Application of the Flag-State Squashing Model to Numerical Quantum Key Distribution Security Analysis

by

Nicky Kai Hong Li

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

Waterloo, Ontario, Canada, 2020

Author's Declaration

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

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

Statement of Contributions

The majority of the abstract, Chapters 4 and 5, and Appendices A, B, D and E are extracted from the paper, "Improving key rates of the unbalanced phase-encoded BB84 protocol using the flag-state squashing model" [1] written by the author and co-authored by Norbert Lütkenhaus.

In Chapter 2, the proof for Theorem 2.1.4 is provided by Vern Paulsen.

Abstract

The squashing model proof technique is a powerful tool in proving security of quantum key distribution (QKD) protocols since it reduces the dimension of the associated computational problem from infinite to finite. In the first half of this thesis, we formally prove that the unconditional asymptotic security of an arbitrary QKD protocol after applying a squashing model implies the same security for the original protocol. We also prove rigorously that the squashing map of the flag-state squashing model is indeed a quantum channel for an infinite-dimensional input Hilbert space.

In the second half of the thesis, we apply the flag-state squashing model to the phase-encoded BB84 protocol. Since all phase-encoded BB84 implementations have signal states with unbalanced amplitudes in practice, the original security analyses a priori do not apply to them. Previous security proofs use signal tagging of multi-photon pulses to recover the behaviour of regular BB84. This is overly conservative, as for unbalanced signals, the photon-number splitting attack does not leak full information to Eve. In this work, we exploit the flag-state squashing model to preserve some parts of the multi-photon generated private information in our analysis. Using a numerical proof technique, we obtain significantly higher key rates compared with previously published results in the low-loss regime. It turns out that the usual scenario of untrusted dark counts runs into conceptual difficulties in some parameter regime. Thus, we discuss the trusted dark count scenario in this paper as well. We also report a gain in key rates when part of the total loss is known to be induced by a trusted device. We highlight that all these key rate improvements can be achieved without modification of the experimental setup.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor Norbert Lütkenhaus for his guidance and support throughout this degree. I owe a lot to him for bring me into doing quantum information research. I also enjoy very much being part of his group with all the wonderful members.

I would also like to thank Vern Paulsen for all the inspiring discussions on different ideas for constructing a general squashing model and being a member of my advisory committee.

I would like to thank Thomas Jennewein and Jon Yard for being the examiners of my thesis defense.

I want to thank Jie Lin and Ian George for all the helpful discussions and for proof-reading parts of my paper and thesis.

I also thank Jie Lin and Shlok Nahar for reviewing the code that generated the results in Section 4.6.

Finally, I would like to thank my girlfriend Keqi Chen and my family for their love and emotional support.

Table of Contents

List of Figures

Chapter 1

Introduction

Since the discovery of Shor's algorithm [6] for polynomial-time factoring, quantum computers can, in theory, break current cryptosystems such as RSA that rely on the computational hardness of factoring large integers. This poses serious threats to the security of all modern communications that use public-key encryption. Later on, there are many proposals for quantum-safe cryptography schemes such as post-quantum cryptography schemes which rely on the fact that efficient algorithms for solving some hard mathematical problems have yet to be discovered. Furthermore, even if there are really no efficient algorithms that can solve these problems, an adversary with unlimited computational resources can still break these encryption schemes. Therefore, all these schemes are providing only computational security (i.e. assuming the adversary to have limited computational power) instead of information-theoretic security.

Quantum key distribution (QKD) is another category of quantum-safe cryptography schemes. The main advantage of QKD compared with other cryptography schemes is that it assumes the adversary to have unlimited computational power. In fact, QKD, if implemented correctly with a one-time pad, can in principle provide information-theoretical security given that our laws of quantum mechanics are accurate and all possible side-channel attacks are addressed. Another advantage of QKD is that any new attack methods discovered by the adversary in the future will not compromise the security of encrypted messages in the past. This is vastly different from any current or post-quantum cryptography schemes where the security of encrypted messages can be fully compromised if an adversary stores the messages and later discover an efficient decryption method or acquire unrestricted computational resources.

The first QKD protocol, BB84, was proposed by Bennett and Brassard in 1984 [7].

Since then many other QKD protocols have been proposed, but all of them share the same setting where two trusted parties Alice and Bob try to establish a shared secret key so that they can use a one-time pad to encrypt their messages. To do so, Alice sends signals that are chosen at random from a predefined set of non-orthogonal quantum states to Bob so that he can extract some information from measuring the states. Note that there are protocols such as measurement-device-independent (MDI) protocols that require both Alice and Bob to send out signal states to an untrusted party Charlie for measurement, but we will not consider these in this thesis. An eavesdropper or adversary Eve is assumed to have full control of the quantum channel for the signal transmission between Alice and Bob, so Eve can also learn something about the signal states. Once the distribution phase is ended, Alice and Bob will communicate via an authenticated classical channel in order to 1) estimate and reduce the leaked information to Eve, 2) increase correlation between their signal preparation and measurement data, and ultimately 3) establish a shared secret key. This will form the starting point of our discussion in Section 2.2.

The outline of this thesis is given as follows. In Chapter 2, we will cover the mathematical representations of physical systems, quantum measurements, and quantum channels as well as the notion of quantum entropy. These form the bases for understanding the QKD security proof framework. There we describe each step of a generic QKD protocol, different attacks that Eve can perform, and how one can prove unconditional asymptotic security even if Eve is restricted to performing collective attacks. At the end, we will look at two equivalent versions of the asymptotic key rate formulas and how the key rate calculation task can be translated into a numerical optimisation problem that will result in a reliable key rate lower bound.

In Chapter 3, our main focus is squashing models which is an important mathematical tool for proving security of QKD protocols that involve measurements of infinite-dimensional signal states. We first review the motivation and general idea behind squashing models. We then give a concise definition of a generic squashing model and prove its unconditional asymptotic security formally. As we move on to discuss the recently proposed flag-state squashing model [8], we will prove that it satisfies all the squashing model criteria even for an infinite-dimensional input Hilbert space provided that there is a non-trivial lower bound on the weight of a preserved subspace. Finally, we will briefly mention that finding a general squashing model which can fit all QKD protocols is still an ongoing quest.

In Chapter 4, we will prove asymptotic security of the unbalanced phase-encoded BB84 protocol using the numerical proof technique described at the end of Chapter 2 and the flag-state squashing model. Since the main objective is to prove higher key rates than what previous results [4, 5] proved, we will highlight the main difference between our approach

and theirs and emphasise that our method is better. As a review, we will describe the full protocol and how the signals and measurements are modelled mathematically. Then, we will explain all the techniques that we have applied to this security proof and the way we simulate our experimental data with realistic assumptions. Note that we have included all the detailed derivations that we skip in the main body in the appendices for those who are interested. At last, we will show that our key rates are indeed higher in the low-loss regime and a trusted loss assumption can improve the key rates further.

The last chapter will conclude this thesis by summarising mainly Chapters 3 and 4 where I have shown contributions. We will also point out some directions for future research.

Chapter 2

Preliminaries

In this chapter, we first review the relevant mathematical and quantum information theory background for understanding the QKD security analysis framework. We will then revisit the asymptotic security analysis of a general QKD protocol in the asymptotic key scenario.

2.1 Quantum information theory

In QKD, the task is to harvest information stored in some physical quantum systems such as photons. To quantify such information requires the usage of quantum information theory which provides mathematical descriptions of the quantum systems, the information stored in them, and their interactions with the environment and measurement devices. Most of the content in this section is based on Refs. [9, 10, 11].

2.1.1 Physical systems and measurements

Quantum systems exist naturally (e.g. atoms, photons, trapped ions) or can be engineered (e.g. superconducting qubits). They have found applications in many information processing tasks such as QKD, quantum computing and quantum metrology. Although the underlying physics of different quantum systems could be vastly different, quantum systems generally obey the big mathematical framework of quantum mechanics which consists of a series of postulates irrespective of the systems' physical details. Before we state the postulates, we need to define the following mathematical objects.

Definition 2.1.1. (Metric space [12])
A metric space is an ordered pair $(\mathcal{M}, d)$ where $\mathcal{M}$ is a set and an associated metric $d : \mathcal{M} \times \mathcal{M} \to \mathbb{R}$ is a function such that for any $x, y, z \in \mathcal{M}$, it holds that

1. $d(x, y) = 0 \Leftrightarrow x = y$,
2. $d(x, y) = d(y, x)$,
3. $d(x, y) + d(y, z) \geq d(x, z)$,
4. $d(x, y) \geq 0$.

Definition 2.1.2. (Cauchy sequence [12])
A sequence $\{x_n\} \subset \mathcal{M}$ in a metric space $(\mathcal{M}, d)$ is Cauchy if for every positive real number $\epsilon > 0$, there exists a positive integer N such that for all integers $n, m \geq N$, it holds that $d(x_n, x_m) < \epsilon$.

Definition 2.1.3. (Completeness [12])
A metric space $\mathcal{M}$ is complete if every Cauchy sequence in $\mathcal{M}$ is convergent (i.e. $\mathcal{M}$ contains the limit to every Cauchy sequence).

Definition 2.1.4. (Hilbert space [13])
A complex vector space $\mathcal{H}$ is a Hilbert space if there exists an inner product $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ such that for all vectors $x, y, z \in \mathcal{H}$,

1. $\langle x|y\rangle = \langle y|x\rangle^*$,
2. $\langle x + y|z\rangle = \langle x|z\rangle + \langle y|z\rangle$,
3. $\langle x|\alpha y\rangle = \alpha\langle x|y\rangle$ for all $\alpha \in \mathbb{C}$,
4. $\langle \alpha x|y\rangle = \alpha^*\langle x|y\rangle$ for all $\alpha \in \mathbb{C}$,
5. $\langle x|x\rangle \geq 0$,
6. $\langle x|x\rangle = 0$ only if $x = 0$,

and if $\mathcal{H}$ is complete in the norm $|| \cdot ||_{\mathcal{H}}$ defined as $||x||_{\mathcal{H}} = \sqrt{\langle x|x\rangle}$ with the metric d defined as $d(x, y) \coloneqq ||x - y||_{\mathcal{H}}$ for every $x, y \in \mathcal{H}$.

In the rest of this thesis, we will use the Dirac notation for vectors in a Hilbert space $\mathcal{H}$ such that a "ket" $|x\rangle$ is equivalent to a vector $x \in \mathcal{H}$ in the definition above, and a "bra" $\langle x|$ represents the complex conjugate transpose of the vector $x \in \mathcal{H}$.

We state the first postulate of quantum mechanics quoted verbatim from Ref. [9].

> **Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its *density operator*, which is a positive operator ρ with trace one, acting on the state space of the system. If a quantum system is in the state ρ_i with probability p_i, then the density operator for the system is $\sum_i p_i \rho_i$. ([9], p.102)

This provides a mathematical representation of the state of a physical system in terms of a density operator ρ acting on a Hilbert space. As the postulate has stated, a system could be in a statistical ensemble of states $\{p_i, \rho_i\}$ where p_i is the probability of the system in the i-th state ρ_i, in which case the state of a system is a probabilistic mixture $\rho = \sum_i p_i \rho_i$. A state ρ is called *pure* if it is rank-1, i.e. $\rho = |\psi\rangle\langle\psi|$. Otherwise, we call the state *mixed* if the rank of the density operator ρ is larger than 1. A more formal definition of density operators will be given in the operator algebra language once we introduce the following definitions.

Definition 2.1.5. (Positive operators [10])
Let $\mathcal{H}$ be a Hilbert space and P be a linear operator that maps $\mathcal{H}$ to $\mathcal{H}$, i.e. $P \in \mathcal{L}(\mathcal{H})$. P is a positive operator which we denote as $P \geq 0$ or $P \in \text{Pos}(\mathcal{H})$ if for all vectors $|x\rangle \in \mathcal{H}$,

$$\langle x|P|x\rangle \geq 0. \tag{2.1}$$

Definition 2.1.6. (Bounded operators [10])
Let $\mathcal{H}$ and $\mathcal{K}$ be two Hilbert spaces and the set of linear operators that map $\mathcal{H}$ to $\mathcal{K}$ as $\mathcal{L}(\mathcal{H}, \mathcal{K})$. An operator $T \in \mathcal{L}(\mathcal{H}, \mathcal{K})$ is bounded if the operator norm which is defined as

$$||T||_{op} \coloneqq \sup\{||T|h\rangle||_{\mathcal{K}} : |h\rangle \in \mathcal{H}, || \, |h\rangle||_{\mathcal{H}}\} \tag{2.2}$$

is finite. We denote the set of bounded linear operators that map $\mathcal{H}$ to $\mathcal{K}$ as $\mathcal{B}(\mathcal{H}, \mathcal{K})$. If $\mathcal{H} = \mathcal{K}$, then we denote the set simply as $\mathcal{B}(\mathcal{H})$.

Definition 2.1.7. (Compact operators [10])
Let $\mathcal{H}$ and $\mathcal{K}$ be two Hilbert spaces. An operator $K \in \mathcal{B}(\mathcal{H}, \mathcal{K})$ is compact if there is a sequence of finite-rank operators $\{F_n\} \subset \mathcal{B}(\mathcal{H}, \mathcal{K})$ such that

$$\lim_{n\to\infty} ||K - F_n||_{op} = 0. \tag{2.3}$$

We denote the set of compact operators that map $\mathcal{H}$ to $\mathcal{K}$ as $\mathbb{K}(\mathcal{H}, \mathcal{K})$. If $\mathcal{H} = \mathcal{K}$, then we denote the set simply as $\mathbb{K}(\mathcal{H})$.

Theorem 2.1.1 (Singular value decomposition (SVD) [14])
Let $\mathcal{H}$ and $\mathcal{K}$ be two Hilbert spaces and let $K \in \mathbb{K}(\mathcal{H}, \mathcal{K})$ be compact. Then, there exist two orthonormal bases $\{|e_i\rangle : i \in \mathbb{N}\} \subset \mathcal{K}$ and $\{|f_i\rangle : i \in \mathbb{N}\} \subset \mathcal{H}$ such that

$$K = \sum_{i=1}^{\infty} s_i(K)|e_i\rangle\langle f_i| \tag{2.4}$$

where $\{s_i(K) \in \mathbb{R} : s_i(K) \geq 0, i \in \mathbb{N}\}$ are the singular values of the operator K and can be found as the eigenvalues of the operator $|K| \coloneqq \sqrt{K^\dagger K}$.

Definition 2.1.8. (Trace class operators and trace norm [10])
Let $\mathcal{H}$ be a Hilbert space with an orthonormal basis $\{|e_i\rangle : i \in \mathbb{N}\}$. The set of trace class operators is defined as

$$\mathcal{C}_1(\mathcal{H}) = \{K \in \mathbb{K}(\mathcal{H}) : \sum_i s_i(K) < \infty\}, \tag{2.5}$$

which is complete in the trace norm (or 1-norm) defined as

$$||K||_1 \coloneqq \sum_i s_i(K) = \sum_i \langle e_i| \, |K| \, |e_i\rangle = \mathrm{Tr}|K| = \mathrm{Tr}\sqrt{K^\dagger K}. \tag{2.6}$$

Therefore, the trace of the operator $|K|$ is finite for all $K \in \mathcal{C}_1(\mathcal{H})$.

These definitions will be referred to throughout the rest of this chapter and Chapter 3. We now give the formal definition of density operators.

Definition 2.1.9. (Density operators)
An operator $\rho \in \mathcal{C}_1(\mathcal{H})$ is a density operator if it satisfies $\rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$. We denote the set of density operators $\mathcal{D}(\mathcal{H})$. Since it is compact and Hermitian (i.e. $\rho^\dagger = \rho$), it has a spectral decomposition

$$\rho = \sum_i \lambda_i |e_i\rangle\langle e_i| \tag{2.7}$$

where $\{|e_i\rangle\}$ is the eigenbasis and $\{\lambda_i\}$ are non-negative, real eigenvalues of ρ.

In many scenarios, we need to consider a physical system with multiple subsystems. As another postulate of quantum mechanics (see p. 102, Postulate 4 in Ref. [9]), the state space $\mathcal{H}_{AB}$ for a bipartite system consisting of two subsystems A and B is the tensor product of the two state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. This can be extended

to any multipartite system where the state space is simply the tensor product of all the state spaces of its subsystems. The reduced density operator ρ_{A_1} of a subsystem A_1 is the result of taking the partial trace of the n-partite density operator $\rho_{A_1,...,A_n} \in \mathcal{D}(\mathcal{H}_{A_1,...,A_n})$ on the rest of subsystems $A_2, ..., A_n$, i.e.

$$\rho_{A_1} = \mathrm{Tr}_{A_2,...,A_n}(\rho_{A_1,...,A_n}). \tag{2.8}$$

Now if we consider a pure state of a bipartite system, we can use the following theorem to decompose the state into a sum of orthonormal states of tensor product form.

Theorem 2.1.2 (Schmidt decomposition [9])
Let $|\psi\rangle_{AB}$ be a pure state of a bipartite system AB. Then there exist orthonormal bases $\{|e_i\rangle_A\}$ for subsystem A and $\{|f_i\rangle_B\}$ for subsystem B such that

$$|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}|e_i\rangle_A \otimes |f_i\rangle_B, \tag{2.9}$$

where $\{\lambda_i\}$ are non-negative, real numbers which satisfy $\sum_i \lambda_i = 1$.

This theorem implies that the two reduced density matrices $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|_{AB})$ and $\rho_B = \mathrm{Tr}_A(|\psi\rangle\langle\psi|_{AB})$ of any bipartite pure state $|\psi\rangle_{AB}$ have the same eigenvalues. It follows that for any mixed state ρ_A, one can construct a pure state $|\psi\rangle_{AB}$ using the eigensystem of ρ_A and Equation (2.9) such that $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|_{AB})$. This brings us to the following theorem of purification.

Theorem 2.1.3 (Purification)
Let $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ be a density operator. There always exists a pure state $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ such that

$$\rho_A = Tr_B(|\psi\rangle\langle\psi|_{AB}), \tag{2.10}$$

in which case, $|\psi\rangle_{AB}$ is said to purify (or is the purification of) the state ρ_A.

We move on to describe the mathematical formalism of measurements on quantum states, which is given by another postulate of quantum mechanics as stated in (p. 102, Postulate 3) Ref. [9]. It says that any quantum measurement can be represented by a set of measurement operators $\{M_k\} \subset \mathcal{L}(\mathcal{H})$ which are labelled by the index k corresponding to the measurement outcomes. For the system in a state $\rho \in \mathcal{D}(\mathcal{H})$, the probability of obtaining measurement outcome k is

$$p(k) = \mathrm{Tr}(M_k^\dagger M_k \rho), \tag{2.11}$$

and the post-measurement state of the system is the normalised state

$$\frac{M_k \rho M_k^\dagger}{\mathrm{Tr}(M_k^\dagger M_k \rho)} \in \mathcal{D}(\mathcal{H}). \tag{2.12}$$

The postulate ends with the completeness relation which demands the measurement operators to satisfy

$$\sum_k M_k^\dagger M_k = \mathbb{1}_{\mathcal{H}}, \tag{2.13}$$

ensuring that the probabilities in (2.11) sum to one. We also know that the operator $M_k^\dagger M_k$ is a positive operator since $\langle\psi|M_k^\dagger M_k|\psi\rangle \geq 0$ for all vectors $|\psi\rangle \in \mathcal{H}$. We can define a set of positive operators $\{P_k \coloneqq M_k^\dagger M_k\}$ which have a richer mathematical structure than the general measurement operators $\{M_k\}$. For the operators $\{P_k\}$ to satisfy the completeness relation (2.13), they must be bounded operators. We call the set $\{P_k\}$ a *Positive Operator-Valued Measure* (POVM) as defined below.

Definition 2.1.10. (POVM)
Let $\{P_k\} \subset \mathcal{B}(\mathcal{H}) \cap \mathrm{Pos}(\mathcal{H})$ be a set of positive, bounded linear operators on a Hilbert space $\mathcal{H}$. The set $\{P_k\}$ is a POVM if it satisfies

$$\sum_k P_k = \mathbb{1}_{\mathcal{H}} \quad \text{and} \quad p(k) = \mathrm{Tr}(P_k \rho) \tag{2.14}$$

for all measurement outcomes k and for any pairs of probabilities associated with the state $\rho \in \mathcal{D}(\mathcal{H})$ being measured, $(\{p(k)\}, \rho)$.

Note that when the Hilbert space is infinite-dimensional, POVMs may not be compact operators (see Definition 2.1.7) meaning that they may not have a spectral decomposition. We now want to verify that the trace of the product between any POVM and density operator is well-defined even in the infinite-dimensional case. We need the following theorem which will also be used in Section 3.4.1.

Theorem 2.1.4 (Hölder's inequality for inner product between $\mathcal{C}_1(\mathcal{H})$ and $\mathcal{B}(\mathcal{H})$)
Let $X \in \mathcal{C}_1(\mathcal{H})$ be any trace class operator and $A \in \mathcal{B}(\mathcal{H})$ be any bounded operator on a Hilbert space $\mathcal{H}$. It holds that

$$|\,Tr(AX)| \leq ||A||_{op} ||X||_1. \tag{2.15}$$

Proof. Let $X \in \mathcal{C}_1(\mathcal{H})$. Since trace class operators are compact, they have an SVD, so we can write

$$X = \sum_i s_i |\psi_i\rangle\langle\phi_i| \tag{2.16}$$

for $s_i \geq 0$ for all i, $\{|\psi_i\rangle\}$ and $\{|\phi_i\rangle\}$ are orthonormal bases of $\mathcal{H}$. The trace norm of X is

$$||X||_1 = \sum_i s_i. \tag{2.17}$$

Then for any bounded operators $A \in \mathcal{B}(\mathcal{H})$,

$$\mathrm{Tr}(AX) = \sum_i s_i \mathrm{Tr}(A|\psi_i\rangle\langle\phi_i|) = \sum_i s_i \langle\phi_i|A|\psi_i\rangle, \tag{2.18}$$

$$\Rightarrow |\mathrm{Tr}(AX)| \leq \sum_i s_i |\langle\phi_i|A|\psi_i\rangle| \leq \sum_i s_i ||A||_{op} = ||A||_{op}||X||_1. \tag{2.19}$$

■

It follows that the trace of the product between any POVM element $P \in \mathcal{B}(\mathcal{H}) \cap \mathrm{Pos}(\mathcal{H})$ and any density operator $\rho \in \mathcal{D}(\mathcal{H})$ is upper bounded by

$$\mathrm{Tr}(P\rho) = |\mathrm{Tr}(P\rho)| \leq ||P||_{op}||\rho||_1 \leq ||\mathbb{1}_{\mathcal{H}}||_{op}||\rho||_1 = 1. \tag{2.20}$$

Therefore, the trace is always finite and well-defined even when $\mathcal{H}$ is infinite-dimensional.

So far, we have gone through the mathematical descriptions of quantum states and measurements, but we still haven't discussed one of the most important properties of quantum mechanics – entanglement. A Bell state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the simplest example of an entangled state. Measurements on the first and second qubits will yield perfectly correlated results (i.e. the joint measurement probabilities satisfy $p(0,1) = 0 = p(1,0)$). This kind of correlations is much stronger than that of spatially separated classical systems, thereby being a prominent property that distinguishes quantum systems from classical ones. We now give the formal definition of entangled states.

Definition 2.1.11. (Separable and entangled states)
A bipartite state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ is *separable* if there exist a probability distribution $\{p_i\}$ and two sets of density operators $\{\sigma_A^i\} \subset \mathcal{D}(\mathcal{H}_A)$ and $\{\tau_B^j\} \subset \mathcal{D}(\mathcal{H}_B)$ such that

$$\rho_{AB} = \sum_i p_i \sigma_A^i \otimes \tau_B^i \,. \tag{2.21}$$

Any bipartite state that cannot be written in the form (2.21) (i.e. not separable) is called *entangled*.

2.1.2 Quantum channels

In general, the state of a quantum system may change over time. From quantum mechanics, we know that the evolution of quantum states is governed by a Hamiltonian. A more precise statement of how quantum states evolve is given by the following postulate of quantum mechanics, which we quote verbatim from Ref. [9] (p. 102).

> **Postulate 2**: The evolution of a closed quantum system is described by a unitary transformation. That is, the state ρ of the system at time t_1 is related to the state ρ' of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,
>
> $$\rho' = U\rho U^\dagger. \tag{2.22}$$

This tells us that a quantum system that does not interact with its environment or any other systems only evolves unitarily.

However, all quantum systems that we encounter in experiments are unavoidably open in the sense that there are always some interactions between the quantum system and the environment. Therefore, we need an alternative mathematical description of how general quantum systems evolve. A *quantum channel* is a map between density operators, which represents a physical process of sending a quantum state ρ to another quantum state ρ'. It is defined axiomatically such that it can describe any physical evolution of general quantum systems. We now define the two properties that any quantum channel needs to satisfy.

Definition 2.1.12. (Completely Positive [10])
Let $V \subseteq \mathcal{B}(\mathcal{H})$ and $W \subseteq \mathcal{B}(\mathcal{K})$ be subspaces and let $\Phi : V \to W$ be a linear map. Define $\mathbb{1}_{\mathbb{C}^{k\times k}}$ to be the identity map for all operators in $\mathbb{C}^{k\times k}$ for all $k \in \mathbb{N}$. The map Φ is called *k-positive* if the map

$$\Phi^{(k)} := \mathbb{1}_{\mathbb{C}^{k\times k}} \otimes \Phi \tag{2.23}$$

is positive, that is, if $\Phi^{(k)}(P)$ is positive for all positive operators $P \in \mathrm{Pos}(\mathbb{C}^{k\times k} \otimes V)$. The map Φ is *completely positive* (CP) if it is k-positive for all $k \in \mathbb{N}$.

Definition 2.1.13. (Trace-non-increasing and trace-preserving)
Let $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$ be a linear map. It is *trace-non-increasing* (TNI) if for all $X \in \mathcal{L}(\mathcal{H})$,

$$\mathrm{Tr}(\Phi(X)) \leq \mathrm{Tr}(X). \tag{2.24}$$

If equality holds in (2.24), then Φ is *trace-preserving* (TP).

We want all quantum channels to satisfy these two conditions because 1) the output of any quantum channel needs to be a valid density operator, and 2) any quantum channel acting only on a subsystem of a multipartite system should still yield a valid multipartite density operator. These lead to the following definition of a quantum channel.

Definition 2.1.14. (Quantum channels)
A *quantum channel* is a linear completely positive trace-preserving (CPTP) map.

There is another equivalent mathematical representation of a quantum channel given by the Stinespring's dilation theorem as stated after we give the definition of strong convergence.

Definition 2.1.15. (Strong convergence)
Let $X \in \mathcal{B}(\mathcal{H}, \mathcal{K})$ be the limit of a sequence of bounded operators $\{X_n : n \in \mathbb{N}\} \subset \mathcal{B}(\mathcal{H}, \mathcal{K})$ such that $\lim_{n\to\infty} X_n = X$. The sequence is strongly convergent, if $\lim_{n\to\infty} ||Xh - X_n h||_{\mathcal{K}} = 0$ for every $h \in \mathcal{H}$ (denote as $X_n \xrightarrow{s} X$).

Theorem 2.1.5 (Stinespring's dilation theorem of quantum channel [10, 15])
Let $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ be a quantum channel. Then there exists a Hilbert space $\mathcal{E}$ with an orthonormal basis $\{|e_a\rangle : a \in A\}$ for A being a non-empty index set with any cardinality and a bounded operator $V \in \mathcal{B}(\mathcal{H} \otimes \mathcal{E}, \mathcal{K})$ such that

$$\Phi(X) = V(X \otimes \mathbb{1}_{\mathcal{E}})V^{\dagger}, \tag{2.25}$$

$$V = \sum_{a\in A} V_a \otimes \langle e_a|, \tag{2.26}$$

$$s - \sum_{a\in A} V_a^{\dagger} V_a = \mathbb{1}_{\mathcal{K}}, \tag{2.27}$$

where $\sum_{a\in A}$ is an unordered sum. The last line means that the sum converges strongly to the identity.

One important class of quantum channels is entanglement breaking channels which as their name suggest, turn any entangled state into separable states when they act on a subsystem. We now state the definition.

Definition 2.1.16. (Entanglement Breaking Channels [16])
Let $\mathcal{H}$, $\mathcal{K}_1$ and $\mathcal{K}_2$ be three Hilbert spaces and let $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K}_2)$ be a quantum channel. We call Φ entanglement breaking if $(\mathbb{1}_{\mathcal{K}_1} \otimes \Phi)(\rho)$ is separable for all density operators $\rho \in \mathcal{D}(\mathcal{K}_1 \otimes \mathcal{H})$.

2.1.3 Quantum entropy

To quantify the information stored in a quantum state, an analogous version of the Shannon entropy for classical information is the von Neumann entropy defined below.

Definition 2.1.17. (von Neumann entropy)
The von Neumann entropy of the state $\rho \in \mathcal{D}(\mathcal{H})$ is defined as

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho). \tag{2.28}$$

To unify the notation for von Neumann (quantum) and Shannon (classical) entropies, we make the following identification

$$H(A_1, A_2, ..., A_n)_\rho = S(\rho_{A_1,A_2,...,A_n}) \tag{2.29}$$

so that we can treat it as the entropy of the quantum systems or registers. The subscript ρ will be omitted if it is clear by context which state the entropy refers to. We now state the definitions of conditional entropy and mutual information for von Neumann entropy, which are the same as the ones for Shannon entropy.

Definition 2.1.18. (Conditional von Neumann entropy & quantum mutual information)
The conditional von Neumann entropy of system X given system Y is

$$H(X|Y) = H(X,Y) - H(Y) \tag{2.30}$$

and the quantum mutual information between systems X and Y is

$$I(X:Y) = H(X) + H(Y) - H(X,Y). \tag{2.31}$$

Entropic inequalities are powerful tools in quantum information theory and are often used in QKD security proofs. The following theorem for strong subadditivity (SSA) of von Neumann entropy will be useful to us in Section 3.3 when we prove the unconditional security of squashing models.

Theorem 2.1.6 (Strong subadditivity of von Neumann entropy [17, 11])
Let X, Y and Z be registers. For every (quantum) state of the register (X, Y, Z),

$$H(X,Y,Z) + H(Z) \leq H(X,Z) + H(Y,Z). \tag{2.32}$$

This theorem implies that

$$H(X|Y,Z) \leq H(X|Z). \tag{2.33}$$

Intuitively, it means that the uncertainty of a system or register X is always lower if you acquire additional knowledge from an extra system Y. Another important quantity in quantum information is the quantum relative entropy which measures how much a quantum state differs from another state. We give a more general definition below.

Definition 2.1.19. (Quantum relative entropy [11])
The quantum relative entropy of a positive operator $P \in \mathrm{Pos}(\mathcal{H})$ with respect to another positive operator $Q \in \mathrm{Pos}(\mathcal{H})$ is defined as

$$D(P||Q) = \begin{cases} \mathrm{Tr}(P\log_2 P) - \mathrm{Tr}(P\log_2 Q), & \text{if } \ker(Q) \subseteq \ker(P) \\ \infty, & \text{otherwise.} \end{cases} \tag{2.34}$$

An important property of quantum relative entropy is that it is always non-negative for all density operators, which is described by Klein's inequality.

