashed measurements)**.** We sometimes refer to the perfect measurements as squashed measurements, depending on the context. Further, we refer to the condition $\Gamma_i = \Lambda^\dagger[F_i]$ as the squashing constraint or squashing condition.

In practice, applying a squashing reduction involves two steps:

- Perfect measurement: Identify a perfect measurement $\{F_i\}_{i=1}^{n_{\text{meas}}}$ that is easier to analyse, and prove the existence of a squashing map relating $\{F_i\}_{i=1}^{n_{\text{meas}}}$ to the real measurement $\{\Gamma_i\}_{i=1}^{n_{\text{meas}}}$.

- Set of restricted attacks $\mathbb{A}$: Characterise the restricted set of attacks $\mathbb{A}$ corresponding to the squashing map in a way that can be conveniently incorporated into the security analysis.
  While $\mathbb{A}$ can always be chosen to be all channels, this choice may lead to trivial key rates for some squashing maps, in which case more restrictive constructions are necessary (see Lemma 3.4 below for such an example).

Name	**"Imperfection"**	**"Perfect" case**	**Comments**
Simple squashers [67, 68]	Optical detection setup	Qubit detection setup	• Requires idealised measurements • Not robust to infinitesimal-deviations from symmetric parameter settings
Flag-state squasher (FSS) [3]	Perfectly characterised optical detection setup	Finite-dimensional POVM	• Generally applicable: only assumes block-diagonal structure • Requires careful construction of attack set $\mathbb{A}$
Weight-preserving flag-state squasher (WPFSS) [11]	Perfectly characterised optical detection setup	Finite-dimensional POVM	• Generalisation of FSS: works when attack set $\mathbb{A}$ is all channels • Only assumes block-diagonal structure
Noise channels [2]	Imperfectly characterised optical detection setups	Perfectly characterised, finite-dimensional POVM	• Builds on FSS: Construction of attack set $\mathbb{A}$ depends on characterisation accuracy • Only assumes block-diagonal structure

Table 3.1: Examples of squashing maps, with brief description of their application and limitations.

Table 3.1 summarises known squashing reductions in the literature, highlighting the different choices of perfect measurements and the corresponding attack sets. For complete-

ness, we list four representative examples: the simple squasher, the flag-state squasher (FSS), the weight-preserving flag-state squasher (WPFSS), and noise channels. We refer the reader to Refs. [67, 68] for further details on the simple squasher, which we will not discuss further here. Noise channels will form the focus of Chapter 4, while in the remainder of this section, we concentrate on the flag-state squasher and its weight-preserving extension.

Flag-state squasher

We motivate the construction of the flag-state squasher [3] by first considering a somewhat trivial squashing map. Given *any* POVM $\{\Gamma_i\}_{i=1}^{n_{\text{meas}}} \subset \text{Pos}(B)$, we can always pick the squashed POVM $\{|i\rangle\langle i|\}_{i=1}^{n_{\text{meas}}} \subset \text{Pos}(F)$, where $\{|i\rangle\}_{i=1}^{n_{\text{meas}}}$ is an orthonormal basis for $\mathcal{H}_F$. The construction of the squashing map depicted in Fig. 3.3 is straightforward — measure the incoming state with the real POVM $\{\Gamma_i\}_{i=1}^{n_{\text{meas}}}$, and then prepare the "flag" $|i\rangle\langle i|$ corresponding to the outcome of the measurement.

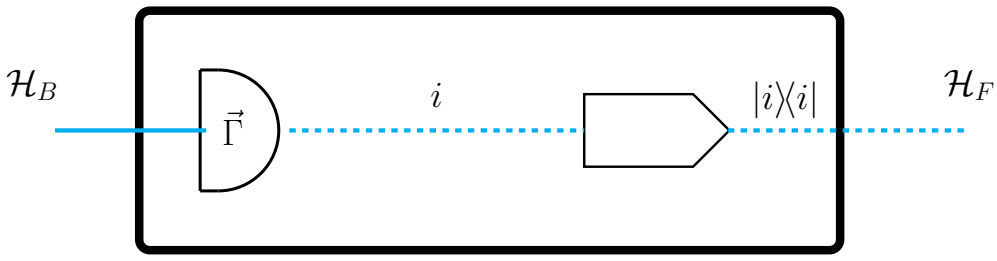


Figure 3.3: Trivial squashing map that always exists.

However, such a POVM cannot be used to obtain non-zero secret key. Intuitively, this can be seen as the squashing map has given the trusted measurement entirely to Eve, and all Bob is now doing is reading out the measurement outcome that Eve obtained. Thus, there is no "quantumness" in the squashed measurement and Eve has a copy of all of Bob's data. The flag-state squasher [3, Theorem 1], which exists whenever the POVM has block-diagonal structure, is a refinement of this simple idea.

Such block-diagonal structure naturally arises in the case of detection setups that employ threshold detectors, where the blocks refer to the total number of photons entering the setup. Thus, for such detection setups,

$$\Gamma_i = \Gamma_{i,m\leq N} \oplus \Gamma_{i,m>N}$$

for every outcome i, where the photon-number cut-off N is a free parameter. The squashed POVM is given by

$$F_i = \Gamma_{i,m\leq N} \oplus |i\rangle\langle i| \,, \tag{3.17}$$

where $\{|i\rangle\}_{i=1}^{n_{\text{meas}}}$ is an orthonormal basis for the space $\mathcal{H}_F$ orthogonal to $\mathcal{H}_{m\leq N}$. The construction of the squashing map, depicted in Fig. 3.4, can be understood as follows. First, projectively measure the state with projection Π onto the space $\mathcal{H}_{m\leq N}$ (termed the *preserved subspace*) and its complement $\overline{\Pi}$ (termed the *flag space*). If the measurement outcome corresponds to the space $\mathcal{H}_{m\leq N}$, do nothing. Otherwise, apply the trivial squashing map.

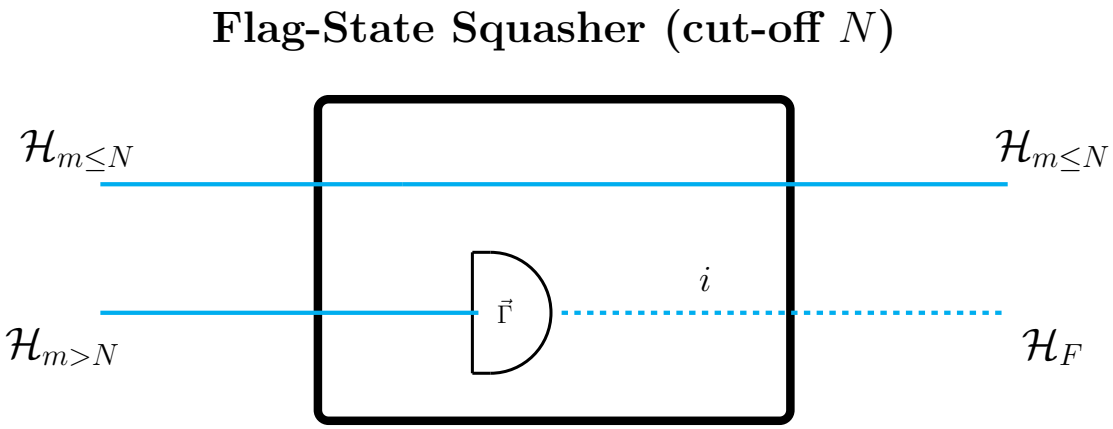


Figure 3.4: Flag-state squashing map (adapted from [3, Fig. 2]).

Already, one might see that naively giving Eve this flag-state squashing map runs into a similar issue as encountered when analysing the trivial squashing map — Eve could always implement an attack where she ignores the preserved subspace, and always forwards flag-states to Bob. This is equivalent to the trivial squashing map. The flag-state squasher is thus only useful if we restrict Eve's attacks (on the squashed protocol) to limit the amount of flag-states she sends. This is typically done by bounding the amount of states outside the preserved subspace sent by Eve *before* the application of the flag-state squasher. By construction, the flag-state squasher does not map any state from the preserved subspace to a flag state, so this bound directly carries over to the number of flag states in the squashed description.

A simple way to see this idea in action is to look at events where multiple detectors click simultaneously. Such outcomes necessarily arise from states with sufficiently many photons, i.e., from outside the preserved subspace. Hence, if we observe that multi-click

events are rare, this directly limits the weight of Eve's states outside the preserved subspace. We will now formalise this intuition mathematically in a form that can be used in security proofs.

Past work [71, 63, 72] focussed on providing a bound on the weight of a single-round state outside the preserved subspace. Although such a bound cannot be directly used at the level of the security definition, the central idea can be readily adapted to restrict Eve's attacks $\mathbb{A}$.

The general structure of the argument is as follows. First, pick a suitable single-round event e (e.g., multiple detectors clicking) and associated POVM element Γ_{e} such that a non-zero lower bound $\lambda_{\min}$ on the minimum eigenvalue $\lambda_{\min}\left(\overline{\Pi}\Gamma_{\mathrm{e}}\overline{\Pi}\right)$ can be computed. In other words, for the choice of event e, $\lambda_{\min}$ is computed such that

$$\Gamma_{\mathrm{e}} \geq \lambda_{\min}\overline{\Pi}. \tag{3.18}$$

Then, for any state ρ the weight outside the preserved subspace $W \coloneqq \mathrm{Tr}\left[\overline{\Pi}\rho\right]$ can be bounded as

$$W \leq \frac{\mathrm{Tr}\left[\Gamma_{\mathrm{e}}\rho\right]}{\lambda_{\min}}. \tag{3.19}$$

> **Technical aside 3.3** (Weight estimation for active setups)**.** The bound $\lambda_{\min}$ is crucial to bounding the weight outside the preserved subspace. While work [72] on finding such a bound for generic passive setups exists, a corresponding bound for active setups does not yet exist. Thus, while the flag-state squasher can be applied to any threshold detection setup in principle, its application to active setups in practice has this missing step.

We now adapt this idea to restrict Eve's attack and construct the restricted attack set $\mathbb{A}$.

Lemma 3.4 (Restricted attack set)**.** *Let $\overline{\Pi}^{\mathrm{Sq}}$ be the projection onto the flag space, and let F_{e}^{j} be the j^{th} round squashed POVM element corresponding to event e. Further, let $\lambda_{\min} > 0$ be such that $\Gamma_{\mathrm{e}} \geq \lambda_{\min}\overline{\Pi}$ holds for the real POVM element corresponding to event e. Here, $\overline{\Pi}$ is the projection outside the preserved subspace prior to squashing. If the restricted attack set is constructed as*

$$\mathbb{A} \coloneqq \left\{\mathcal{A}^{Sq} \in \mathcal{C}\left(A'^{n}, Q^{n}E^{n}\right) \;\middle|\; \mathcal{A}^{Sq\dagger}\left(F_{\mathrm{e}}^{j} \otimes \mathbb{I}\right) \geq \lambda_{\min}\mathcal{A}^{Sq\dagger}\left(\overline{\Pi}^{\mathrm{Sq}} \otimes \mathbb{I}\right) \quad \forall j\right\}, \tag{3.20}$$

where the identity $\mathbb{I}$ is over all unspecified spaces, then $\mathbb{A} \supset \Lambda^{\otimes n} \circ \mathcal{C}\left(A'^{n}, B^{n}E^{n}\right)$, where Λ is the flag-state squasher [3, Theorem 1].

Proof. To prove the set inclusion, consider any $\mathcal{A}^{\mathrm{Sq}} \in \Lambda^{\otimes n} \circ \mathcal{C}\left(A'^n, B^n E^n\right)$, such that $\mathcal{A}^{\mathrm{Sq}} = \Lambda^{\otimes n} \circ \mathcal{A}$ for some $\mathcal{A} \in \mathcal{C}\left(A'^n, B^n E^n\right)$. Then we show that $\mathcal{A}^{\mathrm{Sq}}$ must be an element of the constructed $\mathbb{A}$ as follows:

$$\begin{aligned}
\mathcal{A}^{\mathrm{Sq}\dagger}\left(F_{\mathrm{e}}^{j} \otimes \mathbb{I}\right) &= \mathcal{A}^{\dagger} \circ \left(\Lambda^{\dagger}\right)^{\otimes n}\left(F_{\mathrm{e}}^{j} \otimes \mathbb{I}\right) \\
&= \mathcal{A}^{\dagger}\left(\Gamma_{\mathrm{e}} \otimes \mathbb{I}\right) && (3.21) \\
&\geq \lambda_{\min}\, \mathcal{A}^{\dagger}\left(\overline{\Pi} \otimes \mathbb{I}\right) \\
&= \lambda_{\min}\, \mathcal{A}^{\dagger} \circ \left(\Lambda^{\dagger}\right)^{\otimes n}\left(\overline{\Pi}^{\mathrm{Sq}} \otimes \mathbb{I}\right) && (3.22) \\
&= \lambda_{\min}\, \mathcal{A}^{\mathrm{Sq}\dagger}\left(\overline{\Pi}^{\mathrm{Sq}} \otimes \mathbb{I}\right),
\end{aligned}$$

where Eq. (3.21) follows from the squashing constraint, and Eq. (3.22) follows from the fact that the flag-state squashing construction does not map any state from the preserved subspace to the flag space. $\Lambda^{\dagger}\left[\overline{\Pi}^{\mathrm{Sq}}\right] = \overline{\Pi}$. All other (in)equalities follow from definitions or conditions in the theorem statement. Putting it together, we have shown that any $\mathcal{A}^{\mathrm{Sq}} \in \Lambda^{\otimes n} \circ \mathcal{C}\left(A'^n, B^n E^n\right)$ satisfies $\mathcal{A}^{\mathrm{Sq}\dagger}\left(F_{\mathrm{e}}^{j} \otimes \mathbb{I}\right) \geq \lambda_{\min}\, \mathcal{A}^{\mathrm{Sq}\dagger}\left(\overline{\Pi}^{\mathrm{Sq}} \otimes \mathbb{I}\right)$, which was the defining property for the attack set $\mathbb{A}$. This proves the set inclusion. □

The construction might look somewhat obscure at first sight, but the underlying idea is simple: it enforces the same intuition that Eve cannot send arbitrarily many flag states without also increasing the frequency of detectable multi-click events (corresponding to event e in Lemma 3.4). Importantly, this restriction is formulated at the level of the overall attack channel, rather than for the single round version given in Eq. (3.19).

Thus, we have described the squashed POVMs $\{F_i\}_{i=1}^{n_{\mathrm{meas}}}$ as well as the set of restricted attacks $\mathbb{A}$ that arise as a consequence of the flag-state squasher. These can, in principle, now be applied with any proof technique via Corollary 3.2. However, imposing such restrictions on Eve's attacks cannot always be used with all proof techniques, as discussed in Section 5.3. This motivates the weight-preserving flag-state squasher, which avoids imposing explicit restrictions on Eve's attacks

Weight-preserving flag-state squasher

The construction of the squashed POVM used with the flag-state squasher from Eq. (3.17) is such that every non-trivial event e has $\lambda_{\min}\left(\overline{\Pi}^{\mathrm{Sq}} F_e \overline{\Pi}^{\mathrm{Sq}}\right) = 0$. Thus, no non-trivial analogue to Eq. (3.18) exists for the squashed POVM. The absence of such a bound on

the squashed POVM is what necessitated the restriction on Eve's attacks described in Lemma 3.4. This motivates the construction of a generalisation of the flag-state squasher — the "weight-preserving flag-state squasher" (WPFSS), where the squashed POVM satisfies the bound,

$$F_{\mathrm{e}} \geq \lambda_{\min} \overline{\Pi}^{\mathrm{Sq}}, \tag{3.23}$$

which allows its use without explicitly restricting Eve's attacks on the squashed protocol.

Lemma 3.5 (Weight-preserving flag-state squasher)**.** *Let* $\{\Gamma_i\}_{i=1}^{n_{\mathrm{meas}}} \subset \mathrm{Pos}(B)$ *be a POVM where each element is block-diagonal, i.e.* $\Gamma_i = \Gamma_{i,m\leq N} \oplus \Gamma_{i,m>N}$*. Further, let* $\{|i\rangle\}_{i=1}^{n_{\mathrm{meas}}}$ *be an orthonormal set of vectors for the flag space, and let* $0 \leq \lambda_{\min} \leq \lambda_{\min}\left(\overline{\Pi}\Gamma_{\mathrm{e}}\overline{\Pi}\right)$*, where* $\overline{\Pi}$ *is the projection outside the space corresponding to* $\Gamma_{i,m\leq N}$*, and* $e \in \{1, \ldots, n_{\mathrm{meas}}\}$ *is a measurement outcome. Then, for the following choice of squashed POVM*

$$F_i = \Gamma_{i,m\leq N} \oplus (1 - \lambda_{\min}) |i\rangle\langle i| \quad \forall\ i \neq e \tag{3.24}$$

$$F_{\mathrm{e}} = \Gamma_{e,m\leq N} \oplus \left(|e\rangle\langle e| + \lambda_{\min} \sum_{j\neq e} |j\rangle\langle j| \right), \tag{3.25}$$

there exists a channel $\Lambda \in \mathcal{C}(B, Q)$ *such that* $\Lambda^{\dagger}[F_i] = \Gamma_i$ *for all* i*.*

Proof. First, note that $\lambda_{\min} \leq \lambda_{\min}\left(\overline{\Pi}\Gamma_{\mathrm{e}}\overline{\Pi}\right)$ implies that $\lambda_{\min} \leq 1$. Thus, $\{F_i\}_{i=1}^{n_{\mathrm{meas}}}$ is a POVM. Now define the map

$$\begin{aligned}\Lambda[\rho] =& \Pi\rho\Pi + \left(\mathrm{Tr}\left[\overline{\Pi}\rho\overline{\Pi}\right] - \frac{\mathrm{Tr}\left[\overline{\Pi}\rho\overline{\Pi}\right] - \mathrm{Tr}\left[\Gamma_{\mathrm{e}}\overline{\Pi}\rho\overline{\Pi}\right]}{1-\lambda_{\min}} \right) |e\rangle\langle e| \\ &+ \sum_{j\neq e} \frac{1}{1-\lambda_{\min}} \mathrm{Tr}\left[\Gamma_i\overline{\Pi}\rho\overline{\Pi}\right] |i\rangle\langle i|, \end{aligned} \tag{3.26}$$

for all $\rho \in \mathrm{S}_{\circ}(B)$. It is easy to verify that this map is trace-preserving through explicit computation. Further, $\lambda_{\min} \leq \lambda_{\min}\left(\overline{\Pi}\Gamma_{\mathrm{e}}\overline{\Pi}\right)$ implies that $\mathrm{Tr}\left[\Gamma_{\mathrm{e}} \frac{\overline{\Pi}\rho\overline{\Pi}}{\mathrm{Tr}\left[\overline{\Pi}\rho\overline{\Pi}\right]}\right] \geq \lambda_{\min}$ for any positive semidefinite $\rho \in \mathrm{Pos}(B)$. Thus, it can be easily verified that the map is positive.

For complete positivity, we show that it can be constructed by the composition of channels. The first channel is a measurement with Kraus operators Π and $\overline{\Pi}$. The next channel leaves the outcome corresponding to Π as is, and is a measure-and-prepare channel on the outcome corresponding to $\overline{\Pi}$. The measurements are given by the POVM

$\{\frac{1}{1-\lambda_{\min}}\Gamma_i\}_{i\neq e} \cup \{\frac{\Gamma_e - \overline{\Pi}}{1-\lambda_{\min}}\}$, and the state prepared is the classical state corresponding to each measurement result.

Finally, through explicit computation, we can verify that $\mathrm{Tr}\left[\Gamma_i \rho\right] = \mathrm{Tr}\left[F_i \Lambda[\rho]\right]$ for all i, and $\rho \in \mathrm{S}_\circ(B)$. Thus, $\Lambda^\dagger\left[F_i\right] = \Gamma_i$ for all i. □

Remark 3.5 (Coarse-graining needed in WPFSS)**.** *This construction relies on the fact that the event e used for the weight estimation corresponds to a single POVM element Γ_e. In particular, this implies that the fine-grained outcomes that constitute the event e cannot have POVM elements associated with them independently after the application of the WPFSS.*

> **Technical aside 3.4** (Flag-state squasher as a special case of WPFSS)**.** The extreme case $\lambda_{\min} = 0$ reduces the WPFSS to the flag-state squasher, with the extra condition that all POVM outcomes corresponding to event e are represented by the single POVM element Γ_e.

Unlike the ordinary flag-state squasher, this generalisation automatically preserves the $\lambda_{\min}$ bound (Eq. (3.23)) and therefore requires *no restrictions on Eve's attacks*. The WPFSS can thus be directly applied to reduce security analysis of any QKD protocol using the block-diagonal measurement $\{\Gamma_i\}_{i=1}^{n_{\text{meas}}}$. By Corollary 3.2, this reduces to the security analysis of a protocol using the squashed POVM described in Eqs. (3.24) and (3.25).

3.4.4 Extension to infinite-dimensions

The squashing maps developed throughout this chapter are specifically designed for detection setups, such as those using threshold detectors, that are described by block-diagonal POVMs. A broader challenge in QKD security arises for continuous-variable systems, such as those employing homodyne or heterodyne detection, which do not have such block-diagonal structure. This is particularly relevant for EAT-based proof techniques [13, 14], which technically require that the underlying POVMs are finite-dimensional, even if that dimension can be arbitrarily large.

To address this issue, we prove a general theorem in Appendix A for extending security proofs from finite to infinite dimensions. Our main result formally establishes that if $\varepsilon_{\text{sec}}^{(d)}$-security can be proved for any d-dimensional truncated protocol, then the full, infinite-dimensional protocol is ε_{sec}-secure, where $\varepsilon_{\text{sec}} = \lim_{d\to\infty} \varepsilon_{\text{sec}}^{(d)}$. The key implication of this

result is that it enables the use of proof techniques that are themselves restricted to finite dimensions to establish the security of infinite-dimensional systems, as long as the final limit exists.

Chapter 4

Noise channels in QKD

> "We demand rigidly defined
> areas of doubt and uncertainty!"
>
> — Douglas Adams, *The Hitchhiker's Guide to the Galaxy*

In this chapter, we describe a proof technique-independent framework to addressing detector imperfections via *noise channels*, which were briefly introduced in Table 3.1. This remarkably simple, yet powerful framework builds on ideas in Ref. [62].

4.1 Generic constructions of noise channels

As described in Section 3.4.3 and Fig. 3.2, the key idea is the following. Given a noisy POVM $\vec{\Gamma}_{\text{noise}}$, we represent it as a noise channel Φ_{noise} followed by an ideal POVM $\vec{\Gamma}_{\text{ideal}}$, with adversarial control over the channel as in Corollary 3.2. As a next step, we consider a general but somewhat abstract example in which such a noise channel can always be constructed, before turning to more obviously realistic scenarios later.

Theorem 4.1 (Generic noise channel)**.** *Let the noisy POVM* $\vec{\Gamma}_{\text{noise}} \in \text{Pos}(B)$ *describing the actual imperfect detection setup be related to an ideal POVM* $\vec{\Gamma}_{\text{ideal}} \in \text{Pos}(B)$ *as*

$$\vec{\Gamma}_{\text{noise}} - (1-q)\vec{\Gamma}_{\text{ideal}} \geq 0, \tag{4.1}$$

for some $q \in [0,1]$. *Define an ideal flag POVM* $\vec{F}_{\text{ideal}} \in \text{Pos}(Q)$ *as*

$$F_i^{\text{ideal}} = \Gamma_i^{\text{ideal}} \oplus |i\rangle\langle i|, \tag{4.2}$$

where $\mathcal{H}_Q = \mathcal{H}_B \oplus \mathcal{H}_F$, *and where* $\{|i\rangle\}_{i=1}^{n_{\text{meas}}}$ *is an orthonormal basis for the flag space* $\mathcal{H}_F$. *Then there exists a noise channel* $\Phi_{\text{noise}} \in \mathcal{C}(B,Q)$ *and flag POVM* $\vec{F}_{\text{ideal}}$ *such that the following equations hold:*

$$\Gamma_i^{\text{noise}} = \Phi_{\text{noise}}^{\dagger}\left[F_i^{\text{ideal}}\right] \quad \forall\, i \tag{4.3}$$

$$\Phi_{\text{noise}}^{\dagger}[\Pi_F] = q\mathbb{I}_B, \tag{4.4}$$

where Π_F *is the projection onto the flag space* $\mathcal{H}_F$.

Proof. First, note that Eq. (4.1) implies that there exists a POVM $\vec{R}$ such that

$$\vec{\Gamma}_{\text{noise}} = (1-q)\vec{\Gamma}_{\text{ideal}} + q\vec{R}.$$

We use this POVM to construct the noise channel as depicted in Fig. 4.1:

$$\Phi_{\text{noise}}(\rho) \coloneqq (1-q)\rho \oplus q\left(\sum_i \text{Tr}\left[\rho R_i\right]|i\rangle\langle i|\right), \tag{4.5}$$

where $|i\rangle\langle i|$ are the flag states corresponding to measurement outcome i. It is straightforward to verify that Eqs. (4.3) and (4.4) hold for this noise channel. □

Note that the POVM $\vec{F}_{\text{ideal}}$ that would be used in the security proof following Corollary 3.2 has the flag-space, introduced exactly as in the flag-state squasher. Thus, as explained in Section 3.4.3, granting Eve full control of the noise channel Φ_{noise} would trivialise the security proof reduction. Thus, analogous to Lemma 3.4 we need to restrict her attacks to some attack set $\mathbb{A}$ that limits the amount of flag states she sends to Bob.

Remark 4.1 (Restricted attack set for generic noise channel)**.** *Let* $\Phi_{\text{noise}} \in \text{Pos}(B,Q)$ *be the noise channel constructed in Theorem 4.1, where the Hilbert space* $\mathcal{H}_Q$ *can be decomposed as* $\mathcal{H}_Q = \mathcal{H}_B \oplus \mathcal{H}_F$. *If the restricted attack set is constructed as*

$$\mathbb{A} \coloneqq \left\{\mathcal{A}^{Sq} \in \mathcal{C}(A'^n, Q^n E^n) \;\middle|\; \mathcal{A}^{Sq\dagger}\left(\Pi_{F_j} \otimes \mathbb{I}\right) = q\mathcal{A}^{Sq\dagger}\left(\mathbb{I}_{Q_j} \otimes \mathbb{I}\right) \quad \forall j\right\}, \tag{4.6}$$

where the identity $\mathbb{I}$ *is over all unspecified spaces, then* $\mathbb{A} \supset \Phi_{\text{noise}}^{\otimes n} \circ \mathcal{C}(A'^n, B^n E^n)$.

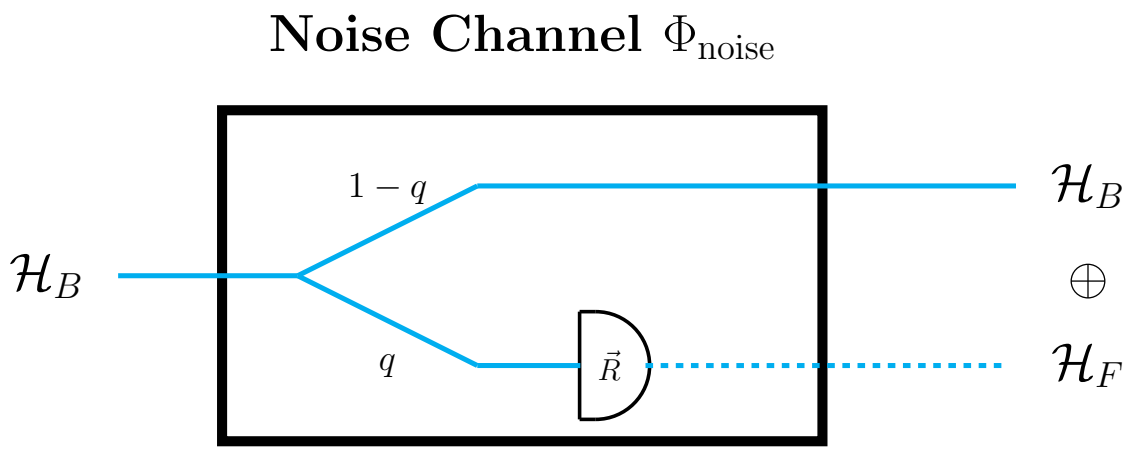


Figure 4.1: Constructive description of the noise channel. With probability q, the noise channel measures and converts the input state into a flag state. The output flag state is depicted by dashed lines.

Proof. The proof is very similar to the proof of Lemma 3.4. To prove the set inclusion, consider any $\mathcal{A}^{\text{Sq}} \in \Phi_{\text{noise}}^{\otimes n} \circ \mathcal{C}\left(A'^n, B^n E^n\right)$, such that $\mathcal{A}^{\text{Sq}} = \Phi_{\text{noise}}^{\otimes n} \circ \mathcal{A}$ for some $\mathcal{A} \in \mathcal{C}\left(A'^n, B^n E^n\right)$. Then we show that $\mathcal{A}^{\text{Sq}}$ must be an element of the constructed $\mathbb{A}$ as follows:

$$\begin{aligned}
\mathcal{A}^{\text{Sq}^\dagger}\left(\Pi_{F_j} \otimes \mathbb{I}\right) &= \mathcal{A}^\dagger \circ \left(\Phi_{\text{noise}}^\dagger\right)^{\otimes n}\left(\Pi_{F_j} \otimes \mathbb{I}\right) \\
&= q\mathcal{A}^\dagger\left(\mathbb{I}_{B_j} \otimes \mathbb{I}\right) \\
&= q\mathcal{A}^{\text{Sq}^\dagger}\left(\mathbb{I}_{Q_j} \otimes \mathbb{I}\right), \qquad (4.7)
\end{aligned}$$

where we have used Eq. (4.4) and the fact that the adjoint of a channel is a unital map. □

Theorem 4.1 has a number of noteworthy features as listed below.

1. **Noisy POVM $\vec{\Gamma}_{\text{noise}}$:** We have generically termed this a noisy POVM. This could be noisy either due to imperfection characterisation, or due to Eve having some limited control over them. Both are treated equivalently in our framework.

2. **Ideal POVM $\vec{\Gamma}_{\text{ideal}}$:** There is a large amount of freedom in choosing this 'ideal' POVM.[1] There are two competing factors when making this choice of POVM. First,

[1] As will be discussed later, the choice of common efficiency η^* in Theorem 4.4 is a manifestation of this degree of freedom.

the ideal POVM should be useful for the application being analysed. Second, the choice of ideal POVM would influence how 'close' the noisy POVM is to the ideal POVM, and thus the 'cost' of using Theorem 4.1 through Eq. (4.4) and Remark 4.1 as expanded on in the next point.

3. **Deviation from ideality q:** Given a choice of ideal POVM $\vec{\Gamma}_{\text{ideal}}$, the optimal choice of q is simply the minimum value that still satisfies Eq. (4.1). This follows from Remark 4.1, which constrains Eve's attack such that the weight in the flag space is q.

Technical aside 4.1 (Deviation metrics)**.** At first glance, the definition we use for the deviation from ideality q given in Eq. (4.1) might seem odd. However, similar metrics have been used for states in the context of QKD to quantify deviations from IID attacks [10] or from IID sources [23]. Moreover, we can establish a loose connection with a possibly more intuitive metric — the spectral norm.

Lemma 4.1. *Let $\vec{F}_{\text{noise}}$ and $\vec{F}_{\text{ideal}}$ be k-element POVMs such that $\left\|F_i^{\text{noise}} - F_i^{\text{ideal}}\right\|_\infty \leq \delta$ for all $i \in \{1, 2, \ldots, k\}$. Then $\vec{F}_{\text{noisier}} - \frac{1}{1+k\delta}\vec{F}_{\text{ideal}} \geq 0$, where $\vec{F}_{\text{noisier}}$ is a POVM with $F_i^{\text{noisier}} = \frac{1}{1+k\delta}F_i^{\text{noise}} + \frac{\delta}{1+k\delta}\mathbb{I}$.*

Proof. The proof follows from straightforward algebra after noting that $\left\|F_i^{\text{noise}} - F_i^{\text{ideal}}\right\|_\infty \leq \delta$ implies that $F_i^{\text{noise}} - F_i^{\text{ideal}} \geq -\delta\mathbb{I}$. □

Given some noisy POVM $\vec{F}_{\text{noise}}$ with k events such that $\left\|F_i^{\text{noise}} - F_i^{\text{ideal}}\right\|_\infty \leq \delta$ for all $i \in \{1, 2, \ldots, k\}$, we can implement the noisier POVM $\vec{F}_{\text{noisier}}$ via a classical post-processing that with probability $\frac{\delta}{1+k\delta}$ discards the measured outcome and uniformly randomly assigns it to another outcome. This can then be used with Lemma 4.1 and Theorem 4.1 to reduce the analysis of this POVM to that of the ideal POVM $\vec{F}_{\text{ideal}}$. We stress the point that this relation is rather loose; a direct estimation of the deviation metric q results in a significantly tighter analysis, as is done in Sections 5.5.5 and 6.4.

Remark 4.2 (Unnecessary flag space)**.** *If $\vec{\Gamma}_{\text{ideal}}$ already contains a flag space, then the extra flag space added in Eq. (4.2) is unnecessary. Instead, the existing flag space can be used to accommodate the imperfections. In this case, Eq. (4.4) would be modified to*

$$\Phi^\dagger_{\text{noise}}[\Pi_F] = q\Pi_P + \Pi_F.$$

(See also [26, Theorem 3] for an explicit description of this version of the theorem.)

The above remark is an example of a situation where certain subspaces (i.e., the flag space) are closer to 'ideal' than others. Thus, this should be accounted for in the analysis. We formally state such a generalisation of Theorem 4.1 below.

Theorem 4.2 (Generic block-diagonal noise channel)**.** *Let the noisy POVM* $\vec{\Gamma}_{\text{noise}} \in \text{Pos}(B)$ *describing the actual imperfect detection setup and the ideal POVM* $\vec{\Gamma}_{\text{ideal}} \in \text{Pos}(B)$ *have the same block-diagonal structure*

$$\Gamma_i^{\text{noise}} = \bigoplus_m \Gamma_{i,m}^{\text{noise}}$$
$$\Gamma_i^{\text{ideal}} = \bigoplus_m \Gamma_{i,m}^{\text{ideal}},$$

for all POVM elements i*. Further, let the relation between each block of the ideal and noisy POVM be given by*

$$\vec{\Gamma}_{m,\ \text{noise}} - (1-q_m)\vec{\Gamma}_{m,\ \text{ideal}} \geq 0, \tag{4.8}$$

for $q_m \in [0,1]$ *and all blocks* m*. Define an ideal flag POVM* $\vec{F}_{\text{ideal}} \in \text{Pos}(Q)$ *as*

$$F_i^{\text{ideal}} = \Gamma_i^{\text{ideal}} \oplus |i\rangle\langle i|,$$

where $\mathcal{H}_Q = \bigoplus_m \mathcal{H}_{B^m} \oplus \mathcal{H}_F$*, and where* $\{|i\rangle\}_{i=1}^{n_{\text{meas}}}$ *is an orthonormal basis for the flag space* $\mathcal{H}_F$*. Then there exists a noise channel* $\Phi_{\text{noise}} \in \mathcal{C}(B,Q)$ *such that the following equations hold:*

$$\Gamma_i^{\text{noise}} = \Phi_{\text{noise}}^\dagger\left[F_i^{\text{ideal}}\right] \quad \forall\, i \tag{4.9}$$
$$\Phi_{\text{noise}}^\dagger[\Pi_{B^m}] = (1-q_m)\Pi_{B^m} \quad \forall\, m, \tag{4.10}$$

where Π_{B^m} *is the projection onto the block* $\mathcal{H}_{B^m}$*.*

Proof. The proof is a straightforward extension of the proof of Theorem 4.1; we construct a similar noise channel for each block individually as described below. First, note that Eq. (4.8) implies the existence of a POVM $\vec{R}$ block-diagonal in m such that $\vec{\Gamma}_{\text{noise},m} = (1-q_m)\vec{\Gamma}_{\text{ideal},m} + q_m\vec{R}_m$ for all blocks m. The noise channel can then be constructed as

$$\Phi_{\text{noise}}(\rho) \coloneqq \sum_m \left((1-q_m)\,\Pi_{B^m}\,\rho\,\Pi_{B^m} \ \oplus q_m \left(\sum_i \text{Tr}\left[\Pi_{B^m}\,\rho\,\Pi_{B^m} R_i\right] |i\rangle\langle i| \right) \right). \tag{4.11}$$

It can be readily verified that Eqs. (4.9) and (4.10) are satisfied. □

So far we have explicitly constructed noise channels that work for arbitrary detection setups. However, this construction was rather abstract, and requires one to identify a suitable ideal POVM $\vec{\Gamma}_{\text{ideal}}$, and bound the abstract deviation metric q. We will now consider threshold detection setups with loss and dark counts, and describe the explicit construction of noise channels for this physically relevant case.

4.2 Construction of noise channel for loss and dark counts for generic detection setups

In this section, we will not attempt to construct the noise channel for the full optical space directly. Such a construction, or even the identification of the deviation parameter from Theorem 4.2, can be more difficult at the level of the entire Fock space. Instead, we first apply the flag-state squasher, thereby reducing the problem to the single-photon subspace together with a flag space. The noise channel for the flag space is trivial, so the task reduces to constructing the channel for the single-photon subspace alone. We will first consider a single-mode detector model, before discussing the multimode case in Section 4.3.

This process is depicted in Fig. 4.2. Here, W represents the weight outside the preserved subspace constraint that arises from using the flag-state squasher as detailed in Lemma 3.4. Similarly, the weight outside the preserved space $W^{\mathbf{d_B},\boldsymbol{\eta}}$ after the application of the noise channel must also be constrained similar to Eq. (4.4) and Remark 4.1.

We shall construct the full noise channel $\Phi_{\mathbf{d_B},\boldsymbol{\eta}}$ in two steps. First we construct a noise channel for the dark counts $\Phi_{\mathbf{d_B}}$, and then another for the loss $\Phi_{\boldsymbol{\eta}}$ such that $\Phi_{\mathbf{d_B},\boldsymbol{\eta}} = \Phi_{\boldsymbol{\eta}} \circ \Phi_{\mathbf{d_B}}$.

4.2.1 Noise channel for dark counts

Any detection setup has single-click events, defined as events where only a single detector clicks, and multi-click events, defined as events where more than one detector clicks. We let S be the set of single-click events, and M be the set of multi-click events. The no-click event will always be denoted by the event 0. The set of all events will be denoted by U.

We first list a set of sufficient conditions we require from the classical post-processing $\mathcal{P}^{\mathbf{d_B}}$ to construct the noise channel. We then physically motivate these conditions.

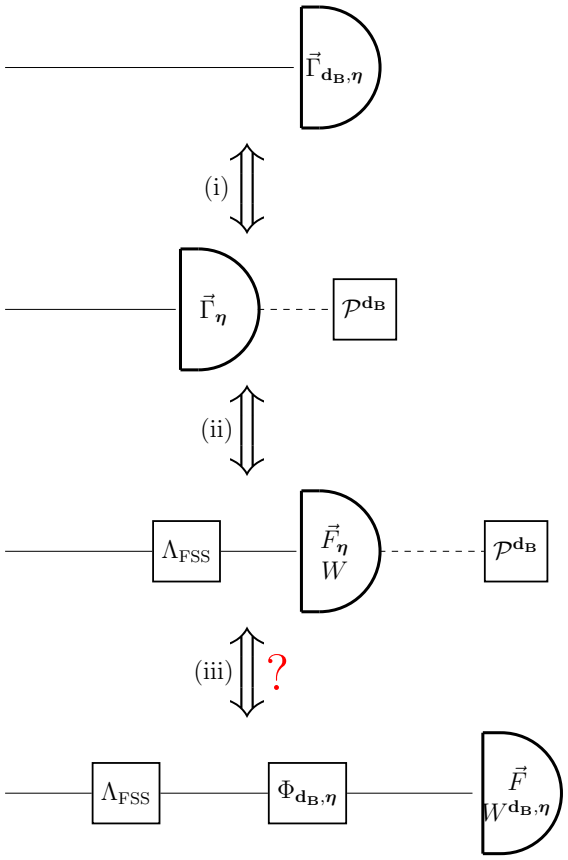


Figure 4.2: A set of equivalences (as quantum-to-classical measurement channels) of detection setups to consider dark counts and loss as part of the noise channel, using the flag-state squasher.

1. The post-processing does not turn one single-click event into another, i.e.,

$$\mathcal{P}^{\mathbf{d_B}}_{s|s'} = 0, \tag{4.12}$$

for all distinct s, $s' \in S$.

2. The post-processing does not turn any click event into a no-click event, i.e.,

$$\mathcal{P}^{\mathbf{d_B}}_{0|i} = 0, \tag{4.13}$$

for all $i \neq 0$.

3. The post-processing is such that

$$\mathcal{P}^{\mathbf{d_B}}_{s|s} \geq \mathcal{P}^{\mathbf{d_B}}_{0|0}, \tag{4.14}$$

for all $s \in S$.

The first two conditions are true for any dark count post-processing, as dark counts do not stop a detector from clicking. To see why the third condition is true, observe that $\mathcal{P}^{\mathbf{d_B}}_{s|s} = \prod_{i \neq s}(1 - d_i)$ is the probability that none of the other detectors have a dark count. On the other hand, $\mathcal{P}^{\mathbf{d_B}}_{0|0} = \prod_i (1 - d_i)$ is the probability that none of the detectors have a dark count. Since $(1 - d_s) \leq 1$, the claim follows.

We also need to make an additional assumption on the POVM without dark counts $\vec{\Gamma}_{\boldsymbol{\eta}}$. Informally, the assumption is that we cannot have more clicks than photons. More formally, this can be expressed as

$$\begin{aligned} \mathrm{Tr}\left[\Gamma^{\boldsymbol{\eta}}_m \rho_1\right] &= 0 \\ \mathrm{Tr}\left[\Gamma^{\boldsymbol{\eta}}_m \left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right|\right] &= 0 \\ \mathrm{Tr}\left[\Gamma^{\boldsymbol{\eta}}_s \left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right|\right] &= 0, \end{aligned} \tag{4.15}$$

for all $m \in M$, $s \in S$ and any single-photon state ρ_1. This naturally holds for typical detection setups, as dark counts are the only way single photons can result in multiple detectors clicking, or the vacuum can result in any detector clicking. Note that this immediately implies that $\mathrm{Tr}\left[\Gamma_0 \left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right|\right] = 1$.

We combine all these properties to define a generic optical detection setup with dark counts.

Definition 4.1 (Threshold detection setup with independent dark counts)**.** We define the POVM $\vec{\Gamma}_{\mathbf{d_B},\boldsymbol{\eta}}$ to be a *threshold detection setup with independent dark counts* if

1. it is equivalent to a POVM without dark counts $\vec{\Gamma}_{\boldsymbol{\eta}}$ followed by a dark count post-processing $\mathcal{P}^{\mathbf{d_B}}$ as described in equivalence (i) of Fig. 4.2,

2. the dark count post-processing satisfies Eqs. (4.12) to (4.14), and

3. the POVM without dark counts $\vec{\Gamma}_{\boldsymbol{\eta}}$ satisfies Eq. (4.15).

While this definition might seem overly general and pedantic at first, such a level of abstraction is in fact necessary for applying the noise channel to the postselection technique, as will be seen in Section 5.3. We also expect that more refined multimode detection models to also satisfy these core properties, so that our results apply directly to a broad class of realistic detection setups.

We now have all the tools to construct the noise channel for dark counts.

Theorem 4.3 (Dark count noise channel)**.** *Let $\vec{F}_{\mathbf{d_B},\boldsymbol{\eta}}$ be the POVM for a flag-state squashed threshold detection setup with independent dark counts as defined in Definition 4.1, where each $F_i^{\mathbf{d_B},\boldsymbol{\eta}} = \Gamma_{i,0}^{\mathbf{d_B},\boldsymbol{\eta}} \oplus \Gamma_{i,m=1}^{\mathbf{d_B},\boldsymbol{\eta}} \oplus |i\rangle\langle i|$ is block-diagonal with an associated Hilbert space $\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ corresponding to the total photon number, and flag space. Then there exists noise channel $\Phi_{\mathbf{d_B}} : \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F \to \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ such that*

$$F_i^{\mathbf{d_B},\boldsymbol{\eta}} = \Phi_{\mathbf{d_B}}^{\dagger}\left[F_i^{\boldsymbol{\eta}}\right] \quad \forall\, i \tag{4.16}$$

$$\Phi_{\mathbf{d_B}}^{\dagger}[\Pi_{\leq 1}] = \mathcal{P}_{0|0}^{\mathbf{d_B}}\Pi_{\leq 1}, \tag{4.17}$$

where $F_i^{\boldsymbol{\eta}} = \Gamma_{i,m=0}^{\boldsymbol{\eta}} \oplus \Gamma_{i,m=1}^{\boldsymbol{\eta}} \oplus |i\rangle\langle i|$, $\Pi_{\leq 1}$ is the projection onto the space $\mathcal{H}_0 \oplus \mathcal{H}_1$, and $\mathcal{P}^{\mathbf{d_B}}$ is the stochastic matrix that models the dark counts.

The proof is similar to that of Theorems 4.1 and 4.2 and is given in Appendix B.

Eq. (4.17) can be used to constrain the set of Eve's attacks analogously to the usage of Eq. (4.4) in Remark 4.1. However, we postpone this discussion till after we construct the noise channel for lossy detectors.