Theorem 2.1.7 (Klein's inequality [11])
Let $P, Q \in Pos(\mathcal{H})$ be positive operators, and assume that $Tr(P) \geq Tr(Q)$. It holds that

$$D(P||Q) \geq 0. \tag{2.35}$$

In particular, it holds that $D(\rho||\sigma) \geq 0$ for every choice of density operators $\rho, \sigma \in \mathcal{D}(\mathcal{H})$.

We now have the mathematical tools to discuss the security analysis framework for QKD.

2.2 Quantum key distribution

In this section, we will revisit the essential ideas of QKD by first describing a generic QKD protocol and two important classes of attacks an eavesdropper can perform. We will then discuss briefly the security definition of QKD and the asymptotic key rate formula. Finally, we will end this section by going through the steps required to turn the key rate calculation task into a semidefinite programming (SDP) problem. Note that some of the content in this section follows a similar discussion in Section 2.2 and Chapter 3 of Lin's Master's thesis [18].

2.2.1 Generic QKD protocol

We now outline the procedure of a generic QKD protocol which comprises of a quantum phase and a classical phase. The quantum phase uses an insecure quantum channel which is assumed to be controlled by the eavesdropper Eve, whereas the classical phase uses a classical authenticated channel through which all communications are public but cannot be altered.

Quantum phase

1. (*State preparation*) The sender Alice prepares N quantum states with each chosen randomly from a countable set $\{\rho_i\}$ of non-orthogonal states according to the probability distribution $\{p_i\}$. We call A'_m the m-th signal register or system. Alice records her random choices in order and sends the total state $\bigotimes_{m=1}^{N} \rho_{i_m}$ through a quantum channel Φ_N to Bob.

2. (*Measurement*) The receiver Bob measures the total output state $\Phi_N(\bigotimes_{m=1}^{N} \rho_{i_m})$ from the channel with a joint POVM $\{\bigotimes_{r=1}^{N} F_{k_r}^B\}$ where the index k_r labels the Bob's measurement outcome corresponding to the r-th output state. Bob records all his measurement outcome in order.

After steps 1 and 2, Alice and Bob proceed to the classical phase which involves purely classical communication procedures.

Classical phase

3. (*Parameter estimation*) Alice and Bob collaboratively select a small random subset of their data (i.e. Alice's choices of state x and Bob's measurement outcomes y) to estimate how much the eavesdropper Eve has learnt about the signal states. They exchange their data corresponding to the selected subset through the classical channel in order to establish a joint frequency distribution $f(x, y)$, which converges to a joint probability distribution in the limit of $N \to \infty$. If $f(x, y)$ fulfills the predefined set of acceptable statistics, then the protocol proceeds, otherwise it aborts.

4. (*Announcement*) If Alice and Bob decide to proceed with the protocol, they may make announcements about the remaining data which are not used in the testing step via the classical channel depending on the protocol. Since the announcements are public, Eve is assumed to know all the content of the announcements.

5. (*Sifting & post-selection*) According to the announcements, Alice and Bob may choose to discard some of their data to increase correlation between the data kept by each of them.

6. (*Key map*) In a direct (reverse) reconciliation scheme, Alice (Bob) performs a key map which maps her (his) sifted and post-selected data into a key string over an alphabet, which we call the raw key. Typically, the alphabet is chosen to be $\{0, 1\}$ so that the key string is a bit string.

7. (*Error correction/Information reconciliation*) The person who does not perform the key map may need additional information to recover a string perfectly correlated to the key held by the other party due to imperfect signal states preparation and transmission, Eve's eavesdropping action, or imperfect measurements. Therefore, whoever does the key map may need to publicly announce error correction information depending on the error correction scheme, which will leak partial information of the raw key to Eve.

8. (*Privacy amplification*) To remove Eve's correlation to the raw key, Alice and Bob need to apply privacy amplification to the key, which essentially reduces the key length based on the maximum amount of information Eve could know about the key. Alice or Bob first picks a hash function from a family of two-universal hash functions (see Definition 5.4.1 in Renner's PhD thesis [19]) which maps the raw key to a shortened string which we call the final key. He or she will then announce the choice of hash function publicly so that the other party can perform the same hashing on his or her raw key.

This is called the *prepare-and-measure* scheme which is commonly practised in experiments since this is straightforward to implement. However, analysing the security of a protocol of such scheme directly is not intuitive and could be conceptually challenging for complicated protocols.

There is an alternative QKD scheme - the *entanglement-based* scheme which involves different procedures in the quantum phase. Instead of having Alice to prepare and send out N signal states, Eve prepares a $2N$-partite entangled state $\rho_{A_1...A_N B_1...B_N}$ which can be entangled with her quantum system. Eve then sends systems $A_1, ..., A_N$ to Alice and systems $B_1, ..., B_N$ to Bob. Now Alice and Bob both have to measure each of the N systems they receive from Eve with the POVMs $\{F_i^A\}$ and $\{F_j^B\}$ respectively. The classical phase of an entanglement-based scheme is basically the same as that of a prepare-and-measure scheme. Note that each step for both schemes may subject to some degree of modifications

depending on the exact protocol, but these variations will not affect the discussion in the remaining of this chapter.

For entanglement-based protocols, we can treat Eve's eavesdropping action as a purification of the shared quantum states between Alice and Bob, which permits an information-theoretic quantification of the leaked information using quantum information theory. Thus, these protocols have the advantage that their security analyses are usually more intuitive than that for the prepare-and-measure ones. Nevertheless, to prepare a large number of copies of highly entangled states in a short period of time could be experimentally challenging, so the entanglement-based scheme may not be as implementation-friendly as a prepare-and-measure scheme.

To enjoy the best of both worlds, one can use the *source replacement* scheme [20, 21, 22, 23] to convert a prepare-and-measure protocol into an entanglement-based one, which we will describe in the following. Let A_m be the m-th private system of Alice and A'_m be the system for the m-th output signal state of Alice. Assume in a prepare-and-measure protocol that Alice randomly picks N pure states* from the ensemble $\{(p_i, |\phi_i\rangle_{A'})\}$ as described in step 1 of the quantum phase. Then for the m-th signal state Alice prepares, we can imagine a fictitious source in Alice's device to prepare an entangled pure state

$$|\psi\rangle_{A_m A'_m} = \sum_i \sqrt{p_i}|i\rangle_{A_m} \otimes |\phi_i\rangle_{A'_m} \tag{2.36}$$

where the orthonormal states $\{|i\rangle_{A_m}\}$ represent Alice's m-th random signal choice. When Alice measures the entangled state $|\psi\rangle_{A_m A'_m}$ with the POVM $\{|i\rangle\langle i|_{A_m}\}$, the reduced density operator of system A'_m collapses to the signal state $|\phi_i\rangle\langle\phi_i|_{A'_m}$ with probability p_i. This is equivalent to her randomly choosing a signal state from $\{|\phi_i\rangle\langle\phi_i|_{A'_m}\}$ according to the probability distribution $\{p_i\}$. Therefore, we have transformed the state preparation step in a prepare-and-measure protocol into Alice measuring the bipartite entangled state $|\psi\rangle_{A_m A'_m}$ with respect to her private system A_m.

In the source replacement scheme, after Alice measures the state $|\psi\rangle_{A_m A'_m}$ with the POVM $\{|i\rangle\langle i|_{A_m}\}$ for each $m \in \{1, 2, ..., N\}$, all N signal systems will go through the quantum channel $\Phi_N : \mathcal{D}(\mathcal{H}_{A'_1 ... A'_N}) \to \mathcal{D}(\mathcal{H}_{B_1 ... B_N})$ and Bob will measure the output state. However, Bob's joint POVM which acts only on his quantum systems $B_1, ..., B_N$ commutes with Alice's joint POVM on systems $A_1, ..., A_N$, so Alice can delay her measurement until Bob receives the total signal state. If Alice's measurements are delayed, then Alice and

*We will discuss the source replacement scheme for the scenario where Alice's signal states are mixed states in Section 4.3.2.

Bob will share the state

$$\rho_{A_1\ldots A_N B_1\ldots B_N} = (\mathbb{1}_{A_1\ldots A_N} \otimes \Phi_N) \left(\bigotimes_{m=1}^{N} |\psi\rangle\langle\psi|_{A_m A'_m} \right), \tag{2.37}$$

which is entangled between Alice's and Bob's systems if Φ_N is not an entanglement breaking channel. Since we assume the worst case where Eve has full control of the quantum channel, Eve has a purification of the state $\rho_{A_1\ldots A_N B_1\ldots B_N}$. Now we recover the last step of the quantum phase of an entanglement-based protocol where Alice and Bob both measure their part of the shared entangled state $\rho_{A_1\ldots A_N B_1\ldots B_N}$ distributed by Eve. We remark that

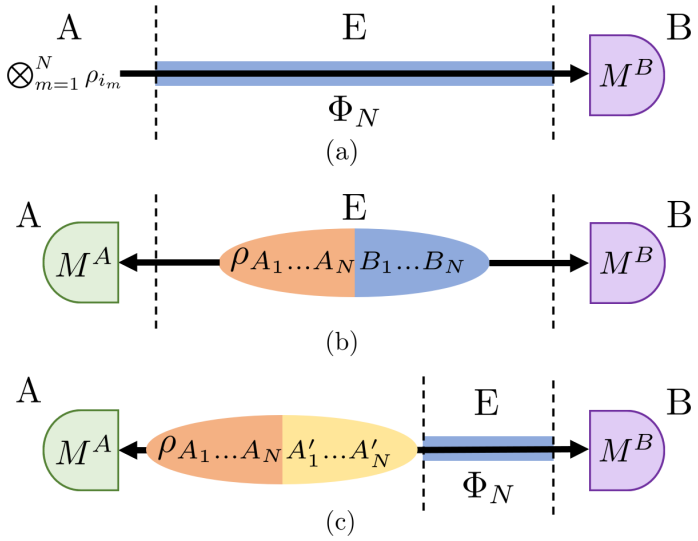


Figure 2.1: Illustration of the quantum phase of three QKD schemes: (a) In the prepare-and-measure scheme, Alice sends $\bigotimes_{m=1}^{N} \rho_{i_m}$ through a quantum channel Φ_N controlled by Eve to Bob who measures with a POVM M^B. (b) In the entanglement-based scheme, Eve sends two parts of an entangled state $\rho_{A_1\ldots A_N B_1\ldots B_N}$ to Alice and Bob who measure their parts with POVMs M^A and M^B respectively. (c) In the source replacement scheme, Alice prepares an entangled state $\rho_{A_1\ldots A_N A'_1\ldots A'_N} = \bigotimes_{m=1}^{N} |\psi\rangle\langle\psi|_{A_m A'_m}$ defined in (2.36), keeps systems $A_1, \ldots, A_N$ and sends systems $A'_1, \ldots, A'_N$ to Bob through the quantum channel Φ_N. Alice and Bob then both measure their parts with POVMs M^A and M^B. We see that picture (c) allows one to convert scheme (a) into scheme (b) but with an extra condition that Alice's state $\rho_{A_1\ldots A_N}$ is fixed by Alice (i.e. not chosen by Eve).

since the map Φ_N only acts on systems A'_m for $m = 1, \ldots, N$ as shown in Equation (2.37), Eve cannot influence Alice's state $\rho_{A_1\ldots A_N}$, so Alice's reduce density operator before and

after she sends out the signals should be the same. This extra condition on Alice's state $\rho_{A_1...A_N}$ makes a source replacement scheme slightly different from an entanglement-based scheme where Eve is free to choose the full state $\rho_{A_1...A_N B_1...B_N}$ without any restriction on $\rho_{A_1...A_N}$. The three schemes are summarised in Figure 2.1.

Hence, we have shown how the quantum phase of a prepare-and-measure protocol can be converted completely into the quantum phase of an entanglement-based protocol. This correspondence between the two types of protocols allows one to analyse the security of any prepare-and-measure protocol as if it is an entanglement-based one, thereby unifying the security analyses of two types of protocols.

2.2.2 Attack models

In the worst-case scenario, Eve fully controls the quantum channel Φ_N in (2.37) and has a purification of the state $\rho_{A_1...A_N B_1...B_N}$ shared between Alice and Bob. Naturally, the action of the quantum channel Φ_N depends entirely on how Eve interacts with the signal systems $A'_1, ..., A'_N$ and what she sends to Bob eventually. We call these collectively Eve's attack or eavesdropping strategy. We list here two types of attacks that Eve can perform.

Coherent attacks

In a coherent attack, Eve interacts coherently with all N signal states with her ancillary system E, which she may measure coherently after Alice and Bob make public announcements in order to gain information of the shared key. As a consequence, Bob may receive a state with systems $B_1, ..., B_N$ dependent on one another. This is the most general form of attacks that Eve can perform.

Collective attacks

In a collective attack, Eve interacts with each of N signals in the same way such that the full quantum channel $\Phi_N = \Phi^{\otimes N}$ is the N-fold tensor product of the quantum channel Φ for an individual signal. This implies that the total state shared between Alice and Bob $\rho_{A_1...A_N B_1...B_N} = \rho_{AB}^{\otimes N}$ is simply N copies of the state ρ_{AB} corresponding to Alice sending one signal. We call this the independent and identically distributed (i.i.d.) scenario where the shared state for each round of signal sending is independent of other rounds. In this case, Eve would keep an ancillary system E for each round in order to purify the state ρ_{AB}. After Alice and Bob make all the announcements, Eve may measure all her ancillary

systems from N copies of purification of the state ρ_{AB} collectively to learn about the shared key. This class of attacks is more restrictive than coherent attacks, so it may not contain the worst attack that Eve can perform for a given protocol. However, in the asymptotic limit where $N \to \infty$, Eve's optimal attack converges to a collective attack, which we will discuss in Section 2.2.4.

2.2.3 Security definition of QKD

We now move on to give the formal security definition of any QKD protocol, which was first stated in Refs. [24, 25, 26]. The idea is to compare the QKD protocol of our interest with an ideal protocol that is perfectly secure. Assume that a QKD protocol either aborts or generates classical keys $s_A, s_B \in \mathcal{S}$ for Alice and Bob, where we denote key space (i.e. the set of all possible output keys) of the protocol to be $\mathcal{S}$.

Definition 2.2.1. (ϵ-security [19])
Let $\mathcal{P}$ be a QKD protocol, which is associated with a CPTNI map $\mathcal{E}^{\mathcal{P}}_{ABE\to S_A S_B E'}$, and let $\rho_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$ be a tripartite state shared by Alice, Bob and Eve. The protocol $\mathcal{P}$ is *ϵ-secure* on the input state ρ_{ABE} if the output $\rho_{S_A S_B E'} \coloneqq \mathcal{E}^{\mathcal{P}}_{ABE\to S_A S_B E'}(\rho_{ABE})$ satisfies

$$\frac{1}{2}||\rho_{S_A S_B E'} - \rho_{UU} \otimes \rho_{E'}||_1 \leq \varepsilon \ , \tag{2.38}$$

where $\rho_{UU} \coloneqq \sum_{s\in\mathcal{S}} \frac{1}{|\mathcal{S}|}|s\rangle\langle s| \otimes |s\rangle\langle s|$ is the state that represents Alice and Bob sharing an identical key and for each key in $\mathcal{S}$ to be equally likely. The states $\rho_{S_A S_B E'}$ and $\rho_{E'}$ can be unnormalised. If the protocol $\mathcal{P}$ is ε-secure on all input states $\rho_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$, then $\mathcal{P}$ is *ε-fully secure*.

The ε-security definition sets an upper bound ε for how much the actual output

$$\rho_{S_A S_B E'} = \sum_{s_A, s_B \in \mathcal{S}} p(s_A, s_B)|s_A\rangle\langle s_A| \otimes |s_B\rangle\langle s_B| \otimes \rho_{E'}^{(s_A, s_B)} \tag{2.39}$$

of a QKD protocol can deviate from an ideal protocol's output $\rho_{UU} \otimes \rho_{E'}$ for which Eve's system decouples completely from Alice's and Bob's perfectly correlated and completely random keys. Note that the protocol's output $\rho_{S_A S_B E'}$ and Eve's reduced density operator $\rho_{E'}$ can have trace less than one since the completely positive trace-non-increasing (CPTNI) map $\mathcal{E}^{\mathcal{P}}_{ABE\to S_A S_B E'}$ is assumed to output a zero operator when the protocol $\mathcal{P}$ aborts. We can interpret the definition in (2.38) as the joint probability of an ε-secure protocol not aborted and its output being imperfect is at most ε. Therefore, a protocol that always

aborts is perfectly secure ($\varepsilon = 0$) under this security definition despite being completely useless in key generation.

In a practical scenario, one should set the security parameter ε prior to carrying out the protocol since it directly affects the acceptance probability of the protocol in the parameter estimation step and also the key rate formula. However, in the asymptotic limit of sending an infinite number of signals, the ε-dependence in the key rate will vanish and the notion of ε-security is no longer needed in the asymptotic key regime. This is because given that Alice and Bob know the joint measurement probabilities, the protocol will either abort if it fails (i.e. Alice's and Bob's keys disagree and/or the key is not secret) or proceed if it succeeds as the key length tends to infinity.

2.2.4 Asymptotic key rate

A formal security proof of any QKD protocol provides a concrete quantification of a protocol's key generation efficiency for a predefined security parameter ε. The secure key rate of a QKD protocol is the number of secure key bits generated per signal sent (or clock cycle), which is what a security proof aims to obtain. In this section, we will see how we can prove unconditional security of any QKD protocol even if we restrict Eve's attack only to collective attacks, and subsequently show the asymptotic key rate formula for an infinite number of signals. Note that we will not discuss the key rate formula for the finite-size scenario where only a finite number of signals are sent from Alice to Bob.

Restricting Eve's attack: coherent to collective

In reality, we need to analyse the security of a QKD protocol under Eve's arbitrary attacks including coherent attacks. However, it is hard to directly prove security under coherent attacks since there is not enough symmetry in the total state shared by Alice and Bob. Fortunately, the quantum de Finetti representation theorem [19, 27, 28] shows us that asymptotically all coherent attacks can be reduced to collective attacks. Therefore, we can prove unconditional security of a protocol in the asymptotic regime by focusing only on collective attacks where the joint state shared by Alice and Bob is of the form $\rho_{AB}^{\otimes N}$.

We briefly introduce the idea of the quantum de Finetti representation theorem here. Let $\rho^{n+k} \in \mathcal{D}(\mathcal{H}^{\otimes(n+k)})$ be a permutation-invariant operator on $n+k$ subsystems, i.e. permuting the order of all the subsystems in any way leaves the operator unchanged. As shown in Ref. [19], the reduced state $\rho^n \in \mathcal{D}(\mathcal{H}^{\otimes n})$ can be approximated by a probabilistic

mixture of states which are superpositions of states satisfying the form

$$\sigma^{\otimes(n-r)} \otimes \tau^r \tag{2.40}$$

where $\sigma \in \mathcal{D}(\mathcal{H})$ and $\tau^r \in \mathcal{D}(\mathcal{H}^{\otimes r})$ are arbitrary states. The approximation of the reduced state ρ^n converges exponentially fast in integers k and r. If n is very large and $k, r \ll n$, then the reduced density operator for $n-r$ subsystems is approximately a convex combination of i.i.d. states, i.e. $\sum_i p_i \sigma_i^{\otimes(n-r)}$. Note that the above description of the quantum de Finetti representation theorem holds for finite-dimensional Hilbert spaces, but the general idea still applies to the case when $\dim(\mathcal{H}) = \infty$ which was proven by Renner and Cirac [28].

To apply the quantum de Finetti theorem here, we set $N = n + k$ to be the number of bipartite systems AB shared between Alice and Bob, then we permute all pairs of bipartite systems to obtain the symmetrised state

$$\overline{\rho}_{AB}^N = \frac{1}{|\Pi|} \sum_{\pi \in \Pi} \rho_{A_{\pi(1)} B_{\pi(1)} \ldots A_{\pi(N)} B_{\pi(N)}} \ , \tag{2.41}$$

where Π is the set of all possible permutations on N elements. Experimentally, this means that Alice and Bob have to simultaneously permute their measurement data for different rounds. However, the permutation of Alice's and Bob's systems does not have to be performed in reality since Scarani and Renner has proven in Lemma 1 [29] that the original version of a QKD protocol is at least as secure as its symmetrised version. Therefore, we can directly assume a protocol is symmetrised in the security proof. By choosing $k, r \ll N$, the state corresponding to $N-k-r$ pairs of Alice's and Bob's shared system is approximately a convex combination of i.i.d. states with each corresponding to a collective attack scenario.

Alternatively, the post-selection technique [30] can be used if the QKD protocol is permutation-invariant in the sense that for any permutation Π on the input states of the protocol $\mathcal{E}$, there exists a CPTP map G_Π such that when it is applied to the outputs of the protocol with permuted inputs, it somehow reverses the effect of the permutation and recovers the original outputs, i.e. $G_\Pi \circ \mathcal{E} \circ \Pi = \mathcal{E}$. The post-selection theorem says that if such a protocol is $\overline{\varepsilon}$-secure when restricted to collective attacks, then it is ε-secure under coherent attacks such that

$$\varepsilon \leq (N+1)^{d^2-1} \, \overline{\varepsilon} \ , \tag{2.42}$$

which grows only polynomially in N where d is the dimension of the Hilbert space $\mathcal{H}_{AB}$ for a single pair of Alice's and Bob's systems. It has been shown in Section 3.4.3 of Beaudry's PhD thesis [31] that a generic protocol $\mathcal{E}$ can be broken down into a sequence of subprotocols which represent steps (2) to (8) of the generic protocol described in Section 2.2.1:

measurement (F), sifting (Sift), parameter estimation (PE), information reconciliation (IR), and privacy amplification (PA), i.e.

$$\mathcal{E} = \mathrm{PA} \circ \mathrm{IR} \circ \mathrm{PE} \circ \mathrm{Sift} \circ F \ .$$

Typically, the first three subprotocols F, Sift, and PE are permutation-invariant, but IR and PA are not. Beaudry [31] shows that the subprotocols IR and PA can be converted into permutation-invariant versions at some cost to the security parameter for coherent attacks, $\bar{\varepsilon}$ in (2.42) (see p. 101 in [31]). Note that in the finite-key scenario, the post-selection technique allows one to prove tighter lower bounds of the key rates than that allowed by the quantum de Finetti theorem [30].

When N tends to infinity, it follows from both the quantum de Finetti theorem and the post-selection technique that Eve's optimal attack converges to a collective attack. Thus, the asymptotic key rate formula introduced below involves only the entropy related to a single round of the protocol due to the i.i.d. structure of Alice's and Bob's shared state in a collective attack.

Asymptotic key rate formula

In the asymptotic limit where $N \to \infty$, all the N-dependent terms that relate to the finite-size effect in the key rate formula vanish, thereby recovering the Devetak-Winter formula [32] for asymptotic secure key rate. Let Z be the key register held by Alice (Bob) in direct (reverse) reconciliation, E be Eve's quantum and classical register, and $\overline{B}$ be Bob's (Alice's) classical register for storing his (her) measurement outcomes. The Devetak-Winter formula can be expressed as

$$R_\infty = p_{\mathrm{pass}}[\min_{\rho \in \mathbf{S}} H(Z|E) - H(Z|\overline{B})], \tag{2.43}$$

where p_{pass} is the probability of passing the sifting and post-selection steps, $\mathbf{S}$ is the set of density operators that satisfy Alice's and Bob's joint statistics. Their statistics in the asymptotic case is a joint probability distribution over their measurement outcomes (in the source replacement scheme).

The first term is called the privacy amplification term which quantifies the minimum uncertainty of the raw key with respect to Eve in terms of bits given that she obtains her ancillary system E through eavesdropping. To be more specific, this term reflects the amount of randomness in the final key in Eve's perspective, which the privacy amplification step (step (8) of the generic protocol described in Section 2.2.1) can distill from the raw key. The second term is the error correction term which counts the amount of information

about the raw key leaked to Eve during the public announcements for the error correction procedure. In practice, no error correction code has an error correction rate that reaches the Shannon limit, so the error correction term can be replaced by $\delta_{\text{EC}} = f_{\text{EC}}\ H(Z|\overline{B})$ with a heuristic classical error-correction efficiency factor $f_{\text{EC}} \geq 1$. Note that the security parameter ε does not appear in (2.43) because the ε-dependent term in the key rate formula vanishes in the asymptotic limit.

2.2.5 Numerical key rate and convex optimisation

The key rate formula (2.43) requires one to minimise the privacy amplification term over all feasible tripartite states shared by Alice, Bob and Eve, which makes it numerically difficult to solve since Eve's system can be very large. An alternative form of the key rate formula [33, 2] replaces the privacy amplification term with a minimisation of the relative entropy over all feasible bipartite states shared between Alice and Bob. This form is more suitable for numerical key rate calculation since Eve's system does not enter the optimisation problem. This alternative form of the key rate formula is given by

$$R_\infty = \min_{\rho_{AB}\in\mathbf{S}} D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB}))) - p_{\text{pass}}\ \delta_{\text{EC}}\ , \tag{2.44}$$

where $\mathcal{G}$ and $\mathcal{Z}$ are two maps that will be discussed below. This formula again has a privacy amplification term as the first term and an error correction term δ_{EC} in the second term as we have discussed earlier. We direct the reader to Theorem 1 by Coles [34] and Section 4.0.3 in Ref. [2] for full details on how the privacy amplification term in the form of minimising a conditional entropy in (2.43) can be converted into the quantum relative entropy minimisation in (2.44).

The map $\mathcal{G}$ is a CPTNI map capturing the effects of measurements, sifting, post-selection and announcements on a single state shared between Alice and Bob. It is not trace-preserving because the map outputs the zero operator if the measurement outcomes or the announcements do not pass sifting and post-selection, which gives rise to an unnormalised state. We now sketch the basic idea behind the map $\mathcal{G}$. Alice and Bob each measures their respective systems on the joint state ρ_{AB} and each of them keeps two classical registers for storing their measurement outcome and announcement. The map $\mathcal{G}$ then projects onto a subspace in the classical registers corresponding to the measurements and announcements that pass the post-selection process. Finally, a key register is added to store the key map result which takes the measurement outcomes and announcements as arguments.

We now provide the full details of the map $\mathcal{G}$ which has been formulated in Section 4.0.2 of Ref. [2] by Winick *et al.* Consider the source replacement scheme. Let the announcements from Alice and Bob be $a \in S^A$ and $b \in S^B$ for S^A and S^B to be their announcement sets, and their measurement outcomes to be labelled by $\tilde{a} \in \Omega_a^A$ and $\tilde{b} \in \Omega_b^B$ respectively, where Ω_a^A and Ω_b^B are the labelling sets for Alice's and Bob's allowed measurement outcomes corresponding to the announcements a and b respectively. For example, in the standard BB84 with active basis choice, both Alice and Bob announce their measurement bases x or z, so $S^A = S^B = \{x, z\}$. For each of the basis announcement $a, b \in \{x, z\}$, Alice's and Bob's labelling sets for their measurement outcomes are $\Omega_a^A = \{0, 1\}$ and $\Omega_b^B = \{0, 1, \text{'no-click'}, \text{'double-click'}\}$.

The construction of map $\mathcal{G}$ follows the three steps in a generic QKD protocol: (1) measurements and announcements, (2) post-selection, and (3) key map. The first step is Alice and Bob performing measurements and announcements on their shared quantum state ρ_{AB}. This can be captured by a quantum channel $\mathcal{A}$ which has a Kraus representation

$$\mathcal{A}(\rho_{AB}) = \sum_{a \in S^A} \sum_{b \in S^B} (K_a^A \otimes K_b^B) \rho_{AB} (K_a^A \otimes K_b^B)^\dagger. \tag{2.45}$$

The Kraus operators associated with Alice's measurement and announcement are

$$K_a^A = \sum_{\tilde{a} \in \Omega_a^A} \sqrt{F_{(a,\tilde{a})}^A} \otimes |a\rangle_{\widetilde{A}} \otimes |\tilde{a}\rangle_{\overline{A}} \tag{2.46}$$

where $\{F_{(a,\tilde{a})}^A : a \in S^A, \tilde{a} \in \Omega_a^A\}$ is Alice's POVM, and $\widetilde{A}$ and $\overline{A}$ are the classical registers that keep her announcement and measurement data. Similarly, Bob's Kraus operator is

$$K_b^B = \sum_{\tilde{b} \in \Omega_b^B} \sqrt{F_{(b,\tilde{b})}^B} \otimes |b\rangle_{\widetilde{B}} \otimes |\tilde{b}\rangle_{\overline{B}} \tag{2.47}$$

where $\{F_{(b,\tilde{b})}^B : b \in S^B, \tilde{b} \in \Omega_b^B\}$ is Bob's POVM, and $\widetilde{B}$ and $\overline{B}$ denote the classical registers that store his announcement and measurement outcome respectively.

The second step is the joint post-selection on Alice's and Bob's data. Let the set of joint announcements that Alice and Bob agree to keep be $\mathbf{K} \subseteq S^A \times S^B$. For standard BB84 with active basis choice, the "keep" set $\mathbf{K}$ corresponding to sifting is $\{(x, x), (z, z)\}$. If we now project the state $\mathcal{A}(\rho_{AB})$ onto the subspace defined by the projector

$$\Pi = \sum_{(a,b) \in \mathbf{K}} |a\rangle\langle a|_{\widetilde{A}} \otimes |b\rangle\langle b|_{\widetilde{B}} \otimes \mathbb{1}_{AB\overline{AB}}\,, \tag{2.48}$$

then the unnormalised state $\Pi\mathcal{A}(\rho_{AB})\Pi$ corresponds to the result of the post-selection.

The last step is the key mapping process. In the direct reconciliation scheme, a key map function $g : S^A \times \Omega_a^A \times S^B \to S^Z$ takes Alice's announcement and measurement outcome together with Bob's announcement as input and outputs a key in the key set S^Z. For instance, the key map satisfies $g(a, \tilde{a}, b) = \tilde{a}$ for any $\tilde{a} \in \{0, 1\}$ and $a, b \in \{x, z\}$ in the case of standard BB84 with active basis choice since Alice simply uses her measurement outcome (signal choice) as the key. Let V be an isometry that adds in a key register R for keeping the key map output. The isometry takes the form

$$V = \sum_{a \in S^A} \sum_{\tilde{a} \in \Omega_a^A} \sum_{b \in S^B} |g(a, \tilde{a}, b)\rangle_R \otimes |a\rangle\langle a|_{\widetilde{A}} \otimes |\tilde{a}\rangle\langle\tilde{a}|_{\overline{A}} \otimes |b\rangle\langle b|_{\widetilde{B}} \otimes \mathbb{1}_{AB\overline{B}} \,. \tag{2.49}$$

The map $\mathcal{G}$ is simply the sequential application of the three steps, which is defined as

$$\mathcal{G}(\rho_{AB}) = V\Pi\mathcal{A}(\rho_{AB})\Pi V^\dagger. \tag{2.50}$$

The other map $\mathcal{Z}$ is a pinching channel that projects the key register onto classical states. The result is a classical-quantum state which represents Alice's and Bob's shared post-measurement and post-announcement state associated with each key map results. More precisely, the map $\mathcal{Z}$ is defined as

$$\mathcal{Z}(\sigma_{ZC}) = \sum_{j=0}^{1} (|j\rangle\langle j|_Z \otimes \mathbb{1}_C)\, \sigma_{ZC}\, (|j\rangle\langle j|_Z \otimes \mathbb{1}_C) \tag{2.51}$$

with register C encapsulates all registers except Z.