4.2.2 Noise channel for loss

Theorem 4.4 (Loss noise channel)**.** *Let $\vec{F}_{\boldsymbol{\eta}}$ be the flag-state squashed POVM for a threshold detection setup with loss (and without dark counts), where for each POVM outcome i, $F_i^{\boldsymbol{\eta}} = \Gamma_{i,m=0} \oplus \Gamma_{i,m=1}^{\boldsymbol{\eta}} \oplus |i\rangle\langle i|$ is block-diagonal with an associated Hilbert space $\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ corresponding to the total photon number, and flag space. Here, the vacuum component*

$F_{i,m=0}$ is independent of loss $\boldsymbol{\eta}$ for all outcomes i. Let $\eta_{\min}$ and $\eta_{\max}$ be the minimum and maximum of all the detector efficiencies used in the detection setup. We can then define a family of noise channels $\Phi_{\boldsymbol{\eta}}^{\eta^*}$ and target POVMs $\vec{F}_{\eta^*}$ parametrised by some parameter η^* as follows. For any value of $\eta^* \in \left[\frac{\eta_{\min}}{1-(\eta_{\max}-\eta_{\min})}, 1\right]$, there exists a noise channel $\Phi_{\boldsymbol{\eta}}^{\eta^*} : \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F \to \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ such that

$$F_i^{\boldsymbol{\eta}} = \Phi_{\boldsymbol{\eta}}^{\eta^*\dagger}\left[F_i^{\eta^*}\right] \quad \forall\, i \tag{4.18}$$

$$\Phi_{\boldsymbol{\eta}}^{\eta^*\dagger}\left[\Pi_{\leq 1}\right] = \Pi_0 + \frac{\eta_{\min}}{\eta^*}\Pi_1, \tag{4.19}$$

where $F_i^{\eta^*} = \Gamma_{i,m=0} \oplus \Gamma_{i,m=1}^{\eta^*} \oplus |i\rangle\langle i|$ is the lossy flag-state squashed POVM where all detectors have the (common) efficiency η^*, Π_1 is the projection onto the space $\mathcal{H}_1$, Π_0 is the projection onto the space $\mathcal{H}_0$, and $\Pi_{\leq 1}$ is the projection onto the space $\mathcal{H}_0 \oplus \mathcal{H}_1$.

The proof amounts to a special case of Theorem 4.2, and is given in Appendix B.

Note that Theorem 4.4 leaves us with some freedom to choose how we define the 'ideal' POVM $\vec{F}_{\eta^*}$. Increasing the efficiency η^* of the ideal POVM decreases the weight $\frac{\eta_{\min}}{\eta^*}$ of the state in the preserved subspace. Additional work must be done to decide what the optimal choice would be. Intuitively, we would expect that the optimal choice would maximise the weight in the preserved subspace (and hence minimise η^*), as any part of the state outside the preserved subspace is entirely classical.

We now refer to the noise channel $\Phi_{\boldsymbol{\eta}}^{\eta^*}$ as $\Phi_{\boldsymbol{\eta}}$ to avoid notational clutter. Finally, combining Theorems 4.3 and 4.4 gives us the noise channel $\Phi_{\mathbf{d_B},\boldsymbol{\eta}} = \Phi_{\boldsymbol{\eta}} \circ \Phi_{\mathbf{d_B}}$ required for equivalence (iii). We can now construct the set of Eve's constrained attacks from Eqs. (4.17) and (4.19) and Lemma 3.4, taking into account the flag-state squasher and noise channels.

Remark 4.3 (Restricted attack set for loss and dark count noise channels)**.** *Let $\Phi_{\mathbf{d_B},\boldsymbol{\eta}} \in \mathrm{Pos}(Q, Q)$ be the noise channel $\Phi_{\mathbf{d_B},\boldsymbol{\eta}} = \Phi_{\boldsymbol{\eta}} \circ \Phi_{\mathbf{d_B}}$. Further, let $F_{\mathrm{e}}^{\eta^* j}$ be the j^{th} round, ideal flag-state squashed POVM element corresponding to event e, and $\lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}} > 0$ be such that $\Gamma_{\mathrm{e}}^{\mathbf{d_B},\boldsymbol{\eta}} \geq \lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}}\Pi_{>1}$ holds for the real POVM element corresponding to event e. Further, let the restricted attack set be constructed as*

$$\mathbb{A} := \left\{ \mathcal{A}^{Sq} \in \mathcal{C}\left(A'^n, Q^n E^n\right) \;\middle|\; \begin{array}{l} \mathcal{A}^{Sq\dagger}\left(F_{\mathrm{e}}^{\eta^* j} \otimes \mathbb{I}\right) \geq \lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}} \Bigg(\mathcal{A}^{Sq\dagger}\left(\mathbb{I}_Q \otimes \mathbb{I}\right) - \\ \dfrac{1}{\mathcal{P}_{0|0}^{\mathbf{d_B}}} \mathcal{A}^{Sq\dagger}\left(\Pi_0 \otimes \mathbb{I}\right) - \dfrac{\eta^*}{\eta_{\min}\mathcal{P}_{0|0}^{\mathbf{d_B}}} \mathcal{A}^{Sq\dagger}\left(\Pi_1 \otimes \mathbb{I}\right) \Bigg) \end{array} \quad \forall j \right\},$$

where the identity $\mathbb{I}$ *is over all unspecified spaces. Then* $\mathbb{A} \supset \Phi_{\text{noise}}^{\otimes n} \circ \Lambda^{\otimes n} \circ \mathcal{C}\left(A'^n, B^n E^n\right)$*, where* Λ *is the flag-state squasher [3, Theorem 1].*

The proof is very similar to the proofs of Lemma 3.4 and Remark 4.1.

So far, we have constructed the noise channels assuming some fixed values of dark count rates $\mathbf{d_B}$ and detector efficiencies $\boldsymbol{\eta}$. In practice, however, we often do not know the exact values of the parameters[2]; either due to imperfect characterisation, or due to partial adversarial control. Indeed, this was the central motivation of the noise channel framework. We now detail the various aspects of the analysis that need to be modified to extend it to the practically relevant case where all detector parameters are only known to be in some range.

1. **Subspace weight estimation** $\lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}}$**:** This can be numerically computed for generic linear optical detection setups by choosing the event e to be the set of all multi-click outcomes as shown in [21, Section III], which builds on the analysis in Ref. [72].

2. **Dark count cost** $1 - \mathcal{P}_{0|0}^{\mathbf{d_B}}$**:** Note that our analysis (specifically, Remark 4.3) only requires a lower bound on the probability of no dark counts $\mathcal{P}_{0|0}^{\mathbf{d_B}}$, which can be obtained from an upper bound on the individual dark count values.

3. **Common efficiency** η^***:** This can be chosen to be any fixed value in the range $\eta^* \in \left[\frac{\eta_{\min}}{1-(\eta_{\max}-\eta_{\min})}, 1\right]$. The lower bound on the permitted value of η^* can be easily ascertained by setting $\eta_{\min}$ to be the lower bound of the range of detector efficiencies, and $\eta_{\max}$ to be the upper bound of the range of detector efficiencies.

   Alternatively, we expect a more optimal solution to be to consider the common efficiency η^* to be a part of the channel.[3] Thus, for the purpose of defining the ideal POVM $\vec{F}_{\eta^*}$, the common efficiency η^* can be set to be 1 without loss of generality. The value of η^* can then be optimised to minimise the efficiency cost as expanded on below.

4. **Efficiency cost** $1 - \frac{\eta_{\min}}{\eta^*}$**:** As before, the analysis requires only an upper bound on this cost. If η^* is set to some fixed value and not given to the channel, then this must be ascertained via setting $\eta_{\min}$ to be the lower bound of the range of detector efficiencies.

[2] In fact, the parameter values could vary across rounds.

[3] For e.g. as described in [73, Section IV. B.], [74, Section III C] or [75, Fig. 1] for a polarisation-encoded BB84 setup.

On the other hand, if the common efficiency η^* is to be considered to be a part of the channel, then the resulting efficiency cost is $(\eta_{\max} - \eta_{\min})$, which can be computed from the range of detector efficiencies.

Technical aside 4.2 (Constrain 0-photon subspace for tighter constraint)**.** The usage of the tighter constraint in Eq. (4.19), which distinguishes between Π_0 and Π_1 is apparent in the construction of the set of restricted attacks in Remark 4.3. Applying this refinement, however, requires imposing an additional constraint on the weight in the 0-photon subspace is needed. For clarity in its initial definition, this requirement is omitted from the description of restricted attacks in Remark 4.3. We refer the interested reader to Chapters 5 and 6 for explicit examples of such a constraint.

4.3 Multimode extensions

We now briefly describe the extension of the noise channel constructions described in Section 4.2 to the independent multimode model[4] described in Section 2.2.7, where each POVM element decomposes independently by mode as

$$\Gamma_i^{\mathbf{d_B},\boldsymbol{\eta}} = \bigoplus_k \Gamma_i^{\mathbf{d_B}(k),\boldsymbol{\eta}(k)}.$$

Here, each block POVM $\Gamma_i^{\mathbf{d_B}(k),\,\boldsymbol{\eta}(k)}$ represents the single-mode POVM with parameters $\mathbf{d_B}(k), \boldsymbol{\eta}(k)$ corresponding to mode k. The flag-state squasher is applied to squash each of the blocks to its corresponding subspace $\Pi_{m\leq 1}^k$ with no more than a single photon. Thus, the preserved subspace $\Pi_{\leq 1} \coloneqq \sum_k \Pi_{m\leq 1}^k$ corresponds to the space with each mode having no more than a single photon. Note that this might not be finite-dimensional in general, but as we shall see, this will not matter.

The usage of the flag-state squasher requires a bound on the weight outside the preserved subspace. This is obtained by finding $\lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}} \geq 0$ such that $\Gamma_e^{\mathbf{d_B},\boldsymbol{\eta}} \geq \lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}} \Pi_{>1}$ for some event e (such as the event corresponding to multiple detectors clicking) as detailed in Section 3.4.3. A complication arises because the losses $\boldsymbol{\eta}(k)$ are expected to vary significantly between modes. This leads to a loose bound on $\lambda_{\min}^{\mathbf{d_B},\boldsymbol{\eta}}$ which must not have any

[4]More complicated multimode models, such as the one described in [18, Section 3], can be treated by using Theorem 4.2 to adapt the proof of Theorem 4.4.

mode dependence. This difficulty is resolved by absorbing the mode-dependent efficiencies into the channel, thereby rescaling the efficiency of each mode so that $\eta_{\max}(k) = 1$.

Once the flag-state squasher is used, the noise channel $\Phi_{\mathbf{d_B},\boldsymbol{\eta}}$ constructed in Theorems 4.3 and 4.4 extends naturally to this multimode setting by acting on each block independently[5] $\Phi_{\mathbf{d_B},\boldsymbol{\eta}} \coloneqq \bigoplus_k \Phi_{\mathbf{d_B}(k),\boldsymbol{\eta}(k)}$. In this multimode setting, the dark count cost $1-\mathcal{P}_{0|0}^{\mathbf{d_B}}$ is obtained from an upper bound on the dark count values across all detectors and modes. Similarly, the common efficiency η^* and efficiency cost $1-\frac{\eta_{\min}}{\eta^*}$ are obtained by setting $\eta_{\min}$ and $\eta_{\max}$ to be the lower and upper bounds on the efficiency over all detectors and modes, respectively.

After using the noise channel, the (flag-state squashed) POVM acts identically on every mode, i.e. each POVM element decomposes as

$$F_i^{\text{multimode}} = \bigoplus_k F_i, \tag{4.20}$$

where F_i is the single-mode flag-state squashed POVM. This can be shown to be equivalent to the single-mode description as follows. Consider the channel

$$\Lambda\left(\bigoplus_k \rho_k + \text{off-diagonal terms}\right) \coloneqq \sum_k \rho_k, \tag{4.21}$$

satisfies the squashing property $\Lambda^\dagger[F_i] = F_i^{\text{multimode}}$ for all POVM outcomes i.

Thus, after applying the noise channel and flag-state squasher, the multimode POVM factors into independent single-mode components. Equivalently, there exists a channel Λ that maps the multimode description to the single-mode one while preserving the squashing property. Hence, the analysis of multimode setups reduces directly to the single-mode case typically considered in the literature.

4.4 Concluding remarks

In this chapter, we have developed a general framework to rigorously address detector imperfections. The results proved in this chapter can be used in conjunction with Corollary 3.2 to prove security for QKD protocols with imperfect detection setups. In particular,

[5]Note that the noise channel described in this chapter act trivially on the flag space. Thus, here we explicitly describe its action only on the preserved subspace.

EAT-based proof techniques [14] can directly make use of the restricted set of Eve's attacks $\mathbb{A}$ constructed in Remark 4.3 to prove security. We will apply our results to the postselection technique in Chapter 5, and to phase-error estimation-based proofs in Chapter 6. Finally, we build on the ideas from this chapter to address correlated detectors in Chapter 7.

We have also sketched an approach to incorporate the simple model of multimode detection setups described in Section 2.2.7 into security proofs via Theorems 4.3 and 4.4. We believe that the analysis of more complex models of multimode detection setups can be similarly addressed by instead applying Theorems 4.1 and 4.2, and leave this for future work.

Chapter 5

Postselection technique for optical QKD protocols

> "If the only tool you have is a hammer, you tend to see every problem as a nail."
>
> — Abraham Maslow

The analysis of QKD protocols against IID attacks is well-studied [76, 52, 77, 78, 79] due to its relative simplicity. However, such an assumption is not realistic, as a non-IID attack is straightforward to implement. For example, Eve could decide to perform an attack in every even round and do nothing in every odd round. The postselection technique [10, 11] is a proof approach that reduces the security of a QKD protocol against general attacks to its security against IID attacks. In this chapter, we will use the tools developed in Chapters 3 and 4 to extend the applicability of the postselection technique to optical prepare-and-measure protocols.

Before diving into the details of this security proof technique, we first give some intuition about the core mathematical result — the de Finetti reduction [10, 80]. This is a more general tool that has found use in more general quantum information processing tasks [81, 82, 83].

5.1 Motivating de Finetti reductions

A de Finetti reduction is a statement of the following form, made for any permutationally invariant state ρ_{A^n}:

$$\rho_{A^n} \leq g_{n,x} \tau_{A^n},$$

where τ_{A^n} is a mixture of IID states, and $g_{n,x}$ is a number that depends on the number of rounds n as well as the dimension d_A of the register A. The utility of such a statement might not be immediately obvious, and so we attempt to motivate its utility by briefly considering its application to concentration inequalities [84, 85, 86].

Notational aside 5.1 (Theorem or reduction?)**.** In earlier works [10, 80], the de Finetti statement was presented as a 'de Finetti theorem'. To avoid conflation with the (classical and quantum) de Finetti theorems [87, 88, 52], a later work [84] introduced the label de Finetti reduction. We adopt that usage here and refer to it as a de Finetti reduction throughout.

As described in Section 2.3, concentration inequalities are used to upper bound the probability of "failure" $\mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \rho_{A^n}\right]$ (defined in Eq. (2.11)). This POVM is often invariant under permutations, a property that arises because its defining set Ω_{bad} is insensitive to the ordering of the outcomes in $\vec{z}$.[1] In this setting, the de Finetti reduction can be used to reduce the problem of upper-bounding the probability of failure for an arbitrary state ρ_{A^n}, to that of bounding the probability of failure for an IID state $\sigma_A^{\otimes n}$.

Theorem 5.1 (Informal)**.** *Let $\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}$ be a permutationally-invariant matrix. Then for any $\rho_{A^n} \in \mathrm{S}_\circ(A^n)$, $\mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \rho_{A^n}\right] \leq g_{n,x} \sup_{\sigma_A \in S_\circ(\tau)} \mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \sigma_A^{\otimes n}\right]$, where $S_\circ(\tau)$ is the set of IID states in the mixture τ_{A^n}.*

Proof Sketch. That $\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}$ is permutationally-invariant means that $\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}} = \pi\left(\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\right)$ for all permutations π. Thus,

$$\mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \rho_{A^n}\right] = \frac{1}{n!}\sum_{\pi} \mathrm{Tr}\left[\pi\left(\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\right)\ \rho_{A^n}\right] \tag{5.1}$$

$$= \frac{1}{n!}\sum_{\pi} \mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \pi^{-1}\left(\rho_{A^n}\right)\right] \tag{5.2}$$

$$=: \mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \bar{\rho}_{A^n}\right], \tag{5.3}$$

[1] For instance, the frequency estimation examples in Section 2.3 are of this type. A statistic such as frequency depends only on the total count of each outcome, not on the order in which they appear.

where Eq. (5.2) follows from the fact that the adjoint of the permutation map is its inverse. Note that by definition, $\bar{\rho}_{A^n}$ is a permutationally-invariant state. Thus, the de Finetti reduction states that $\bar{\rho}_{A^n} \leq g_{n,x}\tau_{A^n}$. Inserting this into Eq. (5.3), we obtain

$$\begin{aligned} \mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \rho_{A^n}\right] &= \mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \bar{\rho}_{A^n}\right] && (5.4)\\ &\leq g_{n,x}\mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \tau_{A^n}\right] && (5.5)\\ &\leq g_{n,x} \sup_{\sigma_A\in S_\circ(\tau)} \mathrm{Tr}\left[\Gamma_{\vec{z}\in\Omega_{\mathrm{bad}}}\ \sigma_A^{\otimes n}\right], && (5.6) \end{aligned}$$

where the last inequality uses the fact that τ_{A^n} is a mixture (i.e., a convex combination) of IID states in $S_\circ(\tau)$. □

Note the importance of the prefactor $g_{n,x}$ that appears in Theorem 5.1, which is directly inherited from the prefactor in the de Finetti reduction. This prefactor can be interpreted as the penalty incurred while using the de Finetti reduction to simplify the general analysis to the IID case, as can be seen from Theorem 5.1. Additionally, note that the maximisation over IID states in Eq. (5.6) can be restricted to all IID states in τ_{A^n}. Both of these are important points that we shall address when applying de Finetti reduction to QKD.

In summary, a de Finetti reduction is a statement of the following form, made for any permutationally invariant state ρ_{A^n}:

$$\rho_{A^n} \leq g_{n,x}\tau_{A^n},$$

with two important points to note.

1. The prefactor $g_{n,x}$ is to be interpreted as a penalty that must be incurred when using the de Finetti reduction. This penalty depends on the dimension of the local system A.

2. τ_{A^n} is a mixture of IID states. The IID states $S_\circ(\tau)$ that comprise this mixture are the states that will be included in the corresponding IID analysis.

5.2 Choice of de Finetti reduction for QKD

The broad proof structure of the postselection technique is very similar to that of the proof of Theorem 5.1 as follows:

1. We start from the definition of ε_{sec}-secrecy in terms of Alice and Bob's state after Eve's attack as stated in Eq. (3.7):

$$\sup_{\substack{\rho_{A^nB^n}\in \mathrm{S}_\circ(A^nB^n)\\ \mathrm{Tr}_{B^n}[\rho_{A^nB^n}]=\mathrm{Tr}_{A'^n}\left[(\rho_{AA'})^{\otimes n}\right]}} \left\| \left(\mathcal{E}_{\text{QKD}}^{(l)} - \mathcal{E}_{\text{QKD}}^{(l),\text{ideal}}\right)\left[\rho_{A^nB^nE^n}\right]\right\|_1 \leq \varepsilon_{\text{sec}}, \tag{5.7}$$

   where $\rho_{A^nB^nE^n}$ is a purification of the optimisation variable $\rho_{A^nB^n}$. For notational conciseness, we define $\hat{\sigma}_A \coloneqq \mathrm{Tr}_{A'}\left[\rho_{AA'}\right]$.

2. We use permutational invariance of the QKD protocol[2] to argue that the supremum in Eq. (5.7) is achieved for a permutationally invariant state $\rho_{A^nB^n}$.

3. We use a de Finetti reduction $\rho_{A^nB^n} \leq g_{n,x}\tau_{A^nB^n}$, where $\tau_{A^nB^n}$ is a mixture of IID states. This gives

$$\sup_{\substack{\rho_{A^nB^n}\in \mathrm{S}_\circ(A^nB^n)\\ \mathrm{Tr}_{B^n}[\rho_{A^nB^n}]=\hat{\sigma}_A^{\otimes n}}} \left\| \left(\mathcal{E}_{\text{QKD}}^{(l)} - \mathcal{E}_{\text{QKD}}^{(l),\text{ideal}}\right)\left[\rho_{A^nB^nE^n}\right]\right\|_1 \lessapprox g_{n,x} \sup_{\sigma_{AB}\in S_\circ(\tau)} \left\| \left(\mathcal{E}_{\text{QKD}}^{(l)} - \mathcal{E}_{\text{QKD}}^{(l),\text{ideal}}\right)\left[\sigma_{ABE}^{\otimes n}\right]\right\|_1, \tag{5.8}$$

   where the supremum is over the set $S_\circ(\tau)$ of all IID states $\sigma_{AB}^{\otimes n}$ that are part of the mixture $\tau_{A^nB^n}$.

Thus, the security of a QKD protocol against general attacks is reduced to a security proof against IID attacks. Once again, we must pay attention to the factors noted at the end of Section 5.1: the penalty $g_{n,x}$, and the set $S_\circ(\tau)$ of IID states that constitute the mixture $\tau_{A^nB^n}$.

Notational aside 5.2 (Penalty of reduction)**.** The penalty function is defined as $g_{n,x} \coloneqq \binom{n+x-1}{x-1}$. In what follows, we only specify the value that x shall take.

The original proof of the postselection technique [10] required $\tau_{A_nB_n}$ to be a mixture over *all* IID states with $x = d_A^2 d_B^2$. This results in the IID security proof to hold for all IID states. While this is suitable for the analysis of EB protocols, this does not allow for the inclusion of the fixed marginal constraint vital for the analysis of PM and MDI QKD protocols as described in Section 3.3.

[2] To guarantee the permutational invariance of the protocol, a random permutation needs to be applied to Alice and Bob's measurement data [89, 11].

This can be easily remedied by using [80, Corollary 3.2], which restricts $\tau_{A^nB^n}$ to be a mixture of all IID states with the same (IID) fixed marginal as $\rho_{A^nB^n}$. This allows for its application to PM and MDI protocols. However, directly applying this de Finetti reduction results in the penalty being large; $x = d_A^2 d_B^4$.

Fortunately, simple modifications to the proof of this de Finetti reduction results in an analogous result with $x = d_A^2 d_B^2$. Further, these results can be improved when it is known that the state $\rho_{A^nB^n}$ has some block-diagonal structure — as is commonly the case for optical QKD protocols with threshold detection setups. In this case, $x = \sum_{i,j=1}^{k_A,k_B} \left(d_i^A\right)^2 \left(d_j^B\right)^2$, where d_i^A and d_j^B are the dimensions of the blocks of Alice's and Bob's systems, respectively. As we show in Fig. 5.5, these improvements, summarised in Table 5.1, result in huge improvements for the key rates. The proofs of these improved de Finetti reductions are given in Appendix C.

Proved in	**Applicability**	**Cost**
Christandl et al. (2009) [10]	EB QKD protocols	$x = d_A^2 d_B^2$
Fawzi et al. (2015, Cor. 3.2) [80]	EB, PM and MDI QKD protocols	$x = d_A^2 d_B^4$
This work [11]	EB, PM and MDI QKD protocols	$x = d_A^2 d_B^2$
	IID-block-diagonal EB, PM and MDI QKD protocols	$x = \sum_{i,j=1}^{k_A,k_B} (d_i^A)^2 (d_j^B)^2$

Table 5.1: de Finetti reductions and their applicability to QKD protocols with penalty parameter x in $g_{n,x} = \binom{n+x-1}{x-1}$. Our work derives de Finetti reductions with the smallest penalty, without sacrificing applicability.

The (in)formal statement obtained at the end of this process is given below.

Theorem 5.2 (Informal)**.** *Let $\mathcal{E}_{\mathrm{QKD}}^{(l)}$ be a QKD protocol that is $\varepsilon_{\mathrm{sec}}$-secret against all IID attacks. Then, the QKD protocol $\mathcal{E}_{\mathrm{QKD}}^{(l')}$ which hashes to length $l' = l - 2\log(g_{n,x}) - 2\log\left(\frac{1}{\widetilde{\varepsilon}}\right)$ is $g_{n,x}(4\sqrt{\varepsilon_{\mathrm{sec}}} + \widetilde{\varepsilon})$-secure against all general attacks. Here, $\widetilde{\varepsilon}$ is a free parameter, and $g_{n,x} = \binom{n+x-1}{x-1}$, where x depends on the exact protocol structure as summarised in Table 5.1.*

Note that this holds for all types of QKD protocols, where PM and MDI QKD protocols would have the required fixed marginal constraints in the IID proofs. We refer the reader to [11, Section III.] for the full proof of this statement.

> **Technical aside 5.1** (Inaccuracy in [10])**.** The increase in secrecy parameter was postulated to simply be $g_{n,x}\varepsilon_{\text{sec}}$ in [10]. However, we were unable to prove this claim, and so settled for the worse, but rigorous bound stated in Theorem 5.2 ($\approx g_{n,x}\sqrt{\varepsilon_{\text{sec}}}$).

We now discuss the subtleties to be kept in mind when applying the postselection technique to infinite-dimensional optical protocols, and describe the use of the tools described in Chapter 4 to address detector imperfections with the postselection technique.

5.3 Imperfect detection setups

Optical implementations are modelled in infinite-dimensional Hilbert spaces. Therefore, the postselection technique cannot be applied directly, since the cost diverges. We obtain an effective finite-dimensional description by using squashing maps and source maps as described in Sections 3.4.2 and 3.4.3. However, the use of these tools — specifically squashing maps — requires care. In particular, the de Finetti reductions we use retain *only* the fixed marginal constraint. Thus, if the flag-state squasher is applied *before* the postselection technique, the IID security proof would have to hold against *all* IID attacks, not just the restricted set described in Lemma 3.4. As described in Section 3.4.3, this would result in trivial bounds. Accordingly, we must use the weight-preserving flag-state squasher (WPFSS) described in Section 3.4.3.

This solution works well for perfect detection setups; for imperfect detection setups, the noise channel constructions of Chapter 4 introduce an additional complication. In particular, Theorems 4.3 and 4.4 assume that the flag-state squasher is applied first, and that security is proved against a restricted set of attacks constructed in Remark 4.3. As these steps do not commute, the argument *must* proceed in the following order:

1. Apply the WPFSS (Lemma 3.5 and Corollary 3.2); this reduces the security analysis to a finite-dimensional protocol.

2. Apply the postselection technique (Theorem 5.2); this reduces the analysis to security against all IID attacks.

3. Apply the flag-state squasher ([3, Theorem 1]); this reduces the analysis to the security of a flag-state squashed protocol against a restricted set of IID attacks (Lemma 3.4).

4. Apply the noise channels (Chapter 4); this reduces the analysis to the security analysis of a protocol with perfect detectors against a restricted set of IID attacks.

For this chain of reasoning to be valid, we must verify that the noise channel constructions remain applicable after applying the WPFSS. We discuss these details further below.

At first glance, one might expect that Theorems 4.3 and 4.4 could be directly applied in Step 4 to establish security against untrusted loss and dark counts. The subtlety is that the application of the WPFSS in Step 1 requires the event e used for the construction of the restricted set Lemma 3.4 to be represented by a single POVM element as stated in Remark 3.5. Consequently, before invoking the flag-state squasher, we fix a coarse-graining of the POVM outcomes that constitute the event e, and work thereafter with the corresponding coarse-grained POVM. In general, the conditions required for the proofs of Theorems 4.3 and 4.4 might not be satisfied. However, for typical choices of this event e, as we shall see, Theorems 4.3 and 4.4 remains unchanged.

We first formalise what it means to coarse-grain the POVM as a classical post-processing of outcomes, in a form convenient for later use. A 'coarse-graining' is a classical post-processing step whose corresponding stochastic matrix only consists of 1s and 0s. For example, consider the passive BB84 detection setup and classically post-process all click patterns that consist of more than a single click into a single 'multi-click' event. The stochastic matrix corresponding to this post-processing is given by

$$\mathcal{P}_{\text{cg}} = \begin{pmatrix} 1 & 0 & 0 & 0 & \overbrace{0 \cdots\cdots 0}^{12} \\ 0 & 1 & 0 & 0 & 0 \cdots\cdots 0 \\ 0 & 0 & 1 & 0 & 0 \cdots\cdots 0 \\ 0 & 0 & 0 & 1 & 0 \cdots\cdots 0 \\ 0 & 0 & 0 & 0 & 1 \cdots\cdots 1 \end{pmatrix}. \tag{5.9}$$

The general structure of the argument is shown in Fig. 5.1. Each equivalence is an equivalence of quantum-to-classical measurement channels.

- We start by considering a generic detection setup that uses threshold detectors with dark counts and loss. Additionally, we allow for some classical post-processing $\mathcal{P}'_{\text{cg}}$. Although this can be chosen to be any arbitrary post-processing, we choose it to be a coarse-graining for simplicity.

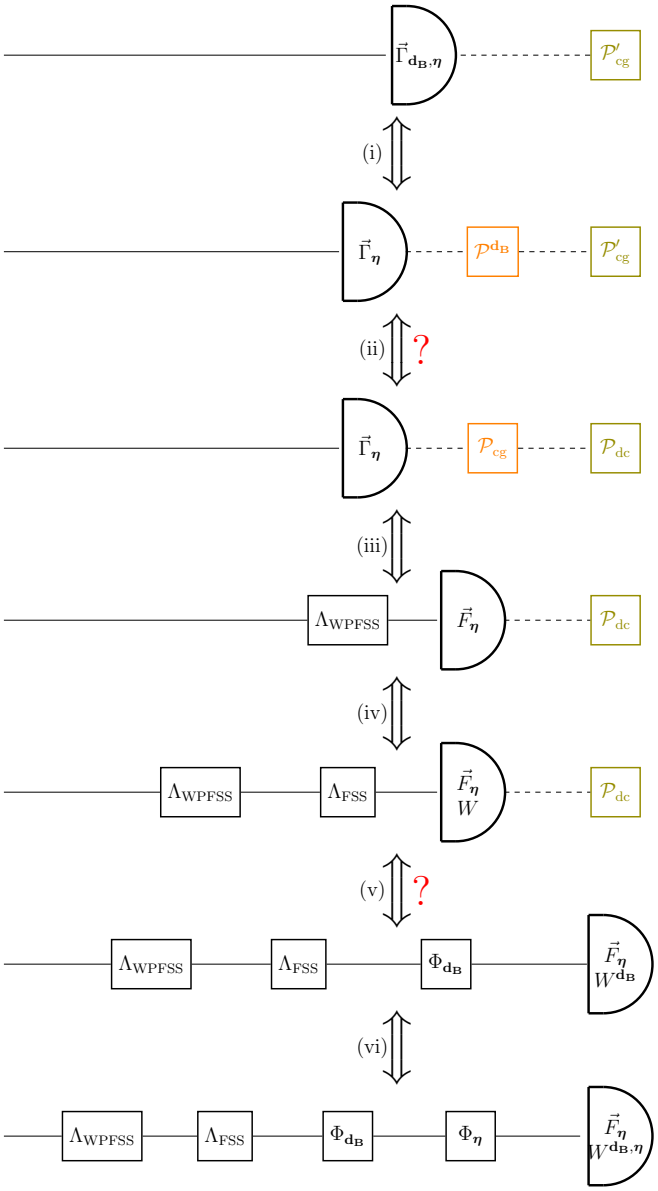


Figure 5.1: A set of equivalences (as quantum-to-classical measurement channels) of detection setups to use Theorems 4.3 and 4.4 with the postselection technique. Here, $\mathcal{P}'_{\mathrm{cg}}$ represents the classical post-processing carried out in the protocol, $\mathcal{P}^{\mathbf{d_B}}$ is the dark count post-processing, $\mathcal{P}_{\mathrm{cg}}$ is the coarse-graining required for the WPFSS Λ_{WPFSS}, and $\mathcal{P}_{\mathrm{dc}}$ is the post-processing fixed by Eq. (5.10). In the figure, olive post-processing maps represent free choices that can be made to make equivalences (ii) and (v) hold. Orange post-processing maps represent stochastic processes fixed by equivalences (i) and (iii).

- Equivalence (i) follows from the fact that dark counts can be modelled as a classical post-processing $\mathcal{P}^{\mathbf{d_B}}$ as described in Section 2.2.5.
- Equivalence (ii) must be shown to hold; we need to find some stochastic matrix $\mathcal{P}_{\text{dc}}$ such that

$$\mathcal{P}'_{\text{cg}}\mathcal{P}^{\mathbf{d_B}} = \mathcal{P}_{\text{dc}}\mathcal{P}_{\text{cg}}. \tag{5.10}$$

  Here $\mathcal{P}_{\text{cg}}$ is the coarse-graining required for the WPFSS.
- Equivalence (iii) follows from the existence of the WPFSS. The postselection technique can then be used on the resulting finite-dimensional systems.
- Equivalence (iv) follows from the existence of the flag-state squasher [3, Theorem 1].
- Equivalence (v) follows from Theorem 4.3, if $\mathcal{P}_{\text{dc}}$ satisfies Eqs. (4.12) to (4.14).
- Equivalence (vi) follows from Theorem 4.4, assuming that the coarse-graining $\mathcal{P}_{\text{cg}}$ used in the WPFSS preserves the single-click and no-click events, as is commonly the case.[3]

The validity of equivalences (ii) and (v) depends on the coarse-graining $\mathcal{P}_{\text{cg}}$ needed for the WPFSS. As explained above, the coarse-graining $\mathcal{P}_{\text{cg}}$ must have the event e used to bound the weight outside the preserved subspace (Lemma 3.4) as one of the coarse-grained POVM elements. In general, for different protocol-dependent choices [71, 63] of the weight estimation event, these equivalences would have to be checked on a case-by-case basis. Fortunately, for the more generic choice of weight estimation event described in Ref. [72, Section VII. F.], we can check the validity of these equivalences *independent* of protocol choice[4], which we now proceed to discuss.

The weight estimation in [72], which can be applied to any passive detection setup, uses the event consisting of any click pattern with more than a single click. The coarse-graining $\mathcal{P}_{\text{cg}}$ corresponding to this weight estimation event does nothing to the no-click and single-click event, but considers the rest of the events to be a single multi-click event.

[3] Theorems 4.1 and 4.2 can be used before or after Theorem 4.4 to address more general forms of imperfections.

[4] This is a valid choice for all passive linear-optical protocols, as described in [72].

Concretely, the stochastic matrix corresponding to this coarse-graining is given by

$$\mathcal{P}_{\text{cg}} = \left(\begin{array}{c|c|c} 1 & 0\cdots\cdots0 & 0\cdots\cdots0 \\ \hline \begin{matrix}0\\ \vdots \\ \vdots \\ 0\end{matrix} & \mathbb{I}_{n_S} & \mathbf{0}_{n_S\times n_M} \\ \hline 0 & \underbrace{0\cdots\cdots0}_{n_S} & \underbrace{1\cdots\cdots1}_{n_M} \end{array}\right), \tag{5.11}$$

where n_S is the number of single-click events, and n_M is the number of multi-click events.

For this coarse-graining, we shall verify that there exists a classical post-processing $\mathcal{P}_{\text{dc}}$ that satisfies Eq. (5.10). First, we set the coarse-graining $\mathcal{P}'_{\text{cg}}$ performed in the protocol to be the same as the coarse-graining $\mathcal{P}_{\text{cg}}$ described in Eq. (5.11). Further, we need to make the physically motivated assumption that the dark count post-processing $\mathcal{P}^{\mathbf{d_B}}$ does not turn multi-clicks into no-click or single-click events, i.e.

$$\mathcal{P}^{\mathbf{d_B}}_{i|m} = 0, \tag{5.12}$$

for all $i \in \{0\} \cup S$, and $m \in M$. Thus, the dark count post-processing can be written as a block-matrix whose top-right block is zero as

$$\mathcal{P}^{\mathbf{d_B}} = \left(\begin{array}{c|c} \overbrace{\mathcal{P}^{\mathbf{d_B}}_{M^C|M^C}}^{n_S+1} & \overbrace{\mathbf{0}_{(n_S+1)\times n_M}}^{n_M} \\ \hline \mathcal{P}^{\mathbf{d_B}}_{M|M^C} & \mathcal{P}^{\mathbf{d_B}}_{M|M} \end{array}\right). \tag{5.13}$$

Importantly, the $\mathbf{0}_{(n_S+1)\times n_M}$ block along with the fact that $\mathcal{P}^{\mathbf{d_B}}_{M|M}$ is a stochastic matrix can be used to verify from explicit computation that the following ansatz satisfies Eq. (5.10) (and hence, equivalence (ii)):

$$\mathcal{P}_{\text{dc}} = \left(\begin{array}{c|c} \overbrace{\mathcal{P}^{\mathbf{d_B}}_{M^C|M^C}}^{n_S+1} & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline s^1_{M|M^C}\cdots\cdots s^{n_S+1}_{M|M^C} & 1 \end{array}\right), \tag{5.14}$$

where $s^i_{M|M^C}$ is the sum of all elements in the i^{th} column of $\mathcal{P}^{\mathbf{d_B}}_{M|M^C}$.

Moreover, it is straightforward to verify that this post-processing $\mathcal{P}_{\text{dc}}$ satisfies Eqs. (4.12) to (4.14). Thus, Theorem 4.3 can be used to show that equivalence (v) holds. We have hence shown that the postselection technique can be used with the noise channel constructions described in Chapter 4 with an appropriate choice of coarse-graining $\mathcal{P}_{\text{cg}}$.

Technical aside 5.2 (Only IID imperfections)**.** The noise channel constructions eliminating the dependence of the POVM on dark counts and loss must be made after the reduction to IID. Thus, the postselection technique, which requires the measurements to be IID, cannot accommodate any variance in dark count rates or loss across protocol rounds. Additionally, if we consider multimode detection setups, the postselection technique cannot be used as before applying the noise channels; the multimode POVM is still infinite-dimensional, even after squashing (see Section 4.3).

5.4 Decoy-state protocols

We now analyse the dimension d_A of Alice's subsystem. If Alice prepares pure states, the dimension d_A is always finite. This can be seen as follows. The shield system A_S constructed in Lemma 3.1 to contain a purification of Alice's prepared states is trivial (one-dimensional). So, the source-replaced state constructed in Lemma 3.2 has the dimension d_A of Alice's system A to be the number of states prepared by Alice, which is finite. Consequently, any infiniteness in the description can only arise from the shield system A_S.

Notational aside 5.3. There is a slight discrepancy in notation here. Throughout most of this chapter, A denoted the system subject to the fixed marginal constraint, i.e. Alice's measured subsystem together with its shield A_S. From now on, we distinguish these explicitly: A is Alice's measured subsystem and A_S the shield system. The fixed marginal constraint applies to AA_S.

In general, if Alice prepares infinite-dimensional mixed states, her purifying shield system A_S is infinite-dimensional. In this case, source maps (using Corollary 3.1) allow us to reduce the effective dimension of the shield system to a finite value. The existence of such a source map needs to be applied on a case-by-case basis. We now detail this process for a widely used family of QKD protocols, crucial for long-distance QKD — decoy-state protocols [59, 60, 61].

Decoy-state protocols are often implemented with phase-randomised laser pulses. Each pulse has the form $\rho_{a,\mu} = \bigoplus_{m=0}^{\infty} p(m \mid \mu)\rho_{a,m} \in \mathrm{S}_\circ\left(\bigoplus_{m=0}^{\infty} \mathcal{H}_m\right)$ with varying intensity μ and encoding choice a. As described in Section 3.4.2, a tagging source map can be constructed

for these phase-randomised laser pulses to reduce the security analysis to that of a protocol with a tagged laser source [62] (see Lemma 3.3):

$$\xi_{a,\mu} = \bigoplus_{m=0}^{N_{\text{ph}}} p(m \mid \mu)\rho_{a,m} + \left(1 - \sum_{m=0}^{N_{\text{ph}}} p(m \mid \mu)\right) |a,\mu\rangle\langle a,\mu| \,, \tag{5.15}$$

where $\{|a,\mu\rangle\}_{a,\mu}$ form an orthonormal basis for a space orthogonal to the physical photon-number subspace $\bigoplus_{m=0}^{N_{\text{ph}}} \mathcal{H}_m$. The photon-number cut-off $N_{\text{ph}} \in \mathbb{N}$ can be chosen freely while constructing the source map, but the choice impacts the key rate.

In particular, increasing the photon-number cut-off N_{ph} increases the dimension of the shield system, and hence dimension-dependent cost $g_{n,x}$ incurred due to the application of the postselection technique. In contrast, decreasing N_{ph} increases the probability of emitting a classical tag, which gives Eve more power in the IID security analysis. We now make these costs precise.

5.4.1 Construction of shield system for decoy-state protocols

We first explicitly construct the fixed marginal state for a tagged laser source. This will enable us to calculate the dimensions of Alice's subsystems AA_S for a decoy-state protocol.

In this subsection, we assume the typical case in which the m-photon states $\rho_{a,m} =: |\zeta_{a,m}\rangle\langle\zeta_{a,m}|$ are all pure.[5] With this assumption, the tagged source described by Eq. (5.15) can be purified as

$$|\xi_{a,\mu}\rangle_{AS A'} = \sum_{m=0}^{N_{\text{ph}}} \sqrt{p(m \mid \mu)}\, |m\rangle_{A_S} \otimes |\zeta_{a,m}\rangle_{A'} + \sqrt{1 - \sum_{m=0}^{N_{\text{ph}}} p(m \mid \mu)}\, |\text{tag}\rangle_{A_S} \otimes |a,\mu\rangle_{A'} \,, \tag{5.16}$$

where $|\text{tag}\rangle$ is a state orthogonal to $\{|m\rangle\}_{m=0}^{N_{\text{ph}}}$. Let there be n_{int} intensities used in the decoy-state analysis. Then, using the source replacement scheme described in Eq. (3.5),

[5] If they are mixed, a similar analysis would apply, while carefully tracking the portion of the shield system corresponding to purifying the m-photon states $\rho_{a,m}$.

we can obtain the fixed marginal

$$\begin{aligned}
&\hat{\sigma}_{AA_S} = \mathrm{Tr}_{A'}\left[\rho_{AA_SA'}\right] \\
&= \sum_{\substack{a,a'=1 \\ \mu,\nu}}^{d_A,n_{\mathrm{int}}} \sqrt{p(a,\mu)\,p(a',\nu)}\,|a,\mu\rangle\langle a',\nu|_A \otimes \mathrm{Tr}_{A'}\left[|\xi_{a,\mu}\rangle\langle\xi_{a',\nu}|_{A_SA'}\right] \\
&= \sum_{\substack{a,a'=1 \\ \mu,\nu}}^{d_A,n_{\mathrm{int}}} \sqrt{p(a,\mu)\,p(a',\nu)}\,|a,\mu\rangle\langle a',\nu|_A \otimes \left(\begin{array}{c} \displaystyle\sum_{m=0}^{N_{\mathrm{ph}}} \sqrt{p(m\mid\mu)\,p(m\mid\nu)}\,\langle\zeta_{a',m}|\zeta_{a,m}\rangle\,|m\rangle\langle m| + \\ \sqrt{\left(1-\displaystyle\sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\mu)\right)\left(1-\displaystyle\sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\nu)\right)}\,|\mathrm{tag}\rangle\langle\mathrm{tag}| \end{array} \right).
\end{aligned} \tag{5.17}$$

Hence, the fixed marginal is block-diagonal in the photon number, with one extra 'tag' block. These $N_{\mathrm{ph}}+2$ blocks, each have dimension at most $n_{\mathrm{int}}d_A$.[6]

The effective dimension can be decreased further since the fixed marginal $\hat{\sigma}_{AA_S}$ constructed in Eq. (5.17) is not full rank, as we now show. For notational brevity, define $p(\mathrm{tag}\mid\mu) \coloneqq 1-\sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\mu)$. In what follows, we will break up the fixed marginal $\hat{\sigma}_{AA_S}$ into blocks similarly to Eq. (5.17). We then compute the rank of the state in each block by looking at the Schmidt rank of the purification of the block [57, Eq. (2)].

[6]Indeed, this is the dimension that would need to be used when accounting for phase imperfections in decoy-state protocols [63].

To compute the rank of $\hat{\sigma}_{AA_S}$ we consider $\rho_{AA_SA'} =: |\psi\rangle\langle\psi|_{AA_SA'}$, where

$$
\begin{aligned}
|\psi\rangle_{AA_SA'} &= \sum_{a,\mu,m} \sqrt{p(a,\mu)\, p(m \mid \mu)}\, |a,\mu\rangle_A \otimes |m\rangle_{A_S} \otimes |\zeta_{a,m}\rangle_{A'} \\
&\quad + \sum_{a,\mu} \sqrt{p(a,\mu)\, p(\mathrm{tag} \mid \mu)}\, |a,\mu\rangle_A \otimes |\mathrm{tag}\rangle_{A_S} \otimes |a,\mu\rangle_{A'} \\
&= \sum_{m=0}^{N_{\mathrm{ph}}} \sqrt{p(m)}\, |m\rangle_{A_S} \otimes \left(\sum_{a,\mu} \sqrt{p(a,\mu \mid m)}\, |a,\mu\rangle_A \otimes |\zeta_{a,m}\rangle_{A'} \right) \\
&\quad + \sqrt{p(\mathrm{tag})}\, |\mathrm{tag}\rangle_{A_S} \otimes \left(\sum_{a,\mu} \sqrt{p(a,\mu \mid \mathrm{tag})}\, |a,\mu\rangle_A \otimes |a,\mu\rangle_{A'} \right). \qquad (5.18) \\
&=: \sum_{m=0}^{N_{\mathrm{ph}}} \sqrt{p(m)}\, |m\rangle_{A_S} \otimes |\psi_m\rangle_{AA'} + \sqrt{p(\mathrm{tag})}\, |\mathrm{tag}\rangle_{A_S} \otimes |\psi_{\mathrm{tag}}\rangle_{AA'}. \qquad (5.19)
\end{aligned}
$$

Here, Eq. (5.18) follows from applying Bayes' theorem, $p(m)p(a,\mu \mid m) = p(a,\mu)p(m \mid a,\mu)$, where the photon number m and encoding choice a are independent, $p(m \mid a,\mu) = p(m \mid \mu)$.

The rank of $\mathrm{Tr}_{A'}[\,|\psi_m\rangle\langle\psi_m|\,]$ corresponds to the Schmidt rank of $|\psi_m\rangle$ [57, Eq. (2)], which is at most the span of $\{|\zeta_{a,m}\rangle\}_{a=1}^{d_A}$. Let this number be d_m^A for the m-photon subspace. Then, the fixed marginal $\hat{\sigma}_{AA_S}$ consists of blocks of dimension $\{d_m^A\}_{m=0}^{N_{\mathrm{ph}}}$ in addition to $n_{\mathrm{int}} d_A$ tagged blocks of dimension 1.

> **Technical aside 5.3** (Improvement over [11])**.** Each $d_m^A \leq d_A$, as the states $|\zeta_{a,m}\rangle$ do not depend on the number of intensity settings n_{int}. Thus, this is a strict improvement over the existing bound [11, Appendix D 1], which used the looser bound $d_m^A = n_{\mathrm{int}} d_A$ for all blocks.

5.4.2 IID decoy-state analysis for tagged sources

When using the postselection technique, the security analysis must be performed using the shield system associated with the tagged states (see Section 5.4.1). This setup differs slightly from the standard decoy-state analysis [60, 61], which is formulated in terms of fully phase-randomised laser pulses. However, we show that the tagged-state formulation can be reduced to the standard analysis. For pedagogical clarity, we restrict our explanation

to the asymptotic case; the extension to the finite-size regime follows directly from the suitable application of concentration inequalities [90].

Under the IID attack setting, the security proof reduces to obtaining a lower bound on a single-round entropic quantity [77, 91], over the set of states consistent with the observed data. Using properties of this entropy, together with the block-diagonal structure of the prepared states, the entropic quantity admits a lower bound given by the contribution from the single photon block (see, e.g. Ref. [71]). However, the relevant observations are not directly accessible for the single-photon block. Thus, the decoy-state analysis aims to infer bounds on the single-photon block from the observed statistics of phase-randomised coherent states [63]:

$$\begin{aligned} &\underset{\Phi}{\text{opt.}}\ \mathrm{Tr}\left[\Phi\left[\rho_{a',1}\right]F_j\right] \\ &\text{s.t. } \mathrm{Tr}\left[\Phi\left[\xi_{a,\mu}\right]F_l\right] = \gamma_{l|a,\mu} \quad \forall l,a,\mu \\ &\quad \Phi \in \mathcal{C}\left(A',B\right), \end{aligned} \tag{5.20}$$

where $\{F_i\}$ is Bob's squashed POVM. Here, 'opt.' indicates that separate optimisations are performed to find the minimum and maximum values. This is a semidefinite program (SDP) that can be numerically computed.

Although the above is an SDP, its structure allows a direct reduction to a simpler linear program to save on computation time as follows. The constraints can be simplified as

$$\begin{aligned} \gamma_{l|a,\mu} &= \mathrm{Tr}\left[\Phi\left[\xi_{a,\mu}\right]F_l\right] \\ &= \sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\mu)\mathrm{Tr}\left[\Phi\left[\rho_{a,m}\right]F_l\right] + (1-\sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\mu))\mathrm{Tr}\left[\Phi\left[|k,\mu\rangle\langle k,\mu|\right]F_l\right]. \end{aligned} \tag{5.21}$$

Next, defining $p(\mathrm{det}_l \mid a,m) = \mathrm{Tr}\left[\Phi\left[\rho_{a,m}\right]F_l\right]$, and $p(\mathrm{det}_l \mid a,\mu,\mathrm{tag}) = \mathrm{Tr}\left[\Phi\left[|a,\mu\rangle\langle a,\mu|\right]F_l\right]$ allows us to recast the generalised decoy-state SDPs described in Eq. (5.20) into linear programs as

$$\begin{aligned} &\text{opt. } p(\mathrm{det}_j \mid a',1) \\ &\text{s.t. } \sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\mu)p(\mathrm{det}_l\mid a,m) + (1-\sum_{m=0}^{N_{\mathrm{ph}}} p(m\mid\mu))p(\mathrm{det}_l\mid a,\mu,\mathrm{tag}) = \gamma_{l|a,\mu} \quad \forall\, l,a,\mu \\ &\quad 0 \le p(\mathrm{det}_l \mid a,m) \le 1 \\ &\quad 0 \le p(\mathrm{det}_l \mid a,\mu,\mathrm{tag}) \le 1. \end{aligned} \tag{5.22}$$

Finally, this can be recast into the standard form [60, 61] by using 0 and 1 as the lower and upper limits of $p(\mathrm{det}_l \mid k,\mu,\mathrm{tag})$ in the linear program constraints. These formulations

make it clear that increasing the photon-number cut-off N_{ph} would increase the IID key rates, at the cost of the increased penalty for the postselection technique.

5.5 Concrete application

So far we have made rigorous the framework to apply the postselection technique to optical prepare-and-measure protocols (including decoy-state protocols). In this section, we first summarise the various results in this chapter, before illustrating our results by applying them to the time-bin encoded three-state protocol.

5.5.1 Recipe for application

Recall that the postselection technique reduces the problem of proving security against general attacks to proving security against IID attacks, while paying some penalty for the reduction (Theorem 5.2). In practice, this can be used as follows:

1. Choose a target secrecy parameter ε_{sec} based on the application in mind.
2. Determine penalty of using the postselection technique as $g_{n,x} = \binom{n+x-1}{x-1} \leq \left(\frac{e(n+x-1)}{x-1}\right)^{x-1}$. Steps 2a and 2b can be carried out in any order.
   (a) Apply tagging [62] to reduce the effective dimensions of Alice's subsystem to a finite number.
   Alice's subsystems (including the shield system) for decoy-state protocols have $N_{\text{ph}} + 2$ blocks whose dimensions $\{d_m^A\}_{m=0}^{N_{\text{ph}}} \cup \{n_{\text{int}} d_A\}$ depend on Alice's state preparation as detailed in Section 5.4.1. Here, N_{ph} is the photon-number cut-off used when tagging the phase-randomised coherent state, n_{int} is the number of intensities used for the decoy analysis, and d_A is the number of encoding setting choices used by Alice.
   (b) Apply the WPFSS[7] to reduce the effective dimensions of Bob's subsystem to a finite number.
   The POVM (see Section 3.4.3 for details on the POVM construction) consists of blocks corresponding to the total incoming photon number or flag states. For

[7] This involves computing a lower bound on the minimum eigenvalue $\lambda_{\min}$ of the POVM element corresponding to the weight-estimation event e as described in Section 3.4.3.

an optical setup which uses two modes to encode the bit information, Bob's subsystem has blocks with dimensions $\{d_m^B\}_{m=0}^N$, where $d_m^B = m+1$, in addition to n_{meas} (flag) blocks, each of dimension 1. Here, N is the photon-number cut-off used when applying the WPFSS, and n_{meas} is the number of POVM outcomes.

(c) Compute the penalty parameter from Steps 2b and 2a;

$$x = \left(\sum_{m=0}^{N_{\text{ph}}} {d_m^A}^2 + n_{\text{int}} d_A\right)\left(\sum_{m=0}^{N}(m+1)^2 + n_{\text{meas}}\right), \tag{5.23}$$

and use it to compute the penalty $g_{n,x}$.

3. Choose value of free parameter $\widetilde{\varepsilon}$ (in principle this value can be optimised over).

4. Apply Theorem 5.2 to reduce the analysis to proving ε_{IID}-secrecy against IID attacks with secrecy parameter $\varepsilon_{\text{IID}} = \left(\frac{\varepsilon_{\text{sec}} - g_{n,x}\widetilde{\varepsilon}}{4g_{n,x}}\right)^2$.

   (a) To address detector imperfections, apply the flag-state squasher and the results of Chapter 4 and Section 5.3.

   (b) Compute key length l for the resultant protocol (see for e.g. [90] for a security proof of decoy-state protocols against IID attacks).

5. Use key length $l' = l - 2\log(g_{n,x}) - 2\log(1/\widetilde{\varepsilon})$ as the final hash length for the protocol. This protocol is ε_{sec}-secret against general attacks.

5.5.2 Optical setup

We first describe the optical setup of the time-bin encoded three-state protocol depicted in Fig. 5.2.

We consider a protocol where Alice uses a laser source to prepare a phase-randomised coherent state in two time-bin modes as follows:

0, μ: $|0\rangle \otimes \left|\sqrt{\mu}e^{i\theta}\right\rangle$

1, μ: $\left|\sqrt{\mu}e^{i\theta}\right\rangle \otimes |0\rangle$

+, μ: $\left|\frac{\sqrt{\mu}e^{i\theta}}{\sqrt{2}}\right\rangle \otimes \left|\frac{\sqrt{\mu}e^{i\theta}}{\sqrt{2}}\right\rangle$,

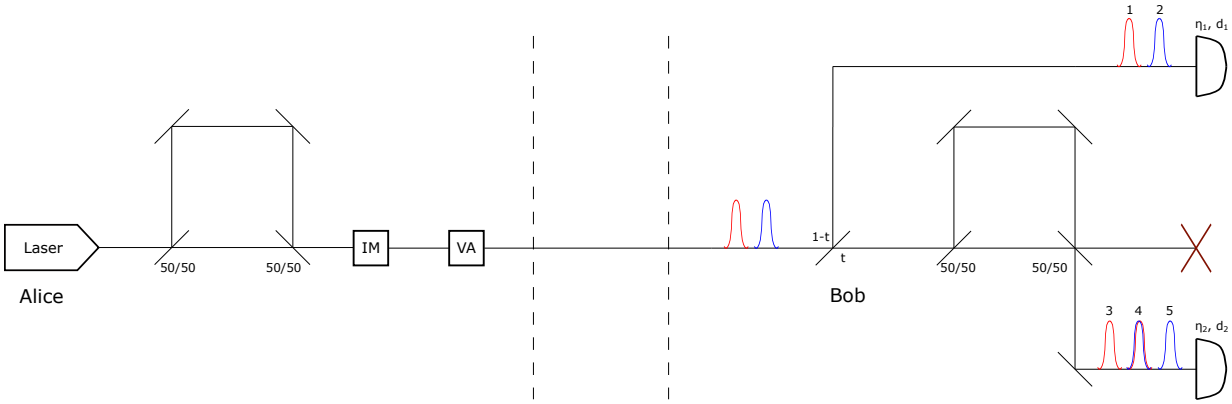


Figure 5.2: Schematics of the implementation of the three-state protocol as in [4]. The numbers below the beam splitters reflect their transmissivity. IM and VA refer to intensity modulator and variable attenuator respectively.

where the phase $\theta \in [0, 2\pi)$ is uniformly random. The variable attenuator and intensity modulator serve to choose the values of the encoding $\{0, 1, +\}$ and intensity μ. Bob's measurement setup is identical to that considered in [63, 4] as depicted in Fig. 5.2. This consists of a passive beam splitter which chooses between the 'Z-basis' arm, which measures the time-of-arrival of the pulses, and the 'X-basis' arm, which consists of a Mach-Zehnder interferometer. Note that the Mach-Zehnder interferometer only uses one detector to minimise implementation costs.

The basis choice beam splitter has reflectivity $t \in [t_{\min}, t_{\max}]$. Both detectors here are threshold detectors, with efficiencies $\eta_1, \eta_2 \in [\eta_{\min}, \eta_{\max}]$ and dark count rates $d_1, d_2 \in [0, d_{\max}]$. The exact values of the ranges are parameters that will be set later. For simplicity, we assume that the 50:50 beam splitters that form a part of the Mach-Zehnder interferometer are perfect, though variations of the same ideas we use for the rest of the imperfections would extend to these imperfections as well.

We now follow the recipe described in Section 5.5.1. First, we pick the target secrecy parameter ε_{sec} to be 2×10^{-12}.

5.5.3 Tagging

We must use tagged states for the security proof as described in Section 5.4. We compute the dimension of the blocks of the resultant fixed marginal described in Section 5.4.1. For the three-state protocol, the states prepared in each photon-number subspace are

pure. Thus, the dimension d_m^A of the m-photon block is given by the number of linearly independent states sent in the m-photon subspace. For $m = 0$, this is just the vacuum state. For $m = 1$, all three states sent lie in the two dimensional space spanned by $\{|0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle\}$. All other blocks are $d_A = 3$-dimensional as there are 3 encodings.

5.5.4 Applying the WPFSS

To apply the WPFSS, we define the weight-estimation event e to be any click pattern that records a click in both detectors, while ignoring all clicks in the middle time slot of the Mach-Zehnder interferometer. That is, the event corresponding to click patterns which contain at least one of time bin 1 or 2, and contain at least one of 3 or 5 (see Fig. 5.2).

Having fewer outcomes leads to a smaller flag space, which is beneficial in reducing the penalty of using the postselection technique (Step 5.23). Thus, we coarse-grain the outcomes to the outcome in which no detector clicks, the outcomes in which a single detector in a single time bin clicks, the weight-estimation event e, and all other outcomes grouped into one. This coarse-graining results in 8 flag states (corresponding to 8 coarse-grained POVM outcomes). For the simulations here, we choose the photon-number cut-off to be 1. Thus, Bob's system consists of 1 block of dimension 2 (qubit space), and 9 blocks of dimension 1 (vacuum and flags).

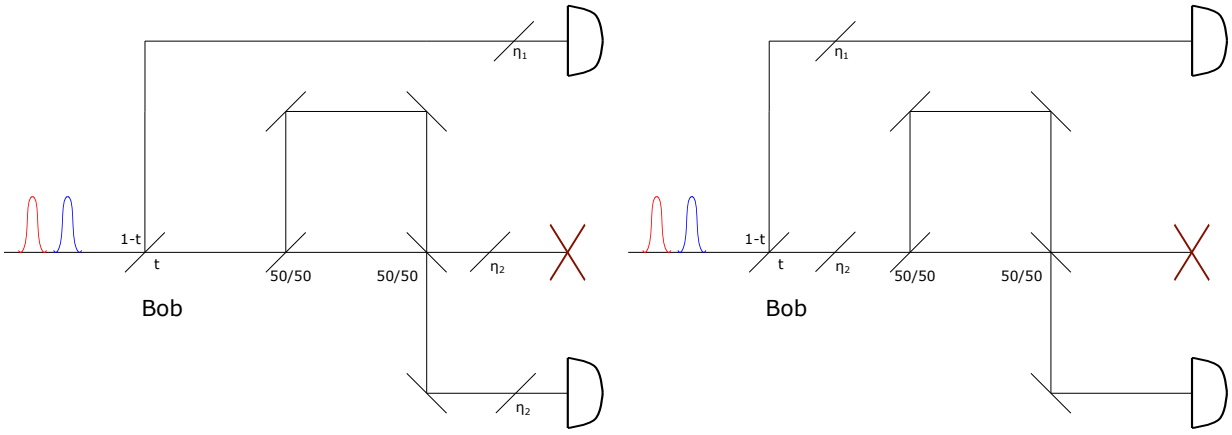
If we assume unit efficiencies, we can use the results proved in Appendix C of Ref. [63], to find

$$\lambda_{\min}\left(\overline{\Pi}_{\leq N}\Gamma_e\overline{\Pi}_{\leq N}\right) \geq 1 - t^{N+1} - \left(1 - \frac{t}{4}\right)^{N+1} + \left(\frac{3t}{4}\right)^{N+1}, \tag{5.24}$$

where t is Bob's basis-choice beam-splitting ratio. We now construct an equivalent detection setup with unit efficiencies in order to use a modified version of this result that accounts for the detection setup parameter ranges.

Equivalent detection setup

We first use the characterisation of a detector with efficiency η described in Section 2.2.6; that of a beam splitter with transmissivity η followed by a lossless detector. The missing detector can always be preceded by a beam splitter of any transmissivity. This is depicted in Fig. 5.3a. Since both beam splitters at both outputs of the Mach-Zehnder interferometer have the same transmissivity, this can be equivalently represented as a single beam splitter at the input of the Mach-Zehnder interferometer, as depicted in Fig. 5.3b.



(a) Detectors with efficiency η_i represented as beam splitters with transmissivity η_i followed by lossless detectors for the three-state protocol detection setup.

(b) The common loss can be pulled to the input arm of the Mach-Zehnder interferometer.

Figure 5.3: Simplifying the description of the detection setup with lossy detectors.

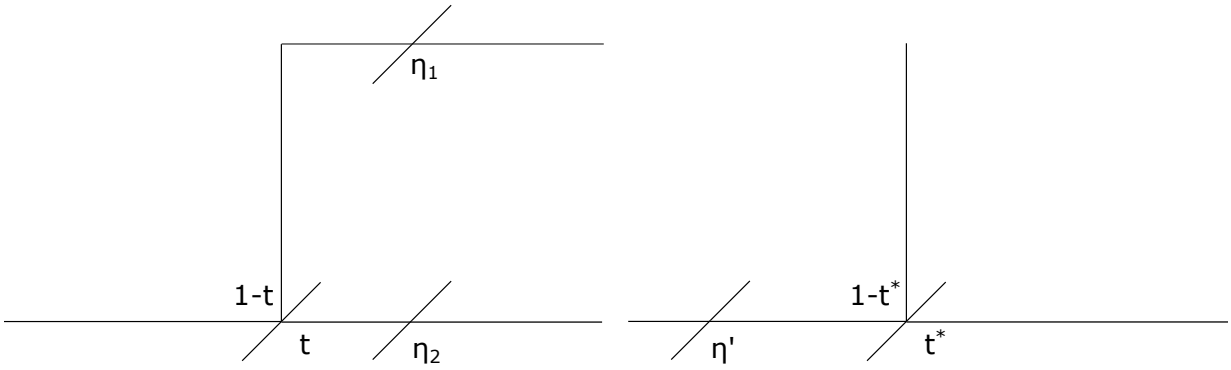
Next, we use ideas from [33, Section 1.5] to pull both beam splitters that represent the loss before the basis-choice beam splitter. Doing so would also change the basis choice beam-splitting ratio. This is depicted in Fig. 5.4. It is sufficient to show that this equivalence holds for any coherent states, as these form a basis for the entire space (of operators). We establish this as follows. Any coherent state $|\alpha\rangle$ input into the setup depicted in Fig. 5.4a has output $\left|\sqrt{(1-t)\,\eta_1}\,\alpha\right\rangle \otimes |\sqrt{t\,\eta_2}\,\alpha\rangle$. Any coherent state $|\alpha\rangle$ input into the setup depicted in Fig. 5.4b has output $\left|\sqrt{\eta'\,(1-t^*)}\,\alpha\right\rangle \otimes \left|\sqrt{\eta'\,t^*}\,\alpha\right\rangle$. This holds if

$$\begin{aligned}(1-t)\,\eta_1 &= \eta'\,(1-t^*)\\ t\,\eta_2 &= \eta'\,t^*.\end{aligned}$$

Adding both equations gives $\eta' = t\,\eta_2 + (1-t)\,\eta_1$. This is a convex combination of η_1 and η_2, and hence lies between the maximum and minimum of the two. Consequently, $\eta' \in [0,1]$ is well-defined. We can use this to solve for the effective beam-splitting ratio t^*:

$$t^* = \frac{t\,\eta_2}{t\,\eta_2 + (1-t)\,\eta_1} \tag{5.25}$$

$$t^*_{\min} \coloneqq t_{\min}\frac{\eta_{\min}}{\eta_{\max}} \leq t^* \leq t_{\max}\frac{\eta_{\max}}{\eta_{\min}} =: t^*_{\max}, \tag{5.26}$$



(a) Zooming in on the part of the equivalent detection setup analysed.

(b) The losses can be pulled to the input arm of the basis-choice beam splitter, with some change in the splitting ratio.

Figure 5.4: Simplifying the description of the detection setup with lossy detectors.

where we have used the ranges of the beam-splitting ratio and efficiencies to bound the effective beam-splitting ratio in Eq. (5.26). Note that although the upper bound in Eq. (5.26) can be larger than 1, the true value of the effective beam-splitting ratio t^* given in Eq. (5.25) cannot be larger than 1:

$$\begin{aligned} t^* &= \frac{t\,\eta_2}{t\,\eta_2 + (1-t)\,\eta_1} \\ &= \frac{1}{1 + \frac{(1-t)\,\eta_1}{t\,\eta_2}} \leq 1. \end{aligned}$$

Thus, the effective beam-splitting ratio $t^* \in [0,1]$ is also well-defined.

The common loss η' can now be considered to be a part of Eve's channel. Thus, we have reduced the detection setup in Fig. 5.2 to one without loss, but with a modified beam-splitting ratio. Thus, using the results proved in [63, Appendix C], we can obtain the required bound

$$\begin{aligned} \lambda_{\min}\left(\overline{\Pi}_{\leq N}\Gamma_{\mathrm{e}}\overline{\Pi}_{\leq N}\right) &\geq 1 - (t^*)^{N+1} - \left(1 - \frac{t^*}{4}\right)^{N+1} + \left(\frac{3t^*}{4}\right)^{N+1} \\ &\geq 1 - (t^*_{\max})^{N+1} - \left(1 - \frac{t^*_{\min}}{4}\right)^{N+1} + \left(\frac{3t^*_{\min}}{4}\right)^{N+1}. \end{aligned}$$

As our analysis uses the single-photon cut-off $N = 1$, we can straightforwardly derive a

tighter and simpler bound:

$$\lambda_{\min}\left(\overline{\Pi}_{\leq 1}\Gamma_{\mathrm{e}}\overline{\Pi}_{\leq 1}\right) \geq 1-(t^*)^2-\left(1-\frac{t^*}{4}\right)^2+\left(\frac{3t^*}{4}\right)^2 \tag{5.27}$$

$$= \frac{t^*}{2}-\frac{16\,(t^*)^2+(t^*)^2-9\,(t^*)^2}{16} \tag{5.28}$$

$$= \frac{1}{2}t^*\,(1-t^*) \tag{5.29}$$

$$\geq \frac{1}{2}t^*_{\min}\,(1-t^*_{\max}) =: \lambda_{\min}. \tag{5.30}$$

This is the bound that we shall use in our key length computations.

Finally, we are able to apply the WPFSS[8] with the bound (Eq. (5.30)) we have derived. The dimensional-dependent term from Eq. (5.23) can be then be computed;

$$x = \left(\sum_{m=0}^{N_{\mathrm{ph}}} {d_m^A}^2 + n_{\mathrm{int}}d_A\right)\left(\sum_{m=0}^{N}(m+1)^2+n_{\mathrm{meas}}\right) \tag{5.31}$$

$$= \left(1+2^2+(N_{\mathrm{ph}}-1)\cdot 3^2+3n_{\mathrm{int}}\right)\cdot(1+4+8)\,, \tag{5.32}$$

where n_{int} is the number of intensity settings chosen, and N_{ph} is the photon-number cut-off used while tagging the phase-randomised states.

5.5.5 Application of noise channels

We follow the steps described in Section 5.3 to use the results of Chapter 4. In particular, we apply the six equivalences in Fig. 5.1, then address the imperfect beam splitter via Theorem 4.1.

Equivalence (i): The equivalence follows from the fact that dark counts can be viewed as a post-processing, as described in Section 5.3.

Equivalence (ii): Although the coarse-graining used for the weight estimation is slightly different from that considered in Section 5.3, a similar analysis allows us to swap the coarse-graining and the dark count post-processing. The swapped dark count post-processing obtained satisfies Eqs. (4.12) to (4.14), which will be useful in establishing equivalence (v).

[8]Technically, we also need to worry about the dark counts. However, as discussed in Section 5.3, we treat dark counts as a classical post-processing which will be pulled into the channel (see Section 5.5.5).

Equivalence (iii): The WPFSS can be applied as described in Section 5.5.4. At this point, the postselection technique (Theorem 5.2) can be applied to restrict Eve's attacks to IID.

Equivalence (iv): The flag-state squasher [3, Theorem 1] can be applied. We describe the restriction of Eve's attacks in terms of a constraint on the weight W of the IID state shared by Alice and Bob outside the preserved subspace:

$$W \coloneqq \mathrm{Tr}\left[\overline{\Pi}_{\leq 1}\rho_{AQ}\right] \leq \frac{\mathrm{Tr}\left[F_e\rho_{AQ}\right]}{\lambda_{\min}}, \tag{5.33}$$

where $\lambda_{\min}$ is defined in Eq. (5.30).

Equivalence (v): This follows from the fact that the swapped dark count post-processing satisfies Eqs. (4.12) to (4.14), as stated in equivalence (ii). Thus, applying Theorem 4.3 we obtain the weight constraint,

$$1 - W^{\mathbf{d_B}} \coloneqq \mathrm{Tr}\left[\Pi_{\leq 1}\rho_{AQ}^{\mathbf{d_B}}\right] \geq (1 - d_{\max})^5\, W, \tag{5.34}$$

where $(1 - d_{\max})^5$ is the minimum probability that none of the 5 time bins encounter a dark count.

Equivalence (vi): In Section 5.5.4, we constructed an equivalent detection setup which has no loss. Thus, we do not need to use Theorem 4.4. However, the basis-choice beam splitter of this equivalent setup is imperfect, i.e, the effective beam-splitting ratio t^* can take any value in the range $t^* \in [t^*_{\min}, t^*_{\max}]$, as given in Eq. (5.26). Hence, we apply Theorem 4.2 to accommodate this imperfection as described below.

In the preserved subspace $\Pi_{\leq 1}$, all POVM elements other than the single-click and no-click outcomes are given by the 0 matrix. Thus, the POVM elements, projected onto the

preserved subspace $\Pi_{\leq 1}$ can be listed as

$$\begin{aligned}
\Pi_{\leq 1} F^{t^*}_{\text{no-click}} \Pi_{\leq 1} &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{t^*}{4} \left(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle\right) \left(\langle 0| \otimes \langle 1| + \langle 1| \otimes \langle 0|\right) \\
\Pi_{\leq 1} F^{t^*}_{1} \Pi_{\leq 1} &= (1-t^*) \, |0\rangle\langle 0| \otimes |1\rangle\langle 1| \\
\Pi_{\leq 1} F^{t^*}_{2} \Pi_{\leq 1} &= (1-t^*) \, |1\rangle\langle 1| \otimes |0\rangle\langle 0| \\
\Pi_{\leq 1} F^{t^*}_{3} \Pi_{\leq 1} &= \frac{t^*}{2} \, |0\rangle\langle 0| \otimes |1\rangle\langle 1| \\
\Pi_{\leq 1} F^{t^*}_{4} \Pi_{\leq 1} &= \frac{t^*}{4} \left(-|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle\right) \left(-\langle 0| \otimes \langle 1| + \langle 1| \otimes \langle 0|\right) \\
\Pi_{\leq 1} F^{t^*}_{5} \Pi_{\leq 1} &= \frac{t^*}{2} \, |1\rangle\langle 1| \otimes |0\rangle\langle 0| \\
\Pi_{\leq 1} F^{t^*}_{\text{others}} \Pi_{\leq 1} &= 0.
\end{aligned} \tag{5.35}$$

In particular, the POVM elements have the same structure as that of an active basis choice with probability $t^* : (1-t^*)$. Using

$$\begin{aligned}
\frac{t^*_{\min}}{t^*_{\max}} t^*_{\max} = t^*_{\min} &\leq t^* \\
\frac{t^*_{\min}}{t^*_{\max}} (1 - t^*_{\max}) \leq \frac{t^*_{\min}}{t^*_{\max}} (1-t^*) &\leq (1-t^*),
\end{aligned} \tag{5.36}$$

In the vacuum subspace, the only non-zero POVM element corresponds to the no-click outcome. As this does not depend on any detection setup parameters, we choose the ideal POVM to be identical to the real POVM in this subspace. Thus, the deviation from ideality q_0 in this subspace is 0.

In the single-photon subspace, it is straightforward to show that $\vec{F}_{1;\, t^*} \geq \frac{t^*_{\min}}{t^*_{\max}} \vec{F}_{1;\, t^*_{\max}}$. A similar computation results in $\vec{F}_{1;\, t^*} \geq \frac{1-t^*_{\max}}{1-t^*_{\min}} \vec{F}_{1;\, t^*_{\min}}$. Thus, we have the freedom to use Theorem 4.2 either with ideal POVM $\vec{F}_0 \oplus \vec{F}_{1;\, t^*_{\max}}$ or $\vec{F}_0 \oplus \vec{F}_{1;\, t^*_{\min}}$, with corresponding deviation metric $q_1 = \frac{\Delta t}{t^*_{\max}}$ or $q_1 = \frac{\Delta t}{1-t^*_{\min}}$, respectively. Here, $\Delta t \coloneqq t^*_{\max} - t^*_{\min}$. As we consider the case with $t_{\max} < 0.5$, the choice with the smallest deviation metric q is

$$\begin{aligned}
\text{Ideal POVM: } & \vec{F}_0 \oplus \vec{F}_{1;\, t^*_{\min}} \\
\text{Deviation metrics: } & q_0 = 0 \\
& q_1 = \frac{\Delta t}{1 - t^*_{\min}}.
\end{aligned} \tag{5.37}$$

In order to bound the final weight outside the preserved subspace after applying Theorem 4.2 we need to upper bound the weight in the single-photon subspace. We do this as follows. Observe from Eq. (5.35) that $F_Z^{t^*} \coloneqq F_1^{t^*} + F_2^{t^*}$ is such that $\Pi_1 F_Z^{t^*} \Pi_1 = (1-t^*)\Pi_1$. Thus,

$$\begin{aligned}
\mathrm{Tr}\left[\rho_{AQ}^{\mathbf{d_B}} \Pi_1\right] &= \frac{\mathrm{Tr}\left[\Pi_1 F_Z^{t^*} \Pi_1 \rho_{AQ}^{\mathbf{d_B}}\right]}{1-t^*} \\
&\leq \frac{\mathrm{Tr}\left[F_Z^{t^*} \rho_{AQ}^{\mathbf{d_B}}\right]}{1-t^*} \\
&\leq \frac{\mathrm{Tr}\left[F_Z^{t^*} \rho_{AQ}^{\mathbf{d_B}}\right]}{1-t^*_{\max}}
\end{aligned}$$

This results in the final weight constraint,

$$1 - W^{\mathrm{final}} = \mathrm{Tr}\left[\rho_{AQ}^{\mathbf{d_B}} \Pi_0\right] + (1-q_1)\mathrm{Tr}\left[\rho_{AQ}^{\mathbf{d_B}} \Pi_1\right] \tag{5.38}$$

$$= \mathrm{Tr}\left[\rho_{AQ}^{\mathbf{d_B}} \Pi_{\leq 1}\right] - q_1 \mathrm{Tr}\left[\rho_{AQ}^{\mathbf{d_B}} \Pi_1\right] \tag{5.39}$$

$$\geq 1 - W^{\mathbf{d_B}} - q_1 \frac{\mathrm{Tr}\left[F_Z^{t^*} \rho_{AQ}^{\mathbf{d_B}}\right]}{1-t^*_{\max}} \tag{5.40}$$

$$= (1-d_{\max})^5 \left(1 - \frac{\mathrm{Tr}\left[F_e \rho_{AQ}\right]}{\lambda_{\min}}\right) - \frac{\Delta t}{(1-t^*_{\min})(1-t^*_{\max})} \mathrm{Tr}\left[F_Z \rho_{AQ}\right]. \tag{5.41}$$

5.5.6 Results

As stated earlier, we chose the target secrecy parameter $\varepsilon_{\mathrm{sec}} = 2 \times 10^{-12}$. We also heuristically choose $\widetilde{\varepsilon} = \varepsilon_{\mathrm{sec}}/2g_{n,x}$. This gives the IID security parameter

$$\varepsilon_{\mathrm{IID}} = \left(\frac{\varepsilon_{\mathrm{sec}} - g_{n,x}\widetilde{\varepsilon}}{4g_{n,x}}\right)^2 = \left(\frac{\varepsilon_{\mathrm{sec}}}{8g_{n,x}}\right)^2. \tag{5.42}$$

We do not explain the details of the (variable-length) IID decoy-state security proof here, and instead refer the interested reader to Ref. [90]. The simulation parameters are listed in Table 5.2 for reference.

To illustrate the impact of our improvements to the de Finetti reduction, we first assume that there are no imperfections; that the detection setup parameters are all known

Parameter	**Value**	**Notes**
IID secrecy parameter ε_{IID}	$\varepsilon_{\text{IID}} = (\varepsilon_{\text{sec}}/8g_{n,x})^2$	Computed in Eq. (5.42).
Privacy amplification portion of secrecy parameter ε_{PA}	$\varepsilon_{\text{PA}} = \varepsilon_{\text{IID}}/2$	Quantifies probability of privacy amplification failing.
Parameter estimation portion of secrecy parameter ε_{AT}	$\varepsilon_{\text{AT}} = \varepsilon_{\text{IID}}/2$	Quantifies probability of parameter estimation failing.
Number of protocol rounds n	$n = 10^{12}$	———
Test sample size	$0.05\,n$	Fraction of signals used for testing.
Channel attenuation	0.16 dB/km	Assumed loss-only channel for simplicity.
Basis-choice beam-splitting ratio $\bar{t}$	$\bar{t} = 0.1$	Midpoint of range of possible values. The setup without imperfections uses this as the fixed beam-splitting ratio.
Detector efficiencies $\bar{\eta}$	$\bar{\eta} = 0.6$	Midpoint of range of possible values. The setup without imperfections uses this as the fixed efficiency for both detectors.
Maximum dark count rate d_{max}	$d_{\text{max}} = 10^{-8}$	The setup without imperfections assumes the dark count rate to be 0.
Probability of Z-basis preparation	$p_Z = 0.9$	———
Decoy intensity	0.01	Only one decoy intensity (total two intensities) used.
Signal intensity	———	Numerical optimisation to find value.
Probability of choosing signal intensity	1/2	———
Tagging photon-number cut-off N_{ph}	$N_{\text{ph}} = 2$	———

Table 5.2: Simulation parameters used for secret key rate plots. We do not optimise all the values.

exactly (as listed in the Table 5.2), and the dark count rate is 0. With this assumption, we compare the postselection key rates against distance in Fig. 5.5 with varying penalty terms as follows:

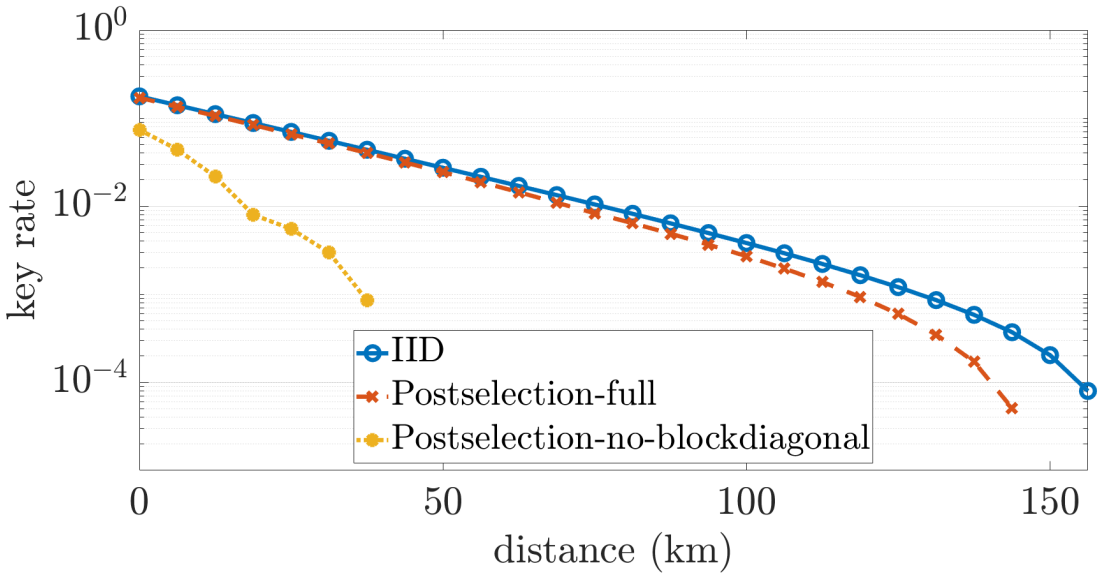


Figure 5.5: Plots demonstrating the performance of the postselection technique for the three-state protocol, and highlighting the importance of our improvements.

1. IID: We plot the key lengths as a function of distance under the assumption that Eve's attack is always IID, which corresponds to no postselection penalty. This serves as an upper bound for the key length plots.

2. Postselection with block-diagonal improvement: We plot the key lengths obtained from using block-diagonal structure to minimise the postselection penalty. The penalty factor x, described in Eq. (5.31), can be evaluated to be $x = 260$.

3. Postselection with no improvement: Directly applying [80, Corollary 3.2] gives no key rates for any distance. This highlights the importance of our improvements.

4. Postselection with generic improvement: We plot the key lengths obtained without using block-diagonal structure, resulting in $x = 5184$.

Next, we illustrate the effect of imperfections on the key rates. We consider the beam-splitting ratio and efficiencies to be in varying intervals about the fixed midpoints, $\bar{t} = 0.2$

and $\bar{\eta} = 0.6$, respectively. We simultaneously vary the ranges of the beam-splitting ratio and detector efficiencies, i.e., we consider the beam-splitting ratio and detector efficiencies to be in ranges[9]

$$\begin{aligned} t &\in [\bar{t}(1-\Delta), \bar{t}(1+\Delta)] \\ \eta_i &\in [\bar{\eta}(1-\Delta), \bar{\eta}(1+\Delta)], \end{aligned} \tag{5.43}$$

for the same parameter deviation Δ. In Fig. 5.6, we plot the key rates for parameter deviations up to $\Delta = 30\%$. We set the maximum dark count rate to be 10^{-8}.

These results demonstrate that our noise channel framework can tolerate significant detector imperfections while maintaining near-optimal key rates. Part of this high performance is due to the noise channel construction of Theorem 4.2, where the penalty for imperfections is incurred only on the detected rounds. Thus, our treatment of detector imperfections scales favourably with loss. However, we do not fully understand why the security proof is so highly resistant to imperfections. This could be a feature of this specific protocol. A deeper understanding of the techniques and more examples are needed before we can make any conclusive statements.

5.6 Concluding remarks

In this chapter, we presented the rigorous application of the postselection technique to practical QKD protocols. In particular, we extended the applicability of the postselection technique to prepare-and-measure protocols and decoy-state protocols. We have also made several improvements to existing de Finetti reductions that significantly reduce the penalty imposed on the key rate when using the postselection technique. Additionally, we detailed the application of noise channels (introduced in Chapter 4) to the postselection technique.

We demonstrated the impact of our results from Chapters 4 and 5 by applying them to a time-bin encoded three-state protocol. This example serves as a pedagogical exercise in applying noise channels, which can directly be applied to EAT-based proofs. We observe that our treatment of detector imperfections achieves near ideal key rates, even with a large amount of imperfections. However, we do not fully understand the origin of this high performance. Thus, more work is needed to better understand the techniques used and to work out more examples.

[9]The beam-splitting ratio and detector efficiencies additionally must lie in the range $[0, 1]$. However, for the values of $\bar{t}$, $\bar{\eta}$, and Δ chosen here, these ranges automatically lie in the range $[0, 1]$ imposed by physical constraints.

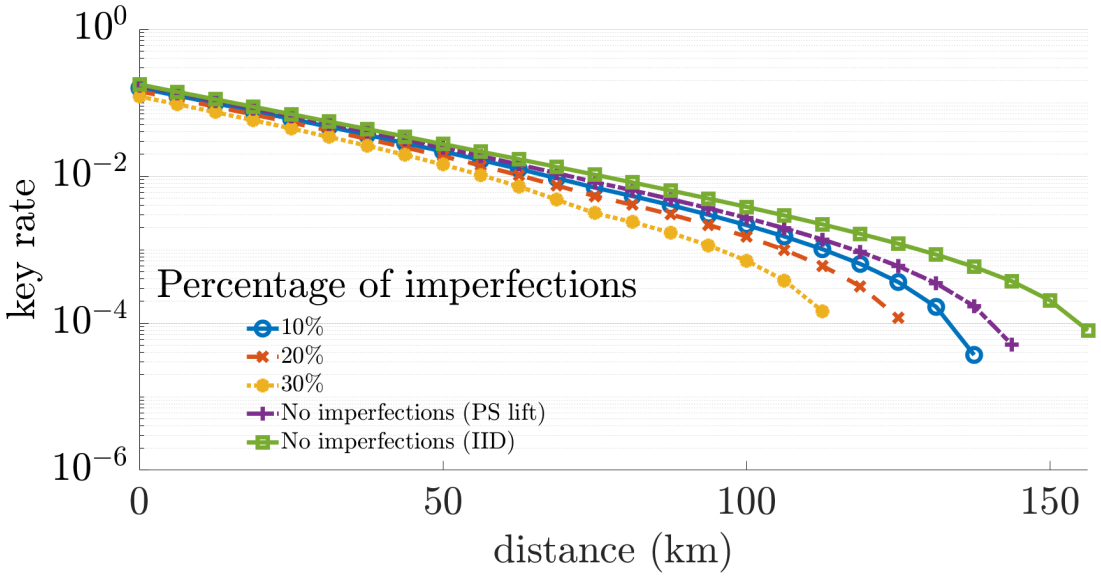


Figure 5.6: Plots demonstrating the effect of imperfections on the key rate. Our security analysis is minimally affected by detector imperfections. We observe non-zero key rates for imperfection values upto 51%, though we only plot the key rates upto imperfection values upto 30%.

As demonstrated by the example of the three-state protocol, our analysis was able to prove security for a highly asymmetric detection setup[10]. This is currently impossible in phase-error rate estimation-based proof techniques. Additionally, the compatibility of treatments of source and detector imperfections clearly follows from the modular nature of our analysis.

We do not claim that the analysis we perform here is as tight as possible; there is much room for improvement. For example, the IID analysis can be tightened via the use of Rényi entropies [91]. Moreover, the decoy-state analysis can be tightened by directly incorporating it into the final key rate optimisation, instead of treating it as a pre-step to the numerical key rate computation as in Ref. [92]. We believe that further improvements to the de Finetti reductions are also possible. For example, [85] improved de Finetti reductions without fixed marginal constraints. A corresponding improvement that incorporates the fixed marginal constraint should exist, but remains to be proved.[11]

[10]The setup we consider (Fig. 5.2) was missing a detector in the X-basis.

[11]Alternately, the tighter de Finetti reduction from [85] can be used along with a protocol change to randomly discard a fraction of the rounds. These discarded rounds can be used to perform 'virtual

The postselection technique has a number of fundamental limitations. For one, the treatment of imperfections is limited to imperfections that are IID across protocol rounds. This is because the noise channels must be applied *after* the postselection technique has reduced secrecy to that against IID attacks. Thus, the postselection technique is also limited in its treatment of multi-mode optical models (see Section 4.3). Additionally, the resultant key rates are outperformed by very recent advances in EAT-based proof techniques [14]. For symmetric protocols, such as BB84, phase-error rate estimation-based proof techniques also outperform the postselection technique.

Another, more technical, limitation of our treatment of detector imperfections thus far is that it is tied to the flag-state squasher. Thus, as stated in Technical aside 3.3, its application to active basis-choice protocols has a missing step in bounding the minimum eigenvalue $\lambda_{\min}$ that we do not yet have.[12] Curiously, the treatment of active basis-choice protocols turns out to be easier in phase-error rate estimation-based proof techniques. This forms the basis of our next chapter.

tomography' on the marginal as described in [93, 94], which results in an IID analysis that does not directly require the fixed marginal constraint.

[12]This is also a limitation of EAT-based proof techniques that follow largely similar steps to treat detector imperfections. However, see Technical aside 6.3 for a way to address this limitation for EAT-based proofs.

Chapter 6

Phase error rate estimation with imperfect detectors

> "Someone is looking at me! ... I am suddenly affected in my being."
>
> — Jean-Paul Sartre, *Being and Nothingness*

The preceding chapter provided a detailed application of the postselection framework to passive detection models. However, as noted in the concluding remarks of Chapter 5, a technical step remains when extending this method to protocols with active basis-choice. The application of the flag-state squasher, a key component of our analysis, relies on establishing a lower bound on the minimum eigenvalue $\lambda_{\min}$ associated with the weight-estimation event (see Technical aside 3.3). While this bound is generically computable [72] for passive setups, its derivation for active setups is still an open problem.

Consequently, to analyse protocols with active basis-choice, we turn to a different class of security proofs — phase error correction-based proofs [7] and those using entropic uncertainty relations [9]. These frameworks do not rely on the flag-state squasher and therefore sidestep the issue of subspace estimation faced by other approaches. In this approach, the security analysis instead hinges on a central task: computing a rigorous upper bound on the phase error rate. This task typically reduces to a sampling problem. First, we briefly provide some intuition of what phase errors are, and why they are important in the context

of QKD.

6.1 Phase errors and secrecy

Let us first consider a toy example for intuition. Let Alice and Bob share an n_{K}-round state $\rho_{A^{n_{\mathrm{K}}}B^{n_{\mathrm{K}}}}$, and Eve holds a purification $|\psi\rangle_{A^nB^nE^n}$. We assume that Alice has a qubit system, which she will measure in the Z-basis to get the key. Then it is useful to expand the pure state as

$$\begin{aligned} |\psi\rangle_{A^{n_{\mathrm{K}}}B^{n_{\mathrm{K}}}E^{n_{\mathrm{K}}}} &= \sum_{\vec{z}\in\{0,1\}^{n_{\mathrm{K}}}} \sqrt{p(\vec{z})}\,|\vec{z}\rangle_{A^{n_{\mathrm{K}}}} \otimes |\psi_{\vec{z}}\rangle_{B^{n_{\mathrm{K}}}E^{n_{\mathrm{K}}}} \\ &= \sum_{\vec{x}\in\{0,1\}^{n_{\mathrm{K}}}} \sqrt{\overline{p}(\vec{x})}\ \overline{|\vec{x}\rangle}_{A^{n_{\mathrm{K}}}} \otimes \overline{|\psi_{\vec{x}}\rangle}_{B^{n_{\mathrm{K}}}E^{n_{\mathrm{K}}}}, \end{aligned} \tag{6.1}$$

where $|\vec{z}\rangle_{A^{n_{\mathrm{K}}}}$ and $\overline{|\vec{x}\rangle}_{A^{n_{\mathrm{K}}}}$ are computational (Z-basis) and conjugate (X-basis) states on Alice's n-qubit system, respectively. The states $|\psi_{\vec{z}}\rangle_{B^{n_{\mathrm{K}}}E^{n_{\mathrm{K}}}}$ and $\overline{|\psi_{\vec{x}}\rangle}_{B^{n_{\mathrm{K}}}E^{n_{\mathrm{K}}}}$ are the corresponding states on Bob and Eve's joint systems, conditioned on Alice's outcome.