For protocols that have a simple key map (e.g. the key map depends only on one party's measurement outcomes), the map $\mathcal{G}$ can be further simplified as pointed out in Appendix A of Ref. [35] by Lin *et al.* We will give a specific form of the maps $\mathcal{G}$ and $\mathcal{Z}$ for the unbalanced phase-encoded BB84 protocol in Chapter 4.

Semidefinite programming (SDP) problem for the key rate

We gave the motivation why the key rate formula in (2.44) is more suitable for numerical key rate calculations. We also know that the error correction term only uses the joint probabilities of the key map outcomes and Bob's measurement outcomes, which can easily be obtained from Alice's and Bob's joint measurement outcome probabilities. Thus, calculating the error correction term is straightforward even by hand. What follows is how

one can convert the calculation of the privacy amplification term in (2.44) from a convex optimisation problem into an SDP problem which guarantees a reliable lower bound on the key rate with the solution to its corresponding dual problem.

First of all, the objective function $D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB})))$ is a convex function with respect to the argument ρ_{AB} [33, 2] based on the property of relative entropy. Therefore, the privacy amplification term is essentially a convex optimisation of the form

$$\begin{aligned} &\min_{\rho_{AB}} D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB}))) \\ \text{subject to } &\mathrm{Tr}[\Gamma_i\ \rho_{AB}] = \gamma_i \text{ for } i = 1, ..., r, \\ &\mathrm{Tr}[\widetilde{\Gamma}_j\ \rho_{AB}] \leq \widetilde{\gamma}_j \text{ for } j = 1, ..., s, \\ &\mathrm{Tr}(\rho_{AB}) = 1,\ \rho_{AB} \geq 0, \end{aligned} \tag{2.52}$$

with Hermitian operators $\{\Gamma_i\}$ and $\{\widetilde{\Gamma}_j\}$ together with the real numbers $\{\gamma_i\}$ and $\{\widetilde{\gamma}_j\}$ set the equality and inequality constraints for the optimisation problem, which are usually obtained from the observed statistics in a QKD experiment and the characterisation of the signal source. These constraints define the feasible set of density operators $\mathbf{S}$ which appears in the key rate formula (2.44). Numerical solvers such as CVX in MATLAB can handle this kind of convex optimisation, but the output solution is often not optimal due to finite numerical precision, in which case the suboptimal solution only provides an upper bound for the actual key rate.

To obtain a reliable lower bound for the key rate, we first have to convert the convex optimisation problem in (2.52) into an SDP problem. An SDP problem concerns with optimising a linear objective function over a subset of positive (semidefinite) operators. The standard form of an SDP problem can be expressed as [36, 11]

Primal Problem

$$\begin{aligned} &\min_{X} \langle A, X\rangle \\ \text{subject to } &\langle B_i, X\rangle = b_i \text{ for } i = 1, ..., r, \\ &\langle \widetilde{B}_j, X\rangle \leq \widetilde{b}_j \text{ for } j = 1, ..., s, \\ &X \geq 0, \end{aligned}$$

Dual Problem

$$\begin{aligned} &\max_{\vec{y}} \sum_{i=1}^{r} b_i y_i + \sum_{j=1}^{s} \widetilde{b}_j y_{j+r} \\ \text{subject to } &\sum_{i=1}^{r} y_i B_i + \sum_{j=1}^{s} y_{j+r} \widetilde{B}_j \leq A, \\ &y_{j+r} \leq 0 \text{ for } j = 1, ..., s, \\ &\vec{y} \in \mathbb{R}^{r+s}, \end{aligned}$$

where $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$ is the Hilbert-Schmidt inner product between two operators A and B. By weak duality of SDP [36], the solution to the primal problem always upper bounds

the solution to the dual problem. If the primal problem is feasible (i.e. the set of operators that satisfy all the constraints of the primal problem is non-empty) and there exists a vector $\vec{y} \in \mathbb{R}^{r+s}$ which satisfies strict inequality for all constraints in the dual problem (i.e. $\exists\ \vec{y} \in \mathbb{R}^{r+s}$ such that $\sum_{i=1}^{r} y_i B_i + \sum_{j=1}^{s} y_{j+r} \widetilde{B}_j < A$ and $y_{j+r} < 0$ for $j = 1, ..., s$), then the optimal primal solution equals to the optimal dual solution. This is called the Slater's condition [11].

The weak duality of SDP tells us that if we can convert the convex optimisation problem in (2.52) into a primal SDP problem with its optimal solution guaranteed to lower bound the key rate, then any solution to the dual problem will be a reliable lower bound for the key rate. Therefore, the suboptimal dual solution provided by a numerical solver will not overestimate the key rate. Moreover, if the Slater's condition is satisfied and the optimal solution to the primal SDP problem is close to the actual key rate (i.e. the optimal solution to (2.52)), then so is the dual optimal solution, which ensures tightness of the key rate lower bound.

The way Winick *et al.* [2] convert (2.52) into a primal SDP problem is to linearise the convex objective function $f(\rho) \coloneqq D(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho)))$ in (2.52) with its matrix gradient

$$\nabla f(\rho) = [\mathcal{G}^{\dagger}(\log \mathcal{G}(\rho)) - \mathcal{G}^{\dagger}(\log \mathcal{Z}(\mathcal{G}(\rho)))]^T \tag{2.53}$$

to obtain the lower bound for the optimal solution to (2.52)

$$\alpha \coloneqq \min_{\rho \in \mathbf{S}} f(\rho) \ \geq \ f(\rho') - \mathrm{Tr}(\rho' \nabla f(\rho')^T) + \min_{\sigma \in \mathbf{S}} \mathrm{Tr}(\sigma \nabla f(\rho')^T). \tag{2.54}$$

for any state $\rho' \in \mathbf{S}$ in the feasible set. The closer the state ρ' to the optimal state $\rho^* \in \mathbf{S}$, the tighter the lower bound, so it is important to choose a ρ' close to ρ^* in the actual key rate calculation. To get ρ' sufficiently close to ρ^*, Ref. [2] uses the Frank-Wolfe algorithm [37] to sequentially minimise the function $\mathrm{Tr}(\Delta\rho \nabla f(\rho_i)^T)$ subject to $\Delta\rho + \rho_i \in \mathbf{S}$ for each step i with a numerical convex optimisation solver. We call this "Step 1".

The last term in (2.54) can be viewed as a primal SDP problem which can then be

turned into its dual problem[†]

$$\begin{aligned} \max_{\vec{y}} \quad & \sum_{i=1}^{r} \gamma_i y_i + \sum_{j=1}^{s} \widetilde{\gamma}_j y_{j+r} \\ \text{subject to} \quad & \sum_{i=1}^{r} y_i \Gamma_i + \sum_{j=1}^{s} y_{j+r} \widetilde{\Gamma}_j \leq \nabla f(\rho')^T, \\ & y_{j+r} \leq 0 \text{ for } j = 1, ..., s, \\ & \vec{y} \in \mathbb{R}^{r+s}. \end{aligned} \tag{2.55}$$

Define $\mathbf{S}^*(\rho')$ to be the dual feasible set which contains all vectors $\vec{y} \in \mathbb{R}^{r+s}$ that satisfy all the above constraints, then the lower bound for the privacy amplification term is

$$f(\rho') - \text{Tr}(\rho' \nabla f(\rho')^T) + \max_{\vec{y} \in \mathbf{S}^*(\rho')} \left(\sum_{i=1}^{r} \gamma_i y_i + \sum_{j=1}^{s} \widetilde{\gamma}_j y_{j+r} \right). \tag{2.56}$$

We refer the reader to Appendix A.2 in Ref. [2] for the derivations. We call the linearisation process together with solving the dual problem "Step 2". The whole numerical framework for lower bounding the privacy amplification term is summarised in Figure 2.2.

If the operator $\mathcal{G}(\rho)$ is singular, the matrix gradient $\nabla f(\rho)$ may be undefined, in which case Ref. [2] proposed a perturbed version of the objective function by replacing the map $\mathcal{G}$ with a perturbed map

$$\mathcal{G}_\epsilon(\rho) \coloneqq (1 - \epsilon)\mathcal{G}(\rho) + \frac{\epsilon}{d'} \mathbb{1}_{d'} \tag{2.57}$$

with d' to be the dimension of $\mathcal{G}(\rho)$ such that $f_\epsilon(\rho) \coloneqq D(\mathcal{G}_\epsilon(\rho) || \mathcal{Z}(\mathcal{G}_\epsilon(\rho)))$, thereby ensuring the gradient of the perturbed objective function $\nabla f_\epsilon(\rho)$ to be defined always. It follows from the proof in Ref. [2] that the optimal solution to the perturbed objective function satisfies

$$\alpha \geq \alpha(\epsilon) - \zeta_\epsilon \text{ where } \alpha(\epsilon) \coloneqq \min_{\rho \in \mathbf{S}} f_\epsilon(\rho), \tag{2.58}$$

and the lower bound for the privacy amplification term under the perturbation is

$$f_\epsilon(\rho') - \text{Tr}(\rho' \nabla f_\epsilon(\rho')^T) + \max_{\vec{y} \in \mathbf{S}^*_\epsilon(\rho')} \left(\sum_{i=1}^{r} \gamma_i y_i + \sum_{j=1}^{s} \widetilde{\gamma}_j y_{j+r} \right) - \zeta_\epsilon \,, \tag{2.59}$$

[†]In the original paper [2], the authors did not consider inequality constraints, so the second line in the constraints of the dual problem (2.55) was not included in Ref. [2].

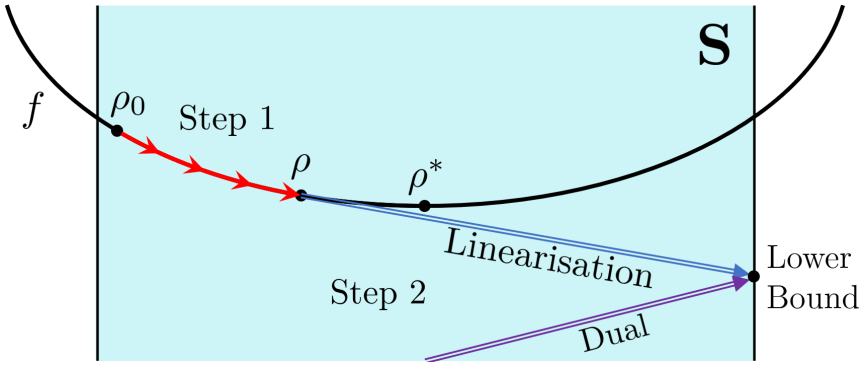


Figure 2.2: Illustration of the numerical approach in obtaining the lower bound for the privacy amplification term. Starting with the initial guess $\rho_0 \in \mathbf{S}$, step 1 takes ρ_0 to a point $\rho \in \mathbf{S}$ near the optimal point $\rho^* \in \mathbf{S}$. Step 2 begins with the linearisation of the convex function f at ρ and ends with finding the suboptimal solution to the dual problem. The linearisation undercuts the convex function, thereby guaranteeing any dual solution to lower bound the optimal value $f(\rho^*)$. This figure is reproduced from Figure 1 of Ref. [2].

where the dual feasible set is

$$\mathbf{S}_\epsilon^*(\rho') \coloneqq \{\vec{y} \in \mathbb{R}^{r+s} : \sum_{i=1}^{r} y_i \Gamma_i + \sum_{j=1}^{s} y_{j+r} \widetilde{\Gamma}_j \leq \nabla f_\epsilon(\rho')^T, y_{j+r} \leq 0 \text{ for } j = 1, ..., s\}$$

and the correction term is $\zeta_\epsilon \coloneqq 2\epsilon(d'-1)\log\frac{d'}{\epsilon(d'-1)}$ provided that the perturbation parameter ϵ satisfies $0 < \epsilon \leq \frac{1}{e(d'-1)}$ for e to be the base of the natural logarithm. The form of the correction term ζ_ϵ comes from the use of Fannes' inequality [38, 39] in upper bounding the difference between the original and the perturbed objective functions when evaluated on the same state, i.e. $|f(\rho) - f_\epsilon(\rho)| \leq \zeta_\epsilon$ (Lemma 8 [2]). We emphasise that the expression in (2.59) is still a valid lower bound for the optimal solution $\alpha = \min_{\rho \in \mathbf{S}} f(\rho)$ (Theorem 2 [2]), so this bound is a generalised version of the unperturbed bound (2.56) which corresponds to the case when $\epsilon = 0$ and $\mathcal{G}(\rho)$ is full-rank.

Due to finite numerical precision in any actual computation (e.g. the constraint matrices could be created with slight deviations, the density operator and the matrix gradient are not stored with infinite precision, numerical optimisation solvers do not return solutions that satisfy all constraints exactly), one must address the reliability issue with the numerically obtained lower bound for the privacy amplification term. To handle this problem, the authors of [2] reformulate the SDP problem such that the constraints do not have

to be satisfied precisely. The basic idea is to allow the constraints for the optimisation problem outlined above to relax slightly, which is equivalent to enlarging the feasible set, so naturally, the lower bound obtained in this case would be more conservative.

We now summarise the way of handling finite numerical precision discussed in Section 3.3 – 3.4 of Ref. [2]. Let the matrices $\{\Gamma'_i\}$ and $\{\widetilde{\Gamma}'_j\}$ together with the real numbers $\{\gamma'_i\}$ and $\{\widetilde{\gamma}'_j\}$ be the finite-precision form stored in a computer, which correspond to the actual equality and inequality constraints: matrices $\{\Gamma_i\}$ and $\{\widetilde{\Gamma}_j\}$ together with the real numbers $\{\gamma_i\}$ and $\{\widetilde{\gamma}_j\}$. Let $\epsilon' > 0$ be a relaxation parameter that is chosen to be sufficiently but not overly large such that the set[‡]

$$\widetilde{\mathbf{S}}_{\epsilon'} = \{\rho \in \mathcal{D}(\mathcal{H}_{AB}) : |\mathrm{Tr}(\Gamma'_i\rho) - \gamma'_i| \leq \epsilon' \ \forall \ i, \mathrm{Tr}(\widetilde{\Gamma}'_j\rho) \leq \widetilde{\gamma}'_j + \epsilon' \ \forall \ j\} \tag{2.60}$$

is guaranteed to contain the original feasible set $\mathbf{S}$, i.e. $\mathbf{S} \subseteq \widetilde{\mathbf{S}}_{\epsilon'}$. There are two sources of imprecision that allow one to determine the relaxation parameter ϵ'. The first one is the imprecision in representing the constraints in a computer, which is described by the parameter [2]

$$\epsilon_{\mathrm{rep}} \coloneqq \max_{i,j}\{||\Gamma'_i - \Gamma_i||_{\mathrm{HS}} \ , ||\widetilde{\Gamma}'_j - \widetilde{\Gamma}_j||_{\mathrm{HS}}\} + \max_{i,j}\{|\gamma'_i - \gamma_i|, |\widetilde{\gamma}'_j - \widetilde{\gamma}_j|\} \tag{2.61}$$

that measures the maximal deviation from the actual constraints, where the Hilbert-Schmidt norm is defined as $||X||_{\mathrm{HS}} \coloneqq \sqrt{\mathrm{Tr}(X^\dagger X)}$. The second source of imprecision comes from the fact that solutions returned by numerical solvers never satisfy all constraints exactly (e.g. the matrix corresponding to the suboptimal solution can have slightly negative eigenvalues). This source of imprecision is measured by the maximal constraint violation ϵ_{sol} of the matrix output from the numerical solver. According to Appendix D of Ref. [2], the relaxation parameter ϵ' can be chosen to be

$$\epsilon' = \max\{\epsilon_{\mathrm{rep}}, \epsilon_{\mathrm{sol}}\} \tag{2.62}$$

in order to ensure the original feasible set is really contained by the enlarged set.

The relaxed equality constraints $|\mathrm{Tr}(\Gamma'_i\rho) - \gamma'_i| \leq \epsilon'$ in (2.60) can be split into two sets of inequality constraints:

$$\mathrm{Tr}(\Gamma'_i\rho) \leq \gamma'_i + \epsilon' \quad \text{and} \quad \mathrm{Tr}(-\Gamma'_i\rho) \leq -\gamma'_i + \epsilon' \quad \text{for } i = 1, ..., r. \tag{2.63}$$

[‡]Note that the authors of Ref. [2] did not consider inequality constraints in the original paper. Here, we generalise the idea to the inequality constraints by adding ϵ' to each finite-precision inequality constraints $\{\widetilde{\gamma}'_j\}$ so that the enlarged feasible set with respect to the imperfect constraints still contains the original feasible set.

Hence, all our constraints are now inequality constraints. Since we enlarge the feasible set, it is intuitive to see that the optimal solution to the perturbed objective function over $\widetilde{\mathbf{S}}_{\epsilon'}$ to be upper bounded by the true optimal value α,

$$\alpha \geq \alpha_{\epsilon'}(\epsilon) - \zeta_\epsilon \text{ where } \alpha_{\epsilon'}(\epsilon) \coloneqq \min_{\rho \in \widetilde{\mathbf{S}}_{\epsilon'}} f_\epsilon(\rho), \tag{2.64}$$

which was proven in Theorem 3 of Ref. [2]. Most importantly, the lower bound for the privacy amplification term as a dual problem corresponding to the optimisation of the perturbed and linearised objective function over the enlarged feasible set is

$$f_\epsilon(\rho') - \mathrm{Tr}(\rho' \nabla f_\epsilon(\rho')^T) + \max_{\vec{y} \in \widetilde{\mathbf{S}}^*_\epsilon(\rho')} \left(\sum_{i=1}^{r} (\gamma_i + \epsilon') y_i + \sum_{i=1}^{r} (-\gamma_i + \epsilon') y_{i+r} + \sum_{j=1}^{s} (\widetilde{\gamma}_j + \epsilon') y_{j+2r} \right) - \zeta_\epsilon \ , \tag{2.65}$$

where the new dual feasible set is

$$\widetilde{\mathbf{S}}^*_\epsilon(\rho') \coloneqq \{\vec{y} \in \mathbb{R}^{2r+s} : \sum_{i=1}^{r} (y_i - y_{i+r}) \Gamma_i + \sum_{j=1}^{s} y_{j+2r} \, \widetilde{\Gamma}_j \leq \nabla f_\epsilon(\rho')^T, y_k \leq 0 \text{ for } k = 1, ..., 2r+s\}.$$

This lower bound for the true key rate will be the secure key rate value quoted from a numerical security proof of a QKD protocol.

Chapter 3

Squashing Models

In this chapter, we will first review the basic ideas behind squashing models and state the formal definition of a valid squashing model. We will then discuss how squashing models can be incorporated into current security proof framework to prove unconditional security of QKD protocols. Finally, we will study the flat-state squashing model as an example. For the closing remark, we will briefly mention the open problems in QKD related to squashing models.

3.1 Introduction

In any QKD protocol, quantum signal states must travel through a quantum channel which is assumed to be controlled by the adversary before it reaches the receiver. As described in the previous chapter, when we prove the security of a protocol, we calculate the key rate with the quantum state corresponding to the adversary's worst attack given that it satisfies the measurement statistics. However, to find the worst attack among all possible attacks allowed by quantum theory, we cannot restrict the dimension of the output state of the quantum channel. Therefore, the key rate calculation which is reformulated as the optimisation problem in (2.52) requires an optimisation over infinite-dimensional density matrices. This is clearly not a numerically tractable optimisation problem because computers can only store and operate on finite-dimensional matrices. We will see that squashing models provide the solution to this issue.

Squashing models connect the actual QKD protocol to a virtual QKD protocol associated with a finite-dimensional optimisation problem. As we will prove in Section 3.3,

the optimal solution to the new finite-dimensional optimisation problem is guaranteed to lower bound the optimal solution to the original problem. Therefore, we can obtain a reliable lower bound for the key rate of the actual protocol by solving the finite-dimensional optimisation problem admitted by a squashing model.

The intuition behind squashing models is as follows. The goal is to build a physical model that ensures the receiver to receive finite-dimension states which are called *squashed states* from the quantum channel. To achieve this, we manually insert an additional physical channel Λ between the actual quantum channel Φ and the receiver as illustrated in Figure 3.1. This additional channel Λ which we call a *squashing map* is constructed to reduce the dimension of incoming states from infinite to finite. We assume the adversary to have full control of the squashing map. The receiver will measure the squashed states with a new set of measurements which reproduce the original statistics. Therefore, we obtain an effective QKD protocol where the receiver's state is finite-dimensional. Proving the security of this virtual protocol only requires one to optimise a finite-dimensional optimisation problem if the sender's state is also finite-dimensional.

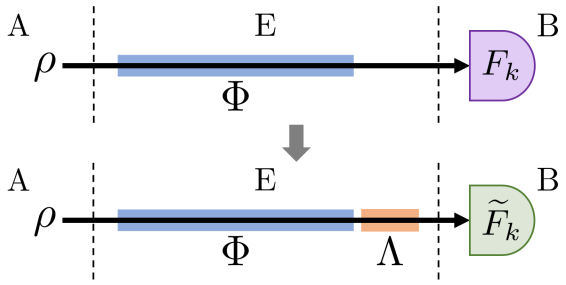


Figure 3.1: Illustration of how a virtual protocol (bottom) with finite-dimensional output states $\Lambda \circ \Phi(\rho)$ and POVM $\{\widetilde{F}_k\}$ can be obtained from applying a squashing model to the original protocol (top) with infinite-dimensional output states $\Phi(\rho)$ and POVM $\{F_k\}$.

The first squashing model's existence was postulated by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [40] to prove security of the weak coherence pulse BB84 protocol by converting the receiver's states into qubit states so that the qubit-to-qubit security analysis [41, 42] can still be applied. We call a squashing model qubit-based if it converts the original protocol into an effective qubit protocol. Later, more qubit-based squashing models were discovered for various QKD protocols [43, 4, 44], which extend the applicability of qubit-to-qubit security analysis to a wider class of QKD protocols. However, it was proven by Beaudry *et al.* [3] with the counterexample of the six-state protocol that not all QKD protocols have an exact qubit-based squashing model. Also, most of the existing qubit-based squashing models rely on randomly assigning certain measurement outcomes that

can only be caused by multi-photons to one of the two qubit measurement outcomes. This will introduce additional qubit errors to the original data and may lower the key rate with this extra noise.

Recently, a new type of squashing model, namely the flag-state squashing model [8], is developed to circumvent the limitations of the qubit-based squashing models. This squashing model can be applied to any QKD protocols with the receiver's POVM being block-diagonal in some basis. Since the POVM associated with a measurement using threshold detectors is block-diagonal in total photon number basis, most discrete-variable protocols using threshold detectors for measurements will admit a flag-state squashing model. We will see more details about this model in Section 3.4 and how it is applied to the unbalanced phase-encoded BB84 protocol in Chapter 4.

3.2 Mathematical definition

In this section, we will state the formal definition of a squashing model and highlight the implications of the definition.

Definition 3.2.1. (Squashing Model)
Let $\mathcal{H}$, $\mathcal{K}$ be two Hilbert spaces where $\dim(\mathcal{H}) = \infty$ and $\dim(\mathcal{K})$ is finite. Let $\mathcal{D}(\mathcal{H})$ and $\mathcal{B}(\mathcal{H})$ denote the set of density matrices and the set of bounded operators acting on a Hilbert space $\mathcal{H}$ respectively. Let $\Lambda : \mathcal{D}(\mathcal{H}) \mapsto \mathcal{D}(\mathcal{K})$ be a linear CPTP map (i.e. a physical quantum channel). Let $\{F_k\} \subset \mathcal{B}(\mathcal{H})$ be a POVM where k labels a finite set of measurement outcomes. Λ is a **squashing map** if:

(1) there exists another POVM $\{\widetilde{F}_k\} \subset \mathcal{B}(\mathcal{K})$ such that

$$\mathrm{Tr}\left(\widetilde{F}_k \Lambda(\rho)\right) = \mathrm{Tr}\left(F_k \rho\right) = p(k) \quad \forall\ \rho \in \mathcal{D}(\mathcal{H}), \tag{3.1}$$

where $p(k)$ denotes the probability of outcome k ,

(2) Λ is not entanglement breaking.

The corresponding adjoint map $\Lambda^\dagger : \mathcal{B}(\mathcal{K}) \mapsto \mathcal{B}(\mathcal{H})$ is CP unital (UCP), not entanglement breaking, and satisfies

$$\Lambda^\dagger(\widetilde{F}_k) = F_k \ \forall\ k\ . \tag{3.2}$$

Since $\Lambda^\dagger$ is linear, any linear dependency between elements F_k is conserved such that

$$\sum_k c_k F_k = 0 \iff \sum_k c_k \widetilde{F}_k = 0 \quad \text{where } c_k \in \mathbb{C}\ \forall\ k. \tag{3.3}$$

The first condition infers that the squashing model needs to preserve the probabilities of all measurement outcomes and for all quantum states. The second condition is necessary because a certain degree of entanglement between the sender's and the receiver's states must be preserved after the receiver's state passes through the squashing map in order for a QKD protocol to distill secure keys [22]. This condition rules out squashing map candidates that take the form $\Phi(\rho) = \sum_k \mathrm{Tr}(F_k\rho)\sigma_k$ where $\sigma_k \in \mathcal{D}(\mathcal{K})$ for each k [16].

In previous literature [3, 43], the actual measurement performed by the experimental setup is described by what they call the "basic" measurement POVM F_B. The basic measurement is differentiated from the "full" measurement which is obtained from classical post-processing the basic measurement statistics as illustrated in Figure 3.2. In general, classical post-processing is not a necessary procedure for a squashing model to work (see flag-state squashing model in Section 3.4). Therefore, we do not include classical post-processing in our definition. To align our notation with Refs. [3, 43], the POVM $\{F_k\}$ in our definition refers to the full measurement POVM F_M or the basic measurement POVM F_B depending on whether classical post-processing of the basic measurement statistics is used. The "target" measurement F_Q in Refs. [3, 43] is equivalent to the squashed POVM $\{\widetilde{F}_k\}$ in the definition above.

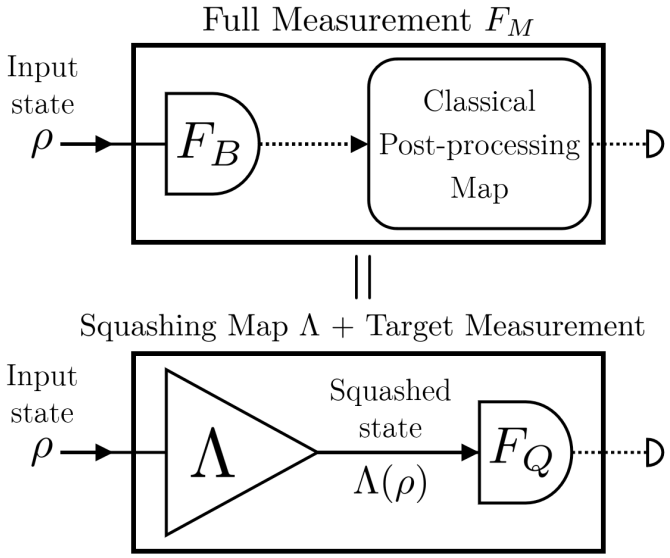


Figure 3.2: Illustration of how the actual measurement in an experiment combined with a classical post-processing scheme can be viewed equivalent to the action of a squashing map followed by a new set of measurements on the squashed states. This figure is reproduced from Figure 1 of Ref. [3].

3.3 Unconditional security of squashing models

When we use squashing model to prove security of a QKD protocol, we need to make sure that proving the virtual (squashed) protocol to be secure entails the original protocol to be secure. In this section, we will prove unconditional security of squashing model in the asymptotic limit which is stated in the following theorem.

Theorem 3.3.1 (Unconditional Asymptotic Security of Squashing Models)
The asymptotic secure key rate of the virtual QKD protocol associated with any squashing model applied to a QKD protocol always lower bounds the asymptotic secure key rate of the original QKD protocol.

Intuitively, allowing Eve to control the squashing channel gives her additional eavesdropping power or knowledge of the signals. Therefore, one can expect the secure key rate of any protocol to reduce under the usage of a squashing model. In the formal proof below, we use the source replacement scheme where Alice sends a quantum state to Bob.

Proof. Let the joint state shared by Alice and Bob be ρ_{AB} and the state $|\psi\rangle_{ABE}$ be the purification of the state ρ_{AB} (i.e. $\rho_{AB} = \mathrm{Tr}_E(|\psi\rangle\langle\psi|_{ABE})$), where A, B and E denotes the registers of Alice, Bob and Eve respectively. By Schmidt decomposition, the pure state can be decomposed as

$$|\psi\rangle_{ABE} = \sum_i \sqrt{\lambda_i}|e_i\rangle_{AB} \otimes |f_i\rangle_E \ , \tag{3.4}$$

where $\lambda_i \in \mathbb{R} \ \forall \ i$, and the two sets of vectors $\{|e_i\rangle_{AB}\}$ and $\{|f_i\rangle_E\}$ form the orthonormal bases of the Hilbert spaces $\mathcal{H}_{AB}$ and $\mathcal{H}_E$ respectively.

In the source-replacement scheme, both Alice and Bob will measure their states. Let Alice's and Bob's joint POVM be $\{P_k\}$ with k labelling their joint measurement outcomes. The state shared by all parties after Alice and Bob perform measurements and public announcements is

$$\rho_{ABMCE} = \sum_{i,j,k} \sqrt{\lambda_i\lambda_j}(\sqrt{P_k}|e_i\rangle\langle e_j|\sqrt{P_k})_{AB} \otimes |k\rangle\langle k|_M \otimes |a_k\rangle\langle a_k|_C \otimes |f_i\rangle\langle f_j|_E \tag{3.5}$$

where M and C denote the classical registers for storing Alice's and Bob's joint measurement outcomes and their public announcements respectively. Since announcements are made public, Eve can keep a copy of register C. A key map is performed by either Alice or Bob depending on the reconciliation scheme. The key map $\tilde{g}$ outputs a key bit z using the measurement data k and the announcement data a_k (i.e. $\tilde{g} : k \times a_k \mapsto z$). We add a

classical key register Z to keep the raw key bit. After tracing out registers A, B and M, the classical-quantum (c-q) state for the key register and Eve's registers is

$$\rho_{ZCE} = \sum_{i,j,k} \sqrt{\lambda_i \lambda_j} \mathrm{Tr}(P_k |e_i\rangle\langle e_j|) |\tilde{g}(k, a_k)\rangle\langle \tilde{g}(k, a_k)|_Z \otimes |a_k\rangle\langle a_k|_C \otimes |f_i\rangle\langle f_j|_E \, . \tag{3.6}$$

We shall see later that if the initial purifying state $|\psi\rangle_{ABE}$ is fixed, the state in Equation (3.6) is also the joint state of the key and Eve's registers when a squashing model is applied.