The second line of the equation provides the perspective needed to define a phase error. A *phase error* is a mismatch between Alice's and Bob's outcomes in a hypothetical measurement of their respective systems in the X-basis. The significance of this quantity is best understood by examining the ideal case where the phase error rate is zero.

In this ideal case, this implies that Bob, by measuring his system, can perfectly determine Alice's X-basis string $\vec{x}$. This is possible if and only if the states on his subsystem, $\left\{\mathrm{Tr}_{E^{n_{\mathrm{K}}}}\left[\overline{|\psi_{\vec{x}}\rangle\langle\psi_{\vec{x}}|}\right]\right\}_{\vec{x}}$, have pairwise orthogonal supports. Assuming this perfect correlation, the joint state on Alice's and Eve's systems is given by the classical-quantum state:

$$\rho_{A^{n_{\mathrm{K}}}E^{n_{\mathrm{K}}}} = \sum_{\vec{x}\in\{0,1\}^{n_{\mathrm{K}}}} \overline{p}(\vec{x})\overline{|\vec{x}\rangle\langle\vec{x}|}_{A^{n_{\mathrm{K}}}} \otimes \rho^{\vec{x}}_{E^{n_{\mathrm{K}}}}, \tag{6.2}$$

where $\rho^{\vec{x}}_{E^{n_{\mathrm{K}}}} = \mathrm{Tr}_{B^{n_{\mathrm{K}}}}\left[\overline{|\psi_{\vec{x}}\rangle\langle\psi_{\vec{x}}|}\right]$.

The final step in the protocol is Alice's measurement of her system in the Z-basis to generate her key. Any X-basis state, when measured in the Z-basis, yields a perfectly uniform random outcome. Crucially, the resulting probability distribution over the key

strings is identical for every term in the sum, independent of $\vec{x}$. Consequently, the final state of the key and Eve's system decouples into a product state:

$$\rho_{K_A E^{n_K}} = \left(\sum_{k \in \{0,1\}^{n_K}} \frac{1}{2^{n_K}} |k\rangle\langle k|_{K_A} \right) \otimes \rho_{E^{n_K}}, \tag{6.3}$$

where $\rho_{E^{n_K}} = \sum_{\vec{x} \in \{0,1\}^{n_K}} \overline{p}(\vec{x}) \rho^{\vec{x}}_{E^{n_K}}$. The key K_A is uniform and uncorrelated with Eve's system, and is therefore perfectly secret.

This toy example demonstrates the crucial connection: a vanishing phase error rate implies perfect security. In a real protocol, the number of phase errors will be non-zero. A full security proof must therefore quantify the impact of phase errors on the final secret key length.

There are two primary frameworks to achieve this. One method [7] recasts the privacy amplification step of the QKD protocol as a virtual quantum phase error correction protocol, whose failure probability determines the final secret key length. The other method uses the leftover hashing lemma [8, Proposition 9], together with an entropic uncertainty relation [9], to directly bound Eve's information [8] from the phase error rate. The key length for both approaches has a similar form[1]:

$$l \geq n_K \left(1 - h(\overline{e_{\text{ph}}})\right) - \lambda_{\text{EC}} - \text{finite size corrections}, \tag{6.4}$$

where $\overline{e_{\text{ph}}}$ is an upper bound on the phase error rate, n_K represents the number of rounds mapped to key generation, $h(\cdot)$ is the binary entropy function, and λ_{EC} is the key length cost due to error correction and verification. Importantly, the phase error rate $\overline{e_{\text{ph}}}$ corresponds to an upper bound on the phase error rate in the rounds mapped to key generation.

Technical aside 6.1 (What is the phase error rate?)**.** The definition of the phase error rate, e_{ph}, is a choice that must be made as part of the security proof. The key rate in Eq. (6.4) is derived assuming e_{ph} is the phase error rate of the state on the (sifted) key generation rounds. However, it is sometimes analytically convenient to define and bound the phase error rate on a different state (e.g., the state prior to sifting). This choice can simplify the estimation procedure, at the cost of an additional analytical step to relate this bound back to the security of the actual key. For clarity, in this

[1] While both proof techniques often yield similar results [95], there are some subtle differences [2, 96]. However, we focus on the phase error rate estimation here, which is a common component to both proof techniques.

chapter we fix the definition of the phase error rate to be defined on the key generation rounds and focus our attention on the challenge of its estimation.

As this key length formula (Eq. (6.4)) shows, the phase error rate limits the amount of secret key that can be distilled from the raw key. Consequently, the central task within these security frameworks is to rigorously upper bound the phase error rate, estimated from the observable statistics gathered during the protocol. Instead of detailing the specific mechanics of these proof techniques, we will concentrate on this common component that underpins them: the estimation of the phase error rate.

Notational aside 6.1 (Phase error rate stimation = phase error rate upper bound)**.** As stated above, the primary task is to *upper bound* the phase error rate. This is sometimes also referred to as phase error estimation in the literature, even though a lower bound is never obtained or used. We also interchangeably use the term phase error rate estimation to mean the derivation of an upper bound on the phase error rate.

6.2 Phase error estimation with no basis-efficiency mismatch

We first describe the crucial (to our analysis) steps of the active basis-choice BB84 protocol, before detailing the phase error estimation. Here, we focus on phase error estimation with imperfect detectors, and assume a perfect qubit source. The extension to decoy-state protocols works as a modular extension [75, 97, 5] to the phase error estimation with a qubit source. For concreteness, we also consider polarisation encoding. Alice's state preparation and Bob's measurement steps are as follows:

1. **Signal Preparation:** Alice randomly prepares $|0\rangle$ and $|1\rangle$ with probability $p_Z^A/2$ each, and $|+\rangle$ and $|-\rangle$ with probability $p_X^A/2$ each. We refer to $\{|0\rangle, |1\rangle\}$ as the Z-basis and $\{|+\rangle, |-\rangle\}$ as the X-basis.

2. **Optical measurement:** Bob randomly picks basis $b \in \{X, Z\}$ with probability p_b^B. The b-basis POVM is given by $\left\{\Gamma_{(\mathrm{b},\ \mathrm{nc})}, \Gamma_{(\mathrm{b},\ 0)}, \Gamma_{(\mathrm{b},\ 1)}, \Gamma_{(\mathrm{b},\ \mathrm{dc})}\right\}$ corresponding to the no-click, 0, 1 and double-click outcomes, respectively. The optical setup makes use of a polarisation rotator to make the basis choice followed by a polarisation beam splitter, and two threshold detectors.

3. **Post-processed measurement:** Bob randomly maps all double-click outcomes to the 0 and 1 outcome within the same basis. Thus, we analyse the effective three-outcome POVM.

All detected X-basis rounds (for both Alice and Bob) are used for testing, and all detected Z-basis rounds are used for key generation. Thus, we interchangeably refer to a Z-basis round as a key generation round, and an X-basis round as a test round.

The state preparation is equivalent to Alice preparing a Bell state $\frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_{A'} + |1\rangle_A \otimes |1\rangle_{A'}\right)$, picking the Z/X-basis with probability p_Z^A/p_X^A, and measuring with Z-basis POVM $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or X-basis POVM $\{|+\rangle\langle +|, |-\rangle\langle -|\}$, respectively. This can be verified either by explicit computation, or by considering the canonical source-replacement scheme described in Eq. (3.5) and then taking its Schmidt decomposition as described in [57, Eq. (2)]. Thus, the protocol is described by Alice and Bob first picking their measurement basis and then measuring with the POVM corresponding to their basis choice.

Given that Bob makes basis choice b, his measurement is equivalently described [75] by a filter F_b, which determines whether the outcome is detected or not, followed by a two-outcome measurement. The defining condition for *no basis-efficiency mismatch* is where

$$\Gamma_{(\mathrm{Z,\ nc})} = \Gamma_{(\mathrm{X,\ nc})}. \tag{6.5}$$

Physically, this corresponds to all detectors having the same loss and dark count rates.

Notational aside 6.2 (Basis-efficiency mismatch)**.** The nomenclature *basis-efficiency mismatch* is a slight misnomer as it makes no reference to the dark count rates. As this term is now established in the literature, we refer to the condition described in Eq. (6.5) as basis-efficiency mismatch.

Eq. (6.5) directly implies that the filter is independent of basis $F_X = F_Z$. Thus, the measurement is equivalently described as *first* applying the basis-independent filter and then making the basis choice and performing the two-outcome measurement. In particular, this equivalent description allows us to focus on the detected rounds. Conditioned on detection and on Alice and Bob's bases matching, the choice between X and Z basis is made randomly (with probabilities $p_X^A p_X^B/(p_X^A p_X^B + p_Z^A p_Z^B)$ and $p_Z^A p_Z^B/(p_X^A p_X^B + p_Z^A p_Z^B)$, respectively). Crucially, this allows the *detected* X-basis rounds (used for testing) to estimate the phase

errors in the *detected* Z-basis rounds (used for key generation). Such an estimate can be obtained via concentration inequalities such as Serfling's inequality [39], as described in Section 2.3.3.

6.3 Phase error estimation with basis-efficiency mismatch

The argument made at the end of the previous section crucially depended on the condition (Eq. (6.5)) for no basis-efficiency mismatch being *exactly* satisfied. This ideal scenario allowed us to treat the detected rounds in the test rounds as a fair random sample for the detected rounds in the key generation rounds, justifying the direct use of Serfling's inequality on the detected rounds. When this condition is violated, the set of detected rounds is no longer a fair sample, and the phase error estimation needs to be modified.

One approach is to directly adapt the statistical analysis to account for this biased sampling, as shown in [5]. The core idea of this method is to construct a new sampling problem that explicitly accounts for the basis-dependent detection efficiency.

6.3.1 Equivalent protocol

This method proceeds by constructing an equivalent protocol and breaking the sampling into smaller steps, as depicted in Fig. 6.1:

1. **Common loss:** Before any of the protocol steps, it is assumed that the common loss is absorbed into the channel so that the two detectors have efficiencies 1 and $\eta \in [\eta_{\min}, 1]$.

2. **Basis-independent filter:** Similar to the ideal case, with no basis-efficiency mismatch, the measurement can be equivalently described as first implementing a basis-independent filter $\tilde{F}$ which implements some of the discards.[2] An important distinction from the ideal case is that not all rounds remaining after this filter will be detected.

3. **Basis choice:** Next, Alice and Bob make their basis choices and discard the rounds where there is a basis mismatch.

[2] As shown in Eq. (D.5), this filter only acts non-trivially on the 0-photon subspace, so that the remaining 0-photon rounds will be detected.

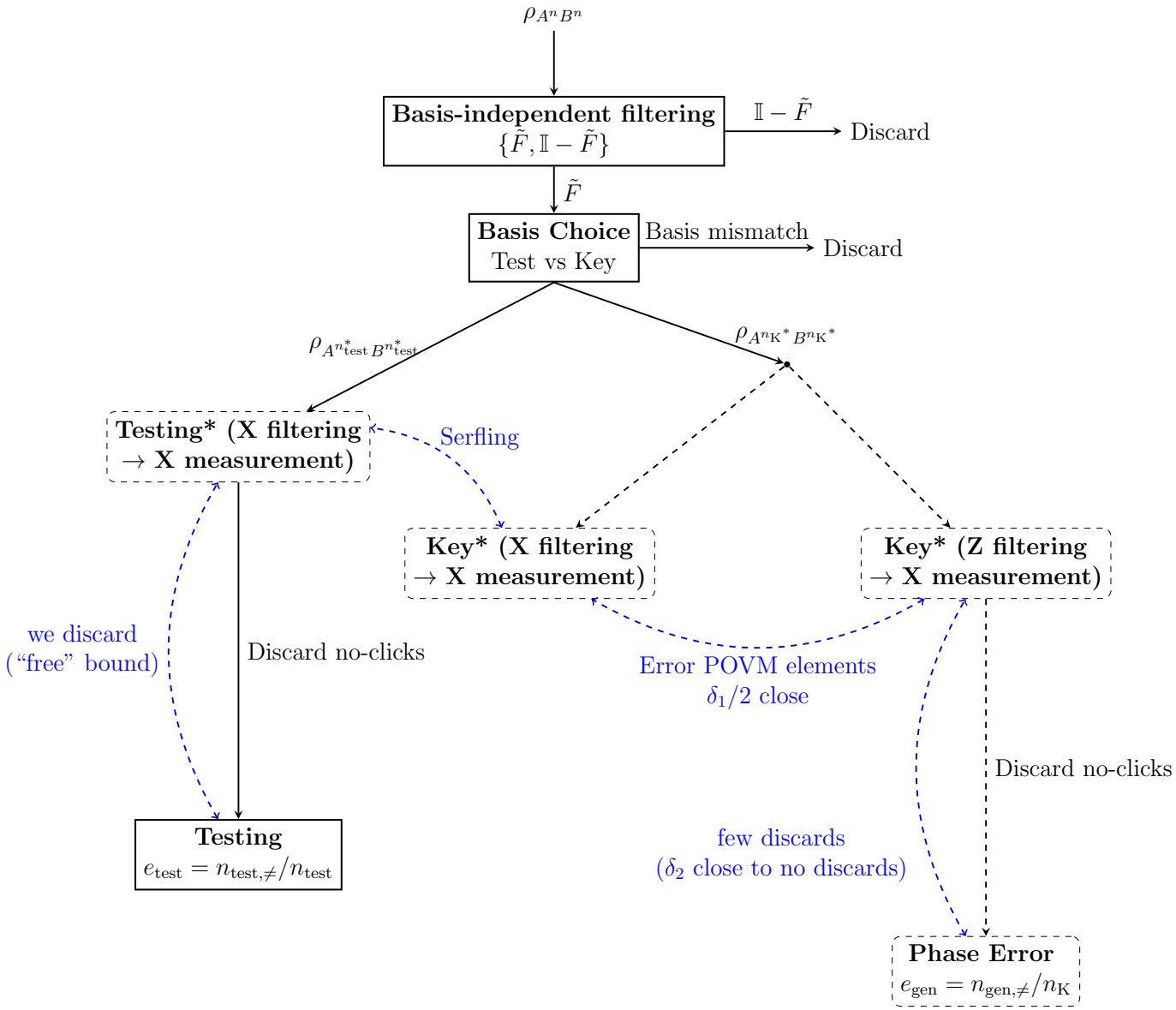


Figure 6.1: Flowchart depicting the phase error estimation strategy. The testing and key generation rounds go through an additional second step filtering measurement that depends on the basis used, which typically results in a few rounds being discarded, before undergoing the final measurement. The basis used in these measurements in indicated in each box, and indicates the basis used by both Alice and Bob. The dotted arrows and boxes represent virtual measurements that do not actually happen in the real protocol. Connections between the error rates in different boxes are highlighted using curved arrows.

4. **Testing*:** For rounds where Alice and Bob both choose the X basis, the measurement is completed via a 3-outcome POVM corresponding to no-clicks, errors and no errors. The no-click outcomes in this step corresponds to the X basis-dependent loss. This is an important intermediate step for the sampling process.

5. **Testing:** This consists of the observed test data. It corresponds to discarding the no-click outcomes from Testing*. The fraction of errors in the test rounds defines the observed error rate $e_{\text{test}} = \frac{n_{\text{test},\neq}}{n_{\text{test}}}$.

6. **Key* ($Z \to X$):** For the key generation rounds (Z basis), we define a virtual measurement in the conjugate X basis to define the phase errors. This step also includes no click outcomes corresponding to the basis-dependent loss in the Z basis. This is an important intermediate step for the sampling process.

7. **Phase error:** The no-click outcomes from Key* ($Z \to X$) are discarded. The phase error rate is defined on the detected key generation rounds n_{K}, as described in Section 6.1. Thus, the fraction of errors in this step corresponds exactly to the phase error rate $e_{\text{gen}} = \frac{n_{\text{gen},\neq}}{n_{\text{K}}}$, which we must estimate.

8. **Key* ($X \to X$):** To connect the observable test data to the unobservable phase errors, a final virtual step is constructed. It is identical to Key* ($Z \to X$) except the basis-dependent filtering is performed as if it were an X basis round. This step acts as a crucial bridge, creating a common reference point that can be related to both Testing* (via Serfling's inequality) and the actual phase error rounds (via a closeness argument), as we see below.

6.3.2 Sampling strategy

To understand the sampling process, we consider the asymptotic scenario, which provides the requisite intuition. We begin with the observed error rate e_{test} in the test rounds, and relate it to the phase error rate e_{gen}.

1. **"Free discards":** The number of errors $n_{\text{test},\neq}$ in Testing is the same as the number of errors in Testing*. Because the observed test rounds n_{test} are only those that were not discarded as 'no clicks', n_{test} is smaller than the total number of Testing* rounds n^*_{test}. Thus the observed test error rate e_{test} is an upper bound on the error rate e^*_{test} in Testing*,

$$e_{\text{test}} = \frac{n_{\text{test},\neq}}{n_{\text{test}}} \geq \frac{n_{\text{test},\neq}}{n^*_{\text{test}}} = e^*_{\text{test}}.$$

2. **Serfling:** As the POVM used in Testing* is identical to the POVM used in Key* ($X \to X$), these two steps represent fair samples of each other. Thus, Serfling's inequality can directly be used to relate the error rates in these steps,[3]

$$e^*_{\text{test}} = e^{X,*}_{\text{gen}}.$$

3. **Error POVM elements close:** The error POVM element for Key* ($X \to X$) and Key* ($Z \to X$) are slightly different due to the different basis-dependent filtering. The ∞-norm $\delta_1/2$ of the difference of these POVM elements bounds how different the error rate $e^{X,*}_{\text{gen}}$ in Key* ($X \to X$) is from the error rate e^*_{gen} in Key* ($Z \to X$). As shown in [5, Lemma 3]:[4]

$$e^{X,*}_{\text{gen}} + \delta_1 \geq e^*_{\text{gen}}.$$

4. δ_2 **close to no discards:** The final phase error rate e_{gen} is defined on a smaller number of rounds n_{K} than the error rate e^*_{gen} (due to discarding no-click outcomes from Key* ($Z \to X$)). Since the number of phase errors $n_{\text{gen},\neq}$ is the same in both steps, an upper bound on the phase error rate e_{gen} follows from a lower bound on the number of rounds ${n_{\text{K}}}^*$ in the Key* ($X \to X$) step. This can be obtained based on the ∞-norm δ_2 of the no-click POVM element [5, Lemma 4]:[5]

$${n_{\text{K}}}^* \leq \frac{n_{\text{K}}}{1-\delta_2}.$$

Combining the error rate bounds,

$$\begin{aligned} e_{\text{gen}} &\leq \frac{e^*_{\text{gen}}}{1-\delta_2} \\ &\leq \frac{e^{X,*}_{\text{gen}} + \delta_1}{1-\delta_2} \\ &= \frac{e^*_{\text{test}} + \delta_1}{1-\delta_2} \\ &\leq \frac{e_{\text{test}} + \delta_1}{1-\delta_2}. \end{aligned} \tag{6.6}$$

[3] The full finite-size analysis would include the relevant finite-size penalty incurred when using Serfling's inequality (see Section 2.3.3).

[4] The full proof in [5] also includes the finite-size correction term for this inequality.

[5] Once again, the full proof in [5] also includes the finite-size correction term for this inequality.

In Appendix D.1, we explicitly derive bounds on the two deviation metrics δ_1 and δ_2, for the detector model with loss and dark counts described in Sections 2.2.5 and 2.2.6:

$$\begin{aligned} \delta_1 &= 4(1 - \sqrt{\eta_{\min}}) \\ \delta_2 &= 1 - \eta_{\min}. \end{aligned} \tag{6.7}$$

> **Technical aside 6.2** (Dark count rates unimportant)**.** Interestingly, the deviation metrics in Eq. (6.7) do not depend on the dark count rates. This is in contrast to the deviation metrics computed in Ref. [5], where the minimum dark count rate needed to be non-zero to obtain non-unital deviations. This improvement stems from a physically motivated assumption not made in Ref. [5]: the detector dark count rates do not depend on the basis chosen. This allows us to choose a basis-independent filter that accounts for the dark count rates in the 0-photon subspace which is where the effect of dark counts was most prominent in Ref. [5].

The computation of δ_1 presents a particular analytical challenge. It requires bounding the ∞-norm of the difference between two POVM elements that are diagonal in different bases — one corresponding to the Z basis filtering and the other to the X basis filtering. Because these operators do not commute, a tight analytical[6] bound on the norm of their difference is difficult to obtain. Consequently, simplifications such as the triangle inequality are used to derive a tractable, albeit looser, bound, as detailed in Appendix D.1.

Another potential looseness is that the two costs δ_1 and δ_2 are incurred independently. A more direct sampling statement from Key* ($X \to X$) to Phase Error might yield a tighter bound.

To provide an alternative approach that addresses some of this looseness, we now describe the use of noise channels.

6.4 Phase error estimation with noise channels

We now detail the application of noise channels for phase error estimation. We first construct an equivalent protocol, depicted in Fig. 6.2, which allows us to mathematically isolate the basis-efficiency mismatch.

[6] These are infinite-dimensional operators which makes numeric computation difficult.

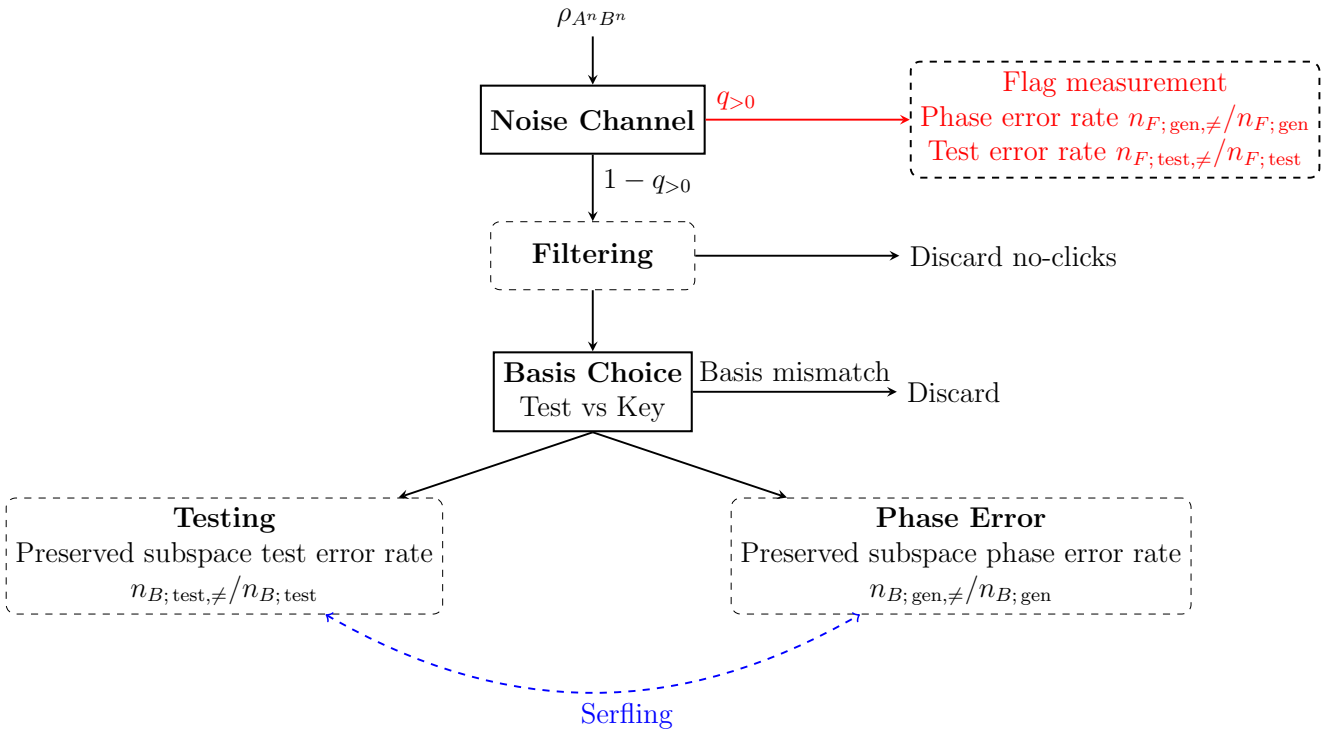


Figure 6.2: Flowchart depicting the equivalent protocol using the noise channel. Each round is first processed by a noise channel, which flags it with probability $q_{>0}$. The remaining non-flag rounds (in the 'preserved subspace') are then acted on by a basis-independent filter so that their error rates in the test and key generation rounds can be related via Serfling's inequality. The error rates in the flag space cannot be related to each other, and must be accounted for (as in Lemma 6.1).

The core of the strategy is to then apply the block-diagonal noise channel from Theorem 4.2. The action of this channel can be understood as a two-step process on each round (see Section 6.4.1 for more details):

1. It performs a QND measurement to determine whether the round has photons or not.

2. When the round has non-zero photons, the noise channel maps the round to an orthogonal flag space with probability $q_{>0}$. This probability depends on the dark count rates and detector efficiency mismatch.

The noise channel acts trivially on the remaining rounds.

Remark 6.1 (Noise channel action on 0-photon subspace)**.** *Here, the noise channel construction acts trivially on the* 0*-photon subspace. This is because we assume that the dark counts are independent of the chosen basis, and so this subspace cannot induce any basis-efficiency mismatch.*

The crucial property of this transformation is that the POVM acting on the non-flag 'preserved subspace' exhibits no basis-efficiency mismatch. This restores the fair sampling condition that was broken by the imperfect detectors. Consequently, the analysis of these preserved rounds can proceed as in the ideal case described in Section 6.2: Serfling's inequality can be applied to rigorously relate the phase errors in the preserved key generation rounds to the observed errors in the preserved test rounds.

Technical aside 6.3 (EAT-based proofs for active basis-choice BB84)**.** This noise channel construction also allows us to compute key rates for active basis-choice BB84 protocols using EAT-based proof techniques. For such proofs, the main limiting step[7] is often an infinite-dimensional numerical optimisation.

For a detection setup with no loss or dark counts, this problem is solved by applying the simple squasher [68, Theorem 10] together with Corollary 3.2 to reduce the POVM to a simple qubit system, making the optimisation numerically tractable.

Our noise channel makes the simple squasher applicable even with imperfect detectors. After applying the noise channel, the resulting POVM $\vec{\Gamma}_{\text{ideal}} = \vec{\Gamma}_{0;\,\mathbf{d_B}} \oplus \vec{\Gamma}_{>0}$ in the preserved subspace *almost* has no loss or dark counts. Crucially, the proof of [68, Theorem 10] constructs a squashing map that acts as identity on the 0-photon (and 1-photon) subspace. The squashing operation only affects the higher photon-number

subspaces. As these subspaces have no dark counts or loss, the construction in [68, Theorem 10] remains a valid squashing map. We can therefore still use the simple squasher to reduce the POVM to a qubit system (with flags), rendering the numerical optimisation tractable.

In contrast to the preserved rounds, no sampling statement is applied to the rounds mapped to the flag space. Instead, these are treated pessimistically to establish a worst-case bound: all flag rounds are assumed to be detected, and every flag key generation round is assumed to be an error, while every flag test round is assumed to be error-free. This approach, formalised in the proof of Lemma 6.1, allows us to derive an upper bound on the total phase error rate e_{gen}.

The resulting bound on the phase error rate after the use of Lemma 6.1 will be a function of two types of random variables:

- Directly observable data, such as the observed error rate e_{test}.
- The number of rounds mapped to the flag space in the test and key generation rounds ($n^*_{F;\,\text{test}}$ and $n^*_{F;\,\text{gen}}$, respectively) which are not directly observed.

Thus, in Section 6.4.1, we will complete the analysis by deriving a rigorous upper bound on these flag rounds in terms of observable data. As the following discussion gets somewhat notation-heavy, we list all the random variables to be used in Table 6.1.

Technical aside 6.4 (Well-defined random variables)**.** Note that all of these random variables can exist at the same time as the measurements that give rise to them all commute; either due to the block-diagonal structure of the POVM elements (for e.g. - n_{test} and $n_{F;\,\text{test}}$), or because the POVM elements act on different rounds (for e.g. - n_{K} and n_{test}).

Lemma 6.1 (Intermediate phase-error rate bound)**.** *Let the number of flags be less than the total number of detected rounds: $n^*_{F;\,\text{test}} \leq n_{\text{test}}$ and $n^*_{F;\,\text{gen}} \leq n_{\text{K}}$. Let the finite-size correction term due to Serfling's inequality as defined in Eq. (2.15) be*

$$\overline{\gamma_{\text{serf}}} \coloneqq \overline{\gamma_{\text{serf}}}(\varepsilon_{\text{serf}}, n_{\text{test}} - n^*_{F;\,\text{test}}, n_{\text{det}} - n^*_{F;\,\text{test}} - n^*_{F;\,\text{gen}}) \leq 1 - \frac{e_{\text{test}}}{1 - f_{\text{test}}}.$$

[7] Technically, the use of EAT statements requires all spaces to be finite-dimensional. However, unlike the postselection technique, they pay no dimension-dependent cost. So, the results of Section 3.4.4 can be used to formally apply the EAT statement.

Symbol	**Description**
n_{K}	Number of key generation rounds
n_{test}	Number of test rounds
$n_{\mathrm{gen},\neq}$	Number of key generation rounds with errors
$n_{\mathrm{test},\neq}$	Number of test rounds with errors
$n_{\mathrm{det}} \coloneqq n_{\mathrm{K}} + n_{\mathrm{test}}$	Number of detected rounds
n_F	Total number of flag rounds
$n^*_{F;\,\mathrm{gen}}$	Number of key generation flag rounds (including no-clicks)
$n^*_{F;\,\mathrm{test}}$	Number of testing flag rounds (including no-clicks)
$n_{F;\,\mathrm{gen}}$	Number of key generation (detected) flag rounds
$n_{F;\,\mathrm{test}}$	Number of testing (detected) flag rounds
$n_{B;\,\mathrm{gen}} \coloneqq n_{\mathrm{K}} - n_{F;\,\mathrm{gen}}$	Number of non-flag generation rounds
$n_{B;\,\mathrm{test}} \coloneqq n_{\mathrm{test}} - n_{F;\,\mathrm{test}}$	Number of non-flag test rounds
$n_{B;\,\mathrm{det}} \coloneqq n_{B;\,\mathrm{gen}} + n_{B;\,\mathrm{test}}$	Number of detected non-flag rounds
$n_{F;\,\mathrm{gen},\neq}$	Number of flag generation rounds with errors
$n_{F;\,\mathrm{test},\neq}$	Number of flag test rounds with errors
$n_{B;\,\mathrm{gen},\neq} \coloneqq n_{\mathrm{gen},\neq} - n_{F;\,\mathrm{gen},\neq}$	Number of non-flag generation rounds with errors
$n_{B;\,\mathrm{test},\neq} \coloneqq n_{\mathrm{test},\neq} - n_{F;\,\mathrm{test},\neq}$	Number of non-flag test rounds with errors
$e_{\mathrm{gen}} \coloneqq \frac{n_{\mathrm{gen},\neq}}{n_{\mathrm{K}}}$	Fraction of key generation rounds with errors
$e_{\mathrm{test}} \coloneqq \frac{n_{\mathrm{test},\neq}}{n_{\mathrm{test}}}$	Fraction of test rounds with errors
$f_{\mathrm{test}} \coloneqq \frac{n^*_{F;\,\mathrm{test}}}{n_{\mathrm{test}}}$	Fraction of flags in the test rounds
$f_{\mathrm{gen}} \coloneqq \frac{n^*_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}}$	Fraction of flags in the key generation rounds
$n^*_{>0;\,\mathrm{test}}$	Number of test rounds with > 0 photons
$n^*_{>0;\,\mathrm{gen}}$	Number of key generation rounds with > 0 photons

Table 6.1: Notation for random variables used in the phase error estimation.

Then, for the active basis-choice BB84 protocol, the phase error rate e_{gen} can be upper bounded by

$$e_{\mathrm{gen}} \underset{\varepsilon_{\mathrm{serf}}}{\leq} \left(\frac{e_{\mathrm{test}}}{1 - f_{\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) (1 - f_{\mathrm{gen}}) + f_{\mathrm{gen}}, \tag{6.8}$$

where n_{test}, e_{test}, and n_{det} are random variables defined in Table 6.1 whose values are observed in the protocol. Here, f_{test} and f_{gen} are random variables corresponding to the fraction of flag-states in the test and key generation rounds after the application of the noise channel, respectively.

Proof. All random variables used in this proof are defined in Table 6.1. The rounds not in the flag space are measured by a POVM with no basis-efficiency mismatch. Thus, Serfling's inequality can be used on these rounds to obtain

$$\frac{n_{B;\,\mathrm{gen},\neq}}{n_{B;\,\mathrm{gen}}} \underset{\varepsilon_{\mathrm{serf}}}{\leq} \frac{n_{B;\,\mathrm{test},\neq}}{n_{B;\,\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}}(\varepsilon_{\mathrm{serf}}, n_{B;\,\mathrm{test}}, n_{B;\,\mathrm{det}}). \tag{6.9}$$

We first upper bound $\overline{\gamma_{\mathrm{serf}}}(\varepsilon_{\mathrm{serf}}, n_{B;\,\mathrm{test}}, n_{B;\,\mathrm{det}})$ as

$$\begin{aligned}
\overline{\gamma_{\mathrm{serf}}}(\varepsilon_{\mathrm{serf}}, n_{B;\,\mathrm{test}}, n_{B;\,\mathrm{det}}) &= \overline{\gamma_{\mathrm{serf}}}(\varepsilon_{\mathrm{serf}}, n_{\mathrm{test}} - n_{F;\,\mathrm{test}}, n_{\mathrm{det}} - n_{F;\,\mathrm{gen}} - n_{F;\,\mathrm{test}}) \\
&\leq \overline{\gamma_{\mathrm{serf}}}(\varepsilon_{\mathrm{serf}}, n_{\mathrm{test}} - n^*_{F;\,\mathrm{test}}, n_{\mathrm{det}} - n_{F;\,\mathrm{gen}} - n^*_{F;\,\mathrm{test}}) \\
&\leq \overline{\gamma_{\mathrm{serf}}}(\varepsilon_{\mathrm{serf}}, n_{\mathrm{test}} - n^*_{F;\,\mathrm{test}}, n_{\mathrm{det}} - n^*_{F;\,\mathrm{gen}} - n^*_{F;\,\mathrm{test}}) =: \overline{\gamma_{\mathrm{serf}}},
\end{aligned} \tag{6.10}$$

where the first inequality follows from the observation made in Section 2.3.3 that $\overline{\gamma_{\mathrm{serf}}}(\varepsilon, k - x, n - x)$ is a monotonically increasing function of $x \in [0, k)$, and the second inequality follows from the fact that $\overline{\gamma_{\mathrm{serf}}}(\varepsilon, k, n)$ is a monotonically decreasing function of n.

The upper bound on the phase error rate e_{gen} follows by a long chain of (in)equalities using Eqs. (6.9) and (6.10) and the conditions of the lemma statement:

$$
\begin{aligned}
e_{\mathrm{gen}} &= \frac{n_{\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \text{[Definition (see Table 6.1)]} \\
&= \frac{n_{B;\,\mathrm{gen},\neq} + n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \text{[Since } n_{\mathrm{gen},\neq} = n_{B;\,\mathrm{gen},\neq} + n_{F;\,\mathrm{gen},\neq}\text{]} \\
&\underset{\varepsilon_{\mathrm{serf}}}{\leq} \frac{n_{B;\,\mathrm{gen}} \left(\frac{n_{B;\,\mathrm{test},\neq}}{n_{B;\,\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right)}{n_{\mathrm{K}}} + \frac{n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \text{[From Eqs. (6.9) and (6.10)]} \\
&= \frac{(n_{\mathrm{K}} - n_{F;\,\mathrm{gen}}) \left(\frac{n_{B;\,\mathrm{test},\neq}}{n_{B;\,\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right)}{n_{\mathrm{K}}} + \frac{n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \text{[Since } n_{B;\,\mathrm{gen}} = n_{\mathrm{K}} - n_{F;\,\mathrm{gen}}\text{]} \\
&= \left(\frac{n_{B;\,\mathrm{test},\neq}}{n_{B;\,\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) \left(1 - \frac{n_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} \right) + \frac{n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \text{[Simplifying]} \\
&= \left(\frac{n_{\mathrm{test},\neq} - n_{F;\,\mathrm{test},\neq}}{n_{\mathrm{test}} - n_{F;\,\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) \left(1 - \frac{n_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} \right) + \frac{n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \left[\text{Since } \begin{array}{c} n_{B;\,\mathrm{test}} = n_{\mathrm{test}} - n_{F;\,\mathrm{test}} \\ n_{B;\,\mathrm{test},\neq} = n_{\mathrm{test},\neq} - n_{F;\,\mathrm{test},\neq} \end{array} \right] \\
&\leq \left(\frac{n_{\mathrm{test},\neq}}{n_{\mathrm{test}} - n^{*}_{F;\,\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) \left(1 - \frac{n_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} \right) + \frac{n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \left[\text{Since } \begin{array}{c} n_{F;\,\mathrm{gen}} \leq n_{\mathrm{K}} \\ n_{F;\,\mathrm{test},\neq} \geq 0 \\ n_{F;\,\mathrm{test}} \leq n^{*}_{F;\,\mathrm{test}} \end{array} \right] \\
&= \left(\frac{e_{\mathrm{test}}}{1 - f_{\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) \left(1 - \frac{n_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} \right) + \frac{n_{F;\,\mathrm{gen},\neq}}{n_{\mathrm{K}}} && \left[\text{Definition (see Table 6.1): } f_{\mathrm{test}} \coloneqq \frac{n_{F;\,\mathrm{test}}}{n_{\mathrm{test}}} \right] \\
&\leq \left(\frac{e_{\mathrm{test}}}{1 - f_{\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) \left(1 - \frac{n^{*}_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} \right) + \frac{n^{*}_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} && \left[\text{Since } \begin{array}{c} n_{F;\,\mathrm{gen},\neq} \leq n_{F;\,\mathrm{gen}} \leq n^{*}_{F;\,\mathrm{gen}} \\ \dfrac{e_{\mathrm{test}}}{1 - f_{\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \leq 1 \end{array} \right] \\
&= \left(\frac{e_{\mathrm{test}}}{1 - f_{\mathrm{test}}} + \overline{\gamma_{\mathrm{serf}}} \right) (1 - f_{\mathrm{gen}}) + f_{\mathrm{gen}} && \left[\text{Definition (see Table 6.1): } f_{\mathrm{gen}} \coloneqq \frac{n_{F;\,\mathrm{gen}}}{n_{\mathrm{K}}} \right]
\end{aligned}
$$

The inequalities in the proof can be intuitively understood as follows:

$n_{F;\,\mathrm{gen},\neq} \leq n_{F;\,\mathrm{gen}} \leq n^{*}_{F;\,\mathrm{gen}}$**:** Since we assume nothing about the flags, the worst-case scenario is when all key generation flags are detected and result in phase errors. This increases the phase error rate without being reflected in any observable data.

$n_{F;\,\text{test}} \geq 0$, $n_{F;\,\text{test}} \leq n^*_{F;\,\text{test}}$: Similarly, for the flags in the test rounds, the worse-case scenario is when all these flags are detected, but none are mapped to errors. Thus, all errors are assumed to arise from the preserved subspace. □

Remark 6.2 (Monotonicity of upper bound)**.** *As already used in the proof of Lemma 6.1, the upper bound on the phase error rate e_{gen} is a monotonically increasing function of the number of flags in the test $n^*_{F;\,\text{test}}$ and generation rounds $n^*_{F;\,\text{gen}}$. Thus, an upper bound on these quantities suffices to upper bound the phase error rate.*

6.4.1 Application of noise channel

We construct the noise channel for our analysis by applying the procedure from the proof of Theorem 4.2. Given the real POVM $\vec{\Gamma}_{\mathbf{d_B},\boldsymbol{\eta}} = \vec{\Gamma}_{0;\ \mathbf{d_B}} \oplus \vec{\Gamma}_{>0;\ (\mathbf{d_B},\boldsymbol{\eta})}$ with dark count rates $\mathbf{d_B}$ and efficiencies $\boldsymbol{\eta}$, we define the ideal POVM (without flags) to be $\vec{\Gamma}_{\text{ideal}} = \vec{\Gamma}_{0;\ \mathbf{d_B}} \oplus \vec{\Gamma}_{>0}$. Here, the ideal POVM is defined as a hybrid:

- Its 0-photon component $\vec{\Gamma}_{0;\ (\mathbf{d_B},\boldsymbol{\eta})}$ is identical to the 0-photon component of the real POVM.
- Its non-zero photon component $\vec{\Gamma}_{>0}$ is defined as the non-zero photon component of the POVM for a detector with no dark counts or loss.

Note that although the 0-photon component contains dark counts[8], this subspace does not induce basis-efficiency mismatch. Thus, the ideal POVM is one with no basis-efficiency mismatch (i.e., satisfying Eq. (6.5)), as depicted in Fig. 6.2.

For each subspace m, the deviation from ideality q_m is such that it satisfies the condition:

$$\begin{aligned} &\vec{\Gamma}_{m;\ \mathbf{d_B}} \geq (1-q_m)\vec{\Gamma}_{m;\ \text{ideal}} \\ \Leftrightarrow \exists \vec{R} \text{ such that } \quad &\vec{\Gamma}_{m;\ (\mathbf{d_B},\boldsymbol{\eta})} = (1-q_m)\vec{\Gamma}_{m;\ \text{ideal}} + q_m \vec{R}_m, \end{aligned} \qquad m \in \{0,\ >0\} \tag{6.11}$$

where $\vec{R}_m$ is the m-photon subspace of the POVM $\vec{R}$. In each subspace m, the noise channel does the following (see Fig. 4.1):

- With probability $1 - q_m$, act trivially.

[8]The 0-photon component of the real POVM does not depend on loss, as can be seen from the detector model described in Section 2.2.6.

- With probability q_m, measure the state with POVM $\vec{R}_m$ and output the measurement result as a classical flag.

From our definition of the ideal POVM, which includes the real 0-photon component, it immediately follows that no deviation exists in this subspace, and therefore $q_0 = 0$. In Appendix D.2.1, we show by explicit computation that the deviation

$$q_{>0} = 1 - \eta_{\min}\left(1 - \frac{d_{\max}}{2}\right), \tag{6.12}$$

satisfies Eq. (6.11). Here, $d_{\max}$ is the maximum possible dark count rate, and $\eta_{\min}$ is the minimum allowed value of the detector efficiency across both detectors (after pulling out common loss).

As a preliminary step to bounding the number of flags, we introduce an equivalent virtual protocol, depicted in Fig. 6.3. In this protocol, Bob's basis selection is made *before* the action of the noise channel. This is possible as the ideal and real POVM (and hence the POVM $\vec{R}$, are described by Bob actively choosing basis b with probability p_b^B, followed by a basis-dependent POVM.

Importantly, this reordering ensures that we do not include flag rounds when Alice and Bob's bases do not match, and that the number of flags in the key generation and test rounds are estimated separately.[9] Now, each round with non-zero photons is identically and independently mapped to flags with probability $q_{>0}$. Thus, an upper bound on the number of flags can be obtaining by using Hoeffding's inequality[10] (see Section 2.3.2) as

$$n^*_{F;\,b} \underset{\varepsilon_{\mathrm{h};b}}{\leq} q_{>0}\; n^*_{>0;\,b} + n^*_{>0;\,b}\; \gamma_{\mathrm{hoeff}}(\varepsilon_{\mathrm{h};b},\, n^*_{>0;\,b}) \qquad b \in \{\mathrm{gen}, \mathrm{test}\}, \tag{6.13}$$

where $\gamma_{\mathrm{hoeff}}(\varepsilon_{\mathrm{h};b},\, n^*_{>0;\,b}) = \sqrt{\frac{1}{2n^*_{>0;\,b}} \ln\left(\frac{1}{\varepsilon_{\mathrm{h};b}}\right)}$.

As the upper bound in Eq. (6.13) is a monotonically increasing function of the number of non-zero photon rounds $n^*_{>0;\,b}$, the remaining task is to upper-bound this quantity. Thus, we obtain an upper bound on $n^*_{>0;\,b}$ in terms of the detected rounds n_b by using [21, Lemma 5].

[9] Alternately, the total number of flag rounds can be estimated in terms of the total number of protocol rounds. Then using the fact that the POVM $\vec{R}$ has the property that it chooses bases in an IID manner, we can estimate the number of flags in the key generation and test rounds.

[10] It would also be valid to use the binomial distribution as this mapping is IID. We use Hoeffding's inequality to simplify the analysis.

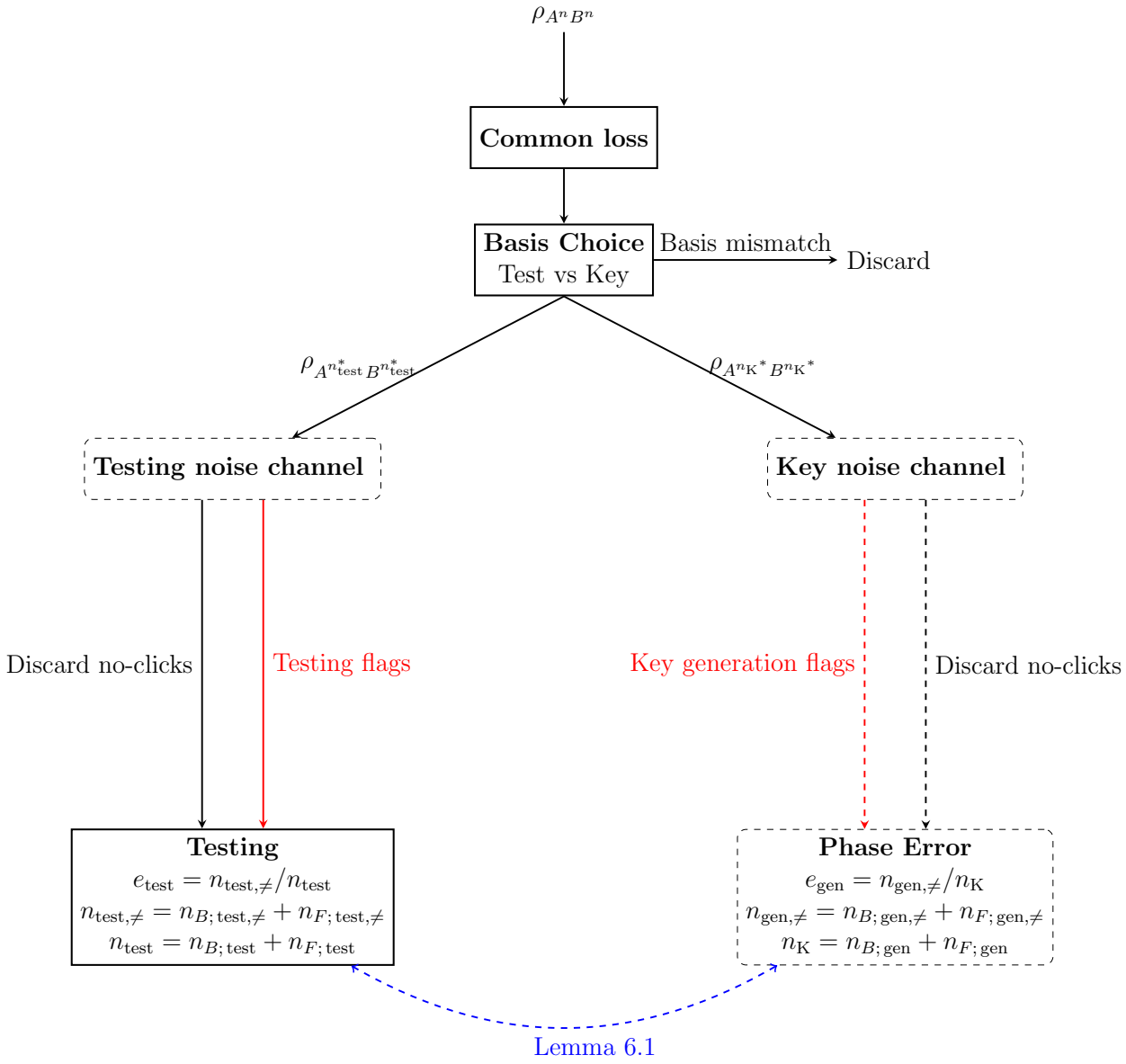


Figure 6.3: The noise channel from Fig. 6.2 can be moved to after the basis choice to construct another equivalent protocol useful for bounding the number of flags in the key generation and test rounds.

This lemma states that for any $\lambda_{\min;\,\mathrm{b}}$ such that $\Gamma_{\mathrm{det},\,b} \geq \lambda_{\min;\,\mathrm{b}}\Pi_{>0}$, where $\Gamma_{\mathrm{det},\,b} = \mathbb{I} - \Gamma_{\text{no-click},\,b}$ is the POVM element corresponding to a detection event in basis b:

$$n^*_{>0;\,b} \underset{\varepsilon_{>0;\,b}}{\leq} \frac{n_b}{\lambda_{\min;\,\mathrm{b}}} + n_b\gamma_{>0}(\varepsilon_{>0;\,b},\, n_b,\, \lambda_{\min;\,\mathrm{b}}) \qquad\qquad b \in \{\mathrm{gen}, \mathrm{test}\}, \tag{6.14}$$

where

$$\gamma_{>0}(\varepsilon_{>0;\,b},\, n_b,\, \lambda_{\min;\,\mathrm{b}}) = \frac{\sqrt{\ln\left(1/\varepsilon_{>0;\,b}\right)\,\left(\ln\left(1/\varepsilon_{>0;\,b}\right) + 2\lambda_{\min;\,\mathrm{b}}\, n_b\right)} + \ln\left(1/\varepsilon_{>0;\,b}\right)}{n_b\lambda^2_{\min;\,\mathrm{b}}}. \tag{6.15}$$

We show in Appendix D.2.2 that $\lambda_{\min;\,\mathrm{b}} = \eta_{\min}$ is a valid choice, resulting in

$$n^*_{>0;\,b} \underset{\varepsilon_{>0;\,b}}{\leq} \frac{n_b}{\eta_{\min}} + n_b\gamma_{>0;\,b} \qquad\qquad b \in \{\mathrm{gen}, \mathrm{test}\}, \tag{6.16}$$

where $\gamma_{>0;\,b} \coloneqq \gamma_{>0}(\varepsilon_{>0;\,b},\, n_b,\, \eta_{\min})$.

Finally, we combine Eqs. (6.12), (6.13) and (6.16) to obtain

$$n^*_{F;\,b} \underset{\varepsilon_{\mathrm{h};b}+\varepsilon_{>0;\,b}}{\leq} \left(1 - \eta_{\min}\left(1 - \frac{d_{\max}}{2}\right)\right)\,\left(\frac{n_b}{\eta_{\min}} + n_b\gamma_{>0;\,b}\right) + \left(\frac{n_b}{\eta_{\min}} + n_b\gamma_{>0;\,b}\right)\,\gamma_{\mathrm{hoeff}}\left(\varepsilon_{\mathrm{h};b},\, \left(\frac{n_b}{\eta_{\min}} + n_b\gamma_{>0;\,b}\right)\right),$$

where $b \in \{\mathrm{gen}, \mathrm{test}\}$.

Notational aside 6.3. For ease of notation, we define $\varepsilon_{\mathrm{h}} \coloneqq \varepsilon_{\mathrm{h;gen}} + \varepsilon_{\mathrm{h;test}}$, $\varepsilon_{>0} \coloneqq \varepsilon_{>0;\,\mathrm{gen}} + \varepsilon_{>0;\,\mathrm{test}}$, and $\varepsilon_F \coloneqq \varepsilon_{\mathrm{h}} + \varepsilon_{>0}$. We further define $1 - \eta_F \coloneqq \frac{1}{\eta_{\min}}\left(1 - \eta_{\min}\left(1 - \frac{d_{\max}}{2}\right)\right)$, and

$$\gamma_{F;\,b} \coloneqq \eta_{\min}(1-\eta_F)\gamma_{>0;\,b} + \left(\frac{1}{\eta_{\min}} + \gamma_{>0;\,b}\right)\,\gamma_{\mathrm{hoeff}}\left(\varepsilon_{\mathrm{h};b},\, \left(\frac{n_b}{\eta_{\min}} + n_b\gamma_{>0;\,b}\right)\right).$$

In this notation, $1 - \eta_F$ can be interpreted as the flagging probability for a *detected round*, which is independent of basis.

Using the simplified notation, we restate the bound on the number (and fraction) of flags

$$\begin{aligned} n^*_{F;\,b} &\underset{\varepsilon_{\mathrm{h};b}+\varepsilon_{>0;\,b}}{\leq} (1-\eta_F)n_b + n_b\,\gamma_{F;\,b} \\ \Leftrightarrow\, f_b &\underset{\varepsilon_{\mathrm{h};b}+\varepsilon_{>0;\,b}}{\leq} 1 - \eta_F + \gamma_{F;\,b}. \end{aligned} \tag{6.17}$$

Finally, we can combine Eq. (6.17) with Lemma 6.1 and Remark 6.2 to obtain the final phase error rate bound.

Theorem 6.1 (Phase error rate bound for active BB84)**.** *Let* $1 - \eta_F + \gamma_{F;b} < 1$ *for* $b \in \{\text{gen}, \text{test}\}$*, where* η_F *and* $\gamma_{F;b}$ *are as defined in Notational aside 6.3. Let the finite-size correction term due to Serfling's inequality as defined in Eq. (2.15) be no greater than* 1*:*

$$\gamma_{\text{serf}} \coloneqq \overline{\gamma_{\text{serf}}}(\varepsilon_{\text{serf}}, n_{\text{test}}(\eta_F - \gamma_{F;\,\text{test}}), n_{\text{det}}\eta_F - n_{\text{test}}\gamma_{F;\,\text{test}} - n_{\text{K}}\gamma_{F;\,\text{gen}}) \leq 1.$$

Then for the active basis-choice BB84 protocol, the phase error rate e_{gen} *can be upper bounded by*

$$e_{\text{gen}} \underset{\varepsilon_{\text{serf}}+\varepsilon_F}{\leq} \left(\frac{e_{\text{test}}}{\eta_F - \gamma_{F;\,\text{test}}} + \gamma_{\text{serf}}\right)(\eta_F - \gamma_{F;\,\text{gen}}) + 1 - \eta_F + \gamma_{F;\,\text{gen}}. \tag{6.18}$$

Here, γ_{serf}*,* $\gamma_{F;\,\text{gen}}$*,* $\gamma_{F;\,\text{test}}$ *are finite-size penalties,* $1 - \eta_F$ *quantifies the deviation from ideality as defined in Notational aside 6.3, and* e_{test} *is the observed error rate in the test rounds.*

Remark 6.3 (Compatibility with source imperfections)**.** *The analysis leading to Theorem 6.1 is notable for being confined almost entirely to Bob's detection apparatus. This property makes the framework highly modular, allowing for a direct combination with analyses of imperfect sources [98, 99, 15, 16, 100, 16] that otherwise presume perfect detection setups. The only required adaptation is the substitution of Serfling's inequality with the appropriate sampling bound for the non-ideal source. This is in contrast to the analysis in Section 6.3, which requires a more complex, non-trivial proof [101] of compatibility.*

We state the following corollary as a special case of Theorem 6.1 that is easier to intuitively grasp.

Corollary 6.1. *If you choose* $\varepsilon_{>0;\,b}$*,* $\varepsilon_{\text{h};b}$ *such that* $\frac{\ln(\varepsilon_{>0;\,\text{gen}})}{n_{\text{K}}} = \frac{\ln(\varepsilon_{>0;\,\text{test}})}{n_{\text{test}}}$*, and* $\frac{\ln\left(\varepsilon_{\text{h;gen}}\right)}{n_{\text{K}}} = \frac{\ln\left(\varepsilon_{\text{h;test}}\right)}{n_{\text{test}}}$*, then the finite-size corrections are independent of basis,* $\gamma_{F;\,\text{gen}} = \gamma_{F;\,\text{test}} =: \gamma_F$*, and hence the phase error rate can be upper bounded as*

$$e_{\text{gen}} \underset{\varepsilon_{\text{serf}}+\varepsilon_F}{\leq} e_{\text{test}} + 1 - \eta_F + \gamma_F + \eta_F\gamma_{\text{serf}} - \gamma_F\gamma_{\text{serf}}. \tag{6.19}$$

Remark 6.4 (Compatibility with decoy-state analysis)**.** *Decoy-state analyses [59, 60, 61] obtain high probability lower bounds on the number of detected key generation and test rounds, and high probability upper bounds on the number of errors in the test rounds that*

arise from single-photons sent by Alice. These bounds can be used with Theorem 6.1 since the upper bound in Eq. (6.18) is a monotonically decreasing function of the number of key generation and test rounds, and a monotonically increasing function of the number of errors in the test rounds.

When using Corollary 6.1, we would need to compute expressions for $\gamma_{>0}$ and γ_{hoeff} in terms of $\varepsilon_{>0}$ and ε_{h}. While an exact analytical expression is hard to find in general, we derive a simple upper bound. Let $\frac{\ln(\varepsilon_{>0;\,\text{gen}})}{n_{\text{K}}} = \frac{\ln(\varepsilon_{>0;\,\text{test}})}{n_{\text{test}}} = -c$, and $\frac{\ln\left(\varepsilon_{\text{h;gen}}\right)}{n_{\text{K}}} = \frac{\ln\left(\varepsilon_{\text{h;test}}\right)}{n_{\text{test}}} = -d$. Then, $\gamma_{>0} = \frac{\sqrt{c(c+2\eta_{\text{min}})}+c}{\eta_{\text{min}}^2}$ and $\gamma_{\text{hoeff}} = \sqrt{\frac{d\eta_{\text{min}}}{2(1+\eta_{\text{min}}\gamma_{>0})}}$. We now upper bound c and d in terms of $\varepsilon_{>0}$ and ε_{h} respectively.

$$\begin{aligned}\varepsilon_{>0} &= \sum_b \varepsilon_{>0;\,b} \\ &= \sum_b e^{-cn_b} \\ &\leq 2e^{-cn_{\text{min}}},\end{aligned}$$

where $n_{\text{min}} \coloneqq \min\{n_{\text{K}}, n_{\text{test}}\}$. The last inequality implies that $c \geq \frac{1}{n_{\text{min}}} \ln\left(\frac{2}{\varepsilon_{>0}}\right)$. Similarly, $d \geq \frac{1}{n_{\text{min}}} \ln\left(\frac{2}{\varepsilon_{\text{h}}}\right)$. This allows us to compute the finite-size correction terms on the error rate upper bound from Corollary 6.1.

6.4.2 Comparison with sampling bound

We now compare the phase error rate bound derived from the noise channel method (Theorem 6.1) with the one derived from the sampling strategy of Eq. (6.6). To build intuition, we first analyse the bounds in the asymptotic limit of an infinite number of rounds, where finite-size effects vanish.

In the asymptotic limit, the upper bound in Eq. (6.18) can be simplified to

$$\begin{aligned}e_{\text{gen}} \leq e_{\text{test}} + 1 - \eta_F &= e_{\text{test}} + \frac{1}{\eta_{\text{min}}}\left(1 - \eta_{\text{min}}\left(1 - \frac{d_{\text{max}}}{2}\right)\right) \\ &= e_{\text{test}} + \frac{1-\eta_{\text{min}}}{\eta_{\text{min}}} + \frac{d_{\text{max}}}{2}.\end{aligned}$$

Historical aside 6.1 (Trojan Pony)**.** This is the same asymptotic behaviour as that of the 'Trojan Pony' attack [62, Eq. (55)] (with an extra term for dark counts). Indeed, our work here is a full, finite-size version of [62, Theorem 7].

The sampling strategy upper bound given in Eqs. (6.6) and (6.7) is

$$e_{\text{gen}} \leq \frac{e_{\text{test}}}{\eta_{\min}} + \frac{4(1-\sqrt{\eta_{\min}})}{\eta_{\min}} =: e_{\text{samp}}. \tag{6.20}$$

For all $\eta_{\min} \in [0,1]$, $4(1-\sqrt{\eta_{\min}}) \geq 1-\eta_{\min}$. Thus, in the practical regime where the maximum dark count rate $d_{\max}$ is small, a direct comparison shows that $e_{\text{noise}} \leq e_{\text{samp}}$.

Thus, asymptotically the noise channel upper bound outperforms the sampling upper bound. We believe that this is in part due to the fact that computing the deviation metric is significantly easier for the noise channel bound, thus allowing for a more optimal computation. However, we believe that even with a more optimal computation, the noise channel approach would outperform the sampling bound, though this is merely an intuitive claim. It is somewhat difficult to directly compare the two approaches as the deviation metrics are different.

We now make a more rigorous, finite-size comparison.

6.4.3 Finite-size plots

In the finite-size regime, we compare the two approaches by plotting the finite-size key rates for the decoy-state BB84 protocol as a function of channel loss. We refer the reader to [5] for the full description of the decoy-state analysis and the variable security proof using the EUR and leftover hashing lemma [8, Proposition 9]. We modify the analysis only by changing the upper bound on the phase error rate. We use the same parameter choices as in [5, Section VI. E.], summarised below.

The overall security parameter is set to be $(2\sqrt{12}+2)\times 10^{-12}$, and all finite-size failure probabilities (including those used for the decoy analysis) are set to be the same value, 10^{-12} for the analysis in Section 6.3. This corresponds to setting $\varepsilon_{\text{serf}} + \varepsilon_F = 3\times 10^{-24}$ in Theorem 6.1. We make use of the simplified Corollary 6.1, and set $\varepsilon_{\text{serf}} = \varepsilon_{\text{h}} = \varepsilon_{>0} = 10^{-24}$.

We set the detector parameters to be[11]

$$\begin{aligned} \eta_i &\in [\bar{\eta}(1-\Delta_\eta), \bar{\eta}(1+\Delta_\eta)] \\ d_i &\in [0, \bar{d}(1+\Delta_{\mathrm{dc}})], \end{aligned} \tag{6.21}$$

where $\bar{\eta} = 0.7$ and $\bar{d} = 10^{-6}$, and vary Δ_η, Δ_{dc}.

We set the basis choice probabilities to be $p_Z^A = p_Z^B = 0.5$ and $p_X^A = p_X^B = 0.5$, and $p_{Z,T} = 0.05$ (probability of Z-basis rounds used for testing for the purpose of error correction). We set the misalignment angle θ to be 2°. We set the number of bits used for error correction to be $\lambda_{\mathrm{EC}}(n_X, \vec{\mu}_k, n_K, \vec{\mu}_k, e^{\mathrm{obs}}_{X,\vec{\mu}_k}, e^{\mathrm{obs}}_Z) = f_{\mathrm{EC}}\, n_K\, h(e^{\mathrm{obs}}_Z)$, where $f_{\mathrm{EC}} = 1.16$ is the error-correction efficiency. The decoy intensities are chosen to be $\mu_1 = 0.9$, $\mu_2 = 0.1$, and $\mu_3 = 0$. Each intensity is chosen with equal probability.

In Fig. 6.4, we plot the finite size key rate against loss for various values of detector characterizations Δ_η, Δ_{dc} for $N_{\mathrm{tot}} = 10^{12}$ number of total signals. The sampling strategy gives 0 key rates for $\Delta_\eta = \Delta_{\mathrm{dc}} = 0.12$ and larger. When $\Delta_\eta = \Delta_{\mathrm{dc}} = 0$, the upper bounds of both methods differ only in the dark count rate, and the finite-size effects. These effects are small in magnitude for the parameter choices made.

In Fig. 6.5, we plot the finite size key rate against loss for various values of total signals sent. We set $\Delta_\eta = \Delta_{\mathrm{dc}} = 0.05$. We find that we get close to asymptotic key rates already at $N_{\mathrm{tot}} = 10^{12}$ signals sent.

6.5 Concluding Remarks

In this chapter, we sketched a security proof for the active basis-choice BB84 protocol, in the presence of detector imperfections. As noted in the preceding chapter, a security proof for active basis-choice protocols using the postselection technique[12] face a technical obstacle in the application of the flag-state squasher. Consequently, our analysis focused on estimating the phase error rate in the presence of basis-efficiency mismatch. This is the crucial step in proofs using the EUR as well as phase error correction-based proofs.

To this end, we presented and compared two distinct approaches: a direct approach based on a multi-step sampling strategy, and a sampling framework based on noise channels.

[11] Similar to the ranges in Eq. (5.43), the detector efficiencies and dark count rates must additionally lie in the range $[0, 1]$. However, for the values of $\bar{\eta}$, $\bar{d}$, Δ_η, and Δ_{dc} considered here, these ranges automatically lie in the range $[0, 1]$ imposed by physical constraints.

[12] This also affects the application of the flag-state squasher for EAT-based proofs.

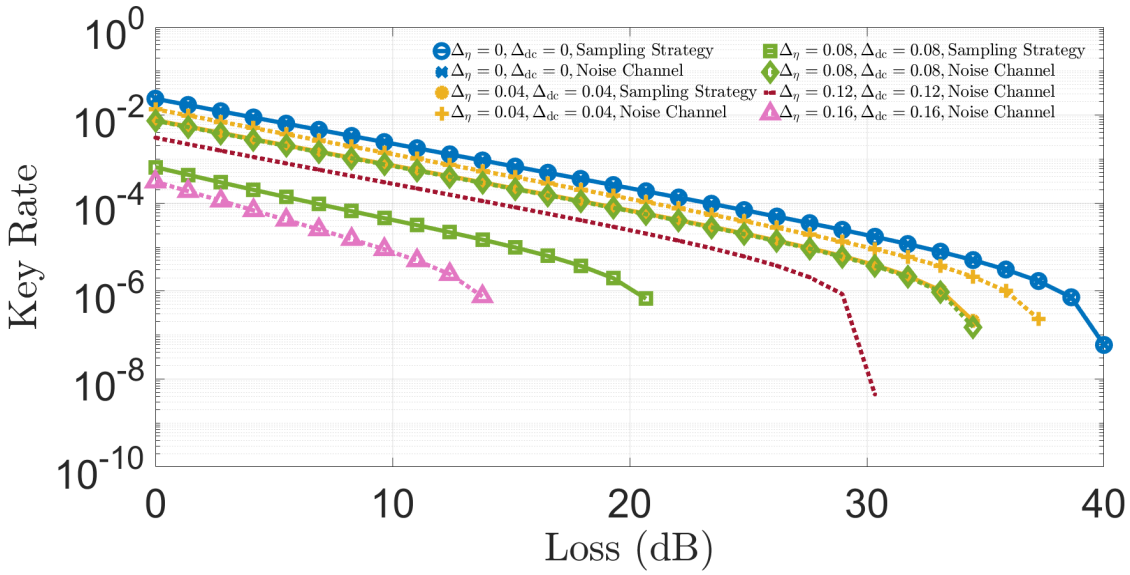


Figure 6.4: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol, against loss. We plot key rates for $N_{\text{tot}} = 10^{12}$ number of total signals sent, for various values of Δ_η, Δ_{dc}. Colours encode the extent of characterisation Δ_η, Δ_{dc}, while line styles distinguish the method (dashed: noise channel approach; solid: sampling strategy). We find that the noise channel method to treat basis-efficiency mismatch results in better key rates.

Both of these approaches represent a significant advance over all prior work [18, 19, 20, 3, 22], which was limited to asymptotic analyses, relied on restricting Eve's attacks to IID attacks, or required physical modifications to the protocol. Among both approaches, we found that the noise channel method outperforms the direct sampling strategy, yielding tighter bounds on the phase error rate and consequently higher secure key rates.

We believe that the analysis can made tighter by combining both approaches. The noise channel method isolates imperfections by probabilistically flagging 'imperfect' rounds, allowing the vast majority of data to be analysed under ideal sampling conditions. The current analysis treats makes no sampling claims in the flag space, instead treating flagged rounds with a pessimistic, worst-case penalty. However, tools from our sampling strategy may be used to derive a sampling bound in this flagged subspace.

Another refinement could be achieved by redefining the phase error rate. In the EUR framework, this corresponds to applying the uncertainty relation not to the total key generation rounds, but specifically to the state conditioned on being in the 'preserved'

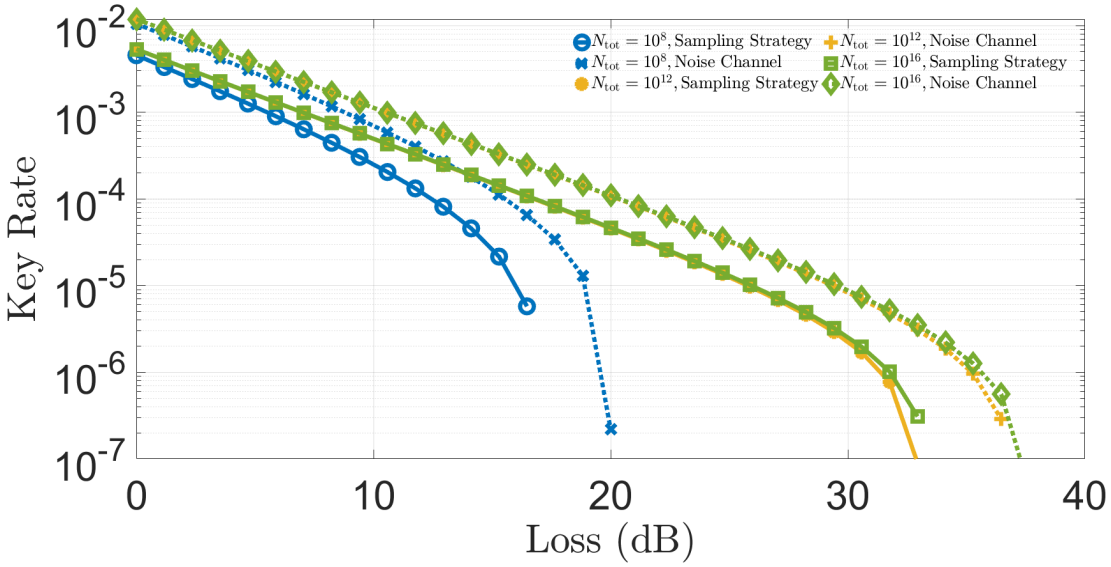


Figure 6.5: Finite-size key rates in the presence of basis-efficiency mismatch, for the decoy-state BB84 protocol against loss. We plot key rates for various values of total number of signals sent (N_{tot}), for $\Delta_\eta = \Delta_{\text{dc}} = 0.05$. Colours encode the total number of signals, while line styles distinguish the method (dashed: noise channel approach; solid: sampling strategy).

subspace. A rigorous treatment of this idea would involve using properties of the smooth-min entropy, combined with sampling argument similar to the ones we presented. We leave these extensions for future work.

While the sampling strategy can also be combined with analyses of source imperfections [98, 99, 15, 16, 100, 16], a dedicated proof of compatibility is required [101]. In contrast, the noise channel framework offers a distinct advantage in its modularity, which makes its compatibility with analyses of source imperfections immediate (see Remark 6.3).

Given that the sampling strategy's core ideas have recently been extended to passive detection setups [21], a compelling direction for future work is to apply our superior noise channel framework to that context, where we expect similar improvements in key rates. Furthermore, the utility of the noise channel construction extends beyond phase error estimation: as noted in Technical aside 6.3, it also provides a method to overcome the infinite-dimensional optimisation problem that arises in EAT-based proofs for active detection setups.

Chapter 7

Security against correlated imperfections

> "No one is finally dead until the ripples they cause in the world die away."
>
> — Terry Pratchett, *Reaper Man*

In the preceding chapters, we constructed a framework to treat detector imperfections and demonstrated its applicability across various proof techniques. A crucial, underlying assumption in that analysis, however, was that imperfections in each round are independent. In practice, this assumption is violated by realistic detectors [32, 102], which exhibit memory effects such as afterpulsing and dead times (see Sections 2.2.5 and 2.2.6). A complete security analysis must therefore address these cross-round correlations. In this chapter, we describe a general technique to address this problem.

Our analysis is structured as a two-stage reduction. First, in Section 7.1, we adapt the methodology of [33, Section 3.3] to formally reduce the problem of infinite-range correlations to one of a finite, effective correlation length. This reduction comes at a quantifiable cost to the security parameter. Second, the subsequent sections reduce the security analysis of the finite correlation length model to that of an IID detection setup. This second reduction crucially relied on a protocol modification that discards rounds following detection events, as described in Section 7.2.

7.1 Reduction to finite correlation length

Empirically-motivated physical models for dead times [34] and afterpulsing [103, 104] describe memory as a process of exponential decay. While this decay is rapid, it formally introduces correlations between all rounds in the protocol, no matter how far apart. As will become clear in the following sections, these long-range correlations introduce significant complexity into the security analysis. To manage this complexity, we first extend the results of [33, Section 3.3] to the incorporate correlated detectors. This extension allows us to effectively truncate the memory to a finite correlation length, at the cost of a calculable penalty to the secrecy parameter.

First, we rewrite the secrecy definition from Remark 3.1 into a form that makes the detector memory explicit. To achieve this, we model Alice and Bob's n-round measurement process as a sequence of measurement channels, $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1$ where each channel acts on the current round and incorporates the memory from the preceding rounds. More formally, the jth measurement channel $\mathcal{M}_j \in \mathcal{C}\left(A_j B_j R^{j-1}, C_j R^j\right)$ acts on Alice and Bob's jth round registers $A_j B_j$, and the memory R^{j-1} from previous rounds[1]. It outputs the classical measurement outcome into register C_j and adds its memory into register R_j.

Notational aside 7.1 (Measurement channels with finite correlation length)**.** If all measurements possess a finite correlation length l_{c}, then the measurement channels act trivially on the registers $R^{j-l_{\mathrm{c}}-1}$. We denote such measurement channels by $\mathcal{M}_j^{l_{\mathrm{c}}}$. Thus, the independent case studied so far consists of measurement channels $\mathcal{M}_j^0$.

Let $\rho_{A^n B^n E^n}$ be the state shared by Alice, Bob and Eve after Eve's attack. The $\varepsilon_{\mathrm{sec}}$-secrecy condition can then be described by

$$\sup_{\substack{\rho_{A^n B^n E^n} \in \mathrm{S}_\circ(A^n B^n E^n) \\ \mathrm{Tr}_{B^n E^n}[\rho_{A^n B^n E^n}] = \mathrm{Tr}_{A'^n}\left[(\rho_{AA'})^{\otimes n}\right]}} \left\| \left(\mathcal{KP} - \mathcal{KP}^{\mathrm{ideal}}\right) \circ \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1 \left[\rho_{A^n B^n E^n}\right] \right\|_1 \leq \varepsilon_{\mathrm{sec}}, \quad (7.1)$$

where $\mathcal{KP}$ is the channel corresponding to all the classical steps of the protocol, and $\mathcal{KP}^{\mathrm{ideal}}$ is the channel which first performs $\mathcal{KP}$ and then replaces the key register with the ideal key.

[1] The first map $\mathcal{M}_1$ does not have any input memory. Thus, technically $\mathcal{M}_1 \in \mathcal{C}\left(A_1 B_1, C_1 R_1\right)$. In what follows, we ignore such edge cases as they do not affect any of the results, but add notational clutter.

Now, from the physical model, it needs to be argued that

$$\left\|\mathcal{M}_j - \mathcal{M}_j^{l_c}\right\|_\diamond \leq \varepsilon_{\mathcal{M}_j^{l_c}}. \tag{7.2}$$

For instance, such a statement follows from the POVM elements corresponding to correlation length l_c being close (in ∞-norm) to those without any finite correlation length [33, Eq. (3.20)]. Obtaining such a bound would involve a detailed study of the physical models underlying these memory effects. For this work, we consider this bound to be given, and leave the more detailed analysis for future work.

This assumption allows us to show that the ε_{sec}-secrecy of a protocol, assuming finite correlation length, implies $\varepsilon_{\text{sec}} + \sum_{j=1}^{n} \varepsilon_{\mathcal{M}_j^{l_c}}$-secrecy for the real protocol as a direct consequence of the following lemma.

Lemma 7.1 (Reduction to finite correlations)**.** *Let $\rho \in \mathrm{S}_\circ(A^n B^n E^n)$, and $\mathcal{M}_j, \mathcal{M}_j^{l_c} \in \mathcal{C}\left(A_j B_j R^{j-1}, C_j R^j\right)$ be such that $\left\|\mathcal{M}_j - \mathcal{M}_j^{l_c}\right\|_\diamond \leq \varepsilon_{\mathcal{M}_j^{l_c}}$ for all $j \in \{1, \ldots, n\}$. Then, for any $\rho \in \mathrm{S}_\circ(A^n B^n E^n)$,*

$$\left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left[\rho\right]\right\|_1 \leq \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_n^{l_c} \circ \cdots \circ \mathcal{M}_1^{l_c}\left[\rho\right]\right\|_1 + \sum_{j=1}^{n} \varepsilon_{\mathcal{M}_j^{l_c}}. \tag{7.3}$$

Proof. We first show that for the $n = 1$ case, we have

$$\left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_1\left[\rho\right]\right\|_1 \leq \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_1^{l_c}\left[\rho\right]\right\|_1 + \varepsilon_{\mathcal{M}_1^{l_c}},$$

as follows:

$$\begin{aligned}
&= \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_1\left[\rho\right]\right\|_1 \\
&= \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \left(\mathcal{M}_1 - \mathcal{M}_1^{l_c} + \mathcal{M}_1^{l_c}\right)\left[\rho\right]\right\|_1 \\
&\leq \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_1^{l_c}\left[\rho\right]\right\|_1 + \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \left(\mathcal{M}_1 - \mathcal{M}_1^{l_c}\right)\left[\rho\right]\right\|_1 && (7.4) \\
&\leq \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_1^{l_c}\left[\rho\right]\right\|_1 + \left\|\left(\mathcal{M}_1 - \mathcal{M}_1^{l_c}\right)\left[\rho\right]\right\|_1 && (7.5) \\
&\leq \left\|\left(\mathcal{KP} - \mathcal{KP}^{\text{ideal}}\right) \circ \mathcal{M}_1^{l_c}\left[\rho\right]\right\|_1 + \varepsilon_{\mathcal{M}_1^{l_c}}, && (7.6)
\end{aligned}$$

where Eq. (7.4) follows from the triangle inequality of the 1-norm, Eq. (7.5)) follows from the fact that the 1-norm is non-increasing under the action of channels, and Eq. (7.6)

follows from the assumption in the lemma statement, and the definition of the $\diamondsuit$-norm. The general case

$$\left\|\left(\mathcal{KP}-\mathcal{KP}^{\text{ideal}}\right)\circ\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1\left[\rho\right]\right\|_1\leq\left\|\left(\mathcal{KP}-\mathcal{KP}^{\text{ideal}}\right)\circ\mathcal{M}_n^{l_c}\circ\cdots\circ\mathcal{M}_1^{l_c}\left[\rho\right]\right\|_1+\sum_{j=1}^{n}\varepsilon_{\mathcal{M}_j^{l_c}}$$

follows by iterating the same argument n times, yielding the claimed result. □

A naive application of this result would be to fix $l_c = 0$, thereby reducing the entire analysis to the memoryless case studied previously. However, as noted in [33], the penalty to the security parameter grows linearly with the number of protocol rounds n. Crucially, each $\varepsilon_{\mathcal{M}_j^{l_c}}$ is a constant[2] determined by the physical device properties, and the chosen correlation length l_c. Consequently, for a fixed l_c, the total correlation penalty would eventually overwhelm the secrecy parameter for any sufficiently large n. A robust security proof must therefore treat the correlation length l_c as a tunable parameter, chosen as a function of the number of protocol rounds n to ensure the total secrecy penalty remains small. Thus, the central objective of the remainder of this chapter is to prove secrecy assuming a finite, non-zero correlation length l_c.

> **Technical aside 7.1** (Unbounded source correlations)**.** A very similar argument can be made for source correlations as well. Such an argument would need to use the triangle inequality on the state $\rho^{\text{prep}}_{A^nA'^n}$ prepared by Alice in Definition 3.3. This is formally presented in Ref. [105].

7.2 Protocol modification

Our analysis addresses a specific, physically-motivated class of detector correlations: those that are heralded by detection events. The measurement POVM for any round j is altered from its default state only if a detection event has occurred within the preceding memory window of l_c rounds. In the absence of such a detection, the POVM for round j remains unaffected. This model assumption is an approximation for the underlying physics for dead times and afterpulsing, which are triggered by detection events.

[2] In practice, this value can be tuned by changing the protocol repetition rate. Lower repetition rates would result in a lesser amount of correlations.

Notational aside 7.2. We denote the correlated POVM that measures the jth round by $\vec{\Gamma}_{k_{j-l_c}^{j-1}}$, where $k_{j-l_c}^{j-1}$ denotes the string of outcomes in the previous l_c rounds. Then the model assumption we make corresponds to the fact that the POVM $\vec{\Gamma}_{\mathbf{d_B},\boldsymbol{\eta}}$, described by the detection model with no correlations in Sections 2.2.5 and 2.2.6, corresponds to the case when the previous l_c rounds are all no-clicks.

Our approach requires a protocol modification in which Alice and Bob retain only the rounds where previous l_c rounds involved no-click events. All other rounds are 'rejected', i.e., thrown away. The idea is that after this postprocessing, the remaining rounds can be thought of as all being measured using uncorrelated POVMs. This postprocessing has a critical consequence for the security analysis. While correlations still exist within the protocol block (i.e., a detection event in a round dictates the whether future rounds are rejected), the form of these correlations is simplified. The correlation no longer depends on the *particular* detector(s) that recorded a detection outcome, rather it depends on whether *any* detector recorded a detection outcome. This idea was formalised specifically for EUR-based proofs in Ref. [21]. We take a different, proof-technique independent approach.

Notational aside 7.3. The correlated measurement channel for round j is denoted by $\mathcal{M}_j \in \mathcal{C}\left(B_j R_{j-l_c}^{j-1}, C_j R_{j-l_c}^{j}\right)$, where $R_{j-l_c}^{j-1} = R_{j-l_c} \dots R_{j-1}$ stores the classical data of previous round outcomes. The classical postprocessing is denoted by $\mathcal{CP}_j \in \mathcal{C}\left(C_j R_{j-l_c}^{j-1}, C_j R_{j-l_c}^{j-1}\right)$. If any of the previous l_c rounds resulted in a detection event, $\mathcal{CP}_j$ outputs $\perp$ into the register C_j, indicating that the round was rejected. The classical postprocessing always forwards the memory registers $R_{j-l_c}^{j-1}$ after reading them.
In our terminology, a round can be *rejected* in this manner due to the postprocessing $\mathcal{CP}$, but may also be *discarded* later based on its detection outcome — for instance, if it results in a no-detection event in a key generation round.

Definition 7.1 (Correlated postprocessed measurement)**.** We define the sequence of channels $\mathcal{CP}_n \circ \mathcal{M}_n \circ \cdots \circ \mathcal{CP}_1 \circ \mathcal{M}_1$ described above as the *correlated postprocessed measurement*.

7.3 Correlated noise channel

The key idea is to construct a correlated noise channel that performs the postprocessing so that the resulting measurements after the noise channel have no correlations. The correlated noise channel is then 'given' to Eve using Corollary 3.2 and Remark 3.4.

To build intuition, we first construct this channel for the idealised case where the uncorrelated POVM (i.e., the POVM following a no-click history) has no loss or dark counts. The extension to the case with loss and dark counts follows after. The construction is based on two key observations:

- For a round that is kept (i.e., preceded by no-clicks), the POVM is ideal and block-diagonal in photon number. Therefore, a non-destructive photon-number measurement can perfectly predict whether a detection will occur, revealing the necessary history information without altering the measurement statistics.
- For a round that is rejected (i.e., preceded by a click), its quantum state is irrelevant to the final key. We are therefore free to perform a full, destructive measurement on it to determine the detect/no-click information needed for subsequent rounds.

Lemma 7.2 ("Perfect" correlated noise channel)**.** *Let $\mathcal{CP}_n \circ \mathcal{M}_n \circ \cdots \circ \mathcal{CP}_1 \circ \mathcal{M}_1$ be the correlated postprocessed measurement, which outputs $\perp$ in round j if any preceding l_c round contained a detection outcome, as defined in Definition 7.1. We assume that the POVM $\vec{\Gamma} \subset \mathrm{Pos}(B)$ (corresponding to the case when the previous l_c rounds are all no-clicks) has no dark counts or loss. Let $B_\perp$ be a one-dimensional extension of B, and $\mathcal{M}^0 \in \mathcal{C}(B_\perp, C)$ be the uncorrelated measurement channel corresponding to the POVM $\vec{F} \subset \mathrm{Pos}(B_\perp)$ whose elements are*

$$\begin{aligned} F_i &= \Gamma_i \oplus 0 \qquad \forall i \\ F_\perp &= \mathbf{0} \oplus |\perp\rangle\langle\perp| , \end{aligned}$$

where $|\perp\rangle$ is a flag denoting that a round was rejected.

Then there exists a noise channel $\Phi_\mathrm{corr} \in \mathcal{C}(B^n, B_\perp^n)$ such that

$$\left(\mathcal{M}^0\right)^{\otimes n} \circ \Phi_\mathrm{corr} = \mathcal{CP}_n \circ \mathcal{M}_n \circ \cdots \circ \mathcal{CP}_1 \circ \mathcal{M}_1. \tag{7.7}$$

Proof. For simplicity, we demonstrate the construction for a correlation length l_c of 1. The extension to larger, finite correlation lengths is straightforward. The noise channel Φ_corr is constructed as a sequence of channels $\Phi_j \in \mathcal{C}\left(B_j R_{j-1}, B_{\perp j} R_j\right)$ acting on each round such that $\Phi_\mathrm{corr} = \Phi_n \circ \cdots \circ \Phi_1$. The operation of Φ_j depends on the memory register R_{j-1}, which stores whether the previous round resulted in a detection.

Round 1: The first round is never rejected. Φ_1 performs a QND photon-number measurement on the input state in B_1. Since the POVM $\vec{\Gamma}$ has no dark counts or loss,

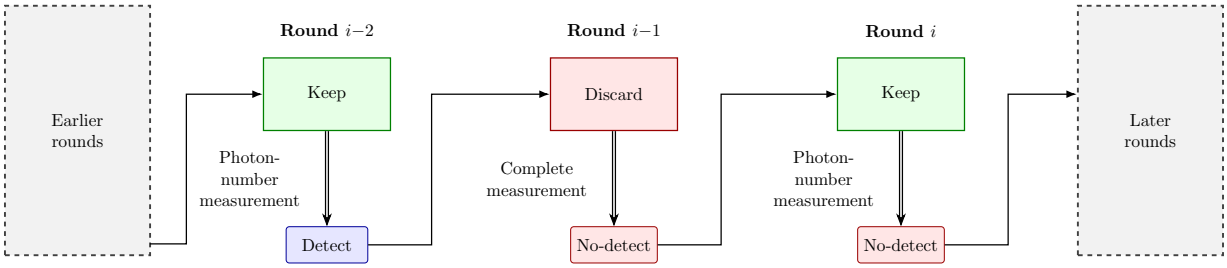


Figure 7.1: Illustration of the noise channel construction which determines whether a round will be rejected or not. The rounds that are not rejected are only measured using a photon-number measurement, which determines the detect vs no-detect outcome. This photon-number measurement does not change the measurement statistics, as the POVM is block-diagonal. The rounds that are rejected have their entire measurements completed in order to determine the detection event. ([5, Fig. 8])

a non-zero photon number perfectly heralds a future detection event. This detect/no-click information is stored in the classical register R_1, and the quantum state is passed to the output register $B_{\perp 1}$. The block-diagonal structure of the POVM ensures this QND measurement does not alter the measurement statistics.

Round $j \geq 2$: The channel's action depends on the memory R_{j-1}:

1. R_{j-1} = no-click: Φ_j operates identically to Φ_1, performing a QND photon-number measurement to create the memory register R_j while passing the state to $B_{\perp j}$.
2. R_{j-1} = detection: Φ_j performs performs a full, destructive measurement on the input state in B_j using the appropriate correlated POVM. The detect/no-click information is stored in the memory register R_j, while the flag $|\perp\rangle\langle\perp|$ is output to $B_{\perp j}$.

This construction (depicted in Fig. 7.1) correctly implements the post-selection. If the real protocol would reject round j, the noise channel outputs the flag state $|\perp\rangle\langle\perp|$, which yields the rejection outcome $\perp$ when measured by the POVM $\vec{F}$. If the real protocol keeps round j, the noise channel performs only a QND measurement that preserves the statistics for the final ideal measurement. This completes the construction. □

This lemma assumes that the uncorrelated POVM $\vec{\Gamma}$ had no dark counts or loss. However, this is not a fundamental limitation. The extension to the case with dark counts and loss is straightforward — we can use the noise channels constructed in the rest of this work before the photon-number measurement that determines detect/no-click.

Corollary 7.1 (Correlated noise channel)**.** *Let $\mathcal{CP}_n \circ \mathcal{M}_n \circ \cdots \circ \mathcal{CP}_1 \circ \mathcal{M}_1$ be the correlated postprocessed measurement, which outputs $\perp$ in round j if any preceding l_c round contained a detection outcome, as defined in Definition 7.1. Let $\vec{\Gamma}_{\mathbf{d_B},\boldsymbol{\eta}} \subset \mathrm{Pos}(B)$ be the POVM corresponding to the case when the previous l_c rounds are all no-clicks. Further, let*

$$\vec{\Gamma}_{\mathbf{d_B},\boldsymbol{\eta}} - (1-q)\vec{\Gamma} \geq 0, \tag{7.8}$$

for some $q \in [0,1]$, where $\vec{\Gamma}$ is the POVM with no dark counts or loss. Let $\mathcal{M}^0 \in \mathcal{C}(Q,C)$ be the ideal measurement channel corresponding to the POVM $\vec{F} \subset \mathrm{Pos}(Q)$ whose elements are

$$\begin{aligned} F_i &= \Gamma_i \oplus |i\rangle\langle i| \oplus 0 \qquad \forall i \\ F_\perp &= \mathbf{0} \oplus |\perp\rangle\langle\perp|, \end{aligned}$$

where $|\perp\rangle$ is a flag denoting that a round was rejected, $|i\rangle\langle i|$ are the flags corresponding to outcome i, and Γ_i is the POVM corresponding to outcome i with no dark counts or loss. Here, $\mathcal{H}_Q = \mathcal{H}_{B_\perp} \oplus \mathcal{H}_F$.

Then there exists a noise channel $\Phi_{\mathrm{corr}} \in \mathcal{C}(B^n, Q^n)$ such that the following equations hold

$$\begin{aligned} \left(\mathcal{M}^0\right)^{\otimes n} \circ \Phi_{\mathrm{corr}} &= \mathcal{CP}_n \circ \mathcal{M}_n \circ \cdots \circ \mathcal{CP}_1 \circ \mathcal{M}_1 \\ \Phi^\dagger_{\mathrm{corr}}[\Pi_{F_j} \otimes \mathbb{I}] &\leq q\mathbb{I}_{B_j} \otimes \mathbb{I}, \end{aligned} \tag{7.9}$$

for all rounds j.