Assume that a squashing model exists for the QKD protocol, which has a squashing map $\Lambda : \mathcal{D}(\mathcal{H}_B) \mapsto \mathcal{D}(\mathcal{H}_{B'})$ and a squashed joint POVM $\{Q_k : \widetilde{\Lambda}^\dagger(Q_k) = P_k\} \subset \mathcal{B}(\mathcal{H}_{AB'})$ with the map $\widetilde{\Lambda}^\dagger$ being the adjoint of the extended squashing map $\widetilde{\Lambda} = \mathbb{1}_A \otimes \Lambda$. A squashing map is by definition a quantum channel, so by Stinespring's dilation theorem, there exists an isometry $V_{B \to B'E'}$ such that

$$\Lambda(\rho) = \mathrm{Tr}_{E'}(V_{B \to B'E'} \, \rho \, V^\dagger_{B \to B'E'}). \tag{3.7}$$

We name Bob's new register corresponding to the squashed states he receives B' and the environment register E'. Since we assume that the squashing map is in Eve's domain, Eve has access to the register E' which means her registers (E, E') together purify Alice's and Bob's new joint state $\rho_{AB'} = (\mathbb{1}_A \otimes \Lambda)(\rho_{AB})$. After squashing, the new pure state is

$$|\widetilde{\psi}\rangle_{AB'EE'} = (\mathbb{1}_A \otimes V_{B \to B'E'}) |\psi\rangle_{ABE} \tag{3.8}$$

$$= \sum_i \sqrt{\lambda_i} (\mathbb{1}_A \otimes V_{B \to B'E'}) |e_i\rangle_{AB} \otimes |f_i\rangle_E \, . \tag{3.9}$$

We now consider the state shared by all parties after Alice and Bob perform their measurements and announcements under a squashing model, which takes the form

$$\tilde{\rho}_{AB'MCE'E} = \sum_{i,j,k} \sqrt{\lambda_i \lambda_j} (\sqrt{Q_k} \otimes \mathbb{1}_{E'}) (\mathbb{1}_A \otimes V_{B \to B'E'}) |e_i\rangle\langle e_j| (\mathbb{1}_A \otimes V^\dagger_{B \to B'E'}) (\sqrt{Q_k} \otimes \mathbb{1}_{E'})$$

$$\otimes |k\rangle\langle k|_M \otimes |a_k\rangle\langle a_k|_C \otimes |f_i\rangle\langle f_j|_E \, . \tag{3.10}$$

Applying the same key map $\tilde{g}$ defined above, the c-q state of the key and Eve's registers is

$$\tilde{\rho}_{ZCE'E} = \sum_{i,j,k} \sqrt{\lambda_i \lambda_j} \mathrm{Tr}_{AB'} [(\sqrt{Q_k} \otimes \mathbb{1}_{E'}) (\mathbb{1}_A \otimes V_{B \to B'E'}) |e_i\rangle\langle e_j| (\mathbb{1}_A \otimes V^\dagger_{B \to B'E'}) (\sqrt{Q_k} \otimes \mathbb{1}_{E'})] \times$$

$$|\tilde{g}(k, a_k)\rangle\langle \tilde{g}(k, a_k)|_Z \otimes |a_k\rangle\langle a_k|_C \otimes |f_i\rangle\langle f_j|_E \, . \tag{3.11}$$

If Eve gives up her additional knowledge from the squashing channel, she discards her system E' (i.e. tracing out register E') resulting in the state

$$\tilde{\rho}_{ZCE} = \sum_{i,j,k} \sqrt{\lambda_i \lambda_j} \mathrm{Tr}[(\sqrt{Q_k} \otimes \mathbb{1}_{E'})(\mathbb{1}_A \otimes V_{B\to B'E'})|e_i\rangle\langle e_j|(\mathbb{1}_A \otimes V^\dagger_{B\to B'E'})(\sqrt{Q_k} \otimes \mathbb{1}_{E'})] \times \\ |\tilde{g}(k,a_k)\rangle\langle\tilde{g}(k,a_k)|_Z \otimes |a_k\rangle\langle a_k|_C \otimes |f_i\rangle\langle f_j|_E \,. \quad (3.12)$$

Using the definition of the dilation isometry $V^\dagger_{B\to B'E'}$, we can simplify the trace as

$$\begin{aligned} &\mathrm{Tr}[(\sqrt{Q_k} \otimes \mathbb{1}_{E'})(\mathbb{1}_A \otimes V_{B\to B'E'})|e_i\rangle\langle e_j|(\mathbb{1}_A \otimes V^\dagger_{B\to B'E'})(\sqrt{Q_k} \otimes \mathbb{1}_{E'})] \\ =&\mathrm{Tr}_{AB'}(Q_k \,\mathrm{Tr}_{E'}[(\mathbb{1}_A \otimes V_{B\to B'E'})|e_i\rangle\langle e_j|(\mathbb{1}_A \otimes V^\dagger_{B\to B'E'})]) && (3.13)\\ =&\mathrm{Tr}_{AB'}[Q_k(\mathbb{1}_A \otimes \Lambda)(|e_i\rangle\langle e_j|)] && (3.14)\\ =&\mathrm{Tr}_{AB'}[Q_k\widetilde{\Lambda}(|e_i\rangle\langle e_j|)] && (3.15)\\ =&\mathrm{Tr}_{AB}[\widetilde{\Lambda}^\dagger(Q_k)|e_i\rangle\langle e_j|] && (3.16)\\ =&\mathrm{Tr}_{AB}(P_k|e_i\rangle\langle e_j|). && (3.17) \end{aligned}$$

Hence, we recover the state ρ_{ZCE} in (3.6) as in

$$\begin{aligned} \tilde{\rho}_{ZCE} &= \sum_{i,j,k} \sqrt{\lambda_i \lambda_j} \mathrm{Tr}(P_k|e_i\rangle\langle e_j|)|\tilde{g}(k,a_k)\rangle\langle\tilde{g}(k,a_k)|_Z \otimes |a_k\rangle\langle a_k|_C \otimes |f_i\rangle\langle f_j|_E && (3.18)\\ &= \rho_{ZCE} \,. \end{aligned}$$

This implies that Eve can perform the same attack as before if she does not utilise the additional register E' from purifying the squashed state.

We are ready to show that the asymptotic secure key rate can only decrease after applying the squashing model. In the Devetak-Winter key rate formula [32], the error-correction term is unaffected by the squashing model since this term only cares about the joint probabilities of the raw key and the measurement outcomes, which are preserved by the squashing model. Therefore, we only need to consider the privacy amplification (PA) term in the rest of the proof.

Let Eve's optimal attack be the purification $|\psi^*\rangle_{ABE}$ meaning that it minimises the PA term in the asymptotic key rate formula. Let the purifying state of the optimal pure state after applying the squashing model be $|\widetilde{\psi^*}\rangle_{AB'EE'} = (\mathbb{1}_A \otimes V_{B\to B'E'})|\psi^*\rangle_{ABE}$. The corresponding mixed states for the two pure states after measurement, announcement and key map be ρ^*_{ZABMCE} and $\tilde{\rho}^*_{ZAB'MCE'E}$. We already showed that $\mathrm{Tr}_{AB'ME'}(\tilde{\rho}^*_{ZAB'MCE'E}) = \tilde{\rho}^*_{ZCE} = \rho^*_{ZCE} = \mathrm{Tr}_{ABM}(\rho^*_{ZABMCE})$. The last step is to show that the PA term of the

original QKD protocol R^{∞}_{PA} (i.e. the first term in (2.43)) is lower bounded by the PA term of the squashed protocol $\widetilde{R}^{\infty}_{\mathrm{PA}}$ as follows

$$\begin{aligned}
R^{\infty}_{\mathrm{PA}} &= \min_{|\psi\rangle_{ABE}\in\mathbf{S}} H(Z|C,E)_{\rho_{ZABMCE}} \\
&= H(Z|C,E)_{\rho^{*}_{ZABMCE}} && (3.19)\\
&= H(Z|C,E)_{\tilde{\rho}^{*}_{ZAB'MCE'E}} \qquad (\because \tilde{\rho}^{*}_{ZCE} = \rho^{*}_{ZCE}) && (3.20)\\
&\geq H(Z|C,E,E')_{\tilde{\rho}^{*}_{ZAB'MCE'E}} \qquad (\mathrm{SSA}) && (3.21)\\
&\geq \min_{|\widetilde{\psi}\rangle_{AB'EE'}\in\widetilde{\mathbf{S}}} H(Z|C,E,E')_{\tilde{\rho}_{ZAB'MCE'E}} && (3.22)\\
&= \widetilde{R}^{\infty}_{\mathrm{PA}}
\end{aligned}$$

where $\mathbf{S}$ denotes the feasible set of pure states that satisfy the measurement statistics and $\widetilde{\mathbf{S}} = \{|\widetilde{\psi}\rangle_{AB'EE'} : \mathrm{Tr}_{E'E}|\widetilde{\psi}\rangle\langle\widetilde{\psi}| \in \mathbf{S}_{AB'} \cap \mathrm{Image}(\widetilde{\Lambda})\}$ is the intersecting set of the feasible set $\mathbf{S}_{AB'} \subset \mathcal{D}(\mathcal{H}_{AB'})$ and the image of the extended squashing map $\widetilde{\Lambda} = \mathbb{1}_A \otimes \Lambda$. To go from the third to the fourth line, we used strong subadditivity (SSA) of von Neumann entropy (Theorem 2.1.6) which introduces the first inequality. The second inequality comes from the fact that $|\widetilde{\psi}^{*}\rangle_{AB'EE'} \in \widetilde{\mathbf{S}}$, so the minimisation over the whole set $\widetilde{\mathbf{S}}$ is at most the value evaluated with $|\widetilde{\psi}^{*}\rangle_{AB'EE'}$. Hence, we proved Theorem 3.3.1. ■

With Theorem 3.3.1, we can prove the asymptotic unconditional security of a QKD protocol using a squashing model if there exists one for the protocol.

3.4 Flag-state squashing model

The flag-state squashing model [8] is non-qubit-based, meaning that it does not squash the protocol into an effective qubit protocol. Instead, it squashes the input states into finite-, multi-dimensional states with some of the original state structure preserved. Note that the flag-state squashing model only holds for cases where the POVM elements are all block-diagonal with respect to two mutually orthogonal subspaces. We will show later that the flag-state squashing model does not conserve probabilities if the POVM is not block-diagonal.

Assume that all POVM elements F_k's are block-diagonal in the sense that each element has the form $F_k = F_{k,P} \oplus F_{k,P^{\perp}}$ in the same basis where P and $P^{\perp}$ are orthogonal subspaces. The flag-state squashing map Λ, as illustrated in Figure 3.3, first projects an input state

ρ onto the two subspaces P and $P^\perp$. We require the projectors for the two subspaces $\{\Pi_P, \Pi_{P^\perp}\}$ sum to identity of the full Hilbert space $\mathcal{H}$ (i.e. $\Pi_P + \Pi_{P^\perp} = \mathbb{1}_\mathcal{H}$). It then applies an identity map to the projected state $\rho_P = \Pi_P \rho \Pi_P$ and measures the projected state $\rho_{P^\perp} = \Pi_{P^\perp} \rho \Pi_{P^\perp}$ to give the squashed state

$$\Lambda(\rho) = \Pi_P \rho \Pi_P \oplus \sum_k \mathrm{Tr}(F_k \Pi_{P^\perp} \rho \Pi_{P^\perp}) |k\rangle\langle k| = \left(\begin{array}{c|c} \rho_P & 0 \\ \hline 0 & \sum_k \mathrm{Tr}(F_k \rho_{P^\perp}) |k\rangle\langle k| \end{array}\right). \tag{3.23}$$

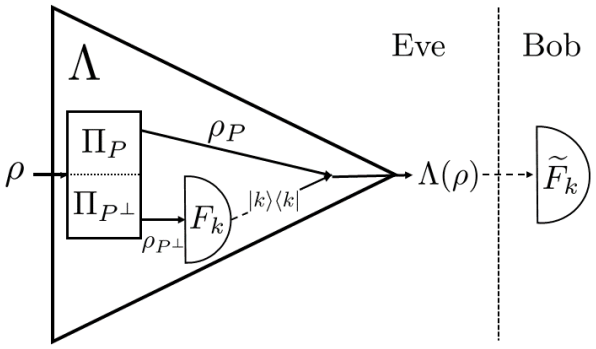


Figure 3.3: A flag-state squashing map Λ projects a state ρ onto orthogonal subspaces P and $P^\perp$ with projectors $\{\Pi_P\ , \Pi_{P^\perp}\}$. Depending on which subspace ρ is projected onto, the projected state will either pass through the map unchanged if it is in subspace P, or it will be measured and replaced by a classical flag-state $|k\rangle\langle k|$ based on the measurement outcome k if it is in the $P^\perp$-subspace. The squashing map is assigned to Eve, allowing her to have more eavesdropping power. The result of the squashing map $\Lambda(\rho)$ will then be sent to Bob who performs the final measurement with the squashed POVM $\{\widetilde{F}_k\}$.

After the state passes through the squashing map, the receiver measures the squashed state with the flag-state POVM $\{\widetilde{F}_k\}$ where

$$\widetilde{F}_k = F_{k,P} \oplus |k\rangle\langle k| = \left(\begin{array}{c|c} F_{k,P} & 0 \\ \hline 0 & |k\rangle\langle k| \end{array}\right) = \left(\begin{array}{c|ccccc} F_{k,P} & & & 0 & & \\ \hline & 0 & & & & \\ & & \ddots & & & \\ 0 & & & 1 & & \\ & & & \uparrow & \ddots & \\ & & & k^{\text{th}} & & 0 \end{array}\right). \tag{3.24}$$

One can verify that the original probabilities for each outcome k are conserved when the squashed state is measured by the flag-state POVM. Thus, condition (1) in Definition 3.2.1 for squashing models is satisfied.

In general, an arbitrary input state does not have to be block-diagonal in the basis where the POVM is block-diagonal. Projecting the state onto subspaces P and $P^{\perp}$ will set its off-diagonal blocks to zeros. Due to the block-diagonal structure of the POVM, the measurement probability is unaffected by the state projections which we call a quantum nondemolition (QND) measurement. However, if the POVM is not block-diagonal, projecting the input state onto subspaces will alter the outcome probabilities. Therefore, condition (1) in Definition 3.2.1 is not satisfied. Note that the dimension of the state and the POVM elements has been reduced to the dimension of the subspace P plus the number of elements in the POVM. If subspace P is finite-dimensional, then the image of the map Λ is also finite-dimensional.

3.4.1 CPTP condition

We will prove that the flag-state squashing map Λ is a physical channel (i.e. a linear CPTP map). The map Λ is by construction linear, so we only need to prove that it is CPTP. We first show that the map Λ is trace-preserving (TP) which goes as

$$\begin{aligned}
\mathrm{Tr}(\Lambda(\rho)) &= \mathrm{Tr}[\Pi_P \rho \Pi_P \oplus \sum_k \mathrm{Tr}(F_k \Pi_{P^\perp} \rho \Pi_{P^\perp}) |k\rangle\langle k|] && (3.25)\\
&= \mathrm{Tr}(\Pi_P \rho \Pi_P) + \sum_k \mathrm{Tr}(F_k \Pi_{P^\perp} \rho \Pi_{P^\perp}) \mathrm{Tr}(|k\rangle\langle k|) && (3.26)\\
&= \mathrm{Tr}(\rho \Pi_P) + \mathrm{Tr}\left[\left(\sum_k F_k \right) \Pi_{P^\perp} \rho \Pi_{P^\perp} \right] && (3.27)\\
&= \mathrm{Tr}(\rho \Pi_P) + \mathrm{Tr}(\Pi_{P^\perp} \rho \Pi_{P^\perp}) && (3.28)\\
&= \mathrm{Tr}(\rho \Pi_P) + \mathrm{Tr}(\rho \Pi_{P^\perp}) && (3.29)\\
&= \mathrm{Tr}[\rho(\Pi_P + \Pi_{P^\perp})] && (3.30)\\
&= \mathrm{Tr}(\rho) = 1, && (3.31)
\end{aligned}$$

where we used the cyclicity of trace, properties of the projectors: 1) $\Pi_P^2 = \Pi_P$ and $\Pi_{P^\perp}^2 = \Pi_{P^\perp}$, 2) $\Pi_P + \Pi_{P^\perp} = \mathbb{1}_{\mathcal{H}}$, and the property of POVM $\sum_k F_k = \mathbb{1}_{\mathcal{H}}$ in the steps above. Hence, the map Λ is indeed trace-preserving.

To prove that the map Λ is completely positive (CP), we need to use the following theorem (Theorem 1) proved by Friedland [45].

Definition 3.4.1. (Norm and weak convergence)
Let $\mathcal{H}$ be a Hilbert space and $X \in \mathcal{B}(\mathcal{H})$ be the limit of a sequence of bounded operators $\{X_n : n \in \mathbb{N}\} \subset \mathcal{B}(\mathcal{H})$ such that $\lim_{n\to\infty} X_n = X$. The sequence is

1. convergent in norm $||\cdot||$, if $\lim_{n\to\infty} ||X_n - X|| = 0$,
2. weakly convergent, if $\lim_{n\to\infty}\langle \tilde{h}, X_n h\rangle = \langle \tilde{h}, Xh\rangle$ for every $h, \tilde{h} \in \mathcal{H}$ (denote as $X_n \xrightarrow{w} X$).

Theorem 3.4.1 (Choi's theorem in infinite dimension [45])
For $i = 1, 2$, assume the following hold:

1. *$\mathcal{H}_i$ is a Hilbert space with a countable orthonormal basis $\{|e_j^{(i)}\rangle : j \in \mathbb{N}\}$.*
2. *$\widetilde{\Pi}_n^{(i)}$ denotes the projection on span$\{|e_1^{(i)}\rangle, ..., |e_n^{(i)}\rangle\}$ for each $n \in \mathbb{N}$.*
3. *V_i is a subspace of $\mathcal{B}(\mathcal{H}_i)$, which is closed with respect to the norm $||\cdot||_i$ and the *-conjugation. Furthermore, V_i contains the subspace of all finite range operators.*
4. *$\Phi : V_1 \to V_2$ is a bounded linear map.*
5. *For each $X \in V_1$, the sequence $\{\Phi(\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)}) : n \in \mathbb{N}\}$ converges weakly to $\Phi(X)$.*

Then the map Φ is completely positive if and only if for each $n \in \mathbb{N}$, the matrix

$$\sum_{i,j=1}^{n} E_{i,j} \otimes \widetilde{\Pi}_n^{(2)} \Phi(E_{i,j}) \widetilde{\Pi}_n^{(2)} \geq 0 \,, \tag{3.32}$$

where we define $E_{i,j} = |e_i^{(1)}\rangle\langle e_j^{(1)}|$.

Here, we let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces with countable orthonormal bases $\{|e_j^{(1)}\rangle : j \in \mathbb{N}\}$ and $\{|e_j^{(2)}\rangle : j \in \mathbb{N}\}$ respectively. The bases are chosen such that $|e_j^{(1)}\rangle = |e_j^{(2)}\rangle$ for $j \in \{1, ..., p\}$, $|e_j^{(2)}\rangle = |j - p\rangle$ which are the flag-states for $j \in \{p+1, ..., p+|K|\}$ where $|K|$ is the total number of POVM elements, and the P and $P^\perp$ projectors can be expressed as

$$\Pi_P = \sum_{i=1}^{p} |e_i^{(1)}\rangle\langle e_i^{(1)}| = \sum_{i=1}^{p} E_{i,i} \,,\ \Pi_{P^\perp} = \sum_{i=p+1}^{\infty} |e_i^{(1)}\rangle\langle e_i^{(1)}| = \sum_{i=p+1}^{\infty} E_{i,i} \,. \tag{3.33}$$

We restrict the domain and image of Λ to trace class operators $\mathcal{C}_1(\mathcal{H}_1) \subset \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{C}_1(\mathcal{H}_2) \subset \mathcal{B}(\mathcal{H}_2)$ respectively which are closed under trace norm $||\cdot||_1$ and satisfy condition (3) in Theorem 3.4.1.

Next, we have to prove that the map Λ is bounded. For any operator $X \in \mathcal{C}_1(\mathcal{H}_1)$, we use the definition of Λ to find the upper bound

$$||\Lambda(X)||_1 \leq ||\Pi_P X \Pi_P||_1 + ||\sum_k \mathrm{Tr}(F_k \Pi_{P^\perp} X \Pi_{P^\perp})|k\rangle\langle k|\,||_1 \tag{3.34}$$

$$\leq ||X||_1 + ||\sum_k |\langle F_k, \Pi_{P^\perp} X \Pi_{P^\perp}\rangle| \cdot |k\rangle\langle k|\,||_1 \tag{3.35}$$

$$\leq ||X||_1 + \sum_k |\langle F_k, \Pi_{P^\perp} X \Pi_{P^\perp}\rangle| \cdot ||\,|k\rangle\langle k|\,||_1 \tag{3.36}$$

$$\leq ||X||_1 + \sum_k ||F_k||_{op} ||\Pi_{P^\perp} X \Pi_{P^\perp}||_1 \tag{3.37}$$

$$\leq ||X||_1 + \sum_k ||X||_1 \tag{3.38}$$

$$= (1 + |K|)||X||_1\,, \tag{3.39}$$

where we use the triangle inequality several times, the Hölder's inequality (see Theorem 2.1.4) to get from (3.36) to (3.37), and the property of POVM elements that their spectra are upper bounded by 1 (i.e. $||F_k||_{op} \leq 1$). This implies $||\Lambda|| \leq 1 + |K|$ and since we assume $|K|$ to be finite, the map Λ is bounded, so condition (4) is satisfied.

We then need to prove that for each $X \in \mathcal{C}_1(\mathcal{H}_1)$, the sequence $\{\Lambda(\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)}) : n \in \mathbb{N}\}$ converges weakly to $\Lambda(X)$ where $\widetilde{\Pi}_n^{(1)}$ is defined in the same way as in Theorem 3.4.1. Since the set $\mathcal{C}_1(\mathcal{H})$ is complete in trace norm $||\cdot||_1$, any sequence of trace class operators $\{X_n : n \in \mathbb{N}\} \subset \mathcal{C}_1(\mathcal{H})$ converges to its limit $X \in \mathcal{C}_1(\mathcal{H})$ in norm (i.e. $\lim_{n\to\infty} ||X_n - X||_1 = 0$). For a sequence $\{\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)} : n \in \mathbb{N}\} \subset \mathcal{C}_1(\mathcal{H})$, there exists $\epsilon > 0$ and a large enough positive integer N_0 such that for any $n \geq N_0$, it holds that $||\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)} - X||_1 < \epsilon$, then

$$||\Lambda(\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)}) - \Lambda(X)||_1 \leq ||\Lambda|| \cdot ||\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)} - X||_1 \tag{3.40}$$

$$< (1 + |K|)\epsilon\,. \tag{3.41}$$

Since $1 + |K|$ is finite, the sequence $\{\Lambda(\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)}) : n \in \mathbb{N}\}$ converges to $\Lambda(X)$ in norm, which also implies weak convergence $\Lambda(\widetilde{\Pi}_n^{(1)} X \widetilde{\Pi}_n^{(1)}) \xrightarrow{w} \Lambda(X)$. Therefore, condition (5) is satisfied, so Theorem 3.4.1 applies here.

We are now ready to show that the Choi matrix that appears in (3.32) is positive for each $n \in \mathbb{N}$. We define projectors $\widetilde{\Pi}_n^{(2)}$ the same way as in Theorem 3.4.1 and consider the

Choi matrix for Λ of the form in (3.32) for a fixed $n \in \mathbb{N}$

$$\sum_{i,j=1}^{n} E_{i,j} \otimes \widetilde{\Pi}_n^{(2)} \Lambda(E_{i,j}) \widetilde{\Pi}_n^{(2)} \tag{3.42}$$

$$= \sum_{i,j=1}^{n} E_{i,j} \otimes \widetilde{\Pi}_n^{(2)} \left(\Pi_P E_{i,j} \Pi_P \oplus \sum_k \mathrm{Tr}(F_k \Pi_{P^\perp} E_{i,j} \Pi_{P^\perp}) |k\rangle\langle k| \right) \widetilde{\Pi}_n^{(2)} \tag{3.43}$$

$$= \begin{cases} \sum_{i,j=1}^{n} E_{i,j} \otimes E_{i,j} \ , & \text{if } n \leq p \ , \\ \sum_{i,j=1}^{p} E_{i,j} \otimes E_{i,j} \oplus \sum_{i,j=p+1}^{n} E_{i,j} \otimes \sum_{k=1}^{\min\{n-p,|K|\}} \mathrm{Tr}(F_k E_{i,j}) |k\rangle\langle k|, & \text{if } n > p \ . \end{cases} \tag{3.44}$$

For $n \leq p$,

$$\sum_{i,j=1}^{n} E_{i,j} \otimes E_{i,j} = \left(\sum_{i=1}^{n} |e_i\rangle \otimes |e_i\rangle \right) \left(\sum_{j=1}^{n} \langle e_j| \otimes \langle e_j| \right) \geq 0. \tag{3.45}$$

For $n > p$, we can consider the two parts in the direct sum in (3.44) separately since they are in two orthogonal subspaces. The first term is positive by the same argument in (3.45). The second term is

$$\sum_{i,j=p+1}^{n} E_{i,j} \otimes \sum_{k=1}^{\min\{n-p,|K|\}} \mathrm{Tr}(F_k E_{i,j}) |k\rangle\langle k| = \sum_{i,j=p+1}^{n} |e_i\rangle\langle e_j| \otimes \sum_{k=1}^{\min\{n-p,|K|\}} \langle e_j| F_k |e_i\rangle |k\rangle\langle k|. \tag{3.46}$$

The vector space V which this operator acts on has an orthonormal basis $\{|e_i\rangle \otimes |k\rangle : p+1 \leq i \leq n, 1 \leq k \leq |K|\}$. Let $|\psi\rangle = \sum_{r=p+1}^{n} \sum_l c_{r,l} |e_r\rangle \otimes |l\rangle$ be an arbitrary vector in V where $c_{r,l} \in \mathbb{C}$ for all $p+1 \leq r \leq n$ and $1 \leq l \leq |K|$. We implicitly assume that the

summation in index k below is over the range $1 \leq k \leq \min\{n-p, |K|\}$ such that

$$\langle\psi| \left(\sum_{i,j=p+1}^{n} |e_i\rangle\langle e_j| \otimes \sum_k \langle e_j|F_k|e_i\rangle |k\rangle\langle k| \right) |\psi\rangle \tag{3.47}$$

$$= \sum_{i,j,r,s=p+1}^{n} \sum_{k,u,v} c^*_{r,u} c_{s,v} \langle e_r|e_i\rangle\langle e_j|e_s\rangle\langle e_j|F_k|e_i\rangle\langle u|k\rangle\langle k|v\rangle \tag{3.48}$$

$$= \sum_{i,j=p+1}^{n} \sum_k c^*_{i,k} c_{j,k} \langle e_j|F_k|e_i\rangle \tag{3.49}$$

$$= \sum_k \left(\sum_{j=p+1}^{n} c_{j,k}\langle e_j| \right) F_k \left(\sum_{i=p+1}^{n} c^*_{i,k}|e_i\rangle \right) \tag{3.50}$$

$$= \underbrace{\left(\sum_{j=p+1}^{n} \sum_u c_{j,u}\langle e_j| \otimes \langle u| \right)}_{=\langle\phi|} \underbrace{\sum_k (F_k \otimes |k\rangle\langle k|)}_{\geq 0} \underbrace{\left(\sum_{i=p+1}^{n} \sum_v c^*_{i,v}|e_i\rangle \otimes |v\rangle \right)}_{=|\phi\rangle} \tag{3.51}$$

$$= \langle\phi| \sum_k (F_k \otimes |k\rangle\langle k|) |\phi\rangle \geq 0 \tag{3.52}$$

is positive for any vector in vector space V, so the second term is also positive. Hence, we have shown that for each $n \in \mathbb{N}$, the Choi matrix for Λ is

$$\sum_{i,j=1}^{n} E_{i,j} \otimes \widetilde{\Pi}^{(2)}_n \Lambda(E_{i,j}) \widetilde{\Pi}^{(2)}_n \geq 0. \tag{3.53}$$

By Theorem 3.4.1, the map Λ is completely positive.

To sum up this section, we have proved that the map Λ is indeed CPTP.

3.4.2 Bounding the weight in the preserved subspace

The map Λ outputs a classical state $\sum_k \mathrm{Tr}(F_k \rho_{P^\perp})|k\rangle\langle k|$ whenever the input state is in the subspace $P^\perp$, which corresponds to an entanglement breaking channel [16]. The adversary can learn the classical orthogonal states exactly, so one cannot distill secret keys out of these states. Thus, we want to make sure the input state lives mostly in the subspace P. To achieve this, we need to derive a lower bound for the weight of the input state in subspace P using the observed statistics of the sender and receiver. With a strictly positive

lower bound, the map Λ is not entanglement breaking, thereby satisfying condition (2) in Definition 3.2.1.

Here, we focus on a scenario where the receiver's detection unit uses purely threshold detectors which are commonly implemented in discrete-variable QKD protocols. In this case, the receiver's POVM $\{F_k\}$ is block-diagonal in the total photon number basis and each POVM element commutes with all photon-number projectors (i.e. $[F_k, \Pi_n] = 0 \ \forall$ k and $n \in \mathbb{N}$). Naturally, if we set a finite photon-number cutoff N, we can define the subspace P that we preserve to be the $(n \leq N)$-photon subspace and the subspace $P^{\perp}$ that we squash to be the $(n > N)$-photon subspace. The two subspaces are two Hilbert spaces containing Fock states of at most N and at least $N+1$ photons respectively. Each element of the POVM $\{F_k\}$ naturally satisfies the block-diagonal condition required by a flag-state squashing model. One can construct an observable M from a linear combination of POVM elements, i.e.

$$M = \sum_k \alpha_k F_k \ , \tag{3.54}$$

where $\alpha_k \in \mathbb{R}$ for all k so that the operator M is Hermitian. This implies that the operator M is also block-diagonal in the same way as each POVM element F_k .