Proof Idea. The proof follows the same sequential construction as in Lemma 7.2. The only modification occurs in the 'no-click history' case. Before performing the QND photon-number measurement, the independent noise channel from Theorem 4.1 is first applied. This initial channel maps the real, imperfect POVM to a flagged, ideal POVM, upon which the subsequent detect/no-click measurement can be performed. The analysis of the rejected rounds remains unchanged. □

Remark 7.1 (Limitation on correlated noise channel)**.** *Corollary 7.1 can be modified by using the different noise channels in Chapter 4. Each contains a different weight in the flag space. However, note that the proof of Corollary 7.1 crucially required that the ideal POVM had no loss and no dark counts. Thus, detector correlations in protocols such as the one considered in Section 5.5 with missing detectors cannot be analysed with the tools developed here, and require more sophisticated analyses.*

Technical aside 7.2 ((Almost) proof technique independent correlated noise channel)**.** The reduction in Lemma 7.2 is truly proof-technique independent. However, Corollary 7.1 is *technically* not proof-technique independent. As noted in Technical aside 5.2, the noise channel must be applied *after* the postselection theorem. However, the postselection theorem cannot be used on a correlated detection setup. Thus, further work is needed to apply Corollary 7.1 to proofs using the postselection technique.

7.4 Future directions

In this chapter, we have developed a general technique to address detector correlations for threshold detection setups. This technique is largely proof-technique independent. The technique follows in two steps. First, the methods in Section 7.1 are used to truncate the correlations to a finite length, at a cost to the security parameter. Then, in Section 7.2 we make use of a protocol modification which rejects rounds following detection events, upto the correlation length, which facilitates the analysis in Section 7.3.

However, if the memory effect is only perturbative, one might expect such a protocol modification to result in overly pessimistic key rates. A more optimal analysis would not discard these rounds, but would instead quantify and pay a precise penalty for the correlations they introduce.

There are two promising avenues for developing such a refined analysis. The first is to extend the noise channel formalism from Chapter 4. Thus, a more sophisticated, correlated noise channel could be designed to map the affected rounds to an orthogonal flag space rather than rejecting them outright.

A second, fundamentally different approach would be to leverage the structure of EAT-based proofs. The EAT framework seems naturally suited to handling memory, particularly those conditioned on publicly available information such as the locations of detection events. A recent sketch using this logic [26, Section V.B.] suggests that this could be a viable path toward a tighter security proof that can more accurately account for the cost of heralded correlations.

Another dimension for future work lies in applying our general analysis to specific, empirically-validated physical models of detector memory. For instance, the physical mechanisms themselves, such as recovery times, are fundamentally characterised by a physical timescale (e.g., nanoseconds). In contrast, our security analysis is formulated in terms of

protocol rounds. Performing such a detailed analysis would involve a trade-off between three tunable parameters.

The protocol's repetition rate is the first tunable parameter that allows us to formulate the time-based mechanisms for detector memory in terms of number protocol rounds. Consequently, the effective correlation length is not a fixed property of the detector alone, but is also a function of the chosen operational rate. A high repetition rate magnifies the reach of a memory effect in terms of rounds, making the correlations more pronounced in the analysis, but also provides the potential to obtain a larger key rate per unit time.

The correlation length is another parameter, which can be traded off with the security parameter. A shorter correlation length minimises the amount of data discarded by post-selection after each detection event, but it incurs a larger security penalty from the truncation described in Section 7.1. Conversely, a longer correlation length reduces the truncation penalty to a negligible level, but at the cost of discarding more data and thus lowering the key rate.

This optimisation would need to be studied before the results of this chapter can be applied to maximise the achievable performance in an experimental QKD system. Thus, such an analysis is a crucial next step for a complete treatment of correlated detectors.

Chapter 8

Conclusion and outlook

> "So long, and thanks for all the fish."
>
> — Douglas Adams, *The Hitchhiker's Guide to the Galaxy*

The implementation security of QKD protocols requires proofs that are robust to imperfect characterisation, and side channel attacks. In this work, we systematically address such imperfections in threshold detection setups.

The core contribution of this work is the noise channel framework, developed in Chapter 4, which provides a modular treatment of detector imperfections that is independent of the specific QKD security proof technique. We demonstrate the versatility of this framework by explicitly applying it to the postselection technique [10, 11] in Chapter 5, and to phase error estimation [8, 7] in Chapter 6. As a significant result stemming from the first application, we also substantially extend the applicability of the postselection technique to a broader class of optical protocols and improve its performance by deriving tighter finite-size bounds, leading to significantly higher key rates.

The versatility of the framework extends beyond these two examples, notably to EAT-based proof techniques [12, 13, 14]. For passive protocols, the application is structurally analogous to the analysis in Section 5.5, and we expect it to obtain comparably tight key rates. Further, for active protocols, as noted in Technical aside 6.3, our framework provides a method to resolve a key technical challenge: the infinite-dimensional optimisation

problem that often limits such proofs.

A surprising result of this work is the significant difference in tolerance to imperfections observed between the two main applications of our framework. The analysis of the passive protocol using the postselection technique in Chapter 5 demonstrates a remarkably high robustness, tolerating parameter deviations exceeding 30%. In contrast, the phase error estimation analysis for the active protocol in Chapter 6 shows a significantly lower tolerance.

We do not fully understand the precise origin of this discrepancy, as the two analyses differ in their proof techniques, the protocol, and their methods for modelling imperfections. We summarise these key differences in Table 8.1. We leave it to future work to form a better understanding of the techniques developed here by applying them to a variety of protocols and comparing their effects across proof techniques.

Proof Technique	Postselection technique + numerical IID key rates	Phase error estimation + analytical security formula
Protocol	Highly asymmetric, time-bin encoded protocol with passive basis choice	Standard polarisation-encoded BB84 protocol with active basis choice
Modelling imperfections	Detector efficiency imperfections absorbed into passive beam splitter and pulled into channel	Only common loss pulled into channel

Table 8.1: Comparison of the two security analyses with noise channels.

In Chapter 4, we also describe the application of noise channels to address the security of multimode detection setups. Specifically, we detail the application for an independent multimode model. While we conjecture that a similar analysis would apply for more general models, this more complete analysis is left to future work.

Moreover, the framework is not limited to IID imperfections. In Chapter 7, we demonstrate how the noise channel concept can be generalised to prove security for detection setups with memory effects such as afterpulsing and dead times. However, translating these theoretical results to experimental scenarios requires further work. In particular, multiple tunable parameters such as protocol repetition rate and effective correlation length whose trade-off must be studied and optimised using physical models of correlations to achieve optimal key rates.

Our modular analysis is naturally compatible with proofs incorporating source imperfections [15, 17, 16], which together constitute a robust finite-size security proof. These

proofs assume that the state prepared, and the detection setup has some model parameters that are in some given ranges. However, such a guarantee is impossible to *exactly* achieve in practice. A more realistic expectation of characterisation protocols is that the model parameters lie in some given range *with high probability*. This failure probability for characterisation can be incorporated into the QKD security parameter [106]. Thus, an important next step toward implementation security is to *rigorously* characterise these parameters.

The analysis in this thesis has focused on the application of the tools developed here to threshold detection setups. Continuous-variable (CV) QKD detection setups do not possess the block-diagonal structure required for a lot of our analysis, and the noise models in such detection setups differ from the models considered here. However, we develop a general theorem in Section 3.4.4 to address some technical complications that arise from infinite-dimensional systems. This is particularly useful for CV QKD, where no known squashing map exists. Further, we believe that our abstract noise channel construction in Theorem 4.1 can be applied to CV QKD detection setups. A rigorous investigation into such an application remains a promising direction for future work.

In conclusion, this thesis has introduced a structured and powerful framework for analysing detector imperfections in QKD, and has demonstrated its versatility by applying it across different proof techniques for threshold detection setups. We also identify multiple avenues for future work — both in improving the framework developed here, and in the application to experimental setups.

References

[1] Shlok Nahar. Decoy-state quantum key distribution with arbitrary phase mixtures and phase correlations. Master's thesis, University of Waterloo, 2022.

[2] 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. *arXiv:2502.10340*, 2025.

[3] 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.

[4] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure quantum key distribution over 421 km of optical fiber, July 2018. arXiv:1807.03222.

[5] Devashish Tupkary, Shlok Nahar, Pulkit Sinha, and Norbert Lütkenhaus. Phase error rate estimation in qkd with imperfect detectors. *Quantum*, 9:1937, 2025.

[6] 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, December 1984. IEEE.

[7] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, April 2009.

[8] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017.

[9] Marco Tomamichel and Renato Renner. Uncertainty Relation for Smooth Entropies. *Physical Review Letters*, 106(11):110506, March 2011.

[10] Matthias Christandl, Robert Koenig, and Renato Renner. Post-selection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2):020504, January 2009. arXiv:0809.3019 [quant-ph].

[11] 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, 2024.

[12] Frédéric Dupuis, Omar Fawzi, and Renato Renner. Entropy Accumulation. *Communications in Mathematical Physics*, 379(3):867–913, November 2020.

[13] Tony Metger and Renato Renner. Security of quantum key distribution from generalised entropy accumulation. *Nature Communications*, 14(1):5272, August 2023.

[14] Amir Arqand and Ernest Y.-Z. Tan. Marginal-constrained entropy accumulation theorem, April 2025. arXiv:2502.02563 [quant-ph].

[15] Guillermo Currás-Lorenzo, Margarida Pereira, Go Kato, Marcos Curty, and Kiyoshi Tamaki. Security of high-speed quantum key distribution with imperfect sources. *arXiv e-prints*, pages arXiv–2305, 2023.

[16] Jia-Xuan Li, Yang-Guang Shan, Rong Wang, Feng-Yu Lu, Zhen-Qiang Yin, Shuang Wang, Wei Chen, De-Yong He, Guang-Can Guo, and Zheng-Fu Han. Secure quantum key distribution against correlated leakage source. *arXiv:2507.11251*, 2025.

[17] Lars Kamin, John Burniston, and Ernest Y-Z Tan. Rényi security framework against coherent attacks applied to decoy-state QKD. *arXiv:2504.12248*, 2025.

[18] Chi-Hang Fred Fung, Kiyoshi Tamaki, Bing Qi, Hoi-Kwong Lo, and Xiongfeng Ma. Security proof of quantum key distribution with detection efficiency mismatch, October 2008. arXiv:0802.3788 [quant-ph].

[19] L. Lydersen and J. Skaar. Security of quantum key distribution with bit and basis dependent detector flaws. (arXiv:0807.0767), January 2010.

[20] Øystein Marøy, Lars Lydersen, and Johannes Skaar. Security of quantum key distribution with arbitrary individual imperfections. *Physical Review A*, 82(3):032337, September 2010.

[21] Zhiyao Wang, Devashish Tupkary, and Shlok Nahar. Phase error estimation for passive detection setups with imperfections and memory effects. *arXiv:2508.21486*, 2025.

[22] 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. *Physical Review Applied*, 23(4):044011, 2025.

[23] Ashutosh Marwah and Frédéric Dupuis. Proving security of BB84 under source correlations, February 2024. arXiv:2402.12346 [quant-ph].

[24] Amir Arqand, Tony Metger, and Ernest Y-Z Tan. Mutual information chain rules for security proofs robust against device imperfections. *arXiv:2407.20396*, 2024.

[25] Devashish Tupkary, Shlok Nahar, Amir Arqand, Ernest Y-Z Tan, and Norbert Lütkenhaus. A complete, self-contained security proof for decoy-state BB84, in preparation, 2025.

[26] Shlok Nahar, Devashish Tupkary, and Norbert Lütkenhaus. Imperfect detectors for adversarial tasks with applications to quantum key distribution. *arXiv:2503.06328*, 2025.

[27] 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 2.0.2, December 2024.

[28] Daniel F Walls and Gerard J Milburn. *Quantum optics*. Springer Science & Business Media, 2007.

[29] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge university press, 2005.

[30] S.J. van Enk. Coherent states, beam splitters and photons. https://pages.uoregon.edu/svanenk/solutions/NotesBS.pdf, September 2011.

[31] Thu Ha Dao, Francesco Amanti, Greta Andrini, Fabrizio Armani, Fabrizio Barbato, Vittorio Bellani, Vincenzo Bonaiuto, Simone Cammarata, Matteo Campostrini,

Samuele Cornia, et al. Single-photon detectors for quantum integrated photonics. *Photonics*, 12(1):8, 2024.

[32] Alan Migdall, Sergey V Polyakov, Jingyun Fan, and Joshua C Bienfang. *Single-photon generation and detection: physics and applications*. Academic Press, 2013.

[33] Varun Narasimhachar. Study of realistic devices for quantum key-distribution. Master's thesis, University of Waterloo, 2011.

[34] Jan Krause and Nino Walenta. Exponential-recovery model for free-running SPADs with capacity-induced dead-time imperfections, July 2025. arXiv:2507.10361 [quant-ph].

[35] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *arXiv preprint quant-ph/0512080*, 2005.

[36] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A—Atomic, Molecular, and Optical Physics*, 74(2):022313, 2006.

[37] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *The collected works of Wassily Hoeffding*, pages 409–426, 1994.

[38] Thomas D Ahle. Asymptotic tail bound and applications, 2017.

[39] Robert J Serfling. Probability inequalities for the sum in sampling without replacement. *The Annals of Statistics*, pages 39–48, 1974.

[40] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3(1):634, 2012.

[41] 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.

[42] Christopher Portmann. Key Recycling in Authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, July 2014. Conference Name: IEEE Transactions on Information Theory.

[43] Michael Ben-Or and Dominic Mayers. General security definition and composability for quantum & classical protocols. *arXiv preprint quant-ph/0409062*, 2004.

[44] Dominique Unruh. Simulatable security for quantum protocols. *arXiv preprint quant-ph/0409125*, 2004.

[45] U. Maurer and R. Renner. Abstract Cryptography. 2011.

[46] Ueli Maurer. Constructive Cryptography – A New Paradigm for Security Definitions and Proofs. In Sebastian Mödersheim and Catuscia Palamidessi, editors, *Theory of Security and Applications*, pages 33–56, Berlin, Heidelberg, 2012. Springer.

[47] Ueli Maurer and Renato Renner. From Indifferentiability to Constructive Cryptography (and Back), 2016. Publication info: Published by the IACR in TCC 2016.

[48] Christian Matt, Ueli Maurer, Christopher Portmann, Renato Renner, and Björn Tackmann. Toward an algebraic theory of systems. *Theoretical Computer Science*, 747:1–25, November 2018.

[49] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94(2):025008, June 2022.

[50] Anne Broadbent and Martti Karvonen. Categorical composable cryptography: extended version. *Logical Methods in Computer Science*, Volume 19, Issue 4:9979, December 2023. arXiv:2208.13232 [cs].

[51] Michael Ben-Or, Michał Horodecki, Debbie W Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference*, pages 386–406. Springer, 2005.

[52] Renato Renner. Security of quantum key distribution, 2006.

[53] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Transforming quantum operations: quantum supermaps. *EPL (Europhysics Letters)*, 83(3):30004, August 2008. arXiv:0804.0180 [quant-ph].

[54] 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. Conference Name: IEEE Transactions on Information Theory.

[55] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, February 1992.

[56] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as a Precondition for Secure Quantum Key Distribution. *Physical Review Letters*, 92(21):217903, May 2004.

[57] 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.

[58] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General Paradigm for Distilling Classical Key From Quantum States. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. Conference Name: IEEE Transactions on Information Theory.

[59] Won-Young Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*, 91(5), 2003.

[60] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[61] Xiang-Bin Wang. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Physical Review Letters*, 94(23), 2005.

[62] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices, September 2004. arXiv:quant-ph/0212066.

[63] 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.

[64] Xiang-Bin Wang, Xiao-Long Hu, and Zong-Wen Yu. Practical long-distance side-channel-free quantum key distribution. *Physical Review Applied*, 12(5):054034, 2019.

[65] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Physical Review A*, 78(3):032302, September 2008.

[66] Toyohiro Tsurumaru. Squash operator and symmetry. *Physical Review A*, 81(1):012328, January 2010.

[67] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing Models for Optical Measurements in Quantum Communication. *Physical Review Letters*, 101(9):093601, August 2008.

[68] 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.

[69] 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.

[70] 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.

[71] Nicky Kai Hong Li and Norbert Lütkenhaus. Improving key rates of the unbalanced phase-encoded BB84 protocol using the flag-state squashing model. *Physical Review Research*, 2(4):043172, November 2020.

[72] Lars Kamin and Norbert Lütkenhaus. Improved Decoy-state and Flag-state Squashing Methods, June 2024. arXiv:2405.05069 [quant-ph].

[73] Norbert Lütkenhaus. Estimates for practical quantum cryptography. *Physical Review A*, 59(5):3301–3319, May 1999.

[74] Yanbao Zhang and Norbert Lütkenhaus. Entanglement verification with detection-efficiency mismatch. *Physical Review A*, 95(4):042319, April 2017.

[75] Masato Koashi. Efficient quantum key distribution with practical sources and detectors, September 2006. arXiv:quant-ph/0609180.

[76] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, 461(2053):207–235, 2005.

[77] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77, July 2018. arXiv:1710.05511 [quant-ph].

[78] Darius Bunandar, Luke C. G. Govia, Hari Krovi, and Dirk Englund. Numerical finite-key analysis of quantum key distribution. *npj Quantum Information*, 6(1):1–12, December 2020.

[79] 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.

[80] Omar Fawzi and Renato Renner. Quantum Conditional Mutual Information and Approximate Markov Chains. *Communications in Mathematical Physics*, 340(2):575–611, December 2015.

[81] Masahito Hayashi. Universal coding for classical-quantum channel. *Communications in Mathematical Physics*, 289(3):1087–1098, 2009.

[82] Masahito Hayashi and Marco Tomamichel. Correlation detection and an operational interpretation of the rényi mutual information. *Journal of Mathematical Physics*, 57(10), 2016.

[83] Ke Li and Dong Yang. Reliability function of classical-quantum channels. *Physical Review Letters*, 134(1):010802, 2025.

[84] 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].

[85] Takaya Matsuura, Shinichiro Yamano, Yui Kuramochi, Toshihiko Sasaki, and Masato Koashi. Tight concentration inequalities for quantum adversarial setups exploiting permutation symmetry. *Quantum*, 8:1540, November 2024.

[86] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical review letters*, 90(16):167904, 2003.

[87] Bruno De Finetti. La prévision: ses lois logiques, ses sources subjectives. In *Annales de l'institut Henri Poincaré*, volume 7, pages 1–68, 1937.

[88] Robin L Hudson and Graham R Moody. Locally normal symmetric states and an analogue of de finetti's theorem. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 33(4):343–351, 1976.

[89] Normand J. Beaudry. Assumptions in Quantum Cryptography, May 2015. arXiv:1505.02792 [quant-ph] version: 1.

[90] Lars Kamin, Devashish Tupkary, and Norbert Lütkenhaus. Improved finite-size effects in QKD protocols with applications to decoy-state QKD. *arXiv:2502.05382*, 2025.

[91] 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.

[92] 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. *PRX Quantum*, 6(2):020342, 2025.

[93] Takaya Matsuura, Shinichiro Yamano, Yui Kuramochi, Toshihiko Sasaki, and Masato Koashi. Asymptotically tight security analysis of quantum key distribution based on universal source compression, April 2025. arXiv:2504.07356 [quant-ph].

[94] Hongyi Zhou, Toshihiko Sasaki, and Masato Koashi. Numerical method for finite-size security analysis of quantum key distribution. *Physical Review Research*, 4(3):033126, August 2022.

[95] 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.

[96] Toyohiro Tsurumaru, Akihiro Mizutani, and Toshihiko Sasaki. Security loophole in error verification in quantum key distribution. *arXiv:2507.21416*, 2025.

[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.

[98] Xoel Sixto, Álvaro Navarrete, Margarida Pereira, Guillermo Currás-Lorenzo, Kiyoshi Tamaki, and Marcos Curty. Quantum key distribution with imperfectly isolated devices, February 2025. arXiv:2411.13948 [quant-ph].

[99] Víctor Zapatero, Álvaro Navarrete, Kiyoshi Tamaki, and Marcos Curty. Security of quantum key distribution with intensity correlations. *Quantum*, 5:602, 2021.

[100] Guillermo Currás-Lorenzo, Shlok Nahar, Norbert Lütkenhaus, Kiyoshi Tamaki, and Marcos Curty. Security of quantum key distribution with imperfect phase randomisation. *Quantum Science and Technology*, 9(1):015025, 2023.

[101] Guillermo Currás-Lorenzo, Margarida Pereira, Shlok Nahar, and Devashish Tupkary. Security of quantum key distribution with source and detector imperfections through phase-error estimation. *arXiv:2507.03549*, 2025.

[102] Iris Cusini, Davide Berretta, Enrico Conca, Alfonso Incoronato, Francesca Madonini, Arianna Adelaide Maurina, Chiara Nonne, Simone Riccardo, and Federica Villa. Historical perspectives, state of art and research trends of single photon avalanche diodes and their applications (part 1: Single pixels). *Frontiers in Physics*, 10:906675, 2022.

[103] Sergio Cova, Andrea Lacaita, and Giancarlo Ripamonti. Trapping phenomena in avalanche photodiodes on nanosecond scale. *IEEE Electron device letters*, 12(12):685–687, 1991.

[104] Abdul Waris Ziarkash, Siddarth Koduru Joshi, Mario Stipčević, and Rupert Ursin. Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors. *Scientific reports*, 8(1):1–8, 2018.

[105] Margarida Pereira, Guillermo Currás-Lorenzo, Akihiro Mizutani, Davide Rusca, Marcos Curty, and Kiyoshi Tamaki. Quantum key distribution with unbounded pulse correlations. *Quantum Science and Technology*, 10(1):015001, 2024.

[106] Ernest Y-Z Tan and Shlok Nahar. Incorporating device characterization into security proofs. *arXiv:2508.15383*, 2025.

[107] Israel Gohberg, Seymour Goldberg, and Marius A Kaashoek. *Classes of linear operators*, volume I. Birkhäuser, 2013.

[108] Paula Belzig. Studying stabilizer de finetti theorems and possible applications in quantum information processing. *arXiv:2403.10592*, 2024.

[109] David Gross, Sepehr Nezami, and Michael Walter. Schur–Weyl duality for the Clifford group with applications: Property testing, a robust hudson theorem, and de finetti representations. *Communications in Mathematical Physics*, 385(3):1325–1393, 2021.

[110] Aram W Harrow. Applications of coherent classical communication and the schur transform to quantum information theory. *arXiv preprint quant-ph/0512255*, 2005.

[111] Matthias Christandl. The structure of bipartite quantum states-insights from group theory and cryptography. *arXiv preprint quant-ph/0604183*, 2006.

[112] Joseph M Landsberg. *Tensors: geometry and applications: geometry and applications*, volume 128. American Mathematical Soc., 2011.

pun

APPENDICES

Appendix A

Extension to infinite-dimensions

First we define some notation that will be used through this appendix. We denote the set of "trace-class" operators $\mathcal{T}(\mathcal{H}_\infty)$ which is the subset of linear operators acting on $\mathcal{H}_\infty$ which have finite trace. In particular, note that density operators are a subset of trace-class operators, i.e., $\mathrm{S}_\circ(\mathcal{H}_\infty) \subset \mathcal{T}(\mathcal{H}_\infty)$. Let $\Phi : \mathcal{T}(\mathcal{H}_\infty) \to \mathcal{T}(\mathcal{H}_\infty)$ be a linear map on the set of trace-class operators acting on $\mathcal{H}_\infty$. We say Φ is bounded if $\|\Phi\|_{1\to 1} \coloneqq \sup_{X\in\mathcal{T}(\mathcal{H}_\infty)} \frac{\Phi(X)}{\|X\|_1} < \infty$. In particular, note that channels, and differences of channels are examples of such bounded linear maps.

Let $\{\Pi_d\}_{d\in\mathbb{N}} \subset \mathrm{Pos}(\mathcal{H}_\infty)$ be a set of nested, finite-dimensional projectors such that $\overline{\bigcup_{d\in\mathbb{N}} \mathrm{range}(\Pi_d)} = \mathcal{H}_\infty$. Here, $\overline{X}$ denotes the closure of a set X, $\mathrm{range}(\Pi_d)$ denotes the range of Π_d, and by "nested" we mean that $\mathrm{range}(\Pi_d) \subset \mathrm{range}(\Pi_{d'})$ for all $d \leq d'$.

Definition A.1 (Projection channels)**.** Let $\{\Pi_d\}_{d\in\mathbb{N}} \subset \mathrm{Pos}(\mathcal{H}_\infty)$ be a set of projectors. Define the projection channels $\mathrm{P}_d : \mathcal{T}(\mathcal{H}_\infty) \to \mathcal{T}(\mathcal{H}_\infty \oplus \mathbb{C})$ corresponding to the set of projectors $\{\Pi_d\}_{d\in\mathbb{N}}$ as

$$\mathrm{P}_d[X] = \Pi_d X \Pi_d + (1 - \mathrm{Tr}[\Pi_d X])\ |\mathrm{flag}\rangle\langle\mathrm{flag}|,$$

where $|\mathrm{flag}\rangle$ is orthogonal to $\mathcal{H}_\infty$.

It is easy to verify that these projection channels are indeed completely positive and trace-preserving.

Notational aside A.1 (Abuse!)**.** There are some comments to be made at this point regarding a minor abuse of notation we shall use. At various points in what follows, we shall take channels (such as the protocol channel $\mathcal{E}_{\mathrm{QKD}}^{(l)}$ and attack channel $\mathcal{A}$) that are defined on $\mathcal{T}(\mathcal{H}_\infty)$, and apply them on some output state of P_d, which would be finite-dimensional. In each such case, we implicitly extend the channels by pinching across the decomposition $\mathcal{H}_\infty \oplus \mathrm{span}(|\mathrm{flag}\rangle)$ and acting as the identity on the flag block as follows:

$$\begin{aligned} |\mathrm{flag}\rangle\langle v| &\mapsto 0 \\ |v\rangle\langle \mathrm{flag}| &\mapsto 0 \\ |\mathrm{flag}\rangle\langle \mathrm{flag}| &\mapsto |\mathrm{flag}\rangle\langle \mathrm{flag}|\,, \end{aligned}$$

for any $|v\rangle \in \mathcal{H}_\infty$. Additionally, we might write P_d as acting on some finite-dimensional space $\mathbb{C}^{d'}$. In such cases, we implicitly interpret $\mathbb{C}^{d'}$ as embedded in $\mathcal{H}_\infty$.

Note that any trace-class operator $\rho \in \mathcal{T}(\mathcal{H}_\infty)$ can be approximated by its finite projections [107, Theorem 4.3], i.e.,

$$\lim_{d\to\infty} \Pi_d \rho \Pi_d \xrightarrow{\|\cdot\|_1} \rho. \tag{A.1}$$

Abusing notation similarly as in Notational aside A.1, we observe that Eq. (A.1) implies that

$$\lim_{d\to\infty} \mathrm{P}_d[\rho] \xrightarrow{\|\cdot\|_1} \rho, \tag{A.2}$$

where ρ is understood to be embedded in $\mathcal{T}(\mathcal{H}_\infty \oplus \mathbb{C})$. This gives us the following lemma.

Lemma A.1. *Let $\{\Pi_d\}_{d\in\mathbb{N}} \subset \mathrm{Pos}(\mathcal{H}_\infty)$ be any set of nested, finite-dimensional projectors such that $\overline{\bigcup_{d\in\mathbb{N}} \mathrm{range}(\Pi_d)} = \mathcal{H}_\infty$, and $\{\mathrm{P}_d\}_{d\in\mathbb{N}}$ be the set of projection channels corresponding to these projectors (as defined in Definition A.1). Then,*

$$\lim_{d\to\infty} \|\Phi \circ \mathrm{P}_d \circ \Psi[\sigma]\|_1 = \|\Phi \circ \Psi[\sigma]\|_1, \tag{A.3}$$

for any trace-class operator $\sigma \in \mathcal{T}(\mathcal{H}_\infty)$, and any bounded linear maps Φ,$\Psi : \mathcal{T}(\mathcal{H}_\infty) \to \mathcal{T}(\mathcal{H}_\infty)$.

Proof. First we remark that

$$\lim_{d\to\infty} \|\Phi \circ (\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma]\|_1 \leq \lim_{d\to\infty} \|\Phi\|_{1\to 1} \|(\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma]\|_1 = 0, \tag{A.4}$$

which follows from the boundedness of Φ, and Eq. (A.2). The rest of the proof follows by using Eq. (A.4) with the triangle inequality of $\|\cdot\|_1$ to upper and lower bound $\lim_{d\to\infty} \|\Phi \circ \mathrm{P}_d \circ \Psi[\sigma]\|_1$ by $\|\Phi \circ \Psi[\sigma]\|_1$, along with the sandwich theorem[1]. First, we lower bound as follows

$$\begin{aligned}
\lim_{d\to\infty} \|\Phi \circ \mathrm{P}_d \circ \Psi[\sigma]\|_1 &= \lim_{d\to\infty} \|\Phi \circ (\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma] - \Phi \circ \Psi[\sigma]\|_1 && \text{(A.5)}\\
&\geq \lim_{d\to\infty} \Big| \; \|\Phi \circ (\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma]\|_1 - \|\Phi \circ \Psi[\sigma]\|_1 \; \Big| && \text{(A.6)}\\
&= \Big| \lim_{d\to\infty} \|\Phi \circ (\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma]\|_1 - \|\Phi \circ \Psi[\sigma]\|_1 \Big| && \text{(A.7)}\\
&= \|\Phi \circ \Psi[\sigma]\|_1, && \text{(A.8)}
\end{aligned}$$

where Eq. (A.6) is the (reverse) triangle inequality of the 1-norm, and Eq. (A.8) follows from Eq. (A.4). Similarly, we upper bound as follows

$$\begin{aligned}
\lim_{d\to\infty} \|\Phi \circ \mathrm{P}_d \circ \Psi[\sigma]\|_1 &= \lim_{d\to\infty} \|\Phi \circ (\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma] - \Phi \circ \Psi[\sigma]\|_1 && \text{(A.9)}\\
&\leq \lim_{d\to\infty} \|\Phi \circ (\mathrm{id} - \mathrm{P}_d) \circ \Psi[\sigma]\|_1 + \|\Phi \circ \Psi[\sigma]\|_1 && \text{(A.10)}\\
&= \|\Phi \circ \Psi[\sigma]\|_1, && \text{(A.11)}
\end{aligned}$$

where Eq. (A.10) is the triangle inequality of the 1-norm Eq. (A.11) follows from Eq. (A.4). Thus, using the sandwich theorem, we obtain Eq. (A.3). □

We will now use Lemma A.1 in the QKD secrecy statement. Recall that from the security definition in Definition 3.3, we wish to find an upper bound $\varepsilon_{\mathrm{sec}}$ on

$$\sup_{\mathcal{A}\in\mathcal{C}(A'^n, B^n E^n)} \left\| \left(\mathcal{E}^{(l)}_{\mathrm{QKD}} - \mathcal{E}^{(l),\mathrm{ideal}}_{\mathrm{QKD}} \right) \circ \mathcal{A}\left[(\rho^{\mathrm{prep}}_{AA'})^{\otimes n} \right] \right\|_1 \leq \varepsilon_{\mathrm{sec}}.$$

for a QKD protocol $\left\{ \mathcal{E}^{(l)}_{\mathrm{QKD}}, (\rho^{\mathrm{prep}}_{AA'})^{\otimes n} \right\}$.

We now prove the main result of this section.

Theorem A.1. *Let $\{\Pi_d\}_{d\in\mathbb{N}} \subset \mathrm{Pos}(\mathcal{H}_\infty)$ be any set of nested, finite-dimensional projectors such that $\overline{\bigcup_{d\in\mathbb{N}} \mathrm{range}(\Pi_d)} = \mathcal{H}_\infty$, and $\{\mathrm{P}_d\}_{d\in\mathbb{N}}$ be the set of projection channels*

[1] The sandwich theorem states that if a function is bounded above and below by two functions with the same limit, then it shares that limit.

corresponding to these projectors (as defined in Definition A.1). Given a QKD protocol $\left\{\mathcal{E}_{\mathrm{QKD}}^{(l)}, (\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right\}$*, let us define*

$$\varepsilon_{\mathrm{sec}}(\mathcal{A}) \coloneqq \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}\right) \circ \mathcal{A}\left[(\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right] \right\|_1,$$

and suppose $\lim_{d\to\infty} \varepsilon_{\mathrm{sec}}^{(d)}(\mathcal{A})$ *exists, where*

$$\varepsilon_{\mathrm{sec}}^{(d)}(\mathcal{A}) \coloneqq \left\| \left(\mathcal{E}_{\mathrm{QKD}}^{(l)} - \mathcal{E}_{\mathrm{QKD}}^{(l),\mathrm{ideal}}\right) \circ \mathrm{P}_d \circ \mathcal{A}\left[(\rho_{AA'}^{\mathrm{prep}})^{\otimes n}\right] \right\|_1.$$

Then,

$$\sup_{\mathcal{A}\in\mathbb{A}} \varepsilon_{\mathrm{sec}}(\mathcal{A}) \leq \lim_{d\to\infty} \sup_{\mathcal{A}\in\mathbb{A}} \varepsilon_{\mathrm{sec}}^{(d)}(\mathcal{A}),$$

where the suprema can be taken over any subset $\mathbb{A}$ *of channels.*

Proof. First note that given a fixed attack channel $\mathcal{A}$, we have

$$\lim_{d_n\to\infty} \cdots \lim_{d_0\to\infty} \varepsilon_{\mathrm{sec}}^{(d)}(\mathcal{A}) = \varepsilon_{\mathrm{sec}}(\mathcal{A}), \tag{A.12}$$

as a direct consequence of Lemma A.1 (noting that differences of CPTP linear maps are bounded linear maps). The claimed result immediately follows by noting

$$\sup_{\mathcal{A}\in\mathbb{A}} \varepsilon_{\mathrm{sec}}(\mathcal{A}) = \sup_{\mathcal{A}\in\mathbb{A}} \lim_{d\to\infty} \varepsilon_{\mathrm{sec}}^{(d)}(\mathcal{A}) \tag{A.13}$$

$$\leq \lim_{d\to\infty} \sup_{\mathcal{A}\in\mathbb{A}} \varepsilon_{\mathrm{sec}}^{(d)}(\mathcal{A}), \tag{A.14}$$

where Eq. (A.13) follows from Eq. (A.12), and Eq. (A.14) holds because moving a supremum into any limit always yields a valid upper bound (as long as the relevant limits all exist):

For any set S and function $f : \mathbb{N} \times S \to \mathbb{R}$,

$$\sup_{x\in S} \lim_{m\to\infty} f(m,x) \leq \sup_{x\in S} \lim_{m\to\infty} \sup_{x'\in S} f(m,x') \tag{A.15}$$

$$= \lim_{m\to\infty} \sup_{x\in S} f(m,x), \tag{A.16}$$

where Eq. (A.15) follows from the trivial upper bound $f(m,x) \leq \sup_{x'\in S} f(m,x')$, and in Eq. (A.16) we simply remove the superfluous outer supremum and relabel the inner supremum. □

Essentially we have proven that if we have security proof techniques that hold for all finite dimensions, then we can obtain security for the infinite-dimensional case by taking a suitable limit of the finite-dimensional results.

Appendix B

Noise Channel constructions

Theorem 4.3 (Dark count noise channel)**.** *Let $\vec{F}_{\mathbf{d_B},\boldsymbol{\eta}}$ be the POVM for a flag-state squashed threshold detection setup with independent dark counts as defined in Definition 4.1, where each $F_i^{\mathbf{d_B},\boldsymbol{\eta}} = \Gamma_{i,0}^{\mathbf{d_B},\boldsymbol{\eta}} \oplus \Gamma_{i,m=1}^{\mathbf{d_B},\boldsymbol{\eta}} \oplus |i\rangle\langle i|$ is block-diagonal with an associated Hilbert space $\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ corresponding to the total photon number, and flag space. Then there exists noise channel $\Phi_{\mathbf{d_B}} : \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F \to \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ such that*

$$F_i^{\mathbf{d_B},\boldsymbol{\eta}} = \Phi_{\mathbf{d_B}}^{\dagger}\left[F_i^{\boldsymbol{\eta}}\right] \quad \forall\, i \tag{4.16}$$

$$\Phi_{\mathbf{d_B}}^{\dagger}[\Pi_{\leq 1}] = \mathcal{P}_{0|0}^{\mathbf{d_B}}\Pi_{\leq 1}, \tag{4.17}$$

where $F_i^{\boldsymbol{\eta}} = \Gamma_{i,m=0}^{\boldsymbol{\eta}} \oplus \Gamma_{i,m=1}^{\boldsymbol{\eta}} \oplus |i\rangle\langle i|$, $\Pi_{\leq 1}$ is the projection onto the space $\mathcal{H}_0 \oplus \mathcal{H}_1$, and $\mathcal{P}^{\mathbf{d_B}}$ is the stochastic matrix that models the dark counts.

Proof. Note that since $\mathcal{H}_0$ is one-dimensional, this can also serve as the flag for the no-click event. We make an ansatz for the noise channel, depicted in Fig. B.1 which we will now elaborate on. The noise channel first projects the input state into $\mathcal{H}_1$ and $\mathcal{H}_0 \oplus \mathcal{H}_F$. On $\mathcal{H}_0 \oplus \mathcal{H}_F$, it first measures the state with the lossy POVM $\vec{F}_{\boldsymbol{\eta}}$, and then applies the dark count post-processing map on the measurement results.

On $\mathcal{H}_1$, it probabilistically chooses between two channels. With probability $\mathcal{P}_{0|0}^{\mathbf{d_B}}$, it acts as the identity channel. Intuitively, this corresponds to the case when there are no dark counts in the setup. When there are dark counts, we assign the detection events to classical states in the flag-space as follows. With probability $1 - \mathcal{P}_{0|0}^{\mathbf{d_B}}$, the noise channel measures the state with $\vec{F}_{\boldsymbol{\eta}}$ to obtain result $\vec{p} = \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}}\rho_1\right]$, where ρ_1 is the part of ρ acting

on $\mathcal{H}_1$. The noise channel then uses the measurement result $\vec{p}$ to prepare the classical state

$$\tau_{\mathrm{C}} = \frac{1}{1-\mathcal{P}^{\mathbf{d_B}}_{0|0}} \left(\sum_{\substack{m\in M \\ j\notin M}} \mathcal{P}^{\mathbf{d_B}}_{m|j} p_j \left|m\right\rangle\!\left\langle m\right| + \sum_{s\in S} \left(\mathcal{P}^{\mathbf{d_B}}_{s|0} p_0 + (\mathcal{P}^{\mathbf{d_B}}_{s|s} - \mathcal{P}^{\mathbf{d_B}}_{0|0}) p_s \right) \left|s\right\rangle\!\left\langle s\right| \right). \tag{B.1}$$

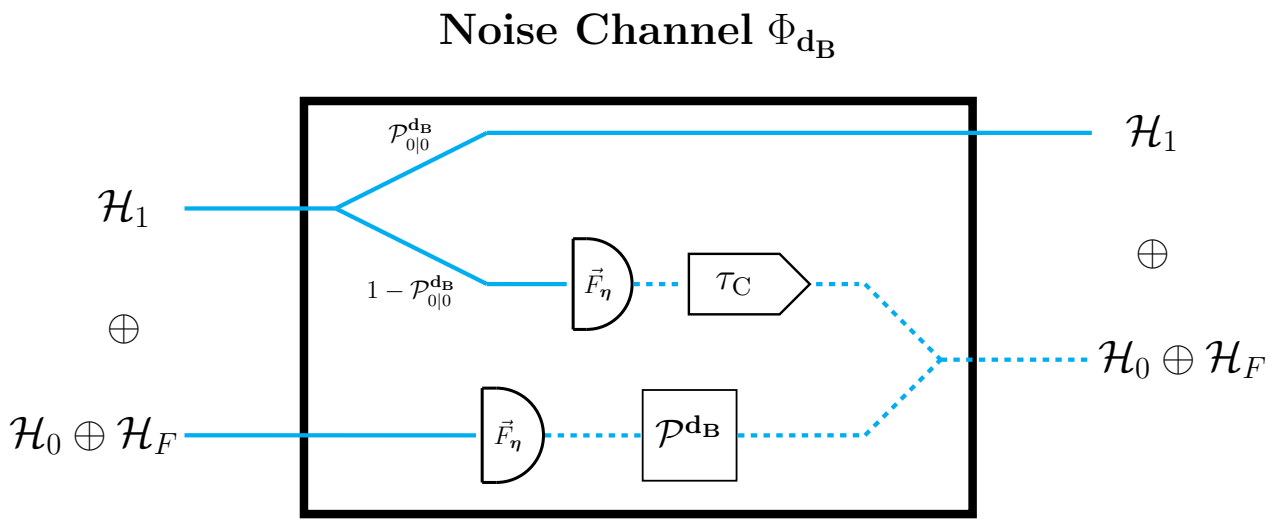


Figure B.1: Constructive description of the noise channel. Each line corresponds to a subspace of the input Hilbert space associated with the block-diagonal decomposition of the POVM elements. The dashed lines refer to classical states.

The rest of the proof follows by proving the following:

1. $\Phi_{\mathbf{d_B}}$ is completely-positive and trace-preserving (CPTP),
2. $\mathcal{P}^{\mathbf{d_B}} \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}} \rho\right] = \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}}\ \Phi_{\mathbf{d_B}}(\rho)\right]$ for all input density matrices ρ,
3. $\mathrm{Tr}\left[\Phi_{\mathbf{d_B}}(\rho)\Pi_{\leq 1}\right] = \mathcal{P}^{\mathbf{d_B}}_{0|0} \mathrm{Tr}\left[\rho\Pi_{\leq 1}\right]$ for all ρ.

$\Phi_{\mathbf{d_B}}$ is CPTP: Since it is clear that measurements and classical post-processing are physical channels, $\Phi_{\mathbf{d_B}}$ can be shown to be CPTP by showing that τ_{C} is a valid classical state as the CPTP property is preserved under channel composition. Note that all the elements of τ_{C} are positive as all elements of the stochastic matrix $\mathcal{P}^{\mathbf{d_B}}$ are positive, and $\mathcal{P}^{\mathbf{d_B}}_{s|s} \geq \mathcal{P}_{0|0}$

for all $s \in S$ as described in Eq. (4.14). Also, note that $\sum_{j \notin M} p_j = 1$ as $p_m = 0$ for all $m \in M$ as stated in Eq. (4.15). Then we compute,

$$\begin{aligned}
\mathrm{Tr}\left[\tau_{\mathrm{C}}\right] &= \frac{1}{1-\mathcal{P}^{\mathbf{d_B}}_{0|0}} \left(\sum_{\substack{m \in M \\ j \notin M}} \mathcal{P}^{\mathbf{d_B}}_{m|j} p_j + \sum_{s \in S} \left(\mathcal{P}^{\mathbf{d_B}}_{s|0} p_0 + (\mathcal{P}^{\mathbf{d_B}}_{s|s} - \mathcal{P}^{\mathbf{d_B}}_{0|0}) p_s \right) \right) \\
&= \frac{1}{1-\mathcal{P}^{\mathbf{d_B}}_{0|0}} \left(\sum_{\substack{s \in S \\ m \in M}} \left(\mathcal{P}^{\mathbf{d_B}}_{m|0} + \mathcal{P}^{\mathbf{d_B}}_{s|0} \right) p_0 + \sum_{\substack{s \in S \\ m \in M}} \left(\mathcal{P}^{\mathbf{d_B}}_{m|s} + \mathcal{P}^{\mathbf{d_B}}_{s|s} - \mathcal{P}^{\mathbf{d_B}}_{0|0} \right) p_s \right) \\
&= \frac{1}{1-\mathcal{P}^{\mathbf{d_B}}_{0|0}} \left(\left(1 - \mathcal{P}^{\mathbf{d_B}}_{0|0} \right) p_0 + \sum_{s \in S} \left(1 - \mathcal{P}^{\mathbf{d_B}}_{0|0} \right) p_s \right) \qquad \text{(B.2)} \\
&= 1,
\end{aligned}$$

where Eq. (B.2) follows from the fact that $\sum_{m \in M} \mathcal{P}^{\mathbf{d_B}}_{m|s} + \mathcal{P}^{\mathbf{d_B}}_{s|s} = 1$ for any $s \in S$ as implied by Eqs. (4.12) and (4.13).

$\mathcal{P}^{\mathbf{d_B}} \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}} \rho\right] = \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}}\ \Phi_{\mathbf{d_B}}(\rho)\right]$ for all input density matrices ρ: Due to the block-diagonal structure of the POVM elements, it suffices to show that this condition holds for flag-states $\{|i\rangle\langle i|\}_{i=1}^{n_{\mathrm{meas}}}$, vacuum state $|\mathrm{vac}\rangle\langle\mathrm{vac}|$ and single-photon states ρ_1 separately. Any input state can then be written as a convex combination of these states, and linearity would extend this for all states.

For any flag-state $|i\rangle\langle i|$, the condition $\mathcal{P}^{\mathbf{d_B}} \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}} |i\rangle\langle i|\right] = \mathrm{Tr}\left[\vec{F}_{\boldsymbol{\eta}}\ \Phi_{\mathbf{d_B}}(|i\rangle\langle i|)\right]$ follows directly from the construction depicted in Fig. 4.2. This similarly holds true for the vacuum state. We now turn our attention to the single-photon states ρ_1. We divide the computation for the single-photon states into three parts. First, consider the statistics of all $m \in M$. Using Eq. (4.15), we have that

$$\begin{aligned}
\mathrm{Tr}\left[F^{\boldsymbol{\eta}}_m\ \Phi_{\mathbf{d_B}}(\rho_1)\right] &= \mathcal{P}^{\mathbf{d_B}}_{0|0} \mathrm{Tr}\left[F^{\boldsymbol{\eta}}_m \rho_1\right] + (1 - \mathcal{P}^{\mathbf{d_B}}_{0|0}) \mathrm{Tr}\left[F^{\boldsymbol{\eta}}_m \tau_{\mathrm{C}}\right] \\
&= 0 + \sum_{j \notin M} \mathcal{P}^{\mathbf{d_B}}_{m|j} \mathrm{Tr}\left[F^{\boldsymbol{\eta}}_j \rho_1\right] \qquad \text{(B.3)} \\
&= \sum_{j \in U} \mathcal{P}_{m|j} \mathrm{Tr}\left[F^{\boldsymbol{\eta}}_j \rho_1\right], \qquad \text{(B.4)}
\end{aligned}$$

where Eqs. (B.3) and (B.4) follow from Eq. (4.15).

Next, we consider the statistics of all $s \in S$.

$$\begin{aligned}
\mathrm{Tr}\left[F_s^{\boldsymbol{\eta}}\, \Phi_{\mathbf{d_B}}(\rho_1)\right] &= \mathcal{P}_{0|0}^{\mathbf{d_B}} \mathrm{Tr}\left[F_s^{\boldsymbol{\eta}} \rho_1\right] + (1 - \mathcal{P}_{0|0}^{\mathbf{d_B}}) \mathrm{Tr}\left[F_s^{\boldsymbol{\eta}} \tau_{\mathrm{C}}\right] \\
&= \mathcal{P}_{0|0}^{\mathbf{d_B}} \mathrm{Tr}\left[F_s^{\boldsymbol{\eta}} \rho_1\right] + \left(\mathcal{P}_{s|0}^{\mathbf{d_B}} \mathrm{Tr}\left[F_0^{\boldsymbol{\eta}} \rho_1\right] + (\mathcal{P}_{s|s}^{\mathbf{d_B}} - \mathcal{P}_{0|0}^{\mathbf{d_B}}) \mathrm{Tr}\left[F_s^{\boldsymbol{\eta}} \rho_1\right]\right) \\
&= \mathcal{P}_{s|0}^{\mathbf{d_B}} \mathrm{Tr}\left[F_0^{\boldsymbol{\eta}} \rho_1\right] + \mathcal{P}_{s|s}^{\mathbf{d_B}} \mathrm{Tr}\left[F_s^{\boldsymbol{\eta}} \rho_1\right] \\
&= \sum_{j \in U} \mathcal{P}_{s|j}^{\mathbf{d_B}} \mathrm{Tr}\left[F_j^{\boldsymbol{\eta}} \rho_1\right], \qquad \text{(B.5)}
\end{aligned}$$

where Eq. (B.5) follows from Eqs. (4.12) and (4.15).

Finally, we consider the no-click statistics,

$$\begin{aligned}
\mathrm{Tr}\left[F_0^{\boldsymbol{\eta}}\, \Phi_{\mathbf{d_B}}(\rho_1)\right] &= \mathcal{P}_{0|0}^{\mathbf{d_B}} \mathrm{Tr}\left[F_0^{\boldsymbol{\eta}} \rho_1\right] + (1 - \mathcal{P}_{0|0}^{\mathbf{d_B}}) \mathrm{Tr}\left[F_0^{\boldsymbol{\eta}} \tau_{\mathrm{C}}\right] \\
&= \mathcal{P}_{0|0}^{\mathbf{d_B}} \mathrm{Tr}\left[F_0^{\boldsymbol{\eta}} \rho_1\right] + 0 \qquad \text{(B.6)} \\
&= \sum_{j \in U} \mathcal{P}_{0|j}^{\mathbf{d_B}} \mathrm{Tr}\left[F_j^{\boldsymbol{\eta}} \rho_1\right], \qquad \text{(B.7)}
\end{aligned}$$

where the last equality follows from Eq. (4.13). Thus, the noise channel $\Phi_{\mathbf{d_B}}$ is a CPTP map that satisfies the squashing constraint.

$\mathrm{Tr}\left[\Phi_{\mathbf{d_B}}(\rho)\Pi_{\leq 1}\right] = \mathcal{P}_{0|0}^{\mathbf{d_B}} \mathrm{Tr}\left[\rho \Pi_{\leq 1}\right]$ **for all** ρ**:** Given some density matrix ρ, we let $\Pi_{\leq 1}\rho\Pi_{\leq 1} = q_0 \left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right| + q_1\rho_1$. From the construction depicted in Fig. B.1, we see that $\Phi_{\mathbf{d_B}}(\left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right|) = \mathcal{P}_{0|0}^{\mathbf{d_B}} \left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right| + \sum_{i \neq 0} \mathcal{P}_{i|0}^{\mathbf{d_B}} \left|i\right\rangle\!\left\langle i\right|$. Moreover, $\Phi_{\mathbf{d_B}}(\rho_1) = \mathcal{P}_{0|0}^{\mathbf{d_B}} \rho_1 + \tau_{\mathrm{C}}$, where τ_{C} is composed entirely of flags. Finally, $\Phi_{\mathbf{d_B}}(\left|i\right\rangle\!\left\langle i\right|)$ only has support on the flag space $\mathcal{H}_F$. Thus, $\Pi_{\leq 1}\Phi_{\mathbf{d_B}}(\rho)\Pi_{\leq 1} = q_0 \mathcal{P}_{0|0}^{\mathbf{d_B}} \left|\mathrm{vac}\right\rangle\!\left\langle\mathrm{vac}\right| + q_1 \mathcal{P}_{0|0}^{\mathbf{d_B}} \rho_1$. Since $q_0 + q_1 = \mathrm{Tr}\left[\Pi_{\leq 1}\rho\right]$, we have that $\mathrm{Tr}\left[\Pi_{\leq 1}\Phi_{\mathbf{d_B}}(\rho)\right] = \mathcal{P}_{0|0}^{\mathbf{d_B}} \mathrm{Tr}\left[\Pi_{\leq 1}\rho\right]$. □

Theorem 4.4 (Loss noise channel)**.** *Let $\vec{F}_{\boldsymbol{\eta}}$ be the flag-state squashed POVM for a threshold detection setup with loss (and without dark counts), where for each POVM outcome i, $F_i^{\boldsymbol{\eta}} = \Gamma_{i,m=0} \oplus \Gamma_{i,m=1}^{\boldsymbol{\eta}} \oplus \left|i\right\rangle\!\left\langle i\right|$ is block-diagonal with an associated Hilbert space $\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ corresponding to the total photon number, and flag space. Here, the vacuum component $F_{i,m=0}$ is independent of loss $\boldsymbol{\eta}$ for all outcomes i. Let $\eta_{\min}$ and $\eta_{\max}$ be the minimum and maximum of all the detector efficiencies used in the detection setup. We can then define a family of noise channels $\Phi_{\boldsymbol{\eta}}^{\eta^*}$ and target POVMs $\vec{F}_{\eta^*}$ parametrised by some parameter η^* as follows. For any value of $\eta^* \in \left[\frac{\eta_{\min}}{1-(\eta_{\max}-\eta_{\min})}, 1\right]$, there exists a noise channel $\Phi_{\boldsymbol{\eta}}^{\eta^*}$:*

$\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F \to \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \mathcal{H}_F$ *such that*

$$F_i^{\boldsymbol{\eta}} = \Phi_{\boldsymbol{\eta}}^{\eta^*\dagger}\left[F_i^{\eta^*}\right] \quad \forall\, i \tag{4.18}$$

$$\Phi_{\boldsymbol{\eta}}^{\eta^*\dagger}\left[\Pi_{\leq 1}\right] = \Pi_0 + \frac{\eta_{\min}}{\eta^*}\Pi_1, \tag{4.19}$$

where $F_i^{\eta^*} = \Gamma_{i,m=0} \oplus \Gamma_{i,m=1}^{\eta^*} \oplus |i\rangle\langle i|$ *is the lossy flag-state squashed POVM where all detectors have the (common) efficiency* η^*, Π_1 *is the projection onto the space* $\mathcal{H}_1$, Π_0 *is the projection onto the space* $\mathcal{H}_0$, *and* $\Pi_{\leq 1}$ *is the projection onto the space* $\mathcal{H}_0 \oplus \mathcal{H}_1$.

Proof. Note that as described in Section 2.2.6, the lossy POVM $\vec{F}_{\boldsymbol{\eta}}$ is related to the lossless POVM $\vec{F}$ with

$$\vec{F}_{\boldsymbol{\eta},m\leq 1} = \mathcal{P}^{\boldsymbol{\eta}} \vec{F}_{m\leq 1}, \tag{B.8}$$

where

$$\mathcal{P}^{\boldsymbol{\eta}} = \begin{pmatrix} 1 & 1-\eta_1 & \cdots & \cdots & 1-\eta_k \\ 0 & \eta_1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \eta_k \end{pmatrix},$$

and $\vec{F}_{\boldsymbol{\eta},m\leq 1} = \vec{F}_{m=0} \oplus \vec{F}_{\boldsymbol{\eta},m=1}$. Additionally, the flag-space portion, and the vacuum ($m = 0$) portion of both the noisy, and noiseless POVMs are identical.

The construction of the noise channel for the lossy POVM $\vec{F}_{\boldsymbol{\eta}}$ is a special case of the construction used in Theorem 4.2. For any value of common efficiency $\eta^* \in \left[\frac{\eta_{\min}}{1-(\eta_{\max}-\eta_{\min})}, 1\right]$, we break up the loss post-processing $\mathcal{P}^{\boldsymbol{\eta}}$ as

$$\mathcal{P}^{\boldsymbol{\eta}} = \frac{\eta_{\min}}{\eta^*}\mathcal{P}^{\eta^*} + \left(1 - \frac{\eta_{\min}}{\eta^*}\right)\mathcal{Q}^{\boldsymbol{\eta},\eta^*}, \tag{B.9}$$

where

$$\mathcal{Q}^{\boldsymbol{\eta},\eta^*} = \begin{pmatrix} 1 & 1-\eta^*\frac{\eta_1-\eta_{\min}}{\eta^*-\eta_{\min}} & \cdots & \cdots & 1-\eta^*\frac{\eta_k-\eta_{\min}}{\eta^*-\eta_{\min}} \\ 0 & \eta^*\frac{\eta_1-\eta_{\min}}{\eta^*-\eta_{\min}} & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \eta^*\frac{\eta_k-\eta_{\min}}{\eta^*-\eta_{\min}} \end{pmatrix},$$

Thus, from Eqs. (B.8) and (B.9) we get

$$\vec{F}_{\boldsymbol{\eta},m\leq 1} = \frac{\eta_{\min}}{\eta^*}\mathcal{P}^{\eta^*}\vec{F}_{m\leq 1} + \left(1-\frac{\eta_{\min}}{\eta^*}\right)\mathcal{Q}^{\boldsymbol{\eta},\eta^*}\vec{F}_{m\leq 1}. \tag{B.10}$$

Further, note that $\vec{F}_{m=0}$ is independent of the loss $\boldsymbol{\eta}$, so that we can refine the above equation to

$$\vec{F}_{\boldsymbol{\eta},m\leq 1} = \vec{F}_{m=0} \oplus \left(\frac{\eta_{\min}}{\eta^*}\mathcal{P}^{\eta^*}\vec{F}_{m=1} + \left(1-\frac{\eta_{\min}}{\eta^*}\right)\mathcal{Q}^{\boldsymbol{\eta},\eta^*}\vec{F}_{m=1}\right). \tag{B.11}$$

Thus, we can construct the noise channel depicted in Fig. B.2:

$$\Phi^{\eta^*}_{\boldsymbol{\eta}}\left(\left(\begin{array}{c|c|c} \rho_0 & B & C \\ \hline B^\dagger & \rho_1 & D \\ \hline C^\dagger & D^\dagger & \rho_F \end{array}\right)\right) \coloneqq \rho_0 \oplus \frac{\eta_{\min}}{\eta^*}\rho_1 \oplus \left(\left(1-\frac{\eta_{\min}}{\eta^*}\right)\sum_i \mathrm{Tr}\left[\rho_1 Q_i\right]|i\rangle\langle i| + \rho_F\right), \tag{B.12}$$

where $\vec{Q} \coloneqq \mathcal{Q}^{\boldsymbol{\eta},\eta^*}\vec{F}_{m=1}$. It is easy to verify that this construction satisfies $\mathrm{Tr}\left[\vec{\Gamma}_{\boldsymbol{\eta}}\rho\right] = \mathrm{Tr}\left[\vec{F}_{\eta^*}\ \Phi^{\eta^*}_{\boldsymbol{\eta}}\left(\Lambda(\rho)\right)\right]$, and that Eq. (4.19) holds. □

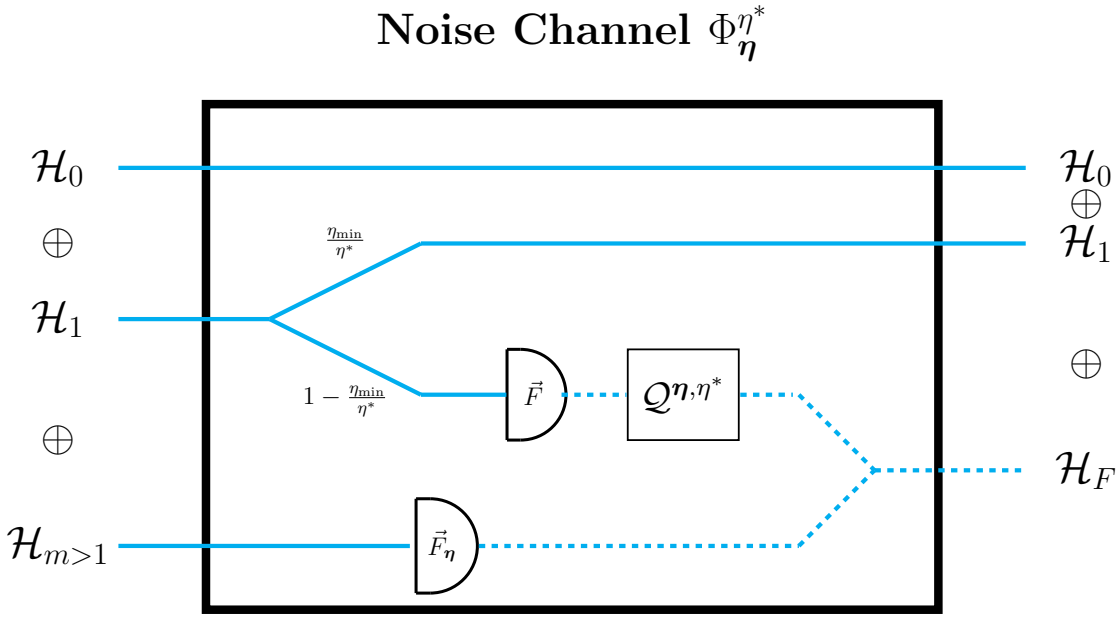


Figure B.2: Constructive description of the noise channel. Each line corresponds to a subspace of the input Hilbert space associated with the block-diagonal decomposition of the POVM elements. The dashed lines refer to classical states.

Appendix C

Improved de Finetti reductions

In this appendix, we improve on quantum de Finetti reductions from Refs. [10, 80], which are of the following form:

$$\rho_{A^nB^n} \leq g_{n,x}\ \tau_{A^nB^n}, \tag{C.1}$$

where $\tau_{A^nB^n} = \int \sigma_{AB}^{\otimes n} \mathrm{d}\sigma_{AB}$ is a normalised density matrix, and $g_{n,x} = \dim\left(\mathrm{Sym}^n\left(\mathbb{C}^x\right)\right) = \binom{n+x-1}{n}$. We refer to a state of the form $\tau_{A^nB^n} = \int \sigma_{AB}^{\otimes n} \mathrm{d}\sigma_{AB}$ as a "de Finetti state". As illustrated in Section 5.1, 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 $\tau_{A^nB^n}$: This should be such that the integral is only over states for which the task has been "analyzed", e.g. in the sense that some security property has been proven for all such IID states.

In particular, the de Finetti reduction proved in [10] is not sufficient for our purposes as the mixture of IID states $\tau_{A^nB^n}$ used in that work constitutes a mixture over *all* IID states. However, the analysis of PM QKD protocols requires $\tau_{A^nB^n}$ to be a mixture of IID states that have the same fixed marginal $\hat{\sigma}_A$. This can easily be remedied by using [80, Corollary 3.2], which therefore forms the natural starting point for our work in this appendix.

In this appendix we make several improvements to the value of $g_{n,x}$. These improvements are of two types. We first improve the dimensional scaling ($g_{n,x}$) in Lemma 3.1 of Ref. [80] for generic states. Second, we also show that the dimensions can be reduced

for states that are invariant under certain symmetries, as an extension of Ref. [84] to the quantum case. We first state the results, to make the structure of the argument clear. Then, we provide the technical proofs, which are simple modifications of the proofs in [80].

C.1 Generic improvement

Theorem C.1 (de Finetti reduction with fixed marginal)**.** *Let* $\hat{\sigma}_A \in \mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$ *and let* $\rho_{A^nR^n}$ *be any purification of* $(\hat{\sigma}_A)^{\otimes n}$ *supported on the symmetric subspace* $\mathrm{Sym}^n\left(\mathbb{C}^{d_Ad_R}\right)$*. Then there exists a probability measure* $d\phi$ *on the set of purifications* $|\phi\rangle\langle\phi|_{AR}$ *of* $\hat{\sigma}_A$*, such that*

$$\rho_{A^nR^n} \leq g_{n,d_Ad_R} \int |\phi\rangle\langle\phi|_{AR}^{\otimes n} \,\mathrm{d}\phi. \tag{C.2}$$

The proof is given in Appendix C.3.

Note that crucially, Theorem C.1 differs from Lemma 3.1 in Ref. [80] in the prefactor $g_{n,x}$, where they had $x = \max[d_A^2, d_R^2]$ instead of $x = d_Ad_R$. This leads to a corresponding improvement in the resulting corollary for mixed states. Before stating this corollary, we need to define permutation-invariance of matrices.

Definition C.1 (Permutation-invariance of matrices)**.** Given a matrix $\rho_{A^nB^n} \in \mathrm{L}\left(\left(\mathbb{C}^{d_Ad_B}\right)^{\otimes n}\right)$ and a permutation $\pi \in S_n$ of its subsystems, we denote the action of π on $\rho_{A^nB^n}$ as $P_\pi^{d_Ad_B,n}\rho_{A^nB^n}P_\pi^{d_Ad_B,n\dagger}$ where $P_\pi^{d_Ad_B,n}$ is the standard representation of π on $(\mathbb{C}^{d_Ad_B})^{\otimes n}$. We say that a matrix is *permutation-invariant* if it is invariant under the action of all permutations $\pi \in S_n$.

Corollary C.1. *Let* $\hat{\sigma}_A \in \mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$ *and* $\rho_{A^nB^n}$ *be any permutation-invariant extension of* $(\hat{\sigma}_A)^{\otimes n}$*. Then there exists a probability measure* $d\sigma_{AB}$ *on the set of non-negative extensions* σ_{AB} *of* $\hat{\sigma}_A$*, such that*

$$\rho_{A^nB^n} \leq g_{n,x} \int \sigma_{AB}^{\otimes n} \mathrm{d}\sigma_{AB} \tag{C.3}$$

holds for $x = d_A^2d_B^2$*.*

Proof. We can use Lemma 4.2.2 from Ref. [52] to construct a purification $\rho_{A^nB^nE^n} \in \mathrm{Sym}^n\left(\mathbb{C}^{d_Ad_B} \otimes \mathbb{C}^{d_Ad_B}\right)$ of $\rho_{A^nB^n}$. From Theorem C.1, it follows that

$$\rho_{A^nB^nE^n} \leq g_{n,d_A^2d_B^2} \int |\phi\rangle\langle\phi|_{ABE}^{\otimes n} \,\mathrm{d}\phi,$$

where $\mathrm{d}\phi$ is a probability measure over purifications of $\hat{\sigma}_A$. Taking the partial trace over E^n on both sides completes the proof. □

Note that the dramatic improvement over Corollary 3.2 from Ref. [80] ($x = d_A^2 d_B^4$ to $x = d_A^2 d_B^2$) is a direct result of Theorem C.1. Additionally, with this improvement we obtain the earlier de Finetti reduction without a fixed marginal [10, Lemma 2] by considering A to be a trivial system, thus unifying both results.

C.2 Improvements with symmetries

In this work, we use the term "symmetries" as a broad term to refer to both block-diagonal structure and invariance under some groups. This is due to the following connection between block-diagonal structure and group invariance. Consider the group $\bigoplus_{i=1}^k \mathcal{U}(1)$ and the representation $\phi : \bigoplus_{i=1}^k \mathcal{U}(1) \to \mathcal{U}(\bigoplus_{i=1}^k \mathbb{C}^{d_i})$ defined as $\phi(u_1, \dots u_k) \mapsto \bigoplus_{i=1}^k \bigoplus_{j=1}^{d_i} u_i$. Note that this representation has k irreps of dimensions $\{d_i\}_{i=1}^k$ each. A state being invariant under the action of this representation is equivalent to saying that the state is block-diagonal with k blocks of dimensions $\{d_i\}_{i=1}^k$ each. Hence, we can view block-diagonal structure as corresponding to invariance with respect to some group representation.

The use of de Finetti-like reductions for symmetries was previously mentioned in [10, footnote 17], and with more details given in Refs. [108, 109]. We extend this analysis to the de Finetti reduction with fixed marginal, and also show that the reduction in the case of "IID-symmetries" can be combined with the reduction in the case of permutational symmetry. A similar analysis to combine permutational symmetry with "IID-symmetries" for the de Finetti reduction *without* a fixed marginal was independently performed by Ref. [85]. Importantly, they also obtain a better cost $g_{n,x}$.

Our improvements to Corollary C.1 in the presence of symmetries are based on observing that the proof in Appendix C.1 had the following structure:

1. Given a permutation-invariant state with a fixed marginal $\hat{\sigma}_A^{\otimes n}$, Lemma 4.2.2 from Ref. [52] is used to obtain a purification in the corresponding symmetric subspace.

2. This purification can then be related to a convex mixture of IID states with the same marginal $\hat{\sigma}_A$, via Theorem C.1.

3. Tracing out the purifying system gives the de Finetti reduction for mixed states as shown in Corollary C.1.

We show that in the presence of symmetries, steps 1 and 2 can be improved. With this, we prove a generalised version of Theorem C.1 that results in better bounds in the presence of symmetries.

Theorem C.2 (de Finetti reduction with symmetries and fixed marginal)**.** *Let* $\hat{\sigma}_A \in \mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$*, and let* $\rho_{A^nR^n}$ *be any purification of* $(\hat{\sigma}_A)^{\otimes n}$ *supported on the symmetric subspace* $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}\right)$ *where* $\bigoplus_{i=1}^k \mathbb{C}^{d_i^A} \subseteq \mathbb{C}^{d_A}$ *and* $\bigoplus_{i=1}^k \mathbb{C}^{d_i^R} \subseteq \mathbb{C}^{d_R}$*. Then there exists a probability measure* $\mathrm{d}\phi$ *on the set of purifications* $|\phi\rangle_{AR} \in \bigoplus_{i=1}^k \mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}$ *of* $\hat{\sigma}_A$ *such that*

$$\rho_{A^nR^n} \leq g_{n,x} \int |\phi\rangle\langle\phi|_{AR}^{\otimes n} \,\mathrm{d}\phi, \tag{C.4}$$

where $x = \sum_{i=1}^k d_i^A d_i^R$*.*

The proof is given in Appendix C.3.

We note that in the case where $k = 1$, $d_1^A = d_A$ and $d_1^R = d_R$ we recover Theorem C.1. More generally, $\sum_{i=1}^k d_i^A d_i^R \leq d_A d_R$ leading to a reduced cost $g_{n,x}$. Block-diagonal symmetries are an important special case of generic symmetries that are often seen in optical implementations of quantum information protocols. Thus, we next describe the usage of Theorem C.2 for the case where the state has some block-diagonal symmetry before considering more general symmetries.

C.2.1 Improvement for IID-block-diagonal states

Definition C.2 (IID-block-diagonal states)**.** Given a matrix $\rho_{A^nB^n} \in \mathrm{L}\left((\mathbb{C}^{d_A d_B})^{\otimes n}\right)$, and a set of orthogonal projections $\{\Pi_i\}_{i=1}^k \subset \mathrm{L}\left(\mathbb{C}^{d_A d_B}\right)$, we say that the matrix is *IID-block-diagonal* if

$$\rho_{A^nB^n} = \sum_{\vec{j} \in [k]^n} \Pi_{\vec{j}} \rho_{A^nB^n} \Pi_{\vec{j}}$$

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.

Just as Lemma 4.2.2 from Ref. [52] was crucial in the proof of Corollary C.1, the heart of the improvement that uses block-diagonal structure is the following lemma.

Lemma C.1. *Let* $\rho_{A^nB^n} \in \mathrm{Pos}\left(\left(\mathbb{C}^{d_Ad_B}\right)^{\otimes n}\right)$ *be a permutation-invariant and IID-block-diagonal matrix with respect to projections* $\{\Pi_i\}_{i=1}^k$ *of dimension* $\{d_i\}_{i=1}^k$*. Then there exists a purification of* $\rho_{A^nB^n}$ *supported on* $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i}\otimes\mathbb{C}^{d_i}\right)$.

The proof is given in Appendix C.3.

Remark C.1. *An important special case of Lemma C.1 is when* $\rho_{A^nB^n}$ *is IID-block-diagonal with respect to projections* $\{\Pi_i^A\otimes\Pi_j^B\}_{i,j=1}^{k_A,k_B}$ *of dimension* $\{d_i^Ad_j^B\}_{i,j=1}^{k_A,k_B}$ *where* d_i^A *and* d_j^B *are the ranks of* $\Pi_i^A\in\mathrm{L}\left(\mathbb{C}^{d_A}\right)$ *and* $\Pi_j^B\in\mathrm{L}\left(\mathbb{C}^{d_B}\right)$ *respectively. In that case, there exists a purification of* $\rho_{A^nB^n}$ *on* $\mathrm{Sym}^n\left(\bigoplus_{i,j=1}^{k_A,k_B}\mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_j^B}\otimes\mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_j^B}\right)=\mathrm{Sym}^n\left(\bigoplus_{i=1}^{k_A}\mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_i^A\sum_{j=1}^{k_B}d_j^{B\,2}}\right)$.

Note that this purification of $\rho_{A^nB^n}$ now belongs to $\mathrm{Sym}^n\left(\bigoplus_{i=1}^{k_A}\mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_i^A\sum_{j=1}^{k_B}d_j^{B\,2}}\right)$ instead of $\mathrm{Sym}^n\left(\mathbb{C}^{d_Ad_R}\right)$ in Theorem C.1. We thus obtain an improved version of Corollary C.1.

Corollary C.1. *Let* $\hat{\sigma}_A\in\mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$ *and* $\rho_{A^nB^n}$ *be any permutation-invariant and IID-block-diagonal extension of* $(\hat{\sigma}_A)^{\otimes n}$ *with with respect to projections* $\{\Pi_i^A\otimes\Pi_j^B\}_{i,j=1}^{k_A,k_B}$ *of dimension* $\{d_i^Ad_j^B\}_{i,j=1}^{k_A,k_B}$*, where* d_i^A *and* d_j^B *are the ranks of* $\Pi_i^A\in\mathrm{L}\left(\mathbb{C}^{d_A}\right)$ *and* $\Pi_j^B\in\mathrm{L}\left(\mathbb{C}^{d_B}\right)$ *respectively. Then there exists some probability measure* $d\sigma_{AB}$ *over the set of block-diagonal extensions* σ_{AB} *of* $\hat{\sigma}_A$ *such that*

$$\rho_{A^nB^n}\leq g_{n,x}\int\sigma_{AB}^{\otimes n}\,\mathrm{d}\sigma_{AB}, \tag{C.5}$$

where $x=\sum_{i,j=1}^{k_A,k_B}d_i^{A\,2}d_j^{B\,2}$.

Proof. The proof of this theorem is similar to the proof of Corollary C.1, replacing the use of Lemma 4.2.2 from Ref. [52] with Lemma C.1 and Theorem C.1 with Theorem C.2. □

C.2.2 Improvement for IID symmetries

Definition C.3 (IID-group-invariant)**.** Let G be a group, and let $\{U_g\}_{g\in G}$ be a unitary representations of G on $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}$. We say a matrix $\rho_{A^nB^n}\in\mathrm{L}\left((\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B})^{\otimes n}\right)$ is *IID-G-invariant* if

$$U_{\vec{g}}\,\rho\,U_{\vec{g}}^\dagger=\rho$$

for all $\vec{g}\in G^n$, where $U_{\vec{g}}:=\bigotimes_{i=1}^n U_{g_i}$ for $\vec{g}=(g_1,\ldots,g_n)\in G^n$.

Similar to the block-diagonal case, the following lemma gives the improvement in the presence of symmetries.

Lemma C.2. *Let G be a compact group and let $\{U_g\}_{g\in G}$ be a unitary representation of G on $\mathbb{C}^{d_A d_B}$ with k irreducible representations with multiplicity $\{m_i\}_{i=1}^k$. If $\rho_{A^nB^n} \in \mathrm{Pos}\left((\mathbb{C}^{d_A d_B})^{\otimes n}\right)$ is permutation invariant and IID-G-invariant, then there exists a purification of $\rho_{A^nB^n}$ on $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{m_i}\otimes\mathbb{C}^{m_i}\right)$.*

The proof is given in Appendix C.3.

Remark C.2. *An important special case of Lemma C.2 is when the group $G = G_A \times G_B$ is a product of compact groups. Let the unitary representations $\{U_{g_A}\}_{g_A\in G_A} \subset \mathrm{L}\left(\mathbb{C}^{d_A}\right)$ and $\{U_{g_B}\}_{g_B\in G_B} \subset \mathrm{L}\left(\mathbb{C}^{d_B}\right)$ with k_A, k_B irreducible representations with multiplicity $\{m_i^A\}_{i=1}^{k_A}$ and $\{m_i^B\}_{i=1}^{k_B}$ respectively. Then there exists a purification of $\rho_{A^nB^n}$ on $\mathrm{Sym}^n\left(\bigoplus_{i,j=1}^{k_A,k_B} \mathbb{C}^{m_i^A}\otimes\mathbb{C}^{m_j^B}\otimes\mathbb{C}^{m_i^A}\otimes\mathbb{C}^{m_j^B}\right) = \mathrm{Sym}^n\left(\bigoplus_i^{k_A}\mathbb{C}^{m_i^A}\otimes\mathbb{C}^{m_i^A\sum_{j=1}^{k_B}m_j^{B\,2}}\right)$.*

This can now be directly used to prove the de Finetti reduction for mixed states in the presence of symmetries.

Corollary C.2. *Let $\{U_{g_A}^A\}_{g_A\in G_A}$ ($\{U_{g_B}^B\}_{g_B\in G_B}$) be a unitary representation of G_A (G_B) on $\mathbb{C}^{d_A}$ ($\mathbb{C}^{d_B}$) with k_A (k_B) irreducible representations with multiplicity $\{m_i^A\}_{i=1}^{k_A}$ ($\{m_j^B\}_{j=1}^{k_B}$). Let $G = G_A \times G_B$, $\hat{\sigma}_A \in \mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$ and $\rho_{A^nB^n}$ be any permutation-invariant extension of $(\hat{\sigma}_A)^{\otimes n}$ that is IID-G-invariant. Then there exists some probability measure $d\sigma_{AB}$ over the set of G-invariant extensions σ_{AB} of $\hat{\sigma}_A$ such that*

$$\rho_{A^nB^n} \leq g_{n,x}\int \sigma_{AB}^{\otimes n}\,\mathrm{d}\sigma_{AB}, \tag{C.6}$$

where $x = \sum_{i,j=1}^{k_A,k_B} m_i^{A\,2} m_j^{B\,2}$.

Proof. The proof of this theorem is similar to the proof of Corollary C.1, replacing the use of Lemma C.1 with Lemma C.2. □

Of course, these improvements would also apply to the de Finetti reduction without the fixed marginal [10, Lemma 2] in the case when A is a trivial register (although in this case, one would be better off using the results from [85] instead). Moreover, these improvements drastically improve upon the previous de Finetti reduction with fixed marginal [80, Corollary 3.2], thereby increasing the key rates obtained via the postselection technique, as shown in Fig. 5.5.

C.3 Proofs of technical statements

In this section, we complete the proofs of the theorems and lemmas in the preceding sections. Our proofs rely heavily on results from representation theory, particularly Schur-Weyl duality and Schur's Lemma. For pedagogical clarity, we begin by summarising the essential concepts from representation theory that form the basis of our arguments.

C.3.1 Toolkit from representation theory

Here, we briefly introduce the key results used in our proofs. There are a number of existing resources that provide a more comprehensive treatment of representation theory within the context of quantum information, for e.g. - [110, 111].

Schur-Weyl Duality

This duality provides a decomposition of the n-fold tensor product of a Hilbert space, $(\mathbb{C}^d)^{\otimes n}$, in terms of the irreducible representations of the following groups:

1. The **unitary group** $\mathcal{U}(d)$, which acts as $U^{\otimes n}$ for $U \in \mathcal{U}(d)$.
2. The **symmetric group** S_n, which acts by permuting the n tensor factors.

Schur-Weyl duality states that the space decomposes into a direct sum of tensor products of irreducible representations (irreps) of these two groups,

$$(\mathbb{C}^d)^{\otimes n} \cong \bigoplus_{\lambda \in \Lambda_{n,d}} W_d^\lambda \otimes [\lambda], \tag{C.7}$$

where

- $\Lambda_{n,d}$ is the set of partitions of the integer n into at most d parts (represented by Young diagrams λ). More formally,

  $$\Lambda_{n,d} := \{\lambda = (\lambda_1, \ldots, \lambda_d) : \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d \geq 0, \sum_{i=1}^{d} \lambda_i = n\}.$$

  We identify a partition $(\lambda_1, \ldots, \lambda_d, 0, \cdots, 0)$ with $(\lambda_1, \ldots, \lambda_d)$, so $\Lambda_{n,d}$ is a subset of $\Lambda_{n,d'}$ for $d \leq d'$.

- W_d^λ is the vector space for the irrep of $\mathcal{U}(d)$ corresponding to λ. The group $\mathcal{U}(d)$ acts non-trivially only on this space. The structure of this space depends on both λ and d.

- $[\lambda]$ is the vector space for the irrep of S_n corresponding to λ. The symmetric group S_n acts non-trivially only on this space. The structure of this space depends only on λ.

An important consequence for our work relates to the symmetric subspace, $\mathrm{Sym}^n\left(\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_R}\right)$, which is the subspace invariant under permutations from S_n. For a bipartite system, the subspace of $(\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_R})^{\otimes n}$ that is invariant under permutations of the n copies is isomorphic to $\bigoplus_{\lambda\in\Lambda_{n,\min(d_A,d_R)}} W_A^\lambda\otimes W_R^\lambda$ (see, e.g., [110, Eq. (5.27)]).

Schur's Lemma and Integration over Unitary Groups

Schur's Lemma is fundamental for evaluating integrals over compact groups. For our purposes, its most important consequence is the following identity. Let W_R^λ be the space for an irrep of $\mathcal{U}(d_R)$ and let $W_R^\lambda(U)$ be the unitary matrix for $U\in\mathcal{U}(d_R)$ in this irrep. For any two vectors $|v\rangle\in W_R^\lambda$ and $|w\rangle\in W_R^{\lambda'}$, we have,

$$\int_{\mathcal{U}(d_R)} W_R^\lambda(U)\,|v\rangle\langle w|\,(W_R^{\lambda'}(U))^\dagger\,\mathrm{d}U = \delta_{\lambda,\lambda'}\frac{\langle w|v\rangle}{\dim(W_R^\lambda)}\,\mathrm{id}_{W_R^\lambda}, \tag{C.8}$$

where $\mathrm{d}U$ is the normalised Haar measure. This shows that integrating over the group projects any operator onto a multiple of the identity operator within each irrep subspace and annihilates operators acting between inequivalent irrep subspaces.

Characters and their Orthogonality

For any representation $\pi: G\to\mathcal{U}(\mathcal{H})$, its **character** is the function $\chi: G\to\mathbb{C}$ defined by the trace of the representation matrices, $\chi(g)\coloneqq\mathrm{Tr}\,[\pi(g)]$. A key property of the character is that it is constant on the conjugacy classes of the group (i.e., $\chi(hgh^{-1})=\chi(g)$). For a compact group, we can define an inner product on the space of such class functions via the Haar measure:

$$\langle\chi_1,\chi_2\rangle\coloneqq\int_G\chi_1(g)\overline{\chi_2(g)}\,\mathrm{d}\mu(g).$$

The **Great Orthogonality Theorem** for characters states that the characters of the irreps form an orthonormal set with respect to this inner product. That is, for two irreps π_i and π_j with characters χ_i and χ_j:

$$\langle \chi_i, \chi_j \rangle = \int_G \chi_i(g)\overline{\chi_j(g)}\,\mathrm{d}\mu(g) = \delta_{ij}.$$

C.3.2 Proofs

We now proceed with the proofs. We first need to establish the following lemma, which characterises the structure of a particular integrated quantum state.

Lemma C.3. *Suppose d_A and d_R are two positive integers with $d_A \leq d_R$. Let $|\theta\rangle := \sum_{i=1}^{d_A} |i\rangle_A \otimes |i\rangle_R \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}$, and let $\mathrm{d}U$ be the Haar measure on $\mathcal{U}(\mathbb{C}^{d_R})$. For every $n \geq 1$, define the operator*

$$T_n := \int_{\mathcal{U}(\mathbb{C}^{d_R})} (\mathrm{id}_{A^n} \otimes U^{\otimes n})\, |\theta\rangle\langle\theta|^{\otimes n}\, (\mathrm{id}_{A^n} \otimes U^{\otimes n})^\dagger \mathrm{d}U.$$

Then there is an invertible operator $\kappa_n \in \mathrm{L}\left((\mathbb{C}^{d_A})^{\otimes n}\right)$ such that

$$(\kappa_n \otimes \mathrm{id}_{R^n})^{-1/2} T_n (\kappa_n \otimes \mathrm{id}_{R^n})^{-1/2} = \mathrm{id}_{\mathrm{Sym}^n\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}\right)}. \tag{C.9}$$

Proof. The proof strategy is to decompose the state $|\theta\rangle\langle\theta|^{\otimes n}$ using Schur-Weyl duality and then apply Schur's Lemma to evaluate the integral over $\mathcal{U}(\mathbb{C}^{d_R})$.

We apply the Schur-Weyl duality decomposition (Equation (C.7)) to both $(\mathbb{C}^{d_A})^{\otimes n}$ and $(\mathbb{C}^{d_R})^{\otimes n}$, noting that since $d_A \leq d_R$, we have $\Lambda_{n,d_A} \subset \Lambda_{n,d_R}$. The state $|\theta\rangle^{\otimes n}$ is invariant under the joint action $V^{\otimes n} \otimes (V^\dagger)^{\otimes n}$ for any $V \in \mathcal{U}(d_A)$ and lies in the symmetric subspace $\mathrm{Sym}^n\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}\right)$. This structure implies that its decomposition can be written as,

$$|\theta\rangle^{\otimes n} = \bigoplus_{\lambda \in \Lambda_{n,d_A}} \left|\Phi^\lambda_{AR}\right\rangle,$$

where each $\left|\Phi^\lambda_{AR}\right\rangle$ is a vector in the corresponding subspace $W^\lambda_A \otimes W^\lambda_R$. Specifically, $\left|\Phi^\lambda_{AR}\right\rangle$ is a maximally entangled state between the W^λ_A and W^λ_R spaces. We can write this as $\left|\Phi^\lambda_{AR}\right\rangle = \sqrt{\dim([\lambda])}\sum_{j=1}^{\dim(W^\lambda_A)} \left|w^{\lambda,A}_j\right\rangle \otimes \left|w^{\lambda,R}_j\right\rangle$ for some orthonormal bases $\left\{\left|w^{\lambda,A}_j\right\rangle\right\}$ of W^λ_A and $\left\{\left|w^{\lambda,R}_j\right\rangle\right\}$ of W^λ_R.[1]

[1] The prefactor $\sqrt{\dim([\lambda])}$ is a result of the fact that $|\theta\rangle\langle\theta|^{\otimes n}$, is unnormalised.

We now compute the integral defining T_n. The unitary $U^{\otimes n}$ acts only on the R system. In the Schur-Weyl basis, its action is $\bigoplus_{\lambda'} W_R^{\lambda'}(U) \otimes \mathrm{id}_{[\lambda']_R}$. The integral therefore decouples across the λ blocks as,

$$\begin{aligned} T_n &= \int \bigoplus_{\lambda,\lambda' \in \Lambda_{n,d_A}} (\mathrm{id}_{W_A^\lambda} \otimes W_R^\lambda(U)) \left|\Phi_{AR}^\lambda\right\rangle\!\left\langle\Phi_{AR}^{\lambda'}\right| (\mathrm{id}_{W_A^{\lambda'}} \otimes W_R^{\lambda'}(U))^\dagger \mathrm{d}U \\ &= \bigoplus_{\lambda,\lambda'} \dim([\lambda]) \sum_{j,j'} \left|w_j^{\lambda,A}\right\rangle\!\left\langle w_{j'}^{\lambda',A}\right| \otimes \int W_R^\lambda(U) \left|w_j^{\lambda,R}\right\rangle\!\left\langle w_{j'}^{\lambda',R}\right| (W_R^{\lambda'}(U))^\dagger \mathrm{d}U. \end{aligned}$$

Applying Schur's Lemma, the integral is non-zero only if $\lambda = \lambda'$ and $j = j'$. This yields,

$$\int W_R^\lambda(U) \left|w_j^{\lambda,R}\right\rangle\!\left\langle w_{j'}^{\lambda',R}\right| (W_R^{\lambda'}(U))^\dagger \mathrm{d}U = \delta_{\lambda,\lambda'}\delta_{j,j'} \frac{1}{\dim(W_R^\lambda)} \mathrm{id}_{W_R^\lambda}.$$

Substituting this back, we find

$$\begin{aligned} T_n &= \bigoplus_{\lambda \in \Lambda_{n,d_A}} \dim([\lambda]) \sum_{j=1}^{\dim(W_A^\lambda)} \left|w_j^{\lambda,A}\right\rangle\!\left\langle w_j^{\lambda,A}\right| \otimes \frac{1}{\dim(W_R^\lambda)} \mathrm{id}_{W_R^\lambda} \\ &= \bigoplus_{\lambda \in \Lambda_{n,d_A}} \frac{\dim([\lambda])}{\dim(W_R^\lambda)} \left(\sum_j \left|w_j^{\lambda,A}\right\rangle\!\left\langle w_j^{\lambda,A}\right|\right) \otimes \mathrm{id}_{W_R^\lambda} \\ &= \bigoplus_{\lambda \in \Lambda_{n,d_A}} \frac{\dim([\lambda])}{\dim(W_R^\lambda)} \mathrm{id}_{W_A^\lambda} \otimes \mathrm{id}_{W_R^\lambda}. \end{aligned}$$

We aim to find an operator κ_n acting on the A system that normalises T_n to the identity on the symmetric subspace. From the structure of T_n above, and recalling that $\mathrm{Sym}^n\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}\right) \cong \bigoplus_{\lambda \in \Lambda_{n,d_A}} W_A^\lambda \otimes W_R^\lambda$, we can see that the identity on this subspace is $\mathrm{id}_{\mathrm{Sym}} = \bigoplus_\lambda \mathrm{id}_{W_A^\lambda} \otimes \mathrm{id}_{W_R^\lambda}$. By inspection, if we define κ_n as

$$\kappa_n := \bigoplus_{\lambda \in \Lambda_{n,d_A}} \left(\frac{\dim([\lambda])}{\dim(W_R^\lambda)}\right) \mathrm{id}_{W_A^\lambda} \otimes \mathrm{id}_{[\lambda]_A},$$

then $(\kappa_n \otimes \mathrm{id}_{R^n})$ acts on the decomposed space as $\bigoplus_\lambda \frac{\dim([\lambda])}{\dim(W_R^\lambda)} \mathrm{id}_{W_A^\lambda} \otimes \mathrm{id}_{W_R^\lambda}$. Applying its inverse square root to T_n yields the desired identity operator. □

Theorem C.1 (de Finetti reduction with fixed marginal)**.** *Let* $\hat{\sigma}_A \in \mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$ *and let* $\rho_{A^nR^n}$ *be any purification of* $(\hat{\sigma}_A)^{\otimes n}$ *supported on the symmetric subspace* $\mathrm{Sym}^n\left(\mathbb{C}^{d_Ad_R}\right)$*. Then there exists a probability measure* $\mathrm{d}\phi$ *on the set of purifications* $|\phi\rangle\langle\phi|_{AR}$ *of* $\hat{\sigma}_A$*, such that*

$$\rho_{A^nR^n} \leq g_{n,d_Ad_R} \int |\phi\rangle\langle\phi|_{AR}^{\otimes n} \,\mathrm{d}\phi. \tag{C.2}$$

Proof. Assume without loss of generality that $d_A \leq d_R$ and that $\hat{\sigma}_A$ has full rank. The proof proceeds by relating the integral over purifications to the operator T_n from Lemma C.3, and then bounding the given state $\rho_{A^nR^n}$ against this integrated state.