The following method was first presented in Lütkenhaus' PhD thesis [46] then adapted by Narasimhachar [44] and Zhang *et al.* [8] to bound the weight $p(n \leq N)$ from below by using the observed double-click and error rates. We generalise the idea to any observable that has the form (3.54). We first define the minimum expectation value of an observable M restricted to n-photon subspace to be

$$m_n^{\min} \coloneqq \min_{\sigma_n \in \mathcal{D}(\mathcal{H})} \{\mathrm{Tr}(M\sigma_n) : \sigma_n = \Pi_n \sigma_n \Pi_n\}. \tag{3.55}$$

We will derive a lower bound for $p(n \leq N)$ with the average value of the observable M

$$\begin{aligned}
\langle M \rangle &= \sum_{n=0}^{N} p(n)\ m_n + \sum_{n=N+1}^{\infty} p(n)\ m_n && (3.56)\\
&\geq \sum_{n=0}^{N} p(n)\ m_n^{\min} + \sum_{n=N+1}^{\infty} p(n)\ m_n^{\min} && (3.57)\\
&\geq m_{n\leq N}^{\min} \sum_{n=0}^{N} p(n) + m_{n>N}^{\min} \sum_{n=N+1}^{\infty} p(n) && (3.58)\\
&= p(n \leq N)\ m_{n\leq N}^{\min} + [1 - p(n \leq N)]\ m_{n>N}^{\min} && (3.59)\\
&= m_{n>N}^{\min} - p(n \leq N)(m_{n>N}^{\min} - m_{n\leq N}^{\min}), && (3.60)
\end{aligned}$$

where we define $m^{\min}_{n\leq N} \coloneqq \min_{0\leq n\leq N} m^{\min}_n$ and $m^{\min}_{n>N} \coloneqq \min_{n>N} m^{\min}_n$. If one can show that $0 \leq m^{\min}_{n\leq N} < m^{\min}_{n>N}$, then by rearranging the last line, we obtain the desired lower bound

$$p(n \leq N) \geq \frac{m^{\min}_{n>N} - \langle M \rangle}{m^{\min}_{n>N} - m^{\min}_{n\leq N}} = 1 - \frac{\langle M \rangle - m^{\min}_{n\leq N}}{m^{\min}_{n>N} - m^{\min}_{n\leq N}} \,. \tag{3.61}$$

For this lower bound to make sense (i.e. ≤ 1) and to be useful (i.e. > 0), we need to choose a sensible N so that the average value $\langle M \rangle$ satisfies $m^{\min}_{n\leq N} \leq \langle M \rangle < m^{\min}_{n>N}$. In addition, if $m^{\min}_n$ **increases monotonically** with $n \in \mathbb{N}$ (i.e. $m^{\min}_n \leq m^{\min}_{n+k}$ for all $n, k \in \mathbb{N}$), we can rewrite Equation (3.61) as

$$p(n \leq N) \geq 1 - \frac{\langle M \rangle - m^{\min}_0}{m^{\min}_{N+1} - m^{\min}_0} \,. \tag{3.62}$$

For a concrete example of such lower bound, see Section 4.4.1 and Appendix B.

3.5 Open problems

We showed that the flag-state squashing model proposed by Zhang *et al.* [8] only applies to QKD protocols where the POVM elements are all block-diagonal with respect to two mutually orthogonal subspaces. In fact, all known squashing models so far [3, 47, 48, 43, 8] rely somehow on the block-diagonal structure of POVM in the Fock basis, which is a common feature of discrete-variable protocols that use threshold detectors for detection. However, as we go into the domain of continuous-variable (CV) protocols, the POVMs associated with homodyne and heterodyne measurements are no longer block-diagonal in the Fock basis*, so none of the previously known squashing models apply. Finding a squashing model for CV protocols still remains as an open problem. Ultimately, this leads to the question: whether a general squashing model that is applicable to all QKD protocols exists at all. An affirmative answer to the question would not only provide a powerful tool to proving security of QKD protocols, but could potentially find applications in other fields such as quantum metrology and quantum computing that involve measurements on quantum systems described by an infinite-dimensional Hilbert space.

*Note that we have not ruled out the existence of a basis, other than the Fock basis, in which the homodyne or heterodyne POVM is block-diagonal.

Chapter 4

Security Proof for the Unbalanced Phase-encoded BB84 Protocol

In this chapter, we will discuss a new security proof for the unbalanced phase-encoded BB84 protocol that uses the flag-state squashing model introduced in Section 3.4 together with the numerical proof method described in Section 2.2.5. Our main achievement is to prove significantly higher secure key rates for this protocol compared with previously published results in the low-loss regime. This chapter reuses all contents from the paper written by the author (and co-authored by Norbert Lütkenhaus) [1] including the exact wording, results and figures, but some parts in this chapter are slightly modified in order to fit the flow of this thesis. Note that extended details and discussions for this chapter that are beyond the scope of Ref. [1] have been provided in (or added to) the six appendices.

4.1 Introduction

The earliest phase-encoding quantum key distribution (QKD) scheme was proposed by Bennett [49] in 1992 as a demonstration that any two non-orthogonal states can be used for generating shared secret keys between two parties. Later, Townsend [50] and then Hughes *et al.* [51] proposed a more practical phase-encoding BB84 protocol which uses two Mach-Zehnder interferometers. In practice, the phase-modulator in each Mach-Zehnder unit will introduce photon loss, thereby causing an asymmetry between the intensities of the phase-encoded pulse and the reference pulse even if the typical observations do not directly reveal this. This asymmetric loss was addressed in Refs. [52, 4, 5] which model

the loss caused by an imperfect phase-modulator with a beam splitter (BS) of the same transmission probability.

The first attempt in giving security proofs for this protocol was made by Li *et al.* [52]. Formal security proofs were later on provided by Ferenczi *et al.* [4] and Sunohara *et al.* [5] which both used qubit-based reduction proof techniques. Despite being a deviation from the standard BB84 protocol, Ref. [5] confirms that the old security analysis for the balanced protocol still holds in the unbalanced case. This calls for a revision of the security statement made by Ref. [4], which we will discuss in detail in Section 4.6.

Both Refs. [4] and [5] use decoy states [53, 54, 55], signal tagging [40, 56], and the qubit squashing model [40, 3, 43, 44] to convert the full security analysis into an effective qubit-to-qubit security analysis problem. Due to the asymmetric intensities of the signal states, a single photon obtained from the photon number splitting (PNS) attack [57] will be in one of two non-orthogonal states, even after basis announcements. According to the Holevo-Helstrom bound [58, 59], there are no measurements that can perfectly discriminate two non-orthogonal states, so the PNS attack will not leak full information of the signal's multi-photon part to Eve. Thus, the tagging approach, which pessimistically assumes that all multi-photon signals leak their full information to an adversary, simplifies the security proof but underestimates the secure key rate of this protocol.

In this chapter, we will answer the following questions: Could we improve the key rates in Ref. [5] if we keep the multi-photon part of the signals? Could the multi-photon part of the signal contribute significantly to key rates when the total loss or the asymmetry is large?

To highlight the differences between our approach and Refs. [4, 5]'s, we apply the numerical analysis formulated in Ref. [2] (see Section 2.2.5) which involves optimisations over finite-dimensional matrices to obtain reliable lower bounds on the key rates. On the source side, we treat lower photon numbers explicitly, while turning to tagging again for higher photon numbers. On the receiver side, we know that the qubit squashing model converts the multi-click events caused by the multi-photon part of the signals into additional qubit errors [43, 4, 44]. The convenience of reaching a qubit picture may thus cost a reduction in key rate. Therefore, we use the flag-state squashing model [8] (see Section 3.4) to circumvent this problem, especially for low-loss channels. The flag-state squashing model preserves any measurement on a low photon-number subspace while tagging the arriving signals of higher photon numbers. As a result, we obtain secret key rates that can exceed the ones quoted in Refs. [4, 5].

During our investigations, we noticed a problem with the common approach which attributes all observed errors to an adversary and describes Bob's detection device by an

idealised set-up. Once the actual detectors have some dark count rate, this approach may lead in some circumstances to unphysical constraints, meaning that such an ideal device could not lead to the actual observations. For that reason, we will also introduce results for *trusted* detector noises, especially dark counts, for which this problem does not exist.

The rest of this chapter is outlined as follows. We first revisit the protocol in Section 4.2 and describe the mathematical model of the protocol in Section 4.3. We will then justify our security proof techniques and state the methods that allow us to speed up our key rate computations in Section 4.4. With the description of how we simulate experimental statistics in Section 4.5, we present our lower bounds for the secure key rates of the protocol in Section 4.6.

4.2 Protocol description

We consider a phase-encoded BB84 protocol with a Mach-Zehnder set-up. The only modification is that we take into account the typical loss in one arm of the interferometer, which results from the insertion loss of phase modulators. This asymmetric loss leads to an unbalance of the amplitudes of the two generated pulses as illustrated in Figure 4.1. We describe here the general outline of the protocol structure. Since we are dealing with the asymptotic key rate in this work, we omit any detail that would be relevant only for a finite-size analysis of the protocol.

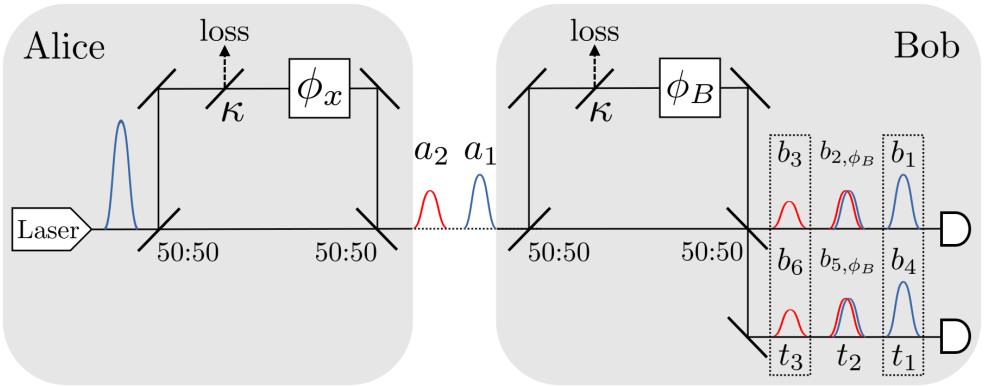


Figure 4.1: The setup for the unbalanced phase-encoded BB84 protocol. All beam splitters (BSs) are labelled by their transmissivities. The grouping of Bob's detection events are represented by the dotted boxes.

1. *State preparation*: Alice prepares a phase-randomised coherent state with mean photon number $|\alpha|^2$ where $\alpha \in \mathbb{C}$ and chooses a random phase ϕ_x from the set $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ with equal probabilities in each round. Alice also sends a small portion of decoy coherent states with different mean photon numbers $\{|\alpha_i|^2 : \forall \alpha_i \in \mathbb{C}\}_{i \in \mathbb{N}}$.

2. *Measurement*: Once Bob receives the signal state, he chooses a random phase ϕ_B from the set $\{0, \frac{\pi}{2}\}$ with equal probabilities and records all events coming from the two detectors at any of the three time slots. A click is termed "outside" if it is not in the 2nd (middle) time slot.

3. *Testing*: After repeating steps 1 & 2 for many times, Alice and Bob jointly announce a random subset of their data (including events coming from decoy states) and decide whether they should abort or proceed with the rest of the protocol.

4. *Announcement, sifting and post-selection*: For each round, Alice announces the basis to be "even" if she picks her phase from $\{0, \pi\}$ or she announces "odd" if her phase is in $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$. Bob announces "even" if he picks $\phi_B = 0$ or "odd" if $\phi_B = \frac{\pi}{2}$. In addition to basis announcements, Bob also announces "discard" for events that have only outside clicks or no click. Alice keeps the ϕ_x's only for the rounds where Bob did not announce "discard" and where her bases match with Bob's. Bob keeps a detection event if his basis matches Alice's and the event is not to be discarded.

5. *Direct reconciliation key map*: Alice maps $\phi_x^{(j)}$ in the j-th kept rounds to the j-th bit z_j of the raw key as
$$z_j = \begin{cases} 0, & \text{if } \phi_x^{(j)} = 0, \pi/2, \\ 1, & \text{if } \phi_x^{(j)} = \pi, 3\pi/2. \end{cases} \tag{4.1}$$

6. *Error correction and privacy amplification*: Alice and Bob perform standard error correction so that Bob also obtains a copy of the key map register. They then proceed with a privacy amplification protocol to obtain a shared secret key.

We point out that our method generalises to any asymmetric basis choice (i.e. probabilities of choosing "even" and "odd" bases are not equal). It was shown by Lo *et al.* [60] that the probability of choosing one basis can be set arbitrarily close to 1 without affecting the asymptotic security analysis. Note that the formalism described here would also allow one to consider the reverse reconciliation approach, where in step 5 of the protocol Bob performs a key map instead of Alice. Then, Alice and Bob would have to swap their respective roles in step 6.

4.3 Mathematical model of the protocol

4.3.1 Optical models

We start by identifying two equivalent optical models for the Mach-Zehnder component that appears in both Alice's and Bob's apparatus. The descriptions for the two models are illustrated in Figure 4.2. Instead of having the loss in one arm of the interferometer, the equivalent model places a loss element in front of the Mach-Zehnder component, which then has an asymmetric beam splitter at the entry [4].

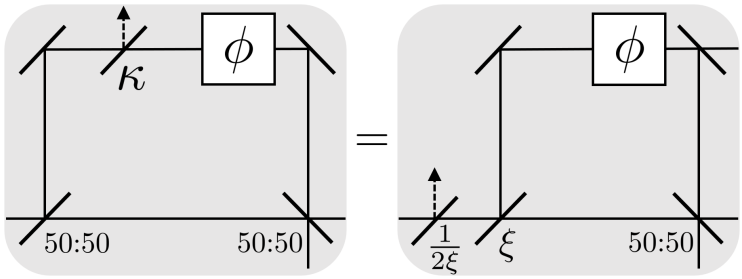


Figure 4.2: Equivalence relationship between a lossy phase modulator in the encoding device and an uneven BS with transmissivity $\frac{1}{2\xi}$ followed by another uneven BS with transmissivity ξ and a perfect phase modulator, where $\xi = \frac{1}{1+\kappa}$ [4].

This replacement picture tells us that Alice's loss can be absorbed into the rescaled amplitude of the incoming single laser pulse, whereas Bob's loss can be absorbed into the channel's action.

4.3.2 State preparation

We use the source-replacement scheme [20, 22] to represent a prepare-and-measure scheme with an entanglement-based scheme. Since Alice's signal state is mixed, we will introduce a purifying "shield" system that will be left behind in the source so that the existing source-replacement framework described in Section 2.2.1 can be applied. We will provide a detailed description of the entangled pure state prepared by Alice below.

To prepare the output signal state, Alice's laser first creates a phase-randomised coherent state

$$\sigma_{\text{in}}(2\alpha) = \int_0^{2\pi} \frac{d\theta}{2\pi} |2\alpha e^{i\theta}\rangle\langle 2\alpha e^{i\theta}| = \sum_{n=0}^{\infty} p_n(2\alpha)|n\rangle\langle n|, \tag{4.2}$$

where $p_n(\beta) = e^{-|\beta|^2}\frac{|\beta|^{2n}}{n!}$ is the Poissonian distribution in photon number n. She then sends it through her encoding device set at a phase ϕ_x which outputs a time-bin signal with two modes,

$$\sigma_x(\alpha) = \int_0^{2\pi} \frac{d\theta}{2\pi} |\psi_x^\theta(\alpha)\rangle\langle\psi_x^\theta(\alpha)|, \tag{4.3}$$

where $|\psi_x^\theta(\alpha)\rangle = |\alpha e^{i\theta}, \sqrt{\kappa}\ \alpha e^{i(\theta-\phi_x)}\rangle$.

In the following steps, we will express the state $\sigma_x(\alpha)$ in a two-mode Fock basis $\{|s_n^x(\xi)\rangle\}$ which is defined later in Equation (4.8). Let $\widetilde{a}_1^\dagger$ and $\widetilde{a}_2^\dagger$ be the creation operators of the two output time modes of the signal. We define a rescaled amplitude $\widetilde{\alpha} \coloneqq \alpha\sqrt{1+\kappa} = \alpha/\sqrt{\xi}$ with the definition $\xi \coloneqq \frac{1}{1+\kappa}$ and a new mode creation operator

$$\widetilde{a}_{\theta,x}^\dagger \coloneqq \frac{1}{\widetilde{\alpha}}(\alpha e^{i\theta}\ \widetilde{a}_1^\dagger + \sqrt{\kappa}\ \alpha e^{i(\theta-\phi_x)}\ \widetilde{a}_2^\dagger) \tag{4.4}$$

$$= \frac{e^{i\theta}}{\sqrt{1+\kappa}}(\widetilde{a}_1^\dagger + \sqrt{\kappa}\ \alpha e^{-i\phi_x}\ \widetilde{a}_2^\dagger) \tag{4.5}$$

$$= e^{i\theta}(\sqrt{\xi}\ \widetilde{a}_1^\dagger + \sqrt{1-\xi}\ e^{-i\phi_x}\ \widetilde{a}_2^\dagger). \tag{4.6}$$

We define a set of two-mode Fock states for $n \in \mathbb{N}$ as

$$|s_n^x(\xi)\rangle = \frac{1}{\sqrt{n!}}(\widetilde{a}_{\theta=0,x}^\dagger)^n|0\rangle \tag{4.7}$$

$$= \sum_{k=0}^{n} \sqrt{\binom{n}{k}} \xi^{\frac{n-k}{2}}(1-\xi)^{\frac{k}{2}} e^{-ik\phi_x}|n-k,k\rangle, \tag{4.8}$$

The state $|\psi_x^\theta(\alpha)\rangle$ can be rewritten in the new basis as

$$\begin{aligned} |\psi_x^\theta(\alpha)\rangle &= e^{-\frac{|\widetilde{\alpha}|^2}{2}} \sum_{n=0}^{\infty} \frac{\widetilde{\alpha}^{\,n}}{n!}(\widetilde{a}_{\theta,x}^\dagger)^n|0\rangle \\ &= e^{-\frac{|\widetilde{\alpha}|^2}{2}} \sum_{n=0}^{\infty} \frac{(\widetilde{\alpha}e^{i\theta})^n}{\sqrt{n!}}|s_n^x(\xi)\rangle \end{aligned} \tag{4.9}$$

which is a coherent state with amplitude $\widetilde{\alpha}$. The phase-randomised signal state is therefore a Poissonian mixture of the new Fock states as in

$$\sigma_x(\alpha) = \sum_{n=0}^{\infty} p_n(\widetilde{\alpha})|s_n^x(\xi)\rangle\langle s_n^x(\xi)|. \tag{4.10}$$

Since the signal state $\sigma_x(\alpha)$ is mixed, Alice can purify the state by introducing an ancillary system A_S such that the following is a pure state

$$|\sigma_x(\alpha)\rangle_{A_S A'} = \sum_{n=0}^{\infty} \sqrt{p_n(\widetilde{\alpha})}\, |n\rangle_{A_S} \otimes |s_n^x(\xi)\rangle_{A'} \quad , \tag{4.11}$$

where the register A' is the signal system. Note that the probability $p_n(\widetilde{\alpha})$ is independent of Alice's choice x.

We can summarise the source description as Alice preparing an entangled pure state

$$|\Psi\rangle_{A A_S A'} = \sum_x \sqrt{p_x}\, |x\rangle_A \otimes |\sigma_x(\alpha)\rangle_{A_S A'} \quad , \tag{4.12}$$

where $\{|x\rangle_A\}_{x=0,\ldots,3}$ is an orthonormal basis of Alice's register A for x corresponding to the phase $\phi_x = \frac{\pi}{2}x$ and $p_x = \frac{1}{4}$ for all $x \in \{0,1,2,3\}$. Note that registers A and A_S are private to Alice, and Eve only has access to the signal system A'. We call the purifying system A_S a "shield" system for it to be inaccessible to Eve (i.e. Eve only gets the mixed state $\sigma_x(\alpha)$ but not the pure state $|\sigma_x(\alpha)\rangle_{A_S A'}$).

4.3.3 Trusted and (semi-)untrusted components

Before we describe the mathematical model for the measurements in this protocol, we should first address the potential security loopholes in the protocol implementation by discussing the assumptions for trusted and (semi-)untrusted components. In an actual QKD experiment, there could be flaws or imperfections in implementing the protocol, particularly, in Alice's and Bob's devices for signal preparation and measurement. The adversary Eve could make use of these flaws unknown to Alice and Bob to compromise the security of a QKD implementation, even if the QKD protocol itself has been proven to be secure theoretically. These are called side-channel attacks and have been demonstrated experimentally, for example, by Qi *et al.* [61] and Fung *et al.* [62]. One way of addressing side-channel attacks that utilise vulnerabilities in Alice's and Bob's devices is to use a *device-independent* (DI) protocol [63] by treating Alice's and Bob's devices as spatially isolated black boxes, thereby not requiring them to be trusted. However, we know that the devices used in an experiment are more than black boxes, so the DI assumption is the most pessimistic scenario for any QKD protocol.

In a more optimistic view, since QKD experiments nowadays will impose countermeasures for known side-channel attacks, experimental components and devices can be trusted

to a certain degree if they are properly calibrated. A careful but not overly conservative assumption would be that some components in a QKD experiment are more trustworthy than others. One may assume these components to be trusted (i.e. not in Eve's control) so that any known defects such as loss and noise of these devices are assumed to originate from the devices but not from Eve. Here, we consider only Bob's measurement device to be defective, which can be mathematically modelled in the way described in Section 4.3.4 with the known defects taken into account. On the other hand, for the components that cannot be fully trusted, we cannot eliminate the possibility that Eve has some control over the defects (e.g. Eve blinds Bob's detectors), but at the same time, we do not want to assume these components to be *fully untrusted*. To find a middle ground between trusted and fully untrusted, we can impose the *semi-untrusted* assumption where we assume the physical modelling for the defects is accurate, but the parameters for the model are unknown to us. For example, the detection inefficiency of a detector can be modelled by a beam splitter with the transmissivity set to its detection efficiency followed by a perfectly efficient detector, but the actual detection inefficiency is unknown. We then assume the result of the defects to come from the quantum channel controlled by Eve while assuming Bob's device is free of these defects. We illustrate the assumption for semi-untrusted defects in Figure 4.3. In this sense, the defects due to the imperfect components are outsourced to Eve who,

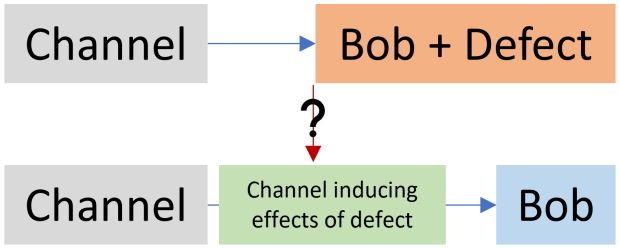


Figure 4.3: Illustration of the replacement model for outsourcing a semi-untrusted defect in Bob's measurement device to the channel. The upper picture shows the original situation where Bob's measurement device suffers from a defect. Assume that we know how to model the defect or its effect on the measurement statistics but not the model parameters. As shown in the lower picture, the semi-untrusted assumption hypothesise the existence of an additional quantum channel that can reproduce the same effect of the defect as in the upper picture while assuming Bob's device to not have such defect. Note that no proofs have confirmed the existence of such channel for all kinds of defects except for detection inefficiency when there is no efficiency mismatch.

intuitively, would gain more eavesdropping power under such an assumption. Therefore, treating some components to be semi-untrusted is supposed to be more conservative than

seeing them as trusted. Since our treatment for semi-untrusted components has not been formally proven to be able to address side-channel attacks completely, one can view our method more of a toy model or a working assumption than a solution to the problem.

In fact, the semi-untrusted assumption has been a common practice to treat detection inefficiency and noise as defects potentially caused or influenced by Eve. We remark that the replacement picture shown in Figure 4.3 applies to semi-untrusted detection inefficiency when there is no efficiency mismatch, but not to mismatched detection inefficiencies and dark counts simply because no channel has been found to reproduce their exact effects if Bob were to measure with lossless or dark-count-free detectors. Nonetheless, we keep the analysis for semi-untrusted dark counts in this work just to flag the consequence of this commonly practised assumption. This issue will be elaborated more in Section 4.5. To simplify our language, we will refer to any semi-untrusted defects simply as "untrusted" since fully untrusted defects are not considered in this work.

4.3.4 Measurements

In the prepare-and-measure scheme, the action of Alice randomly choosing the phase ϕ_x in the signal state is equivalent to a measurement on $|\Psi\rangle_{AA_SA'}$ with POVM $\{|x\rangle\langle x|_A\}_{x=0,\ldots,3}$. Alice's measurement can be performed before or after Bob performs his measurement.

We start out by describing the POVM of Bob's measurement assuming ideal devices, especially without dark counts of the detectors. We will later on derive the POVM of devices with specified dark counts. To characterise all of Bob's possible measurement outcomes, we construct his POVM using the creation and annihilation operators for six optical modes arriving at 3 different time slots and at 2 detectors. Ignoring global phases, the six annihilation operators of a fixed phase ϕ_B, which correspond to the six "click" locations depicted in Figure 4.1, are

$$b_1 = b_4 \to \sqrt{\frac{\xi}{2}}\, a_1 \,, \tag{4.13}$$

$$b_3 = b_6 \to \sqrt{\frac{1-\xi}{2}}\, a_2 \,, \tag{4.14}$$

$$b_{2,\phi_B} \to \sqrt{\frac{1-\xi}{2}}\, a_1 - e^{i\phi_B}\sqrt{\frac{\xi}{2}}\, a_2 \,, \tag{4.15}$$

$$b_{5,\phi_B} \to \sqrt{\frac{1-\xi}{2}}\, a_1 + e^{i\phi_B}\sqrt{\frac{\xi}{2}}\, a_2 \,, \tag{4.16}$$

where a_1 and a_2 are annihilation operators of the two incoming time modes of the signal.

Since $b_1 = b_4$ and $b_3 = b_6$, the POVM elements corresponding to click events at 1 and 4 (3 and 6) are the same. Hence, each pair can be combined into a single time-mode annihilation operator. The corresponding operators for the two pairs are

$$b_{t_1} \to \sqrt{\xi}\, a_1 \ , \quad b_{t_3} \to \sqrt{1-\xi}\, a_2 \tag{4.17}$$

where t_1 and t_3 denote the 1st and the 3rd time slots in Fig 4.1. This is equivalent to coarse-graining the outside-only click POVM elements and outcome probabilities but without losing information about the relative phase, $\phi_x - \phi_B$. This reduces the redundancy in constraints for the optimisation which will be described in Section 4.4.3.

As Bob's measurement outcomes consist of all combinations of click events at different time slots, detectors, and basis choices, his POVM elements are obtained by summing weighted projectors of all possible states that could lead to a particular click pattern. Based on the fact that Bob uses threshold detectors for detection, all POVM elements are block-diagonal in total photon number basis [3, 43].

These allow the construction of Bob's POVM elements in terms of the modes impinging on the detectors by first restricting to the n-total photon subspace of Bob's entire system, and defining the following operators corresponding to different click events:

- no-click: (for $n = 0$)
$$F_0^{\phi_B} = p(\phi_B)|0\rangle\langle 0|, \tag{4.18}$$
- single-click: (for $n \geq 1$)
$$F_{i_1}^{n,\phi_B} = p(\phi_B)\frac{1}{n!}(b_{i_1}^\dagger)^n|0\rangle\langle 0|b_{i_1}^n \ , \tag{4.19}$$
- double-click: (for $n \geq 2$)
$$F_{i_1,i_2}^{n,\phi_B} = p(\phi_B)\sum_{k=1}^{n-1}\frac{(b_{i_1}^\dagger)^{n-k}(b_{i_2}^\dagger)^k|0\rangle\langle 0|b_{i_1}^{n-k}\, b_{i_2}^k}{(n-k)!\, k!} \ , \tag{4.20}$$
- triple-click: (for $n \geq 3$)
$$F_{i_1,i_2,i_3}^{n,\phi_B} = p(\phi_B)\sum_{k=1}^{n-2}\sum_{j=1}^{n-k-1}|\beta_3(n,j,k)\rangle\langle\beta_3(n,j,k)| \tag{4.21}$$
with $|\beta_3(n,j,k)\rangle = \frac{(b_{i_1}^\dagger)^{n-k-j}(b_{i_2}^\dagger)^k(b_{i_3}^\dagger)^j|0\rangle}{\sqrt{(n-k-j)!\, k!\, j!}}$,

- all-click: (for $n \geq 4$)

$$F_{\text{ac}}^{n,\phi_B} = p(\phi_B) \sum_{k=1}^{n-3} \sum_{j=1}^{n-k-2} \sum_{l=1}^{n-k-j-1} |\beta_4(n,j,k,l)\rangle\langle\beta_4(n,j,k,l)| \tag{4.22}$$

$$\text{with } |\beta_4(n,j,k,l)\rangle = \frac{(b_{i_1}^\dagger)^{n-k-j-l}(b_{i_2}^\dagger)^k(b_{i_3}^\dagger)^j(b_{i_4}^\dagger)^l|0\rangle}{\sqrt{(n-k-j-l)!\; k!\; j!\; l!}} \;,$$

where $p(\phi_B)$ is the probability of choosing the phase ϕ_B and $b_{i_\mu}^\dagger \in \{b_{t_1}^\dagger, b_{2,\phi_B}^\dagger, b_{5,\phi_B}^\dagger, b_{t_3}^\dagger\}$ are the mode creation operators for a fixed phase ϕ_B, with $b_{i_\mu}^\dagger \neq b_{i_\nu}^\dagger$ for all $\mu \neq \nu$ and $\mu, \nu \in \{1,2,3,4\}$. We can express Bob's POVM elements in terms of the incoming modes, a_1 and a_2, by substituting the final modes with Equations (4.15) – (4.17).

To obtain Bob's POVM elements for the full Hilbert space, one simply sums over all contributions from all photon number subspaces to get

$$F_k = \sum_{n=0}^{\infty} F_k^n \;, \tag{4.23}$$

where k labels the 16 possible click patterns (Bob's measurement outcomes) in each of the two measurement bases. For n to be less than the minimum photon number to trigger the click event k, F_k^n is a zero operator. If k is the no-click event, F_k^n is a zero operator for all $n \geq 1$.

To reduce the number of linearly dependent POVM elements for better numerical performance in calculating key rates*, we combine the pairs of ϕ_B-independent POVM elements of the two measurement bases into one by summing the two elements together. This reduces the cardinality of Bob's POVM from 32 to 28 since the following four click patterns: no-click, t_1-only, t_3-only, and t_1&t_3 are basis-independent.

In a trusted dark-count scenario where dark counts are not controlled by Eve, we incorporate the effect of dark counts into Bob's POVM by applying a classical post-processing map, $\mathcal{P}$, on Bob's POVM elements $\{F_k\}$. The output of the map is a new POVM $\{P_k\}$ with each element corresponding to a linear combination of the original POVM such that

*As we will point out in Section 4.4.1, the number of POVM elements is related to the dimension of the flag-state subspace. If the two POVM elements are linearly dependent, they are essentially the same constraint for the convex optimisation problem in (4.37) up to a scaling factor. Therefore, omitting either of the two elements will not affect the optimisation result, but the flag-state subspace dimension will reduce by one. As for all numerical optimisations, the smaller the dimension of the problem, the shorter the runtime.

$P_k = \sum_i \mathcal{P}_{k,i}\ F_i$ where $\mathcal{P}_{k,i}$ are the matrix elements of the linear map $\mathcal{P}$. We illustrate the action of the map $\mathcal{P}$ with the new POVM elements listed in Appendix A. Since the map $\mathcal{P}$ acts the same on all photon-number subspaces, it also holds that

$$P_k^n = \sum_i \mathcal{P}_{k,i}\ F_i^n\ . \tag{4.24}$$

The map $\mathcal{P}$ models the effect of dark counts as a classical noise in the sense that for each detector and at each detection time window, a no-click event flips to a click event with probability, p_d. We can recover Bob's dark-count-free POVM $\{F_k\}$ by setting the dark-count probability $p_d = 0$ in the case with untrusted dark counts.

Overall, we obtain the joint POVM of Alice's and Bob's measurements $\{|x\rangle\langle x|_A \otimes P_k\}$ where $x \in \{0, ..., 3\}$ and $k \in \{1, ..., 28\}$ since Bob has 28 coarse-grained outcomes in total if no-click is included.

4.4 Security proof techniques

4.4.1 Flag-state squashing model

In order to numerically compute the secure key rate, we need to reduce the dimension of Bob's state from infinite to finite so that numerical optimisation solvers can be used. Since Bob uses threshold detectors, his POVM elements are block-diagonal, so the qubit squashing model [3, 43, 4, 44] can be applied. However, by reassigning the multi-click events to single-click events randomly, the squashing model introduces additional qubit errors to the original data. Instead, the flag-state squashing model [8] is used here to circumvent this problem.

We set a finite photon-number cutoff N_B and define the $(n \leq N_B)$- and $(n > N_B)$-photon subspaces[†] to be two Hilbert spaces containing Fock states of at most N_B and at least $N_B + 1$ photons respectively. The flag-state squashing map Λ first projects Bob's state ρ onto the two subspaces. It then applies an identity map to the projected state $\rho_{n\leq N_B}$ and measures the projected state $\rho_{n>N_B}$ with the POVM $\{P_k\}$ to give the squashed state

$$\Lambda(\rho) = \begin{pmatrix} \rho_{n\leq N_B} & 0 \\ 0 & \sum_k \mathrm{Tr}(P_k\ \rho_{n>N_B})|k\rangle\langle k| \end{pmatrix}. \tag{4.25}$$

[†]We identify $(n \leq N_B)$- and $(n > N_B)$-photon subspaces as the P- and $P^\perp$-subspaces mentioned in Section 3.4 respectively.

Bob's corresponding flag-state squashed POVM elements are

$$\widetilde{P}_k = \left(\sum_{n=0}^{N_B} P_k^n \right) \oplus |k\rangle\langle k|, \tag{4.26}$$

where N_B is a finite-number photon cutoff and k labels Bob's detection events. The joint POVM of Alice's and Bob's measurements in the flag-state squashing model is $\{|x\rangle\langle x|_A \otimes \widetilde{P}_k\}$ where $x \in \{0, ..., 3\}$ and $k \in \{1, ..., 28\}$.

Since the measurement channel acting on the $(n > N_B)$-photon subspace is entanglement breaking [16], one needs to lower bound $\mathrm{Tr}(\Pi_{n \leq N_B}\, \rho)$ with Bob's measurement statistics to ensure that some entanglement between Alice and Bob is preserved in order for them to establish a secret key [22]. For trusted dark counts, we show in Appendix B that the lower bound for the weight of the $(n \leq N_B)$-photon signal subspace conditioned on Alice choosing signal x is given by

$$p(n \leq N_B|x) \geq 1 - \frac{p(\mathrm{cc}|x) - p(\mathrm{cc}|0)}{p_{\min}(\mathrm{cc}|N_B + 1) - p(\mathrm{cc}|0)}\,, \tag{4.27}$$

$$p(\mathrm{cc}|0) = 1 - (1 - p_d)^2[1 + p_d(1 - p_d)^2(2 - p_d)], \tag{4.28}$$

$$p_{\min}(\mathrm{cc}|n) = 1 - (1 - p_d)^2\xi^n - (1 - p_d)^4(1 - \xi)^n, \tag{4.29}$$

where the conditional cross-click probability, $p(\mathrm{cc}|x)$, is the sum of the observed probabilities of all events excluding no-click events, events with clicks only in time slot t_2 (inside-only), and events with clicks only in time slots t_1, t_3 (outside-only) given that Alice picks signal x. We also show in Appendix B that the bound in (4.27) is always tighter than the dark-count-free bound ($p_d = 0$) derived by Narashimhachar [44], so we could also obtain a lower bound of the secure key rate using that dark-count-free bound. For untrusted dark counts, one simply has to use that bound.

4.4.2 Decoy state & decomposition of key rate formula

In this work, we prove the security of the protocol against any collective attack. Since the signal states and measurements are permutation invariant between different rounds, the quantum de Finetti theorem [27] (see Section 2.2.4) or the postselection technique [30] can be applied to uplift our security statement to the security against coherent attacks, which will both lead to the same asymptotic key rate. From that we obtain a composable ε-security proof [19] of the protocol under Eve's general attacks with the same asymptotic key rate as under the collective attack.

Recall the asymptotic key rate formula (2.44) for collective attack

$$R_\infty = \min_{\rho_{AA_SB}\in\mathbf{S}} D(\mathcal{G}(\rho_{AA_SB})||\mathcal{Z}(\mathcal{G}(\rho_{AA_SB}))) - p_{\text{pass}}\,\delta_{\text{EC}}\,.$$

For this specific protocol, the explicit forms of the quantities p_{pass} and $H(Z|\overline{B})$ are shown in Appendix C, and the $\mathcal{G}$ map that was introduced in Section 2.2.5 takes the form [2, 35]

$$\mathcal{G}(\rho) = \sum_i K_i\,\rho\,K_i^\dagger \tag{4.30}$$

with the Kraus operators of this protocol defined as

$$K_0 = (|0\rangle_Z \otimes |0\rangle\langle 0|_A + |1\rangle_Z \otimes |2\rangle\langle 2|_A) \otimes \mathcal{F}_0^B \otimes |0\rangle_{\widetilde{B}}\ , \tag{4.31}$$

$$K_1 = (|0\rangle_Z \otimes |1\rangle\langle 1|_A + |1\rangle_Z \otimes |3\rangle\langle 3|_A) \otimes \mathcal{F}_1^B \otimes |1\rangle_{\widetilde{B}}\ , \tag{4.32}$$

where $\{|0\rangle_{\widetilde{B}}, |1\rangle_{\widetilde{B}}\}$ is Bob's basis announcement bit, $\mathcal{F}_j^B = \sqrt{\sum_{b\in\mathbf{K}} F_{b,\phi_B=\frac{\pi}{2}j}}$ and $\mathbf{K}$ denotes Bob's post-selected outcomes. Also, recall that the $\mathcal{Z}$ map introduced in Section 2.2.5 is given by

$$\mathcal{Z}(\sigma_{ZC}) = \sum_{j=0}^{1}(|j\rangle\langle j|_Z \otimes \mathbb{1}_C)\,\sigma_{ZC}\,(|j\rangle\langle j|_Z \otimes \mathbb{1}_C) \tag{4.33}$$

with register C encapsulates all registers except Z.

Since Alice is sending a Poissonian mixture of Fock states, Eve can, in principle, perform a QND measurement on Alice's signal to learn its photon number without disturbing the signal itself. We show in Appendix D that as a direct consequence of this the state ρ_{AA_SB} is block-diagonal in Alice's output photon number $\widetilde{n}$. Therefore, without loss of generality, we can restrict the minimisation in Equation (2.44) to be taken over a smaller set $\mathbf{S}' = \{\rho_{AA_SB} \in \mathbf{S} : \rho_{AA_SB} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\,|\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \rho_{AB}^{\widetilde{n}}\}$ where $\{\rho_{AB}^{\widetilde{n}}\}$ are the normalised states conditioned on Alice sending out $\widetilde{n}$ photons. This allows one to split the PA term into a probabilistic combination of PA terms associated with different $\widetilde{n}$ as in

$$R_\infty = \min_{\rho_{AA_SB}\in\mathbf{S}'} \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\,D(\mathcal{G}(\rho_{AB}^{\widetilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\widetilde{n}}))) - p_{\text{pass}}\,\delta_{\text{EC}}\,. \tag{4.34}$$

See Appendix D for the proof of the decomposition.

For our analysis, we assume a decoy-state scenario [53, 54, 55], which means that in addition to the usual signal states, Alice prepares also decoy states that are represented

by dephased laser pulses with different intensity levels $|\alpha_i|^2$. More precisely, we assume for simplicity the infinite-decoy scenario, where a countably infinite number of decoy intensities are used so that a decoy data analysis can reveal to Alice and Bob the conditional probabilities of any observable, where the condition is with respect to Alice's output photon number $\widetilde{n}$.

These conditional probabilities constrain the feasible set of normalised states $\mathbf{S}_{\widetilde{n}}$ for each of Alice's output photon number $\widetilde{n}$ independently, which further restricts the minimisation in Equation (4.34) to be taken over a smaller set $\mathbf{S}'' = \{\rho_{AA_SB} \in \mathbf{S} : \rho_{AA_SB} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}} \, |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \rho_{AB}^{\widetilde{n}}, \, \rho_{AB}^{\widetilde{n}} \in \mathbf{S}_{\widetilde{n}} \; \forall \; \widetilde{n} \in \mathbb{N}\} \subset \mathbf{S}'$. Given that the probability distribution $\{p_{\widetilde{n}}\}_{\widetilde{n}\in\mathbb{N}}$ is fixed by the intensity of the signal, the minimisation over $\mathbf{S}''$ can be pulled into the summation and split into minimisations over individual $\mathbf{S}_{\widetilde{n}}$, resulting in the following key rate formula

$$R_{\infty} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}} \min_{\rho_{AB}^{\widetilde{n}} \in \mathbf{S}_{\widetilde{n}}} D(\mathcal{G}(\rho_{AB}^{\widetilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\widetilde{n}}))) - p_{\text{pass}} \, \delta_{\text{EC}} \, . \tag{4.35}$$

We remark that the inclusion of a finite number of decoy states would be a natural extension of this work, in which case the description of each set $\mathbf{S}_{\widetilde{n}}$ would depend on other sets $\{\mathbf{S}_{n'} : n' \neq \widetilde{n}\}$. Hence, a more careful treatment of the PA term would be needed.

The major benefit of breaking down the PA term into individual minimisations is to avoid the need of keeping the infinite-dimensional shield system A_S in the argument of the optimisation as seen in Equation (2.44). Instead of optimising over the set of infinite-dimensional states, we convert our problem into an infinite number of optimisations with finite-dimensional arguments.

Notice that when Alice sends out vacuum (0 photons), Eve learns nothing about Alice's choice x, so each key bit $z \in \{0, 1\}$ is equally likely to Eve, which implies that $H(Z|E) = H(Z) = 1$. Therefore, the first term in the summation in Equation (4.35) is equal to $p_{\text{pass}}^{\widetilde{n}=0}$ which is the contribution from Alice sending out vacuum to the probability of passing sifting and post-selection.

By Klein's inequality (Theorem 2.1.7), we have that $D(\mathcal{G}(\rho_{AB}^{\widetilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\widetilde{n}}))) \geq 0$ for all $\widetilde{n} \in \mathbb{N}$. Thus, omitting any terms in the summation will only reduce the total value on the right-hand side of Equation (4.35). In fact, omitting an $\widetilde{n}$-photon term is the same as treating all $\widetilde{n}$-photon output signals as being tagged for which the encoded state is fully known to Eve. Since we can only optimise a finite number of terms in the infinite sum, we can truncate the infinite sum at $\widetilde{n} = N_A$ where N_A is a positive finite integer to obtain a lower bound for the key rate. The choice of $N_A = 1$ corresponds to the tagging as used in

Refs. [4, 5]. We then have the key rate expression as

$$R_\infty \geq p_{\text{pass}}^{\widetilde{n}=0} + \sum_{\widetilde{n}=1}^{N_A} p_{\widetilde{n}} \min_{\rho_{AB}^{\widetilde{n}} \in \mathbf{S}_{\widetilde{n}}} D(\mathcal{G}(\rho_{AB}^{\widetilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\widetilde{n}}))) - p_{\text{pass}}\, \delta_{\text{EC}} \,. \tag{4.36}$$

This allows us to reduce the number of finite-dimensional optimisations from infinity to a finite number that corresponds to the limited computational resources available to us.

4.4.3 The optimisation problem

The convex optimisation problem corresponding to each PA term in Equation (4.36) can be formulated as

$$\begin{aligned}
&\text{minimise } D(\mathcal{G}(\rho_{AB}^{\widetilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\widetilde{n}}))) \\
&\text{subject to} \\
&\quad \text{Tr}[(|x\rangle\langle x|_A \otimes \widetilde{P}_k)\ \rho_{AB}^{\widetilde{n}}] = p(x,k|\widetilde{n}), \\
&\quad \text{Tr}[(|x\rangle\langle x|_A \otimes \Pi_{n\leq N_B})\ \rho_{AB}^{\widetilde{n}}] \geq p(x)\ p_{n\leq N_B|x}^{\min}\ , \\
&\quad \text{Tr}_B(\rho_{AB}^{\widetilde{n}}) = \frac{1}{p_{\widetilde{n}}} \text{Tr}_{A_S A'}[(|\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \mathbb{1}_{A'})\ |\Psi\rangle\langle\Psi|_{AA_SA'}], \\
&\quad \text{Tr}(\rho_{AB}^{\widetilde{n}}) = 1, \\
&\quad \rho_{AB}^{\widetilde{n}} \geq 0.
\end{aligned} \tag{4.37}$$

The first line in the constraints demands the shared state $\rho_{AB}^{\widetilde{n}}$ conditioned on Alice sending out $\widetilde{n}$ photons to satisfy Alice's and Bob's joint measurement outcome probabilities conditioned on $\widetilde{n}$, which are obtained from the infinite-decoy analysis. The second line lower bounds the weight of $\rho_{AB}^{\widetilde{n}}$ in the $(n \leq N_B)$-photon subspace by Equation (4.27). The third line demands that Alice's reduced density matrix is unchanged. The last two lines ensure that $\rho_{AB}^{\widetilde{n}}$ is a valid, normalised density matrix.

4.4.4 Implementation of numerical security analysis

Following the procedure in Ref. [2] (also see Section 2.2.5), the suboptimal solutions to the convex optimisation problem (4.37) for $1 \leq \widetilde{n} \leq N_A$ are obtained numerically using the MATLAB optimisation package CVX and the Frank-Wolfe algorithm [37]. These suboptimal solutions infer the upper bound for the individual privacy amplification terms

in Equation (4.36). A linearisation of each of the optimisation problems at its suboptimal solution results in a primal SDP problem of the form (2.54) which can be further converted into a dual SDP problem as in (2.56). Using the CVX numerical solver again, the dual suboptimal solutions for $1 \leq \widetilde{n} \leq N_A$ provide a reliable lower bound on the whole privacy amplification term.

Solving the convex optimisation problem is computationally demanding in terms of time and memory even if the flag-state squashing model is applied to reduce the dimension of the matrix variables $\rho_{AB}^{\widetilde{n}}$. One can further utilise the structure of the flag-state squashed state as described in Equation (4.25) to reduce the number of complex variables in the allowed matrices $\rho_{AB}^{\widetilde{n}}$. Bob's flag-state squashed POVM elements also enable us to split multiplications between constraint matrices and the state variable $\rho_{AB}^{\widetilde{n}}$. In addition, the objective function in (4.37) can be evaluated much faster if the computation is restricted only to the non-zero subspaces in the images of the maps $\mathcal{G}$ and $\mathcal{Z}$. With these three techniques, we managed to reduce the computation time of the convex optimisation by a significant amount. See Appendix E for the technical details.

We utilise the fact that the optimisation problem specified in (4.37) is independent of the mean photon number $|\alpha|^2$ of Alice's phase-randomised coherent state because the minimisations in Equation (4.35) are over each set $\mathbf{S}_{\widetilde{n}}$ separately. In other words, the choice of $|\alpha|^2$ only affects the photon number distribution $\{p_{\widetilde{n}}\}$ and the error-correction term δ_{EC} in the key rate formula (4.36). Therefore, we can maximise the key rate lower bound over the signal intensity $|\alpha|^2$ efficiently once we have the dual suboptimal solutions since the error-correction term can be directly calculated from the observables of the corresponding simulation.

4.5 Simulation of experiments

In the absence of experimental data, we have to perform a simulation of an experiment to obtain realistic probability distributions which replace the experimental data as input of our security analysis. To address imperfections in an experimental implementation of the protocol, we consider both trusted and untrusted defects in our simulations as discussed in Section 4.3.3. Note that the details of the simulation model are independent of the actual security proof.

4.5.1 Channel simulations & detection efficiency

We simulate the quantum channel between Alice and Bob with a loss-only channel which is essentially an uneven beam splitter. We also assume that both detectors of Bob have equal detection efficiency η_{det}, where each detector can be modelled as a beam splitter with a transmission rate η_{det} followed by an ideal detector. In this simple model, a single parameter η which we call the total transmissivity describes the combined loss caused by the following three effects: the inefficiency in the process of coupling the signal light to the optical fibre, the absorption and scattering processes of light in transmission through the fibre, and the detection efficiency of Bob's threshold detectors. The simulated outcome probabilities for Bob's measurement (with no dark counts) are derived in Appendix F.

We also investigate the case where we assume the detection efficiency η_{det} to be outside of Eve's control, as a trusted, characterised loss element of the receiver. In that case, we keep the beam splitter with transmissivity η_{det} in Bob's apparatus, which in turn modifies the POVM elements described in Section 4.3.4. Bob's POVM with known detection efficiency can be obtained with a similar approach used in Ref. [8]. Note that the statistics shown in Appendix F are unchanged under this trusted loss assumption.

4.5.2 Dark counts

To simulate our statistics when dark counts are present, we generate the outcome probabilities with Bob's classically post-processed POVM described in Section 4.3.4 and Appendix A, which is associated with a dark-count probability, p_d, for each detector and at each detection time window. These statistics are equivalent to the dark-count-free statistics derived in Appendix F after being classically post-processed in the same way as the POVM elements in Appendix A.

If dark counts are assumed to be trusted in the sense that they are not in Eve's control, we use the classically post-processed flag-state POVM $\{\widetilde{P}_k\}$ as the constraint matrices in the optimisation problem (4.37) to calculate the privacy amplification term. This approach guarantees the optimisation problem to be feasible since measurement probabilities correspond directly to a quantum state in the simulation.

However, if we consider untrusted dark counts, that is, if we pessimistically attribute the effect of dark count noise to Eve, the flag-state POVM of dark-count-free detectors is used as the optimisation constraint matrices instead. Note that unlike the existence of a physical model for pulling out the equal detection efficiency into the channel, this approach is not covered by any physical equivalence model that allows one to outsource the dark

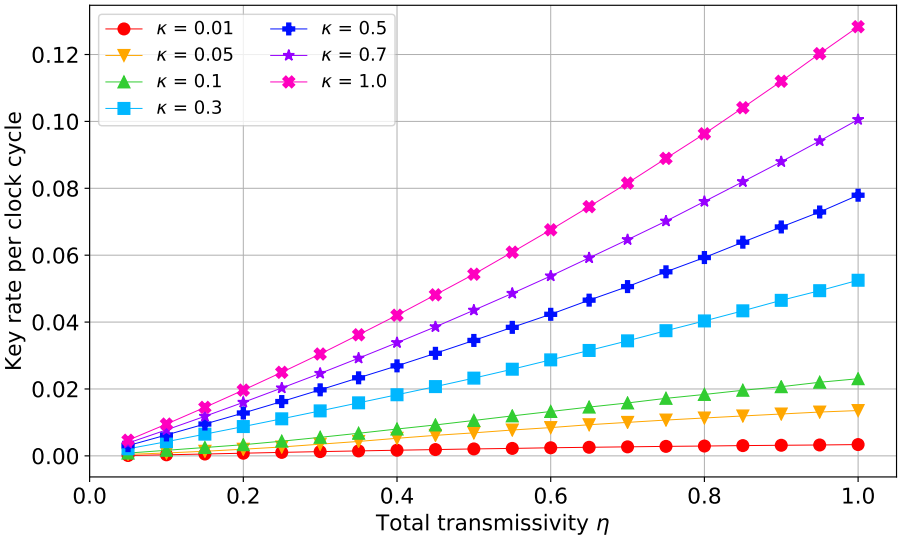
counts to Eve. Therefore, it is possible that no quantum states could have led to the classically post-processed statistics if the measurement is assumed to be dark-count-free. In that case, the optimisation problem becomes infeasible due to unphysical constraints. This is what we encounter in some parameter regime of our calculation, as we will point out in the next section.

4.6 Key rates

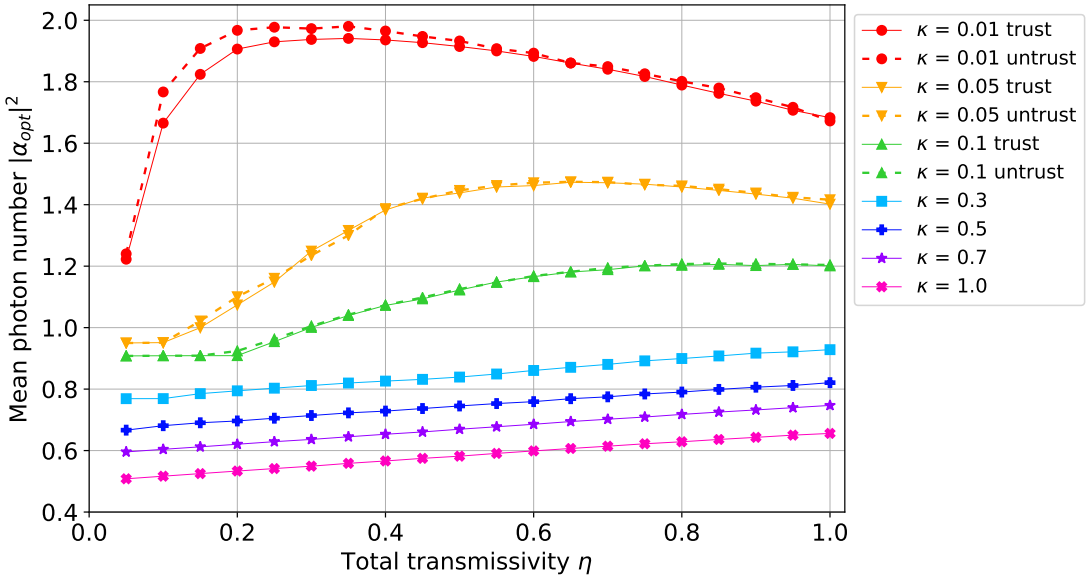
Before diving into our main results, we start by stating the parameters used throughout this section. We set Bob's flag-state photon number cutoff to be $N_B = 4$ so that the PA term can be computed within a reasonable amount of time. The maximum number of terms kept in the PA summation in Equation (4.36) is set to be $N_A = 3$ since we observe that the key rate in the low-loss regime does not improve even if we keep more than 3 terms. Furthermore, we set the dark count probability to be $p_d = 8.5 \times 10^{-7}$ and the error-correction efficiency to be $f_{\mathrm{EC}} = 1.22$ as quoted by Gobby *et al.* [64].

In Figure 4.4(a), we present lower bounds for the secure key rates per clock cycle corresponding to different values of the phase-modulator transmissivity κ and the total transmissivity η in the two scenarios with trusted and untrusted dark counts. The total transmissivity η captures both the transmission efficiency of the loss-only channel and the detection efficiency of Bob's detectors. We obtain these bounds by maximising the lower bounds for key rates over the mean photon number $|\alpha|^2$ as specified in Section 4.4.4. The optimal $|\alpha|^2$ for each point in Figure 4.4(a) are shown in Figure 4.4(b).

Let us expand on the infeasibility issue with untrusted dark counts mentioned in Section 4.5.2. In the high-loss regime where the total transmissivity $\eta \leq 0.2$, the optimisation problem for some parameters becomes infeasible meaning that no physical states can satisfy the constraints that are imposed by observed statistics. This is a somehow surprising observation since many previous security analyses (e.g. [4, 5, 40, 65]) assume dark counts to be untrusted but did not encounter any issue with infeasible constraints. Most of these analyses use coarse-grained statistics (e.g. bit/phase error rate) to bound Eve's knowledge. However, the use of refined statistics in our optimisation constraints poses more stringent conditions on the feasible set which makes it less robust against infeasibility issues. Therefore, at least when infeasibility is detected, we cannot outsource the dark counts simulated by a classical noise model entirely to Eve as previous literature did. In the case of having infeasible data, we allow the numerical solver to relax the satisfiability of constraints in the sense that we are enlarging the search set to the degree where it is feasible. Due to large constraint violations and a minimisation over an enlarged search set, we expect the key



(a)



(b)

Figure 4.4: (a) Our optimal lower bounds and (b) the corresponding mean photon numbers for secure key rates per clock cycle for both trusted (solid lines) and untrusted dark counts (dotted lines) versus total transmissivity η. For clarity, we omit labelling the lines for trusted and untrusted dark counts in the cases where the two lines are indistinguishable.

rate lower bound obtained by this method to be much lower than the true value. As for the feasible cases, Figure 4.4(a) shows that turning dark counts from untrusted to trusted increases the key rates. In the remaining of this section, if we make statements about the key rates without mentioning whether dark counts are trusted or untrusted, then the statement applies to both cases.

In the design view of a QKD security analysis, the goal is to optimise over all parameters and find the optimal setting of the experimental setup. Here, we seek the optimal asymmetric transmission parameter κ and the corresponding optimal signal intensity $|\alpha|^2$ that gives the highest key rate at different total transmissivity η. We see that the smaller the value of κ, the lower the key rates in Figure 4.4(a) because Alice would need to send more photons (as one can see from Figure 4.4(b)) in order to maintain an adequate proportion of middle-click detection events, which allow Bob to infer the relative phase $\phi_x - \phi_B$. Therefore, one should always aim at reducing the loss at the phase modulator in order to increase the overall key rate.

To elaborate more on the optimality of the intensities in Figure 4.4(b), we point out the two competing factors for using more photons in the signal. First, sending higher intensity signals causes more photons to pass through Eve's domain, which allows her to gain more information about the signal, thereby reducing the key rate. Second, as more information can be transmitted from Alice to Bob via multi-photon signals, the key rate may increase if the cost of error correction increases less than the information gain by Eve.

These two factors pull the key rate into opposite directions, so there is an optimal point for the key rate to be maximised, of which the corresponding optimal mean photon number is shown in Figure 4.4(b). These values appear to be higher than the optimal values for the key rates in Ref. [5]. This indicates that some multi-photon signals carry useful information from Alice to Bob of which Eve does not possess full knowledge, and hence favours signals with higher intensity.

4.6.1 Comparison with previous results

At this point, we would like to compare our results with previous results in Refs. [4, 5] which both contain valid security proofs that make use of the single-photon components only. Note that although the technical analysis of Ref. [4] is correct, the conclusion that the key rate of the unbalanced BB84 protocol will be overestimated if one blindly uses the security analysis of a balanced protocol is not. While Ref. [4] has shown that the key rate for unbalanced signals is lower than that for balanced ones, the authors of Ref. [5]

correctly point out that the drop in key rate is due to a smaller success rate of the unbalanced protocol, followed by the same key reduction during privacy amplification as for a balanced protocol. So in effect, during the operation of an unbalanced protocol, the use of privacy amplification terms from a balanced BB84 protocol still gives valid secret key rates. Therefore, it is incorrect for Ref. [4] to conclude that the drop in secure key rates for the unbalanced cases is due to the application of a new security analysis. Since Ref. [5] provides a known analytical key rate of this scenario, we use that result as the baseline of our investigations to show that in fact the secret key rate is underestimated by this security analysis, and thus less privacy amplification is required in this situation.

We compare our key rates with Ref. [5]'s in Figure 4.5, which shows that our analysis provides higher key rates for total transmissivity $\eta > 0.1$ (<10 dB), especially for small κ values. Our method shows advantage in low-loss cases because the PA components from the multi-photon part of Alice's signals are larger in the low-loss regime, which are pessimistically set to zero in Ref. [5]. This can be understood as Eve does not learn too much of the multi-photon signals, thereby allowing more information to reach Bob.

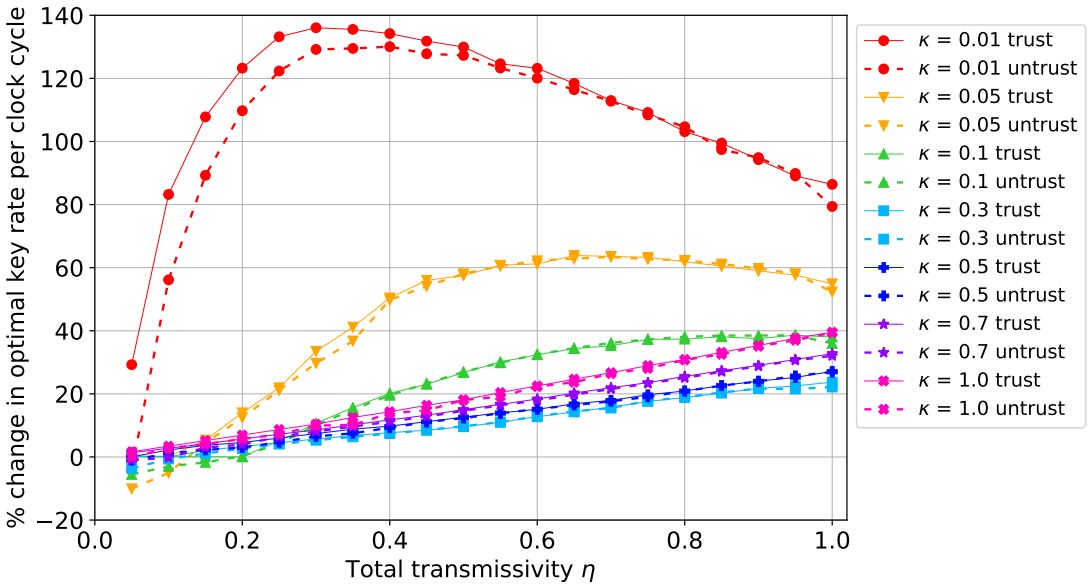


Figure 4.5: Percentage change in key rates comparing our optimal lower bounds for key rates with Ref. [5]'s optimal key rates versus total transmissivity η. We label the changes for trusted (untrusted) dark counts with solid (dotted) lines. A positive change means that our key rate is higher.