First, note that the set of purifications of $\hat{\sigma}_A$ on $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}$ can be generated by applying local unitaries on the purifying system R to a fixed purification. Specifically, let $|\phi_0\rangle = (\hat{\sigma}_A^{1/2} \otimes \mathrm{id}_R)\,|\theta\rangle$ be a canonical purification, where $|\theta\rangle = \sum_i |i\rangle_A\,|i\rangle_R$. Then any other purification can be written as $|\phi_U\rangle = (\mathrm{id}_A \otimes U)\,|\phi_0\rangle$ for some $U \in \mathcal{U}(\mathbb{C}^{d_R})$. The integral over all such purifications with respect to the Haar measure $\mathrm{d}U$ is

$$\begin{aligned}
\tau_n &:= \int_{\mathrm{Puri}_R(\hat{\sigma}_A)} |\phi\rangle\langle\phi|^{\otimes n} \,\mathrm{d}\phi = \int_{\mathcal{U}(\mathbb{C}^{d_R})} |\phi_U\rangle\langle\phi_U|^{\otimes n} \,\mathrm{d}U \\
&= \int (\mathrm{id}_{A^n} \otimes U^{\otimes n})((\hat{\sigma}_A^{1/2})^{\otimes n} \otimes \mathrm{id}_{R^n})\,|\theta\rangle\langle\theta|^{\otimes n}\,((\hat{\sigma}_A^{1/2})^{\otimes n} \otimes \mathrm{id}_{R^n})(\mathrm{id}_{A^n} \otimes (U^\dagger)^{\otimes n})\mathrm{d}U \\
&= (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n}) \left[\int (\mathrm{id}_{A^n} \otimes U^{\otimes n})\,|\theta\rangle\langle\theta|^{\otimes n}\,(\mathrm{id}_{A^n} \otimes (U^\dagger)^{\otimes n})\mathrm{d}U\right] (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n}) \\
&= (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n}) T_n (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n}),
\end{aligned}$$

where T_n is the operator defined in Lemma C.3.

We wish to prove $\rho_{A^nR^n} \leq g_{n,d_Ad_R}\tau_n$. This is equivalent to showing

$$(\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n})^{-1} \rho_{A^nR^n} (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n})^{-1} \leq g_{n,d_Ad_R} T_n. \tag{C.10}$$

Let us define an operator $\widetilde{\rho} := (\kappa_n \otimes \mathrm{id}_{R^n})^{-1/2} (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n})^{-1} \rho_{A^nR^n} (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n})^{-1} (\kappa_n \otimes \mathrm{id}_{R^n})^{-1/2}$, where κ_n is the operator from Lemma C.3. Using the identity from Equation (C.9), the inequality we need to prove, Equation (C.10), becomes

$$\widetilde{\rho} \leq g_{n,d_Ad_R}\, \mathrm{id}_{\mathrm{Sym}^n\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_R}\right)}. \tag{C.11}$$

Since $\rho_{A^nR^n}$ is supported on the symmetric subspace, so is $\widetilde{\rho}$. As $\widetilde{\rho}$ is a positive semi-definite operator, its ∞-norm (its largest eigenvalue) is bounded by its trace[2]: $\|\widetilde{\rho}\|_\infty \leq$

[2]This inequality is an equality when $\rho_{A^nR^n}$ is a pure state.

$\mathrm{Tr}\left[\widetilde{\rho}\right]$. We now bound this trace. A key observation is that because both $\rho_{A^nR^n}$ and the de Finetti state τ_n are purifications of $\hat{\sigma}_A^{\otimes n}$, their partial trace over system R^n must be equal. This allows us to substitute $\rho_{A^nR^n}$ with τ_n when calculating the trace of an operator acting only on system A^n. More formally, $\mathrm{Tr}\left[\rho_{A^nR^n}(M_{A^n}\otimes \mathrm{id}_{R^n})\right] = \mathrm{Tr}\left[\hat{\sigma}_A^{\otimes n} M_{A^n}\right] = \mathrm{Tr}\left[\tau_n(M_{A^n}\otimes \mathrm{id}_{R^n})\right]$. This lets us proceed as follows:

$$\begin{aligned}
\mathrm{Tr}\left[\widetilde{\rho}\right] &= \mathrm{Tr}\left[(\kappa_n\otimes \mathrm{id}_{R^n})^{-1/2}(\sqrt{\hat{\sigma}_A}^{\otimes n}\otimes \mathrm{id}_{R^n})^{-1}\rho_{A^nR^n}(\sqrt{\hat{\sigma}_A}^{\otimes n}\otimes \mathrm{id}_{R^n})^{-1}(\kappa_n\otimes \mathrm{id}_{R^n})^{-1/2}\right]\\
&= \mathrm{Tr}\left[(\kappa_n\otimes \mathrm{id}_{R^n})^{-1/2}(\sqrt{\hat{\sigma}_A}^{\otimes n}\otimes \mathrm{id}_{R^n})^{-1}\tau_n(\sqrt{\hat{\sigma}_A}^{\otimes n}\otimes \mathrm{id}_{R^n})^{-1}(\kappa_n\otimes \mathrm{id}_{R^n})^{-1/2}\right]\\
&= \mathrm{Tr}\left[(\kappa_n\otimes \mathrm{id}_{R^n})^{-1/2}T_n(\kappa_n\otimes \mathrm{id}_{R^n})^{-1/2}\right]\\
&= \mathrm{Tr}\left[\mathrm{id}_{\mathrm{Sym}^n\left(\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_R}\right)}\right]\\
&= \dim(\mathrm{Sym}^n\left(\mathbb{C}^{d_Ad_R}\right)) = g_{n,d_Ad_R}.
\end{aligned}$$

Since $\widetilde{\rho}$ is supported on the symmetric subspace and its trace is g_{n,d_Ad_R}, its maximum eigenvalue is at most g_{n,d_Ad_R}. This confirms Equation (C.11) and completes the proof. □

Theorem C.2 (de Finetti reduction with symmetries and fixed marginal)**.** *Let $\hat{\sigma}_A \in \mathrm{Pos}\left(\mathbb{C}^{d_A}\right)$, and let $\rho_{A^nR^n}$ be any purification of $(\hat{\sigma}_A)^{\otimes n}$ supported on the symmetric subspace $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_i^R}\right)$ where $\bigoplus_{i=1}^k \mathbb{C}^{d_i^A}\subseteq\mathbb{C}^{d_A}$ and $\bigoplus_{i=1}^k \mathbb{C}^{d_i^R}\subseteq\mathbb{C}^{d_R}$. Then there exists a probability measure $d\phi$ on the set of purifications $|\phi\rangle_{AR}\in\bigoplus_{i=1}^k \mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_i^R}$ of $\hat{\sigma}_A$ such that*

$$\rho_{A^nR^n} \leq g_{n,x}\int |\phi\rangle\langle\phi|_{AR}^{\otimes n}\,\mathrm{d}\phi, \tag{C.4}$$

where $x=\sum_{i=1}^k d_i^Ad_i^R$.

Proof. The proof extends the logic of the generic case (Theorem C.1) to states with a block-diagonal structure. The core idea is to show that the entire analysis, including the Hilbert space structure, the set of purifications, and the Haar integration, respects this block-diagonal form. This allows us to apply the result of Lemma C.3 within each block and then combine the results.

The state $\rho_{A^nR^n}$ is supported on the symmetric subspace of $\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i^A}\otimes\mathbb{C}^{d_i^R}\right)^{\otimes n}$. A fundamental result for symmetric powers of direct sums states that this space itself decomposes into sectors, corresponding to how the n 'particles' are distributed among the k blocks. If we choose n_1 particles from block 1, n_2 from block 2, and so on, such that

$\sum_{i=1}^{k} n_i = n$, the resulting state must be symmetric under permutations of the n_i particles within each block. This leads to the isomorphism [112, Eq. (6.7.1)],

$$\mathrm{Sym}^n\left(\bigoplus_{i=1}^{k} \mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}\right) = \bigoplus_{n_1+\cdots+n_k=n} \left(\bigotimes_{i=1}^{k} \mathrm{Sym}^{n_i}\left(\mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}\right)\right).$$

This decomposition is the key structural feature we will exploit.

The marginal state $\hat{\sigma}_A$ is block-diagonal, i.e., $\hat{\sigma}_A = \bigoplus_{i=1}^{k} \hat{\sigma}_A^i$ where $\hat{\sigma}_A^i$ acts on $\mathbb{C}^{d_i^A}$. A purification $|\phi\rangle$ of $\hat{\sigma}_A$ that lies within the block-diagonal space $\bigoplus_{i=1}^{k} \mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}$ must itself be a direct sum of purifications of the block marginals: $|\phi\rangle = \bigoplus_{i=1}^{k} |\phi_i\rangle$, where $\mathrm{Tr}_{R_i}\left[|\phi_i\rangle\langle\phi_i|\right] = \hat{\sigma}_A^i$. The set of all such purifications can be generated by applying local unitaries $U_i \in \mathcal{U}(\mathbb{C}^{d_i^R})$ within each block i. The de Finetti state $\tau_n = \int |\phi\rangle\langle\phi|^{\otimes n} \, \mathrm{d}\phi$ is related to an operator T via $\tau_n = (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n}) T (\sqrt{\hat{\sigma}_A}^{\otimes n} \otimes \mathrm{id}_{R^n})$, where T is given by the integral,

$$T = \int \left(\bigoplus_{i=1}^{k} (\mathrm{id}_{A_i} \otimes U_i) \, |\theta_i\rangle\langle\theta_i| \, (\mathrm{id}_{A_i} \otimes U_i^\dagger)\right)^{\otimes n} \mathrm{d}U_1 \cdots \mathrm{d}U_k.$$

Here, $|\theta_i\rangle = \sum_{j=1}^{d_i^A} |j\rangle_{A_i} |j\rangle_{R_i}$. Expanding the tensor power using the multinomial theorem produces terms corresponding to choosing n_i copies of the i-th block for all combinations where $\sum n_i = n$. Formally,

$$T = \bigoplus_{n_1+\cdots+n_k=n} \bigotimes_{i=1}^{k} T_{n_i}^{(i)}, \quad \text{where} \quad T_{n_i}^{(i)} = \int \left((\mathrm{id}_{A_i} \otimes U_i) \, |\theta_i\rangle\langle\theta_i| \, (\mathrm{id}_{A_i} \otimes U_i^\dagger)\right)^{\otimes n_i} \mathrm{d}U_i.$$

Each $T_{n_i}^{(i)}$ is precisely the operator studied in Lemma C.3 for n_i copies on the Hilbert space $\mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}$.

From Lemma C.3, for each block i and each copy number $m \in \{1, \ldots, n\}$, there exists an invertible operator $\kappa_m^{(i)} \in \mathrm{L}\left((\mathbb{C}^{d_i^A})^{\otimes m}\right)$ such that $(\kappa_m^{(i)} \otimes \mathrm{id}_{R_i^m})^{-1/2} T_m^{(i)} (\kappa_m^{(i)} \otimes \mathrm{id}_{R_i^m})^{-1/2} = \mathrm{id}_{\mathrm{Sym}^m(\mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R})}$. We construct a global normalising operator κ that respects the block structure of T as,

$$\kappa := \bigoplus_{n_1+\cdots+n_k=n} \bigotimes_{i=1}^{k} \kappa_{n_i}^{(i)}.$$

Applying this operator to T normalises each block of the direct sum correctly,

$$(\kappa \otimes \mathrm{id}_{R^n})^{-1/2} T (\kappa \otimes \mathrm{id}_{R^n})^{-1/2} = \bigoplus_{n_1+\cdots+n_k=n} \bigotimes_{i=1}^{k} \mathrm{id}_{\mathrm{Sym}^{n_i}(\mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R})}$$
$$= \mathrm{id}_{\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i^A} \otimes \mathbb{C}^{d_i^R}\right)}.$$

The rest of the proof follows similarly as in the proof of Theorem C.1. □

Lemma C.1. *Let $\rho_{A^nB^n} \in \mathrm{Pos}\left(\left(\mathbb{C}^{d_A d_B}\right)^{\otimes n}\right)$ be a permutation-invariant and IID-block-diagonal matrix with respect to projections $\{\Pi_i\}_{i=1}^k$ of dimension $\{d_i\}_{i=1}^k$. Then there exists a purification of $\rho_{A^nB^n}$ supported on $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i} \otimes \mathbb{C}^{d_i}\right)$.*

Proof. This proof is very similar to the proof of Lemma 4.2.2 from Ref. [52]. The proof is constructive. We will explicitly build a purification for $\rho_{A^nB^n}$ and then demonstrate that it has the required properties: first, that it lies in the Hilbert space corresponding to the block-diagonal structure, and second, that it is invariant under permutations. A vector that satisfies both these properties must lie in the symmetric subspace of the block-diagonal Hilbert space.

Let the spectral decomposition of $\rho_{A^nB^n}$ be $\rho_{A^nB^n} = \sum_\lambda \lambda \Pi_\lambda$, where Π_λ is the projector onto the eigenspace corresponding to the eigenvalue λ. Since $\rho_{A^nB^n}$ is IID-block-diagonal, it commutes with the projectors $\Pi_{\vec{j}} \coloneqq \Pi_{j_1} \otimes \cdots \otimes \Pi_{j_n}$. This means we can choose an orthonormal basis of eigenvectors $\{|x\rangle\}$ for $\rho_{A^nB^n}$ such that each eigenvector $|x\rangle$ lies entirely within a single block, i.e., $\Pi_{\vec{j}} |x\rangle = |x\rangle$ for some $\vec{j}$.

Let $\mathcal{H}_{ABE} = (\mathbb{C}^{d_A d_B}) \otimes (\mathbb{C}^{d_A d_B})$ be the extended Hilbert space, where the purifying system E is a copy of the original system AB. We define an unnormalised pure state for each eigenspace λ as,

$$\left|\Psi^\lambda\right\rangle \coloneqq \sum_{x \in \mathcal{X}_\lambda} |x\rangle_{AB} \otimes \overline{|x\rangle}_E,$$

where $\mathcal{X}_\lambda$ is an orthonormal basis for the eigenspace of λ, and the complex conjugation is taken in the standard basis used to define the eigenvectors. The overall purification of $\rho_{A^nB^n}$ is then constructed as,

$$|\Psi\rangle \coloneqq \sum_\lambda \sqrt{\lambda} \left|\Psi^\lambda\right\rangle = \sum_x \sqrt{\lambda_x} |x\rangle_{AB} \otimes \overline{|x\rangle}_E.$$

It can be verified that this is a valid purification as

$$\begin{aligned}\mathrm{Tr}_E\left[|\Psi\rangle\langle\Psi|\right] &= \sum_{x,y}\sqrt{\lambda_x\lambda_y}\mathrm{Tr}_E\left[|x\rangle\langle y|)_{AB}\otimes(|\overline{x}\rangle\langle\overline{y}|)_E\right] \\ &= \sum_x \lambda_x\,|x\rangle\langle x| = \rho_{A^nB^n}.\end{aligned}$$

Now, we show that $|\Psi\rangle$ lies in the correct block-diagonal subspace. Each eigenvector $|x\rangle$ is a tensor product $|x\rangle = |x_1\rangle\otimes\cdots\otimes|x_n\rangle$, where each $|x_m\rangle$ lies in the subspace associated with a single projector Π_{j_m}. Therefore, $|x\rangle$ lies in the subspace $\bigotimes_{m=1}^n \mathbb{C}^{d_{j_m}}$. Its conjugate, $\overline{|x\rangle}$, lies in the corresponding conjugate space, which for purification purposes we identify with a copy of the same space. Since the full purification $|\Psi\rangle$ is a linear combination of such states, it must lie in the direct sum of all such possible tensor product spaces,

$$|\Psi\rangle \in \bigoplus_{\vec{j}\in[k]^n}\bigotimes_{m=1}^n\left(\mathbb{C}^{d_{j_m}}\otimes\mathbb{C}^{d_{j_m}}\right).$$

This space is precisely the n-fold tensor product of the direct-sum space describing a single system, i.e.,

$$|\Psi\rangle \in \left(\bigoplus_{i=1}^k \mathbb{C}^{d_i}\otimes\mathbb{C}^{d_i}\right)^{\otimes n}.$$

The permutation invariance of $\rho_{A^nB^n}$ means that for any permutation $\pi\in S_n$, the corresponding unitary operator $P_\pi^{d_Ad_B,n}$ commutes with $\rho_{A^nB^n}$. This implies that $P_\pi^{d_Ad_B,n}$ preserves the eigenspaces of $\rho_{A^nB^n}$; it maps the eigenspace Π_λ to itself. The state $\left|\Psi^\lambda\right\rangle$ is constructed as a sum over a complete basis for the eigenspace Π_λ. As shown in detail in [52], this implies that $\left|\Psi^\lambda\right\rangle$ is invariant under the action of the permutation on the joint system,

$$(P_\pi^{d_Ad_B,n})_{AB}\otimes(\overline{P_\pi^{d_Ad_B,n}})_E\left|\Psi^\lambda\right\rangle = \left|\Psi^\lambda\right\rangle.$$

Since the full purification $|\Psi\rangle$ is a linear combination of these invariant states, it too must be permutation-invariant.

We have shown that the purification $|\Psi\rangle$ satisfies two properties:

1. It belongs to the tensor product space $\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i}\otimes\mathbb{C}^{d_i}\right)^{\otimes n}$.

2. It is invariant under permutations of the n tensor factors.

A vector is, by definition, in the symmetric subspace $\mathrm{Sym}^n(\mathcal{H})$ if and only if it belongs to $\mathcal{H}^{\otimes n}$ and is invariant under permutations. By identifying $\mathcal{H} = \bigoplus_{i=1}^k \mathbb{C}^{d_i} \otimes \mathbb{C}^{d_i}$, we see that $|\Psi\rangle$ satisfies both conditions for this choice of $\mathcal{H}$. Therefore, the purification $|\Psi\rangle$ is supported on $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{d_i} \otimes \mathbb{C}^{d_i}\right)$, as required. □

Lemma C.2. *Let G be a compact group and let $\{U_g\}_{g\in G}$ be a unitary representation of G on $\mathbb{C}^{d_A d_B}$ with k irreducible representations with multiplicity $\{m_i\}_{i=1}^k$. If $\rho_{A^nB^n} \in \mathrm{Pos}\left((\mathbb{C}^{d_A d_B})^{\otimes n}\right)$ is permutation invariant and IID-G-invariant, then there exists a purification of $\rho_{A^nB^n}$ on $\mathrm{Sym}^n\left(\bigoplus_{i=1}^k \mathbb{C}^{m_i} \otimes \mathbb{C}^{m_i}\right)$.*

To prove this, we first prove the following lemma.

Lemma C.4. *Suppose $\pi_1 : G \to \mathcal{U}(\mathbb{C}^d)$ and $\pi_2 : G \to \mathcal{U}(\mathbb{C}^{d'})$ are two irreps of a compact group G. Let $\Pi := \int_G \pi_1(g) \otimes \overline{\pi_2(g)}\,\mathrm{d}\mu(g)$, where μ is the Haar measure on G. Then Π is an orthogonal projection, and its rank is given by its trace*

$$\mathrm{Tr}\,[\Pi] = \begin{cases} 1 & \text{if } \pi_1 \cong \pi_2 \text{ (\textit{the irreps are equivalent})} \\ 0 & \text{if } \pi_1 \ncong \pi_2 \text{ (\textit{the irreps are inequivalent})} \end{cases}.$$

Proof. The proof proceeds in two parts. First, we show Π is a projector. Second, we calculate its trace using the orthogonality of characters for irreducible representations.

The operator Π is constructed by averaging over the entire group, which makes it invariant under the group action. Specifically, for any $h \in G$,

$$\begin{aligned}(\pi_1(h) \otimes \overline{\pi_2(h)})\Pi &= \int_G \pi_1(h)\pi_1(g) \otimes \overline{\pi_2(h)\pi_2(g)}\,\mathrm{d}\mu(g) \\ &= \int_G \pi_1(hg) \otimes \overline{\pi_2(hg)}\,\mathrm{d}\mu(g) = \int_G \pi_1(g') \otimes \overline{\pi_2(g')}\,\mathrm{d}\mu(g') = \Pi,\end{aligned}$$

where we used the left-invariance of the Haar measure ($g' = hg$, $\mathrm{d}\mu(g') = \mathrm{d}\mu(g)$). Now we can show $\Pi^2 = \Pi$ as

$$\Pi^2 = \Pi\left(\int_G \pi_1(g) \otimes \overline{\pi_2(g)}\,\mathrm{d}\mu(g)\right) = \int_G \Pi(\pi_1(g) \otimes \overline{\pi_2(g)})\,\mathrm{d}\mu(g) = \int_G \Pi\,\mathrm{d}\mu(g) = \Pi.$$

Since $\Pi^2 = \Pi$ and it is self-adjoint, it is an orthogonal projection.

The trace of the integral is the integral of the trace. The trace of a tensor product of operators is the product of their traces. Let $\chi_1(g) = \operatorname{Tr}[\pi_1(g)]$ and $\chi_2(g) = \operatorname{Tr}[\pi_2(g)]$ be the characters of the two representations.

$$\operatorname{Tr}[\Pi] = \int_G \operatorname{Tr}\left[\pi_1(g) \otimes \overline{\pi_2(g)}\right] \mathrm{d}\mu(g) = \int_G \operatorname{Tr}[\pi_1(g)] \operatorname{Tr}\left[\overline{\pi_2(g)}\right] \mathrm{d}\mu(g) = \int_G \chi_1(g)\overline{\chi_2(g)}\, \mathrm{d}\mu(g).$$

This last expression is the inner product of the characters, $\langle \chi_1, \chi_2 \rangle$. The Great Orthogonality Theorem for characters of irreducible representations states that this inner product is 1 if the representations are equivalent ($\pi_1 \cong \pi_2$) and 0 otherwise. This completes the proof of the lemma. □

We now use this result to prove the main lemma.

Proof of Lemma C.2. The logic of this proof closely mirrors that of Lemma C.1. We first construct a purification for $\rho_{A^n B^n}$ and then show that the combined symmetries of permutation-invariance and IID-G-invariance confine this purification to the desired smaller symmetric subspace.

The construction of the purification is identical to the construction in Lemma C.1. We define the purification $|\Psi\rangle = \sum_x \sqrt{\lambda_x}\, |x\rangle_{AB} \otimes \overline{|x\rangle}_E$, where $\{|x\rangle\}$ are the eigenvectors of $\rho_{A^n B^n}$ with corresponding eigenvalues λ_x. The permutation-invariance of $\rho_{A^n B^n}$ implies the permutation-invariance of its eigenspaces, which in turn implies that the constructed purification $|\Psi\rangle$ is invariant under permutations of the n tensor factors.

The IID-G-invariance of $\rho_{A^n B^n}$ means that for any choice of group elements $\vec{g} = (g_1, \ldots, g_n) \in G^n$, the state is invariant: $U_{\vec{g}} \rho_{A^n B^n} U_{\vec{g}}^\dagger = \rho_{A^n B^n}$, where $U_{\vec{g}} = \bigotimes_{i=1}^n U_{g_i}$. This implies that the operator $U_{\vec{g}}$ preserves the eigenspaces of $\rho_{A^n B^n}$. Following the same logic as for permutation invariance, the canonical purification $|\Psi\rangle$ constructed from these eigenspaces must also be invariant under the corresponding action on the purifying system

$$(U_{\vec{g}} \otimes \overline{U_{\vec{g}}})\, |\Psi\rangle = |\Psi\rangle \quad \text{for all } \vec{g} \in G^n.$$

Now, consider the operator $\Pi = \int_G \pi(g) \otimes \overline{\pi(g)}\, \mathrm{d}\mu(g)$, where $\pi(g) = U_g$. The purification

$|\Psi\rangle$ lies in the support of $\Pi^{\otimes n}$,

$$\begin{aligned}\Pi^{\otimes n}|\Psi\rangle &= \left(\int_G \pi(g)\otimes\overline{\pi(g)}\,\mathrm{d}\mu(g)\right)^{\otimes n}|\Psi\rangle \\ &= \int_{G^n}\left(\bigotimes_{i=1}^n \pi(g_i)\otimes\overline{\pi(g_i)}\right)|\Psi\rangle\ \mathrm{d}\mu(\vec{g}) \\ &= \int_{G^n}(U_{\vec{g}}\otimes\overline{U_{\vec{g}}})\,|\Psi\rangle\ \mathrm{d}\mu(\vec{g}) = \int_{G^n}|\Psi\rangle\ \mathrm{d}\mu(\vec{g}) = |\Psi\rangle\,.\end{aligned}$$

Since $\Pi^{\otimes n}$ is a projector, this identity means that $|\Psi\rangle$ lies entirely within the support of $\Pi^{\otimes n}$.

The support of the projector Π is the G-invariant subspace of $\mathbb{C}^{d_{AB}}\otimes\mathbb{C}^{d_{AB}}$. To find its dimension, we decompose the representation π on $\mathbb{C}^{d_{AB}}$ into its k inequivalent irreps with multiplicities $\{m_i\}_{i=1}^k$. Using Lemma C.4, the rank of Π is the sum of ranks from all pairs of equivalent irreps:

$$\mathrm{rank}(\Pi) = \mathrm{Tr}\left[\Pi\right] = \sum_{i=1}^k\sum_{j,j'=1}^{m_i}\mathrm{Tr}\left[\int_G \pi_i^{(j)}(g)\otimes\overline{\pi_i^{(j')}(g)}\,\mathrm{d}\mu(g)\right] = \sum_{i=1}^k\sum_{j,j'=1}^{m_i}1 = \sum_{i=1}^k m_i^2.$$

Thus, the support of Π is a Hilbert space of dimension $\sum_i m_i^2$. We have shown that the purification $|\Psi\rangle$ satisfies two properties:

1. It belongs to the space $(\mathrm{supp}(\Pi))^{\otimes n}$, which is isomorphic to $(\mathbb{C}^{\sum m_i^2})^{\otimes n}$.
2. It is invariant under permutations of the n tensor factors.

Together, these facts imply that $|\Psi\rangle$ must lie in the symmetric subspace of the G-invariant space, $\mathrm{Sym}^n(\mathrm{supp}(\Pi))$. This subspace is isomorphic to $\mathrm{Sym}^n(\mathbb{C}^{\sum m_i^2})$, which completes the proof. □

Appendix D

Computing deviation metrics for phase error estimation

In this appendix we compute the various deviations from ideality required for phase error estimation in Chapter 6.

D.1 Deviation metrics for sampling strategy in Section 6.3

In this section we compute upper bounds on the deviation metrics δ_1, δ_2. To do so, we follow the following recipe:

1. Start with POVM $\{\Gamma_{(b_A,b_B),(\neq)}, \Gamma_{(b_A,b_B),(=)}, \Gamma_{(b_A,b_B),(\text{no-click})}\}$ 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.

2. Pick basis-independent filter $\tilde{F} \geq \Gamma_{(b_A,b_B),(\neq)} + \Gamma_{(b_A,b_B),(=)}$ 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 [5, Lemma 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 $\{\tilde{F}_{(b_A,b_B),(\text{no-click})}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$ where

$$\begin{aligned}
\tilde{F}_{(b_A,b_B),(\text{no-click})} &= \sqrt{\tilde{F}}^{+}(\tilde{F} - \Gamma_{(b_A,b_B),(\neq)} - \Gamma_{(b_A,b_B),(\neq)})\sqrt{\tilde{F}}^{+} + \mathbb{I} - \Pi_{\tilde{F}} \\
\tilde{F}_{(b_A,b_B),(\neq)} &= \sqrt{\tilde{F}}^{+}\Gamma_{(b_A,b_B),(\neq)}\sqrt{\tilde{F}}^{+} \\
\tilde{F}_{(b_A,b_B),(=)} &= \sqrt{\tilde{F}}^{+}\Gamma_{(b_A,b_B),(=)}\sqrt{\tilde{F}}^{+}
\end{aligned} \tag{D.1}$$

where $\Pi_{\tilde{F}}$ denotes the projector onto the support of $\tilde{F}$. This projector plays a trivial rule in the measurement itself, and is only included to ensure that we obtain a valid POVM.

3. Consider the new POVM $\{\tilde{F}_{(b_A,b_B),(\text{no-click})}, \tilde{F}_{(b_A,b_B),(=)}, \tilde{F}_{(b_A,b_B),(\neq)}\}$. Using [5, Lemma 1] again, divide this POVM measurement into two steps. The first step is implemented using $\{F_{(b_A,b_B),(\text{con})}, F_{(b_A,b_B),(\text{no-click})}\}$ 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

$$\begin{aligned}
F_{(b_A,b_B),(\text{con})} &= \tilde{F}_{(b_A,b_B),(\neq)} + \tilde{F}_{(b_A,b_B),(=)} \\
F_{(b_A,b_B),(\text{no-click})} &= \tilde{F}_{(b_A,b_B),(\text{no-click})} \\
G^{\text{con}}_{(b_A,b_B),(\neq)} &= \sqrt{F_{(b_A,b_B),(\text{con})}}^{+}\tilde{F}_{(b_A,b_B),(\neq)}\sqrt{F_{(b_A,b_B),(\text{con})}}^{+} \\
G^{\text{con}}_{(b_A,b_B),(=)} &= \sqrt{F_{(b_A,b_B),(\text{con})}}^{+}\tilde{F}_{(b_A,b_B),(=)}\sqrt{F_{(b_A,b_B),(\text{con})}}^{+} + \mathbb{I} - \Pi_{F_{(b_A,b_B),(\text{con})}}
\end{aligned} \tag{D.2}$$

where $\Pi_{F_{(b_A,b_B),(\text{con})}}$ is the projector onto the support of $F_{(b_A,b_B),(\text{con})}$. This projector plays a trivial rule in the measurement itself, and is only included to ensure that we obtain a valid POVM.

4. Compute

$$\begin{aligned}
\delta_1 &= 2\left\| \sqrt{F_{(Z),(\text{con})}}G^{\text{con}}_{(X),(\neq)}\sqrt{F_{(Z),(\text{con})}} - \sqrt{F_{(X),(\text{con})}}G^{\text{con}}_{(X),(\neq)}\sqrt{F_{(X),(\text{con})}}\right\|_\infty \\
\delta_2 &= \left\|\mathbb{I} - F_{(Z),(\text{con})}\right\|_\infty
\end{aligned} \tag{D.3}$$

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 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. (D.3) over all possible choices of η_{b_i}, d_{b_i}.

D.1.1 Computing POVMs

The joint Alice-Bob POVM elements for the basis b are given by

$$\begin{aligned}
\Gamma_{(b,b),(\text{no-click})} =& \mathbb{I}_A \otimes \sum_{N_0,N_1=0}^{\infty} (1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
\Gamma_{(b,b),(\neq)} =& \left|0\right\rangle\!\left\langle 0\right|_b \otimes (1-d_0) \sum_{N_0,N_1=0}^{\infty} (1-\eta_0)^{N_0}(1-(1-d_1)(1-\eta_1)^{N_1}) \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \left|1\right\rangle\!\left\langle 1\right|_b \otimes (1-d_1) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_0)(1-\eta_0)^{N_0})(1-\eta_1)^{N_1} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \mathbb{I}_A \otimes \frac{1}{2}\Gamma^{(B)}_{(b,\text{dc})} \\
\Gamma_{(b,b),(=)} =& \left|0\right\rangle\!\left\langle 0\right|_b \otimes (1-d_1) \sum_{N_0,N_1=0}^{\infty} (1-(1-d_0)(1-\eta_0)^{N_0})(1-\eta_1)^{N_1} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \left|1\right\rangle\!\left\langle 1\right|_b \otimes (1-d_0) \sum_{N_0,N_1=0}^{\infty} (1-\eta_0)^{N_0}(1-(1-d_1)(1-\eta_1)^{N_1}) \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b \\
&+ \mathbb{I}_A \otimes \frac{1}{2}\Gamma^{(B)}_{(b,\text{dc})},
\end{aligned} \tag{D.4}$$

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. Bob's double click POVM for basis $b \in \{Z,X\}$ is $\Gamma^{(B)}_{(b,\text{dc})} = \sum_{N_0,N_1=0}^{\infty}(1-(1-d_0)(1-\eta_0)^{N_0})(1-(1-d_1)(1-\eta_1)^{N_1}) \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b$, where $\left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_b$ 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.

We can choose

$$\begin{aligned}
\tilde{F} &= \mathbb{I}_A \otimes \left((1-(1-d_0)(1-d_1)) \left|0,0\right\rangle\!\left\langle 0,0\right| + \sum_{N_0,N_1=0}^{\infty} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_Z \right) \\
&= \mathbb{I}_A \otimes \left((1-(1-d_0)(1-d_1)) \left|0,0\right\rangle\!\left\langle 0,0\right| + \sum_{N_0,N_1=0}^{\infty} \left|N_0,N_1\right\rangle\!\left\langle N_0,N_1\right|_X \right),
\end{aligned} \tag{D.5}$$

In this appendix, as in the rest of this work, we assume that $d_i \in [0, d_{\max}]$.

It is straightforward to verify that $\tilde{F}$ satisfies our requirement $\tilde{F} \geq \Gamma_{(b_A,b_B),(\neq)} + \Gamma_{(b_A,b_B),(=)} = \mathbb{I} - \Gamma_{(b_A,b_B),(\text{no-click})}$ for all choices of b_A, b_B. Then, we calculate the POVM elements from Eq. (D.2) as

$$\begin{aligned}
F_{(b),(\text{con})} &= \mathbb{I}_A \otimes |0,0\rangle\langle 0,0| \\
&\quad + \sum_{\substack{N_0,N_1 \\ N_0+N_1\neq 0}}^{\infty} \left(1-(1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1}\right) |N_0,N_1\rangle\langle N_0,N_1|_b \\
G^{\text{con}}_{(b),(\neq)} &= \sum_{N_0,N_1=0}^{\infty} |0\rangle\langle 0|_b \otimes \frac{(1+(1-d_0)(1-\eta_0)^{N_0})(1-(1-d_1)(1-\eta_1)^{N_1})}{2(1-(1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
&\quad + |1\rangle\langle 1|_b \otimes \frac{(1+(1-d_1)(1-\eta_1)^{N_1})(1-(1-d_0)(1-\eta_0)^{N_0})}{2(1-(1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
G^{\text{con}}_{(b),(=)} &= \sum_{N_0,N_1=0}^{\infty} |0\rangle\langle 0|_b \otimes \frac{(1+(1-d_1)(1-\eta_1)^{N_1})(1-(1-d_0)(1-\eta_0)^{N_0})}{2(1-(1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \\
&\quad + |1\rangle\langle 1|_b \otimes \frac{(1+(1-d_0)(1-\eta_0)^{N_0})(1-(1-d_1)(1-\eta_1)^{N_1})}{2(1-(1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1})} |N_0,N_1\rangle\langle N_0,N_1|_b \,.
\end{aligned} \tag{D.6}$$

D.1.2 Computing δ_1

To compute the costs in Eq. (D.3), we first note that all POVMs are block-diagonal in the total photon number $N_0 + N_1$. We wish to compute the infinity norm, i.e

$$\delta_1 = 2\left\| \sqrt{F_{(Z),(\text{con})}} G^{\text{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\text{con})}} - \sqrt{F_{(X),(\text{con})}} G^{\text{con}}_{(X),(\neq)} \sqrt{F_{(X),(\text{con})}} \right\|_{\infty}.$$

Due to block-diagonal structure, the operator appearing inside the $\|.\|_\infty$ in the above expressions are also block-diagonal in photon number $N_0 + N_1$. From the properties of the norm, we have that

$$\delta_1 = \max_N \delta_1^{(N)}, \tag{D.7}$$

where $\delta_1^{(N)}$ is the infinity norm for the block corresponding to total photon number $N = N_0 + N_1$. We now focus on computing $\delta_1^{(N)}$.

First, we compute $\delta_1^{(0)} = 0$ as we assume that the dark count rates do not depend on basis choice:

$$\begin{aligned}
\frac{\delta_1^{(0)}}{2} =& \left\| |0,0\rangle\langle 0,0| \left(\sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right) |0,0\rangle\langle 0,0| \right\|_\infty \\
=& \left| \frac{1-(1-d_0)(1-d_1)}{1-(1-d_0)(1-d_1)} - \frac{1-(1-d_0)(1-d_1)}{1-(1-d_0)(1-d_1)} \right| \\
& \max\left\{ \frac{d_1(2-d_0)}{2(1-(1-d_0)(1-d_1))}, \frac{d_0(2-d_1)}{2(1-(1-d_0)(1-d_1))} \right\} \\
=& 0.
\end{aligned}$$

To bound $\delta_1^{(N)}$ for $N \neq 0$, we write

$$\begin{aligned}
\frac{\delta_1}{2} =& \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \\
\leq& \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \\
& + \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \qquad \text{(D.8)} \\
\leq& \left\| \sqrt{F_{(Z),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \right\|_\infty \left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \\
& + \left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \left\| G^{\mathrm{con}}_{(X),(\neq)} \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty, \qquad \text{(D.9)}
\end{aligned}$$

where Eq. (D.8) follows from the triangle inequality, and Eq. (D.9) follows from the submultiplicativity of the ∞-norm. We can then compute each term individually. Note that due to the submultiplicativity of the ∞-norm, we have

$$\left\| \sqrt{F_{(b),(\mathrm{con})}} G^{\mathrm{con}}_{(X),(\neq)} \right\|_\infty \leq \left\| \sqrt{F_{(b),(\mathrm{con})}} \right\|_\infty \left\| G^{\mathrm{con}}_{(X),(\neq)} \right\|_\infty \leq 1. \qquad \text{(D.10)}$$

Thus, we only need to bound $\left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty$. To do so, we define

$$\begin{aligned}
P \coloneqq & \mathbb{I}_A \otimes \sum_{N=0}^{\infty} \sum_{N_0+N_1=N} \frac{1+\sqrt{1-(1-\eta)^N}}{2} |N_0,N_1\rangle\langle N_0,N_1|_X \\
= & \mathbb{I}_A \otimes \sum_{N=0}^{\infty} \sum_{N_0+N_1=N} \frac{1+\sqrt{1-(1-\eta)^N}}{2} |N_0,N_1\rangle\langle N_0,N_1|_Z ,
\end{aligned} \qquad \text{(D.11)}$$

and obtain

$$\left\| \sqrt{F_{(Z),(\mathrm{con})}} - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty \leq \left\| \sqrt{F_{(Z),(\mathrm{con})}} - P \right\|_\infty + \left\| P - \sqrt{F_{(X),(\mathrm{con})}} \right\|_\infty, \qquad \text{(D.12)}$$

where Eq. (D.12) is a consequence of the triangle inequality. Let us focus on a fixed value of $N = N_0 + N_1 \neq 0$. In this case, combining Eqs. (D.9), (D.10) and (D.12) allows us to obtain

$$\begin{aligned}\delta_1^{(N)} &\leq 8\left|\sqrt{1-(1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1}} - \frac{1+\sqrt{1-(1-\eta)^{N_0+N_1}}}{2}\right| \\ &\leq 4\left|1-\sqrt{1-(1-\eta)^N}\right|,\end{aligned} \tag{D.13}$$

where the final inequality above follows from the monotonicity of the expression inside the modulus with respect to η_0, η_1, d_0, d_1. Finally, the monotonicity of Eq. (D.13) with respect to N, gives

$$\delta_1 \leq 4\left(1-\sqrt{\eta_{\min}}\right). \tag{D.14}$$

where $\eta_{\min} < \eta$ is the minimum allowed efficiency.

D.1.3 Computing δ_2

We can now also compute $\delta_2 = \left\|\mathbb{I} - F_{(Z),(\mathrm{con})}\right\|_\infty$ in a similar way, using Eqs. (D.3) and (D.6). Again, we have $\delta_2 = \max_N \delta_2^{(N)}$. First we compute $\delta_2^{(0)} = 0$ as

$$\delta_2^{(0)} = 1 - \frac{1-(1-d_0)(1-d_1)}{1-(1-d_0)(1-d_1)} = 0.$$

Thus, we compute δ_2 as

$$\begin{aligned}\delta_2 &= \max_{N_0+N_1=N\neq 0}\left\{(1-d_0)(1-d_1)(1-\eta_{Z_0})^{N_0}(1-\eta_{Z_1})^{N_1}\right\} \\ &\leq \max_{N_0+N_1=N}\left\{(1-\eta_{\min})^N\right\} &\text{(D.15)} \\ &\leq 1-\eta_{\min}, &\text{(D.16)}\end{aligned}$$

where the second inequality follows from the fact that the term inside is monotonous with respect to $\eta_{Z_0}, \eta_{Z_1}, d_0, d_1$.

D.2 Bounding number of flags for phase error estimation with noise channel

In this section, we bound the quantities needed to upper bound the number of flags used in the phase error estimation in Section 6.4.1. Specifically,

- we upper bound the deviation from ideality $q_{>0}$ which represents the probability of the noise channel to send a round to the flag space, and
- we lower bound the minimum eigenvalue of $\Pi_{>0}\Gamma_{\text{det},\,b}\Pi_{>0}$ required to upper bound the number of non-zero photon rounds.

These bounds depend on the POVM elements in each basis:

$$\begin{aligned}
\Gamma^{\mathbf{d_B},\boldsymbol{\eta}}_{\text{no-click},\,b} &= \sum_{N_0,N_1=0}^{\infty} (1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1}\,|N_0,N_1\rangle\langle N_0,N_1|_b \\
\Gamma^{\mathbf{d_B},\boldsymbol{\eta}}_{0,\,b} &= \sum_{N_0,N_1=0}^{\infty} \frac{1}{2}(1-(1-d_0)(1-\eta_0)^{N_0})(1+(1-d_1)(1-\eta_1)^{N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_b \\
\Gamma^{\mathbf{d_B},\boldsymbol{\eta}}_{1,\,b} &= \sum_{N_0,N_1=0}^{\infty} \frac{1}{2}(1+(1-d_0)(1-\eta_0)^{N_0})(1-(1-d_1)(1-\eta_1)^{N_1})\,|N_0,N_1\rangle\langle N_0,N_1|_b\,,
\end{aligned} \tag{D.17}$$

where d_0, d_1 and η_0, η_1 are the dark count rates and efficiencies of the two detectors, and $|N_0,N_1\rangle\langle N_0,N_1|_b$ 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. These POVM elements are related to the POVM elements in Eq. (D.4), except we only need to consider Bob's POVM elements.

D.2.1 Bounding deviation from ideality

We now proceed by upper bounding the deviation from ideality $q_{>0}$. This is defined such that $\Gamma^{\mathbf{d_B},\boldsymbol{\eta}}_{>0;\;i,\,b} \geq (1-q_{>0})\Gamma_{>0;\;i,\,b}$ for all outcomes i and bases b. As both POVM elements corresponding to a specific outcome are diagonal in the same photon-number basis, the operator inequality reduces to a set of scalar inequalities on their corresponding eigenvalues. Thus, it is sufficient to lower bound the ratio of their eigenvalues[1] $\lambda^{\mathbf{d_B},\boldsymbol{\eta}}_{i;\;N_0,N_1}$ and $\lambda_{i;\;N_0,N_1}$:

$$q_{>0} \geq 1 - \min_{\substack{i \\ N_0+N_1\neq 0}} \left\{ \frac{\lambda^{\mathbf{d_B},\boldsymbol{\eta}}_{i;\;N_0,N_1}}{\lambda_{i;\;N_0,N_1}} \right\}. \tag{D.18}$$

The ideal $\Gamma_{>0;\;\text{no-click},\,b}$ is the 0 operator outside the zero photon subspace, and so the minimisation can be restricted to the 0 and 1 outcomes.

[1] Note that these eigenvalues do not depend on the basis b chosen.

We explicitly compute the ratio for outcome 0. First, note from Eq. (D.17) that

$$\begin{aligned} \lambda_{0;\,0,N_1} &= 0 && \forall\, N_1 \neq 0 \\ \lambda_{0;\,N_0,0} &= 1 && \forall\, N_0 \neq 0 \\ \lambda_{0;\,N_0,0} &= 1/2 && \forall\, N_0, N_1 \neq 0. \end{aligned} \tag{D.19}$$

$\lambda_{0;\,0,N_1} = 0$ for all N_1, $\lambda_{0;\,N_0,0} = 1$ for all $N_0 \neq 0$, and $\lambda_{0;\,N_0,0} = 1/2$ for all $N_0, N_1 \neq 0$. When $N_0 = 0$, the ratio diverges. Thus, we compute the ratio for the remaining two cases separately, and then we minimise over all cases after:

$$\begin{aligned} \min_{N_0 \neq 0} \left\{ \frac{\lambda^{\mathbf{d_B},\boldsymbol{\eta}}_{0;\,N_0,0}}{\lambda_{0;\,N_0,0}} \right\} &= \min_{N_0 \neq 0} \left\{ (1 - (1-d_0)(1-\eta_0)^{N_0}) \left(1 - \frac{d_1}{2}\right) \right\} \\ &= (1 - (1-d_0)(1-\eta_0)) \left(1 - \frac{d_1}{2}\right) \\ &\geq \eta_{\min} \left(1 - \frac{d_{\max}}{2}\right) \end{aligned} \tag{D.20}$$

$$\begin{aligned} \min_{N_0, N_1 \neq 0} \left\{ \frac{\lambda^{\mathbf{d_B},\boldsymbol{\eta}}_{0;\,N_0,N_1}}{\lambda_{0;\,N_0,N_1}} \right\} &= \min_{N_0, N_1 \neq 0} \left\{ (1 - (1-d_0)(1-\eta_0)^{N_0})(1 + (1-d_1)(1-\eta_1)^{N_1}) \right\} \\ &= (1 - (1-d_0)(1-\eta_0)) \\ &\geq \eta_{\min}. \end{aligned} \tag{D.21}$$

By a similar computation for outcome 1, we achieve the same minimum ratio, $\eta_{\min}\left(1 - \frac{d_{\max}}{2}\right)$, so that

$$q_{>0} = 1 - \eta_{\min} \left(1 - \frac{d_{\max}}{2}\right).$$

D.2.2 Bounding minimum eigenvalue

The central quantity needed to bound the number of non-zero photon rounds using [21, Lemma 5] is a lower bound on the minimum eigenvalue $\lambda_{\min;\,\mathrm{b}}$ of $\Pi_{>0}\Gamma_{\mathrm{det},\,b}\Pi_{>0} = \Pi_{>0} - \Pi_{>0}\Gamma_{\text{no-click},\,b}\Pi_{>0}$. This can be obtained from Eq. (D.17) by minimising over all eigenvalues of $\Gamma_{\mathrm{det},\,b}$ outside the zero-photon subspace,

$$\lambda_{\min;\,\mathrm{b}} = \min_{N_0 + N_1 \neq 0} \left\{ 1 - (1-d_0)(1-d_1)(1-\eta_0)^{N_0}(1-\eta_1)^{N_1} \right\} \geq \eta_{\min}. \tag{D.22}$$