When the total transmissivity satisfies $\eta \leq 0.2$, we encounter the issue with infeasible constraints with untrusted dark counts. We recover approximately the same key rates in Ref. [5] for most cases, but some of our lower bounds for the key rates (obtained from maximising the dual SDP problem) in the untrusted noise scenario appear to be slightly lower than Ref. [5]'s. To understand the gaps between our key rate upper bounds (which are on par with Ref. [5]'s key rates) and lower bounds (see Sections 2.2.5 and 4.4.4 for the meaning of the two bounds), we recall that our way of getting around the infeasibility issue with untrusted noise is to relax the required precision for the constraints to be satisfied in the numerical solver. The first-step suboptimal solution to the relaxed problem will naturally suffer from stronger constraint violations which lead to a lower dual suboptimal solution [2].

Notice that when the asymmetric loss parameter reaches $\kappa = 0.3$, the percentage increase of our key rate relative to Ref. [5]'s is the least compared to other values of κ. This phenomenon is also observed when we make the following choices of parameters: flag-state photon cutoff $N_B \in \{1, 2, 3, 4\}$, dark count probability $p_d \in \{0, 10^{-5}, 10^{-4}\}$, and total transmissivity $\eta = 1$. As our numerical data suggest, the ratio between the optimal values of the privacy amplification terms attributed to Alice sending out 1-photon and 2-photon signals,

$$r_{21} = \frac{\min_{\rho^2_{AB} \in \mathbf{S}_2} D(\mathcal{G}(\rho^2_{AB}) || \mathcal{Z}(\mathcal{G}(\rho^2_{AB})))}{\min_{\rho^1_{AB} \in \mathbf{S}_1} D(\mathcal{G}(\rho^1_{AB}) || \mathcal{Z}(\mathcal{G}(\rho^1_{AB})))}, \tag{4.38}$$

reaches its smallest value when $\kappa \approx 0.3$. This can be interpreted as the amount of private information carried by 2-photon signals relative to the amount carried by 1-photon signals is the least when $\kappa \approx 0.3$, which corresponds to the points with the least key rate improvement.

As a remark, the optimal signal intensities $|\widetilde{\alpha}_{\text{opt}}|^2$'s for Ref. [5]'s optimal key rates (corresponding to Equation (6) in Ref. [5]), which we compare with in Figure 4.5, are slowly decreasing as η increases. They satisfy $|\widetilde{\alpha}_{\text{opt}}|^2 \leq \min\{1, |\alpha_{\text{opt}}|^2\}$ where $|\alpha_{\text{opt}}|^2$ is the corresponding optimal intensity of our analysis as plotted in Figure 4.4(b). This means that Ref. [5]'s optimal signal intensity is always smaller than our optimal intensity $|\alpha_{\text{opt}}|^2$. It is also true that Ref. [5]'s optimal intensity increases as κ reduces for all tested values of η.

In the post-processing view, the goal is to determine the amount of key reduction from privacy amplification that guarantees a secure final key for a given set of experimental parameters. Particularly, in the case where the attenuation of the laser has already been set to Ref. [5]'s optimal intensity for a chosen set of parameters, we compare the privacy amplification term from our analysis with the one from Ref. [5]'s. To see this, we first show

in Figure 4.6 that our method still gives higher key rates than Ref. [5]'s in the low-loss regime ($\eta > 0.15$) even when our signal intensities are set to Ref. [5]'s. We then make the connection between this result and the difference in privacy amplification with two observations: 1) the probability of passing post-selection p_{pass} is equal for both methods and 2) the costs of error correction are approximately equal when the same signal intensity is used in both approaches. It follows that the difference in key rates translates to the difference in the privacy amplification terms in the key rate formula. Thus, our method requires less key reduction from privacy amplification compared to Ref. [5] for low-loss scenarios. This allows us to extract more secret key out of these unbalanced protocols than previously thought.

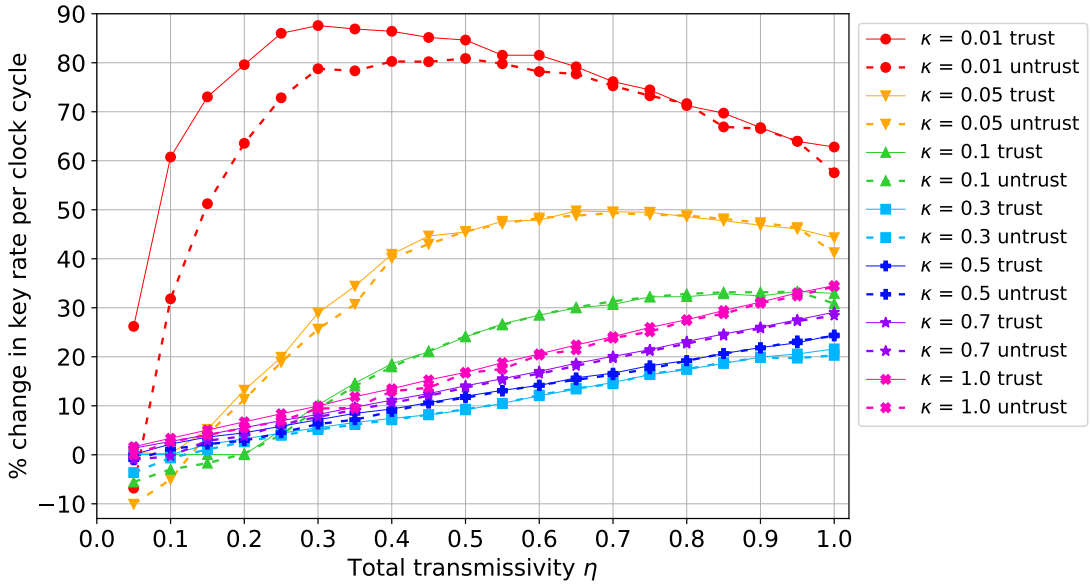


Figure 4.6: Percentage change in key rates comparing our lower bounds for key rates per clock cycle evaluated at Ref. [5]'s optimal $\widetilde{\alpha}_{\text{opt}}$ with Ref. [5]'s optimal key rates versus total transmissivity η. We label the changes for trusted (untrusted) dark counts with solid (dotted) lines. A positive change means that our key rate is higher.

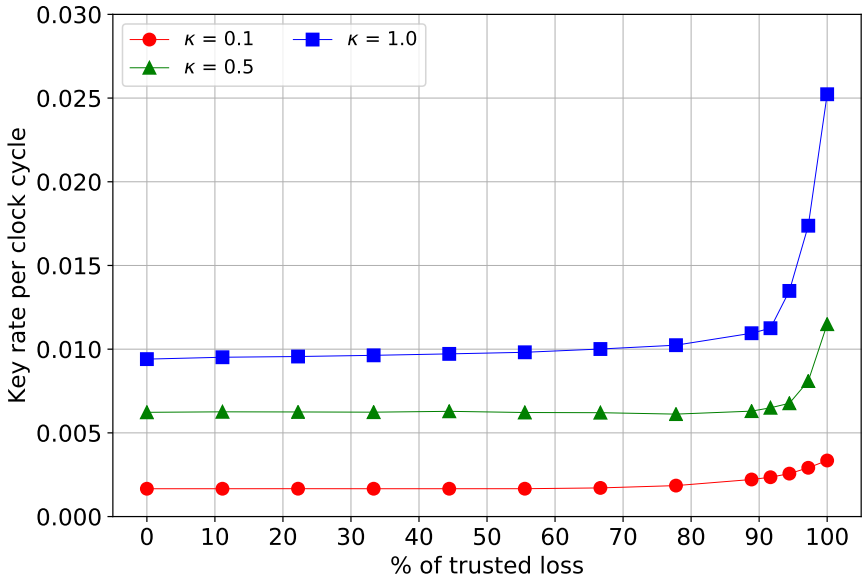
4.6.2 Trusted loss

We now turn to study the effect of trusted loss on the key rates. Previously, we assume that the quantum channel contributes completely to the total loss. However, if we know

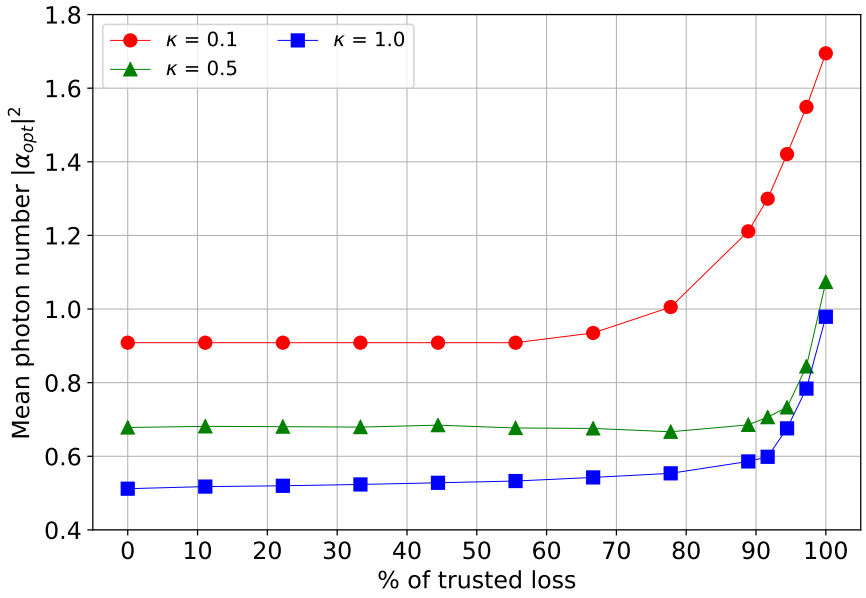
that a certain part of the total loss is caused by some trusted components (e.g. Bob's detectors), the key rate can be improved since the channel loss is effectively smaller. The key rate improvement has already been shown in both active and passive BB84 protocol [8] where the detection efficiency of the receiver's detectors is assumed to be beyond Eve's control. We will present a similar behaviour of the key rates of this protocol under different trusted loss conditions.

We fix the total transmissivity to be $\eta = 0.1$ and assume dark counts to be trusted, and then we vary the detection efficiency of Bob's trusted detectors η_{det}. Indeed, Figure 4.7(a) shows that the lower bound of our optimal key rate increases with the proportion of the trusted loss component coming from Bob's detectors to the total loss, which takes the form $\frac{1-\eta_{\text{det}}}{1-\eta}$. The optimal mean photon numbers corresponding to the optimal key rates are displayed in Figure 4.7(b).

To summarise this section, we report a significant gain in key rates in the low-loss regime (<10 dB) with our analysis. To be precise, with our security analysis, higher key rates can be obtained when the signal intensities are set to our optimal and Ref. [5]'s optimal values. We emphasise that the reported improvement can be attained without any modification to the experimental setup. Lastly, we show that the key rates can be increased if we know that the detection inefficiency contributes a considerable amount to the total loss.



(a)



(b)

Figure 4.7: Assuming trusted dark counts, (a) our lower bounds for key rates and (b) the mean photon numbers plotted against the proportion (in percentage) of the trusted loss coming from the detection inefficiency of Bob's detectors to a fixed total loss corresponding to total transmissivity $\eta = 0.1$.

Chapter 5

Conclusion and Outlook

In this thesis, we reviewed all the mathematical details that allow us to understand the QKD security proof framework and how squashing models can be an important tool in QKD security analyses. In Chapter 3, we proved the unconditional asymptotic security under the usage of a generic squashing model formally for the first time. Moreover, we discuss the flag-state squashing model in a more general setting than when it was first introduced by Zhang *et al.* [8], and proved rigorously that the associated squashing map is a quantum channel for an infinite-dimensional input Hilbert space. We pointed out that lower bounding the weight of the preserved subspace in a flag-state squashing model is essential for the squashing map to preserve some degree of entanglement. Subsequently, we specialised in the case where the POVM is block-diagonal in the Fock basis and described the method of using any observable that has a minimum observed value increasing with the restricted detection photon number. Since the existences of all known squashing models [3, 47, 48, 43, 8] are proved under the condition that the POVM is block-diagonal, it is still an open problem whether a general squashing model that is applicable to all kinds of QKD protocols, particularly continuous-variable protocols, exists or not.

In Chapter 4, we provide a new numerical security proof for the unbalanced phase-encoded BB84 protocol. Using the newly developed flag-state squashing model [8], we are able to derive additional private information from the multi-photon components of the signal states. We compare our key rates with the key rates proved in Ref. [5] under the same simulation parameters and show that our analysis results in significantly higher key rates in the low-loss regime. In the design view, we find that a balanced protocol ($\kappa = 1$) gives a higher key rate than an unbalanced protocol so that a design cannot take advantage of an artificial induction of asymmetry. In the post-processing view, our method requires less key reduction from privacy amplification compared to Ref. [5] for low-loss cases. We

prove that our key rates are still better than Ref. [5]'s even when their optimal mean signal photon numbers are used. Hence, any experiments that are already implementing the optimal settings of Ref. [5] can profit from our higher key rates. We also explore the advantage of characterising the receiver's detection inefficiency as a trusted loss, which is not allowed by Refs. [4, 5]'s proof technique. Our results suggest that the key rate can be improved when the proportion of trusted loss due to detection inefficiency to the total loss is significant.

We conclude here by pointing out some future directions of investigation related to the work described in Chapter 4: It is important to find a formal way of incorporating untrusted dark counts into the security analysis without leading to unphysical constraints. As mentioned in Section 4.4.2, to extend our analysis to the use of a finite number of decoy states, one must consider the dependence among different feasible conditional state sets when handling the privacy amplification term. Finally, some of our proof techniques can be transferred to a finite-key analysis. It would be worth comparing the key rates from a finite-key analysis [66] with the asymptotic key rates reported here.

References

[1] Nicky Kai Hong Li and Norbert Lütkenhaus, "Improving key rates of the unbalanced phase-encoded BB84 protocol using the flag-state squashing model," (2020), arXiv:2007.08662 [quant-ph] .

[2] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles, "Reliable numerical key rates for quantum key distribution," Quantum **2**, 77 (2018).

[3] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus, "Squashing models for optical measurements in quantum communication," Phys. Rev. Lett. **101**, 093601 (2008).

[4] Agnes Ferenczi, Varun Narasimhachar, and Norbert Lütkenhaus, "Security proof of the unbalanced phase-encoded Bennett-Brassard 1984 protocol," Phys. Rev. A **86**, 042327 (2012).

[5] Satoshi Sunohara, Kiyoshi Tamaki, and Nobuyuki Imoto, "Blind post-processing for the unbalanced BB84," (2013), arXiv:1302.1701 [quant-ph] .

[6] Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.

[7] Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science **560**, 7–11 (2014).

[8] Yanbao Zhang, Patrick J. Coles, Adam Winick, Jie Lin, and Norbert Lütkenhaus, "Security proof of practical quantum key distribution with detection-efficiency mismatch," (2020), arXiv:2004.04383 [quant-ph] .

[9] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[10] Vern Paulsen, "Lecture notes in operator algebra methods in QIT," `https://www.math.uwaterloo.ca/~vpaulsen/OpAlgQIT.pdf` (2020).

[11] John Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[12] Walter Rudin, *Principles of Mathematical Analysis*, International series in pure and applied mathematics (McGraw-Hill, 1976).

[13] Walter Rudin, *Real and Complex Analysis, 3rd Ed.*, Mathematics series (McGraw-Hill, 1987).

[14] Tailen Hsing and Randall Eubank, "Compact operators and singular value decomposition," in *Theoretical Foundations of Functional Data Analysis, with an Introduction to Linear Operators* (John Wiley Sons, Ltd, 2015) Chap. 4, pp. 91–128.

[15] Maxim Raginsky, "Radon–Nikodym derivatives of quantum operations," Journal of Mathematical Physics **44**, 5003–5020 (2003).

[16] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai, "Entanglement breaking channels," Reviews in Mathematical Physics **15**, 629–641 (2003).

[17] Elliott H. Lieb and Mary Beth Ruskai, "Proof of the strong subadditivity of quantum-mechanical entropy," Journal of Mathematical Physics **14**, 1938–1941 (1973).

[18] Lin, Jie, *Security Proofs for Quantum Key Distribution Protocols by Numerical Approaches*, Master's thesis, University of Waterloo (2017).

[19] Renato Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zurich (2005), arXiv:quant-ph/0512258 [quant-ph] .

[20] Charles H. Bennett, Gilles Brassard, and N. David Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).

[21] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," Quantum Info. Comput. **3**, 535–552 (2003).

[22] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus, "Entanglement as a precondition for secure quantum key distribution," Phys. Rev. Lett. **92**, 217903 (2004).

[23] Agnes Ferenczi and Norbert Lütkenhaus, "Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning," Phys. Rev. A **85**, 052310 (2012).

[24] Michael Ben-Or and Dominic Mayers, "General security definition and composability for quantum & classical protocols," (2004), arXiv:quant-ph/0409062 [quant-ph] .

[25] Dominique Unruh, "Simulatable security for quantum protocols," (2004), arXiv:quant-ph/0409125 [quant-ph] .

[26] 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*, edited by Joe Kilian (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 386–406, arXiv:quant-ph/0409078 [quant-ph] .

[27] Renato Renner, "Symmetry of large physical systems implies independence of subsystems," Nature Physics **3**, 645–649 (2007).

[28] R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Phys. Rev. Lett. **102**, 110504 (2009).

[29] Valerio Scarani and Renato Renner, "Security bounds for quantum cryptography with finite resources," in *Theory of Quantum Computation, Communication, and Cryptography: Third Workshop, TQC 2008 Tokyo, Japan, January 30 - February 1, 2008. Revised Selected Papers* (Springer-Verlag, Berlin, Heidelberg, 2008) p. 83–95.

[30] Matthias Christandl, Robert König, and Renato Renner, "Postselection technique for quantum channels with applications to quantum cryptography," Phys. Rev. Lett. **102**, 020504 (2009).

[31] Normand J. Beaudry, *Assumptions in quantum cryptography*, Ph.D. thesis, ETH Zurich, Zürich (2014).

[32] 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**, 207–235 (2005).

[33] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus, "Numerical approach for unstructured quantum key distribution," Nature Communications **7**, 11712 (2016).

[34] Patrick J. Coles, "Unification of different views of decoherence and discord," Phys. Rev. A **85**, 042103 (2012).

[35] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution," Phys. Rev. X **9**, 041064 (2019).

[36] Stephen Boyd and Lieven Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).

[37] Marguerite Frank and Philip Wolfe, "An algorithm for quadratic programming," Naval Research Logistics Quarterly **3**, 95–110 (1956).

[38] Mark Fannes, "A continuity property of the entropy density for spin lattice systems," Communications in Mathematical Physics **31**, 291–294 (1973).

[39] Koenraad M R Audenaert, "A sharp continuity estimate for the von Neumann entropy," Journal of Physics A: Mathematical and Theoretical **40**, 8127–8136 (2007).

[40] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill, "Security of quantum key distribution with imperfect devices," Quantum Info. Comput. **4**, 325–360 (2004).

[41] Hoi-Kwong Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).

[42] Peter W. Shor and John Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).

[43] 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," Phys. Rev. A **89**, 012325 (2014).

[44] Narasimhachar, Varun, *Study of realistic devices for quantum key-distribution*, Master's thesis, University of Waterloo (2011).

[45] Shmuel Friedland, "Infinite dimensional generalizations of Choi's theorem," Special Matrices **7**, 67 – 77 (2019).

[46] Norbert Lütkenhaus, *Generalised Measurements and Quantum Cryptography*, Ph.D. thesis, University of Strathclyde, Glasgow (1996).

[47] Toyohiro Tsurumaru and Kiyoshi Tamaki, "Security proof for quantum-key-distribution systems with threshold detectors," Phys. Rev. A **78**, 032302 (2008).

[48] Chi-Hang Fred Fung, H. F. Chau, and Hoi-Kwong Lo, "Universal squash model for optical communications using linear optics and threshold detectors," Phys. Rev. A **84**, 020303 (2011).

[49] Charles H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121–3124 (1992).

[50] P. D. Townsend, "Secure key distribution system based on quantum cryptography," Electronics Letters **30**, 809–811 (1994).

[51] Richard J. Hughes, G. G. Luther, G. L. Morgan, and C. Simmons, "Quantum cryptography over 14 km of installed optical fiber," in *Coherence and Quantum Optics VII*, edited by Joseph H. Eberly, Leonard Mandel, and Emil Wolf (Springer US, Boston, MA, 1996) pp. 103–111.

[52] Hong-Wei Li, Zhen-Qiang Yin, Zheng-Fu Han, Wan-Su Bao, and Guang-Can Guo, "Security of practical phase-coding quantum key distribution," (2009), arXiv:0911.2938 [quant-ph] .

[53] Won-Young Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).

[54] Xiang-Bin Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).

[55] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).

[56] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," The European Physical Journal D **41**, 599–627 (2007).

[57] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330–1333 (2000).

[58] Alexander S. Holevo, "Statistical decision theory for quantum systems," Journal of Multivariate Analysis **3**, 337 – 394 (1973).

[59] Carl W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering : a series of monographs and textbooks (Academic Press, 1976).

[60] Hoi-Kwong Lo, H.F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," Journal of Cryptology **18**, 133–165 (2004).

[61] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma, "Time-shift attack in practical quantum cryptosystems," Quantum Info. Comput. **7**, 73–82 (2007).

[62] Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo, "Phase-remapping attack in practical quantum-key-distribution systems," Phys. Rev. A **75**, 032314 (2007).

[63] Dominic Mayers and Andrew Yao, "Self testing quantum apparatus," Quantum Info. Comput. **4**, 273–286 (2004).

[64] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Applied Physics Letters **84**, 3762–3764 (2004).

[65] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).

[66] Ian George, Jie Lin, and Norbert Lütkenhaus, "Numerical calculations of finite key rate for general quantum key distribution protocols," (2020), arXiv:2004.11865 [quant-ph] .

APPENDICES

Appendix A

Explicit Form of Dark Count Post-Processing

In this appendix, we will explicitly show the action of the classical post-processing map $\mathcal{P}$ for simulating the effect of dark counts as mentioned in Section 4.3.4. We now list the new POVM elements after the map $\mathcal{P}$ as follows.

- Post-processed no-click POVM element:

$$P_0^{\phi_B} = (1-p_d)^6 \; F_0^{\phi_B} \; . \tag{A.1}$$

- Post-processed single-click POVM elements:

$$P_{t_1}^{\phi_B} = (1-p_d)^4 (F_{t_1}^{\phi_B} + (1-(1-p_d)^2) F_0^{\phi_B}), \tag{A.2}$$

$$P_{t_3}^{\phi_B} = (1-p_d)^4 (F_{t_3}^{\phi_B} + (1-(1-p_d)^2) F_0^{\phi_B}), \tag{A.3}$$

$$P_2^{\phi_B} = (1-p_d)^5 (F_2^{\phi_B} + p_d \; F_0^{\phi_B}), \tag{A.4}$$

$$P_5^{\phi_B} = (1-p_d)^5 (F_5^{\phi_B} + p_d \; F_0^{\phi_B}). \tag{A.5}$$

- Post-processed double-click POVM elements:

$$P_{t_1,t_3}^{\phi_B} = (1-p_d)^2 \{F_{t_1,t_3}^{\phi_B} + [1-(1-p_d)^2](F_{t_1}^{\phi_B} + F_{t_3}^{\phi_B}) + [1-(1-p_d)^2]^2 \; F_0^{\phi_B}\}, \tag{A.6}$$

$$P_{2,5}^{\phi_B} = (1-p_d)^4 [F_{2,5}^{\phi_B} + p_d (F_2^{\phi_B} + F_5^{\phi_B}) + p_d^2 \; F_0^{\phi_B}], \tag{A.7}$$

$$P^{\phi_B}_{t_1,2} = (1-p_d)^3\{F^{\phi_B}_{t_1,2} + p_d F^{\phi_B}_{t_1} + [1-(1-p_d)^2]F^{\phi_B}_{2} + p_d[1-(1-p_d)^2]F^{\phi_B}_{0}\}, \tag{A.8}$$

$$P^{\phi_B}_{t_1,5} = (1-p_d)^3\{F^{\phi_B}_{t_1,5} + p_d F^{\phi_B}_{t_1} + [1-(1-p_d)^2]F^{\phi_B}_{5} + p_d[1-(1-p_d)^2]F^{\phi_B}_{0}\}, \tag{A.9}$$

$$P^{\phi_B}_{t_3,2} = (1-p_d)^3\{F^{\phi_B}_{t_3,2} + p_d F^{\phi_B}_{t_3} + [1-(1-p_d)^2]F^{\phi_B}_{2} + p_d[1-(1-p_d)^2]F^{\phi_B}_{0}\}, \tag{A.10}$$

$$P^{\phi_B}_{t_3,5} = (1-p_d)^3\{F^{\phi_B}_{t_3,5} + p_d F^{\phi_B}_{t_3} + [1-(1-p_d)^2]F^{\phi_B}_{5} + p_d[1-(1-p_d)^2]F^{\phi_B}_{0}\}. \tag{A.11}$$

- Post-processed triple-click POVM elements:

$$\begin{aligned} P^{\phi_B}_{t_1,t_3,2} = (1-p_d)\{&F^{\phi_B}_{t_1,t_3,2} + p_d F^{\phi_B}_{t_1,t_3} + [1-(1-p_d)^2](F^{\phi_B}_{t_1,2} + F^{\phi_B}_{t_3,2}) \\ &+ p_d[1-(1-p_d)^2](F^{\phi_B}_{t_1} + F^{\phi_B}_{t_3}) + [1-(1-p_d)^2]^2 F^{\phi_B}_{2} + p_d[1-(1-p_d)^2]^2 F^{\phi_B}_{0}\}, \end{aligned} \tag{A.12}$$

$$\begin{aligned} P^{\phi_B}_{t_1,t_3,5} = (1-p_d)\{&F^{\phi_B}_{t_1,t_3,5} + p_d F^{\phi_B}_{t_1,t_3} + [1-(1-p_d)^2](F^{\phi_B}_{t_1,5} + F^{\phi_B}_{t_3,5}) \\ &+ p_d[1-(1-p_d)^2](F^{\phi_B}_{t_1} + F^{\phi_B}_{t_3}) + [1-(1-p_d)^2]^2 F^{\phi_B}_{5} + p_d[1-(1-p_d)^2]^2 F^{\phi_B}_{0}\}, \end{aligned} \tag{A.13}$$

$$\begin{aligned} P^{\phi_B}_{t_1,2,5} = (1-p_d)^2\{&F^{\phi_B}_{t_1,2,5} + p_d(F^{\phi_B}_{t_1,2} + F^{\phi_B}_{t_1,5}) + [1-(1-p_d)^2]F^{\phi_B}_{2,5} + p_d^2 F^{\phi_B}_{t_1} \\ &+ p_d[1-(1-p_d)^2](F^{\phi_B}_{2} + F^{\phi_B}_{5}) + p_d^2[1-(1-p_d)^2]F^{\phi_B}_{0}\}, \end{aligned} \tag{A.14}$$

$$\begin{aligned} P^{\phi_B}_{t_3,2,5} = (1-p_d)^2\{&F^{\phi_B}_{t_3,2,5} + p_d(F^{\phi_B}_{t_3,2} + F^{\phi_B}_{t_3,5}) + [1-(1-p_d)^2]F^{\phi_B}_{2,5} + p_d^2 F^{\phi_B}_{t_3} \\ &+ p_d[1-(1-p_d)^2](F^{\phi_B}_{2} + F^{\phi_B}_{5}) + p_d^2[1-(1-p_d)^2]F^{\phi_B}_{0}\}. \end{aligned} \tag{A.15}$$

- Post-processed all-click POVM elements:

$$\begin{aligned} P^{\phi_B}_{t_1,t_3,2,5} = &F^{\phi_B}_{t_1,t_3,2,5} + p_d(F^{\phi_B}_{t_1,t_3,2} + F^{\phi_B}_{t_1,t_3,5}) + [1-(1-p_d)^2](F^{\phi_B}_{t_1,2,5} + F^{\phi_B}_{t_3,2,5}) \\ &+ p_d[1-(1-p_d)^2](F^{\phi_B}_{t_1,2} + F^{\phi_B}_{t_1,5} + F^{\phi_B}_{t_3,2} + F^{\phi_B}_{t_3,5}) + p_d^2\, F^{\phi_B}_{t_1,t_3} + [1-(1-p_d)^2]^2\, F^{\phi_B}_{2,5} \\ &+ p_d^2[1-(1-p_d)^2](F^{\phi_B}_{t_1} + F^{\phi_B}_{t_3}) + p_d[1-(1-p_d)^2]^2(F^{\phi_B}_{2} + F^{\phi_B}_{5}) \\ &+ p_d^2[1-(1-p_d)^2]^2 F^{\phi_B}_{0}. \end{aligned} \tag{A.16}$$

It can be easily checked that the POVM elements above from (A.1) to (A.16) for a fixed ϕ_B sums to $p(\phi_B)\mathbb{1}_B$.

Appendix B

Derivation of the lower bound for the weight of $(n \leq N_B)$-photon subspace

We aim at lower bounding the weight of the $(n \leq N_B)$-photon signal subspace, $p(n \leq N_B)$, with Bob's observed statistics. In this appendix, we use the cross-click probability to derive a lower bound for $p(n \leq N_B)$ in the following steps. The cross-click probability for any signal satisfies

$$\begin{aligned} p(\mathrm{cc}) &= \sum_{n=0}^{N_B} p(n)p(\mathrm{cc}|n) + \sum_{n=N_B+1}^{\infty} p(n)p(\mathrm{cc}|n) \\ &\geq \sum_{n=0}^{N_B} p(n)p_{\min}(\mathrm{cc}|n) + \sum_{n=N_B+1}^{\infty} p(n)p_{\min}(\mathrm{cc}|n) \\ &\geq p(n \leq N_B)C^{\min}_{n\leq N_B} + [1 - p(n \leq N_B)]C^{\min}_{n>N_B} \\ &= C^{\min}_{n>N_B} - p(n \leq N_B)(C^{\min}_{n>N_B} - C^{\min}_{n\leq N_B}). \end{aligned} \tag{B.1}$$

In the second line, $p_{\min}(\mathrm{cc}|n)$ denotes the minimal cross-click probability given that Bob receives an n-photon signal. In the last two lines, we define $p(n \leq N_B) \coloneqq \sum_{n=0}^{N_B} p(n)$, $C^{\min}_{n\leq N_B} \coloneqq \min_{0\leq n\leq N_B} p_{\min}(\mathrm{cc}|n)$ and $C^{\min}_{n>N_B} \coloneqq \min_{n>N_B} p_{\min}(\mathrm{cc}|n)$. If $p_{\min}(\mathrm{cc}|n)$ is monotonically increasing with n, then $C^{\min}_{n\leq N_B} = p_{\min}(\mathrm{cc}|0)$ and $C^{\min}_{n>N_B} = p_{\min}(\mathrm{cc}|N_B+1)$. If we also have strict inequality $C^{\min}_{n>N_B} > C^{\min}_{n\leq N_B}$, then we can turn the inequality in (B.1) into the desired lower bound

$$p(n \leq N_B) \geq 1 - \frac{p(\mathrm{cc}) - p_{\min}(\mathrm{cc}|0)}{p_{\min}(\mathrm{cc}|N_B+1) - p_{\min}(\mathrm{cc}|0)} =: B^{\min}_{n\leq N_B} . \tag{B.2}$$

We will show that the minimum cross-click probabilities indeed satisfy the monotonicity and the strict inequality conditions.

To obtain the minimum conditional probabilities $p_{\min}(\text{cc}|0)$ and $p_{\min}(\text{cc}|N_B+1)$, we start by considering the new POVM elements after classical post-processing due to dark counts, which appear in Equations (A.1) – (A.7). We first group the pre-processed POVM elements into two coarse-grained POVM elements: outside-only (t_1, t_3, $t_1\&t_3$) and inside-only (2, 5, 2&5). Using Equations (4.19) and (4.20), the two elements can be expressed as

$$F_{\text{out}} = \sum_{\phi_B\in\{0,\pi/2\}} (F^{\phi_B}_{t_1,t_3} + F^{\phi_B}_{t_1} + F^{\phi_B}_{t_3}) \tag{B.3}$$

$$= \sum_{n=1}^{\infty}\sum_{i=0}^{n} \xi^i(1-\xi)^{n-i}|i,n-i\rangle\langle i,n-i|, \tag{B.4}$$

$$F_{\text{in}} = \sum_{\phi_B\in\{0,\pi/2\}} (F^{\phi_B}_{2,5} + F^{\phi_B}_{2} + F^{\phi_B}_{5}) \tag{B.5}$$

$$= \sum_{n=1}^{\infty}\sum_{i=0}^{n} \xi^{n-i}(1-\xi)^{i}|i,n-i\rangle\langle i,n-i|. \tag{B.6}$$

Similarly, the two coarse-grained post-processed POVM elements can be found to be

$$P_{\text{out}} = \sum_{\phi_B\in\{0,\pi/2\}} (P^{\phi_B}_{t_1,t_3} + P^{\phi_B}_{t_1} + P^{\phi_B}_{t_3}) \tag{B.7}$$

$$= \sum_{\phi_B}\{(1-p_d)^2\{F^{\phi_B}_{t_1,t_3} + [1-(1-p_d)^2](F^{\phi_B}_{t_1} + F^{\phi_B}_{t_3}) + [1-(1-p_d)^2]^2\ F^{\phi_B}_0\} \tag{B.8}$$
$$+ (1-p_d)^4[F^{\phi_B}_{t_1} + (1-(1-p_d)^2)F^{\phi_B}_0] + (1-p_d)^4[F^{\phi_B}_{t_3} + (1-(1-p_d)^2)F^{\phi_B}_0]\}$$

$$= \sum_{\phi_B}\{(1-p_d)^2(F^{\phi_B}_{t_1,t_3} + F^{\phi_B}_{t_1} + F^{\phi_B}_{t_3})$$
$$+ \{(1-p_d)^2[1-(1-p_d)^2]^2 + 2(1-p_d)^4[1-(1-p_d)^2]\}F^{\phi_B}_0\} \tag{B.9}$$

$$= (1-p_d)^2\{F_{\text{out}} + [1-(1-p_d)^2][1+(1-p_d)^2]F_0\} \tag{B.10}$$

$$= (1-p_d)^2\{F_{\text{out}} + [1-(1-p_d)^4]F_0\}, \tag{B.11}$$

$$P_{\text{in}} = \sum_{\phi_B \in \{0,\pi/2\}} (P_{2,5}^{\phi_B} + P_2^{\phi_B} + P_5^{\phi_B}) \tag{B.12}$$

$$= \sum_{\phi_B} \{(1-p_d)^4 [F_{2,5}^{\phi_B} + p_d(F_2^{\phi_B} + F_5^{\phi_B}) + p_d^2\, F_0^{\phi_B}] + (1-p_d)^5 (F_2^{\phi_B} + p_d\, F_0^{\phi_B}) + (1-p_d)^5 (F_5^{\phi_B} + p_d\, F_0^{\phi_B})\} \tag{B.13}$$

$$= \sum_{\phi_B} \{(1-p_d)^4 (F_{2,5}^{\phi_B} + F_2^{\phi_B} + F_5^{\phi_B}) + p_d(1-p_d)^4 [p_d + 2(1-p_d)] F_0^{\phi_B}\} \tag{B.14}$$

$$= (1-p_d)^4 \{F_{\text{in}} + p_d(2-p_d) F_0\}, \tag{B.15}$$

where the pre-processed no-click POVM element is $F_0 = |0,0\rangle\langle 0,0|$. Therefore, the post-processed coarse-grained POVM elements for inside-only and outside-only clicks are diagonal in the two-mode Fock basis $\{|i, n-i\rangle : i = 0, ..., n\}$ for all $n \in \mathbb{N}$. The cross-click POVM element is

$$P_{\text{cc}} = \mathbb{1}_B - (P_{\text{out}} + P_{\text{in}} + \sum_{\phi_B} P_0^{\phi_B}) \tag{B.16}$$

which is also diagonal in the two-mode Fock basis. Since P_{cc} is already diagonal, it is straightforward to find P_{cc}'s minimum eigenvalue restricted to the n-photon subspace, which corresponds to the minimum cross-click probability for any n-photon input states, analytically. For an eigenstate $|i, n-i\rangle$, the associated cross-click probability (the eigenvalue of P_{cc}) can be found using Equations (A.1) – (B.16) as

$$p(\text{cc}|\ |i, n-i\rangle) = 1 - (1-p_d)^2\, \xi^i (1-\xi)^{n-i} - (1-p_d)^4\, \xi^{n-i} (1-\xi)^i \tag{B.17}$$

for $n \geq 1$, and for the vacuum state $|0,0\rangle$ to be

$$p(\text{cc}|0) = 1 - \{(1-p_d)^2 [1-(1-p_d)^4] + p_d(1-p_d)^4(2-p_d) + (1-p_d)^6\} \tag{B.18}$$

$$= 1 - (1-p_d)^2 [1 + p_d\, (1-p_d)^2 (2-p_d)]. \tag{B.19}$$

as stated in Equation (4.28). Since there is only one eigenvalue in the vacuum subspace, we need not minimise the conditional probability (i.e. $p_{\min}(\text{cc}|0) = p(\text{cc}|0)$). We exclude the case where the phase modulator has zero transmissivity ($\kappa = 0$), then $\xi = \frac{1}{1+\kappa} \in [\frac{1}{2}, 1)$, so the minimum cross-click probability for any ($n \geq 1$)-photon input state is

$$p_{\min}(\text{cc}|n) = 1 - (1-p_d)^2\, \xi^n - (1-p_d)^4\, (1-\xi)^n \tag{B.20}$$

as stated in Equation (4.29), which is valid for all $n \geq 1$. Notice that $p_{\min}(\text{cc}|n)$ is monotonically increasing with n which agrees with our intuition that cross-click events are more

likely with more incoming photons. If we compare the second term in (B.19) with the second and third terms in (B.20), we see that

$$(1-p_d)^2 \underbrace{\left[1+p_d\,(1-p_d)^2(2-p_d)\right]}_{\geq 1} \geq (1-p_d)^2 \underbrace{\left(\xi^n+(1-p_d)^2\,(1-\xi)^n\right)}_{\leq 1} \tag{B.21}$$

which implies for all $n \geq 1$, $p(\mathrm{cc}|0) \leq p_{\min}(\mathrm{cc}|n)$.

As we further restrict the dark count probability to $p_d \in [0,1)$, it is analytically straightforward to verify that for all $n \geq 1$ and $\xi \in [\frac{1}{2},1)$,

$$p(\mathrm{cc}|0) \leq p_{\min}(\mathrm{cc}|n) < p_{\min}(\mathrm{cc}|n+1), \tag{B.22}$$

so the monotonicity and the strict inequality conditions for (B.2) to hold are satisfied. The inequality (B.2) is of the same form as (4.27) in Section 4.4.1 except that the observed cross-click probability in (4.27) is conditioned on Alice's signal choice x.

We now move on to prove that the lower bound in the inequality (B.2) is tighter than the lower bound derived by Narasimhachar [44] for no dark counts. We use the fact that

$$\frac{a-c}{b-c} \leq \frac{a}{b} \quad \text{, if } 0 \leq c \leq a \leq b \tag{B.23}$$

and all probabilities are positive to show that

$$\frac{p(\mathrm{cc})-p(\mathrm{cc}|0)}{p_{\min}(\mathrm{cc}|N_B+1)-p(\mathrm{cc}|0)} \leq \frac{p(\mathrm{cc})}{p_{\min}(\mathrm{cc}|N_B+1)}\,. \tag{B.24}$$

With (4.29), we can further show that

$$p_{\min}(\mathrm{cc}|N_B+1) \geq 1-\xi^{N_B+1}-(1-\xi)^{N_B+1}\,. \tag{B.25}$$

Thus, the lower bound in (B.2) is larger than the lower bound derived by Narasimhachar [44] which is the expression in (4.29) for a zero dark-count rate as in

$$p(n \leq N_B) \geq B^{\min}_{n\leq N_B} \geq 1-\frac{p(\mathrm{cc})}{1-\xi^{N_B+1}-(1-\xi)^{N_B+1}}\,. \tag{B.26}$$

The secure key rate should only reduce as we loosen the lower bound for the $(n \leq N_B)$-photon subspace since the flag-state squashing map can be more entanglement-breaking and so Eve could gain more information from purification. As a result, we can use the dark-count-free lower bound blindly on Bob's measurement data to obtain a secure key rate even if the dark-count rate is assumed to be zero.

Appendix C

Explicit Form of p_{pass} and $H(Z|\overline{B})$

For the unbalanced phase-encoded BB84 protocol described in Section 4.2, the passing post-selection probability that appears in the key rate formula (2.44) can be found as

$$\begin{aligned} p_{\text{pass}} = \sum_{b\in\mathbf{K}} & p(x=0,b,\phi_B=0) + p(x=1,b,\phi_B=\frac{\pi}{2}) \\ & + p(x=2,b,\phi_B=0) + p(x=3,b,\phi_B=\frac{\pi}{2}), \end{aligned} \tag{C.1}$$

where $\mathbf{K}$ denotes Bob's post-selected outcomes. This factor takes into account the basis sifting between Alice and Bob as well.

The error correction term for the key rate formula (if we ignore the heuristic classical error-correction efficiency factor f_{EC}) is the entropy of Alice's key register Z conditioned on Bob's register $\overline{B}$ for his post-selected outcomes

$$H(Z|\overline{B}) = -\sum_{z=0}^{1}\sum_{b\in\mathbf{K}}\sum_{\phi_B\in\{0,\frac{\pi}{2}\}} p(z,b,\phi_B)\log\frac{p(z,b,\phi_B)}{p(b,\phi_B)} \tag{C.2}$$

where $p(z,b,\phi_B)$ are normalised probabilities

$$p(z=0,b,\phi_B=0) = p(x=0,b,\phi_B=0)/p_{\text{pass}}\ , \tag{C.3}$$

$$p(z=0,b,\phi_B=\frac{\pi}{2}) = p(x=1,b,\phi_B=\frac{\pi}{2})/p_{\text{pass}}\ , \tag{C.4}$$

$$p(z=1,b,\phi_B=0) = p(x=2,b,\phi_B=0)/p_{\text{pass}}\ , \tag{C.5}$$

$$p(z=1,b,\phi_B=\frac{\pi}{2}) = p(x=3,b,\phi_B=\frac{\pi}{2})/p_{\text{pass}}\ . \tag{C.6}$$

Appendix D

Proof of Decomposing the Privacy Amplification term

In this appendix, we will prove the decomposition of the privacy amplification term for the key rate equation mentioned in Section 4.4.2. In Section 4.3.2, Equations (4.8), (4.11) and (4.12) together describe the entangled pure state that Alice prepares to be

$$|\Psi\rangle_{AA_SA'} = \sum_x \sqrt{p_x}\,|x\rangle_A \otimes \sum_{\widetilde{n}=0}^{\infty} \sqrt{p_{\widetilde{n}}}\,|\widetilde{n}\rangle_{A_S} \otimes |s^x_{\widetilde{n}}\rangle_{A'}$$

where we simplify the notation here with $p_{\widetilde{n}} \coloneqq p_{\widetilde{n}}(\frac{\alpha}{\sqrt{\xi}})$. Since the phase-randomised coherent signal states are block-diagonal in total photon number basis in Eve's point of view, Eve can, without loss of generality, perform QND measurements to determine the total photon number in the signal states. This allows her to keep an extra classical register that tells her the total number of photons in the signal without degrading her eavesdropping power as we will see below.

To see why allowing Eve to measure the total photon number in the signal state will not affect our security statement, we first consider the most general scenario where we do not assume anything about Eve's attack. By Stinespring's dilation theorem, the action of a quantum channel on the signal state can be described by an isometry $V_{A'\to BE}$ that takes Alice's signal system, A', to Bob's system, B, and Eve's purifying system, E, such that the pure state shared among all parties is

$$|\widetilde{\Psi}\rangle_{AA_SBE} = \sum_x \sqrt{p_x}\,|x\rangle_A \otimes \sum_{\widetilde{n}=0}^{\infty} \sqrt{p_{\widetilde{n}}}\,|\widetilde{n}\rangle_{A_S} \otimes V_{A'\to BE}\,|s^x_{\widetilde{n}}\rangle_{A'}\ .$$

Eve's general reduced state conditioned on Alice's measurement outcome x is

$$\rho_E^x = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}} \operatorname{Tr}_B(V_{A'\to BE} \, |s_{\widetilde{n}}^x\rangle\langle s_{\widetilde{n}}^x| \, V_{A'\to BE}^\dagger). \tag{D.1}$$

In the alternative scenario, we assume that Eve performs the QND measurement and could perform adaptive attack according to her knowledge of the photon number. Let Eve's purifying system of the signal be E and the extra register for recording the photon number in Alice's signal be $\widetilde{E}$. Again by Stinespring's dilation theorem, one can describe the action of a quantum channel on the signal state by an isometry $V_{A'\to BE\widetilde{E}}$ which takes the form

$$V_{A'\to BE\widetilde{E}} = \sum_{\widetilde{n}=0}^{\infty} V_{A'\to BE}^{\widetilde{n}} \, \Pi_{\widetilde{n}}^{A'} \otimes |\widetilde{n}\rangle_{\widetilde{E}} \tag{D.2}$$

where $V_{A'\to BE}^{\widetilde{n}}$ is Eve's isometry for purifying Bob's quantum state given that she learns the total photon number $\widetilde{n}$ and $\Pi_{\widetilde{n}}^{A'}$ is a projector which projects onto the $\widetilde{n}$-total photon subspace of the signal system A'. The shared pure state between Alice, Bob and Eve before any announcements is

$$|\Psi\rangle_{AA_SBE\widetilde{E}} = \sum_x \sqrt{p_x} \, |x\rangle_A \otimes \sum_{\widetilde{n}=0}^{\infty} \sqrt{p_{\widetilde{n}}} \, |\widetilde{n}\rangle_{A_S} \otimes V_{A'\to BE}^{\widetilde{n}} \, |s_{\widetilde{n}}^x\rangle_{A'} \otimes |\widetilde{n}\rangle_{\widetilde{E}} \tag{D.3}$$

and Eve's reduced state conditioned on Alice's measurement outcome x is

$$\rho_{E\widetilde{E}}^x = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}} \operatorname{Tr}_B[V_{A'\to BE}^{\widetilde{n}} \, |s_{\widetilde{n}}^x\rangle\langle s_{\widetilde{n}}^x| \, (V_{A'\to BE}^{\widetilde{n}})^\dagger] \otimes |\widetilde{n}\rangle\langle\widetilde{n}|_{\widetilde{E}} \, . \tag{D.4}$$

If we further trace out Eve's register $\widetilde{E}$, her reduced state ρ_E^x clearly contains the general attack in (D.1) where Eve performs the same purification (i.e. $V_{A'\to BE}^{\widetilde{n}} = V_{A'\to BE}$) for all $\widetilde{n} \in \mathbb{N}$. Therefore, the assumption that Eve can measure the photon number of the signal and the pure state shared by all parties to be (D.3) will not affect the security statement of our proof.

To decompose the relative entropy in Equation (2.44), we can assume the pure state shared by all parties to be (D.3) as argued above. Hence, the state shared by Alice and Bob is

$$\rho_{AA_SB} = \sum_{x,y} \sqrt{p_x p_y} \, |x\rangle\langle y|_A \otimes \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}} \, |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \Phi(|s_{\widetilde{n}}^x\rangle\langle s_{\widetilde{n}}^y|), \tag{D.5}$$

where the quantum channel between Alice and Bob is defined as $\Phi(\cdot) \coloneqq \mathrm{Tr}_E(V_{A'\to BE} \cdot V^\dagger_{A'\to BE})$. If we reorder the positions of the three registers in the tensor product and define the conditional state $\rho^{\widetilde{n}}_{AB} = \sum_{x,y} \sqrt{p_x p_y}\ |x\rangle\langle y|_A \otimes \Phi(|s^x_{\widetilde{n}}\rangle\langle s^y_{\widetilde{n}}|)$, the state in (D.5) can be expressed as

$$\rho_{AA_SB} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \rho^{\widetilde{n}}_{AB}\ . \tag{D.6}$$

We will utilise this block-diagonal structure to decompose the relative entropy

$$D(\mathcal{G}(\rho_{AA_SB})||\mathcal{Z}(\mathcal{G}(\rho_{AA_SB})))$$

in the following steps.

According to the definitions of $\mathcal{G}$ and $\mathcal{Z}$ maps stated in Equations (4.30) – (4.33), both maps act trivially on Alice's shield system A_S (i.e. apply $\mathbb{1}_{A_S}$ to the input state). Hence, the unnormalised states $\mathcal{G}(\rho_{AA_SB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AA_SB}))$ are also block-diagonal as in

$$\mathcal{N}(\rho_{AA_SB}) = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \mathcal{N}(\rho^{\widetilde{n}}_{AB}) \tag{D.7}$$

for $\mathcal{N}$ to be the substitute for the maps $\mathcal{G}$ and $\mathcal{Z}\circ\mathcal{G}$. Taking the matrix logarithm gives us

$$\log\mathcal{N}(\rho_{AA_SB}) = \sum_{\widetilde{n}=0}^{\infty} |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes [(\log p_{\widetilde{n}})\mathbb{1} + \log\mathcal{N}(\rho^{\widetilde{n}}_{AB})]. \tag{D.8}$$

By the definition of relative entropy, we decompose the PA term into

$$\begin{aligned}
&D(\mathcal{G}(\rho_{AA_SB})||\mathcal{Z}(\mathcal{G}(\rho_{AA_SB})))\\
=&\mathrm{Tr}\{\mathcal{G}(\rho_{AA_SB})\left[\log\mathcal{G}(\rho_{AA_SB}) - \log\mathcal{Z}(\mathcal{G}(\rho_{AA_SB}))\right]\}\\
=&\sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ \mathrm{Tr}\{\mathcal{G}(\rho^{\widetilde{n}}_{AB})\left[\log\mathcal{G}(\rho^{\widetilde{n}}_{AB}) - \log\mathcal{Z}(\mathcal{G}(\rho^{\widetilde{n}}_{AB})\right]\}\\
=&\sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ D(\mathcal{G}(\rho^{\widetilde{n}}_{AB})||\mathcal{Z}(\mathcal{G}(\rho^{\widetilde{n}}_{AB}))),
\end{aligned} \tag{D.9}$$

which completes the proof.

Appendix E

Justifications for speeding up numerical optimisations

In this appendix, we will cover all three techniques for speeding up the numerical optimisation, which were mentioned in Section 4.4.4.

E.1 Reducing the number of variables

To speed up the optimisation for the problem specified in (4.37), we make use of the structure of the flag-state squashed state. The joint state shared between Alice and Bob ρ_{AB} can be expressed as

$$\rho_{AB} = \sum_{i,j=1}^{d_A} \sum_{n,m=1}^{\infty} \rho_{i,j}^{n,m} E_{i,j} \otimes E_{n,m} \quad , \tag{E.1}$$

where $E_{i,j} = |i\rangle\langle j|$ with $\{|i\rangle\}$ being an orthonormal basis and $\rho_{i,j}^{n,m} \in \mathbb{C} \; \forall \; i, j, n, m$. Recall that the flag-state squashing map takes the form of (4.25):

$$\Lambda(\rho) = \Pi_{\leq N_B} \rho \Pi_{\leq N_B} + \sum_k \mathrm{Tr}(F_k \; \Pi_{>N_B} \; \rho \; \Pi_{>N_B}) |k\rangle\langle k|, \tag{E.2}$$

and since the dimension of the 2-mode ($n \leq N_B$)-photon subspace is $\mathrm{Tr}(\Pi_{n\leq N_B}) = \frac{(N_B+1)(N_B+2)}{2}$, the joint state after squashing can be written as

$$\begin{aligned}
\widetilde{\rho}_{AB} &= (\mathbb{1}_A \otimes \Lambda)\rho_{AB} \\
&= \sum_{i,j=1}^{d_A} \sum_{n,m=1}^{\infty} \rho_{i,j}^{n,m} E_{i,j} \otimes \Lambda(E_{n,m}) \\
&= \sum_{i,j=1}^{d_A} E_{i,j} \otimes \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leq N_B})} \rho_{i,j}^{n,m} E_{n,m} + \sum_{k=1}^{M_B} c_{i,j}^{k} \widetilde{E}_{k,k} \right) \qquad \text{(E.3)} \\
&= (\mathbb{1}_A \otimes \Pi_{n\leq N_B})\rho_{AB}(\mathbb{1}_A \otimes \Pi_{n\leq N_B}) \\
&+ \sum_{k=1}^{M_B} \left(\sum_{i=1}^{d_A} c_{i,i}^{k} E_{i,i} + \sum_{i<j}^{d_A} c_{i,j}^{k} E_{i,j} + (c_{i,j}^{k})^* E_{j,i} \right) \otimes \widetilde{E}_{k,k} \qquad \text{(E.4)}
\end{aligned}$$

where we define $\widetilde{E}_{k,l} = E_{\mathrm{Tr}(\Pi_{n\leq N_B})+k,\, \mathrm{Tr}(\Pi_{n\leq N_B})+l}$, $c_{i,j}^{k} = \mathrm{Tr}[P_k \, (\sum_{n,m=\mathrm{Tr}(\Pi_{n\leq N_B})+1}^{\infty} \rho_{i,j}^{n,m} E_{n,m})]$, and M_B to be the number of POVM elements. Since ρ_{AB} is Hermitian, we also know that

$$(\rho_{i,j}^{n,m})^* = \rho_{j,i}^{m,n} \text{ and } (c_{i,j}^{k})^* = c_{j,i}^{k} \, . \qquad \text{(E.5)}$$

Therefore, we only have to optimize over $(d_A \ \mathrm{Tr}(\Pi_{n\leq N_B}))^2 + d_A^2 \times M_B$ real parameters instead of $[d_A(\mathrm{Tr}(\Pi_{n\leq N_B}) + M_B)]^2$ real parameters if we simply take the squashed state as a $d_A(\mathrm{Tr}(\Pi_{n\leq N_B}) + M_B)$-dimensional density matrix before imposing any optimisation constraints. By reducing the number of parameters, we observe a significant speedup in the optimisation (for $d_A = 4$ and $M_B = 28$).

E.2 Speedup in checking constraints

In the optimisation problem (4.37), to impose each of the constraints require explicit evaluation of the inner product between the updated squashed state ρ and each constraint matrix Γ_μ. As the squashed state and all the constraint matrices in (4.37) admit a block-diagonal structure, we only need to consider the matrix elements of ρ and $\{\Gamma_\mu\}$ that are contained in these blocks to calculate the inner product. We will show that by defining new optimisation variables of smaller dimensions, the optimisation problem (4.37) can be restructured so that each constraint can be checked faster. By doing so, the optimisation problem can be solved quicker.

Let Γ be a squashed constraint matrix, which is Hermitian and can be expressed in the squashed basis as

$$\Gamma = \sum_{i,j=1}^{d_A} E_{i,j} \otimes \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leq N_B})} \Gamma_{i,j}^{n,m} E_{n,m} + \sum_{k,l=1}^{M_B} \Gamma_{i,j}^{k,l} \widetilde{E}_{k,l} \right) \tag{E.6}$$

where $\Gamma_{i,j}^{n,m} \in \mathbb{C}$, and satisfy $(\Gamma_{i,j}^{n,m})^* = \Gamma_{j,i}^{m,n}\ \forall\ i,j,n,m$. We can split $\mathrm{Tr}(\Gamma\widetilde{\rho}_{AB})$ into three terms as in

$$\begin{aligned}
\mathrm{Tr}(\Gamma\widetilde{\rho}_{AB}) &= \sum_{i,j=1}^{d_A} \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{\leq N_B})} \Gamma_{i,j}^{n,m} \rho_{j,i}^{m,n} + \sum_{k=1}^{M_B} \Gamma_{i,j}^{k,k} c_{j,i}^{k} \right) \\
&= \mathrm{Tr}[\Gamma\widetilde{\rho}_{AB}(\mathbb{1}_A \otimes \Pi_{\leq N_B})] + \sum_{k=1}^{M_B} \left(\sum_{i=1}^{d_A} \Gamma_{i,i}^{k,k} c_{i,i}^{k} + \sum_{i>j}^{d_A} [\Gamma_{i,j}^{k,k} c_{j,i}^{k} + (\Gamma_{i,j}^{k,k} c_{j,i}^{k})^*] \right) \qquad \text{(E.7)} \\
&= \mathrm{Tr}(\Gamma\rho_{\leq N_B}) + \sum_{k=1}^{M_B} \left(\sum_{i=1}^{d_A} \Gamma_{i,i}^{k,k} c_{i,i}^{k} + 2\sum_{i>j}^{d_A} \mathrm{Re}(\Gamma_{i,j}^{k,k} c_{j,i}^{k}) \right) \qquad \text{(E.8)} \\
&= \mathrm{Tr}(\Gamma\rho_{\leq N_B}) + \langle \vec{\Gamma}_{\mathrm{flag}} | \vec{c}_{\mathrm{diag}} \rangle + 2\mathrm{Re}(\langle \vec{\Gamma}_{\mathrm{flag}} | \vec{c}_{\mathrm{off}} \rangle), \qquad \text{(E.9)}
\end{aligned}$$

where we define $\rho_{n\leq N_B} = (\mathbb{1}_A \otimes \Pi_{n\leq N_B})\ \rho_{AB}\ (\mathbb{1}_A \otimes \Pi_{n\leq N_B})$, $|\vec{\Gamma}_{\mathrm{flag}}\rangle = \sum_{i,j=1}^{d_A} \sum_{k=1}^{M_B} \Gamma_{i,j}^{k,k} |i\rangle \otimes |j\rangle \otimes |k\rangle$, $|\vec{c}_{\mathrm{diag}}\rangle = \sum_{i=1}^{d_A} \sum_{k=1}^{M_B} c_{i,i}^{k} |i\rangle \otimes |i\rangle \otimes |k\rangle$ and $|\vec{c}_{\mathrm{off}}\rangle = \sum_{i<j}^{d_A} \sum_{k=1}^{M_B} c_{i,j}^{k} |i\rangle \otimes |j\rangle \otimes |k\rangle$. The expression (E.9) requires much fewer calculations in tracing the matrix product in the flag-state subspace (i.e. $\mathrm{span}\{\widetilde{E}_{k,l}\}$).

Define a function $\mathcal{R}(\sigma) = D(\mathcal{G}(\sigma)||\mathcal{Z}(\mathcal{G}(\sigma)))$ and an operator-valued function $\mathcal{M}$ which maps $\rho_{n\leq N_B}$, $|\vec{c}_{\mathrm{diag}}\rangle$ and $|\vec{c}_{\mathrm{off}}\rangle$ to the density matrix $\widetilde{\rho}_{AB}$ of the form in (E.4) where the coefficients can be retrieved from $c_{i,i}^{k} = \langle i,i,k|\vec{c}_{\mathrm{diag}}\rangle$ and $c_{i,j}^{k} = \langle i,j,k|\vec{c}_{\mathrm{off}}\rangle$ with $|i,j,k\rangle \coloneqq |i\rangle \otimes |j\rangle \otimes |k\rangle$. The convex optimisation problem can be restructured into

$$\begin{aligned}
&\text{minimise } \mathcal{R}\left(\mathcal{M}\left(\rho_{n\leq N_B}\ ,\ |\vec{c}_{\mathrm{diag}}\rangle,\ |\vec{c}_{\mathrm{off}}\rangle\right)\right) \\
&\text{subject to} \\
&\quad \mathrm{Tr}(\Gamma_\mu\ \rho_{n\leq N_B}) + \langle \vec{\Gamma}_{\mu,\mathrm{flag}} | \vec{c}_{\mathrm{diag}} \rangle + 2\mathrm{Re}(\langle \vec{\Gamma}_{\mu,\mathrm{flag}} | \vec{c}_{\mathrm{off}} \rangle) = \gamma_\mu\ , \\
&\quad \mathrm{Tr}(\widetilde{\Gamma}_\nu\ \rho_{n\leq N_B}) + \langle \vec{\widetilde{\Gamma}}_{\nu,\mathrm{flag}} | \vec{c}_{\mathrm{diag}} \rangle + 2\mathrm{Re}(\langle \vec{\widetilde{\Gamma}}_{\nu,\mathrm{flag}} | \vec{c}_{\mathrm{off}} \rangle) \geq \widetilde{\gamma}_\nu\ , \\
&\quad \mathcal{M}\left(\rho_{n\leq N_B}\ ,\ |\vec{c}_{\mathrm{diag}}\rangle,\ |\vec{c}_{\mathrm{off}}\rangle\right) \geq 0,
\end{aligned} \tag{E.10}$$

where the free variables for the numerical optimisation are $\rho_{n\leq N_B} \in \mathcal{D}(\mathbb{C}^{d_A \mathrm{Tr}(\Pi_{n\leq N_B})})$, $|\vec{c}_{\mathrm{diag}}\rangle \in \mathbb{R}^{d_A M_B}$, and $|\vec{c}_{\mathrm{off}}\rangle \in \mathbb{C}^{d_A(d_A-1)M_B/2}$.

Since the equality and inequality constraints (133 constraints in (4.37)) have to be checked for each run of the optimisation, reducing the time and memory used in matrix multiplications of $\{\Gamma_\mu\}$ (and $\{\widetilde{\Gamma}_\nu\}$) with the squashed state $\widetilde{\rho}_{AB}$ substantially improves the runtime of the whole key rate calculation.

E.3 Speedup in evaluating $D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB})))$

Recall the definitions of the $\mathcal{G}$ and $\mathcal{Z}$ maps as stated in Equations (4.30) – (4.33). Using the form of the shared state ρ_{AB} specified in Equation (E.3) with $i,j \in \{0,1,2,3\}$ and $M_B = 28$, the state $\mathcal{G}(\rho_{AB})$ can be expanded into

$$\begin{aligned}\mathcal{G}(\rho_{AB}) = \big[&(|0\rangle\langle 0|_R \otimes E^A_{0,0}) \otimes \sigma_{0,0} \\ &+ (|0\rangle\langle 1|_R \otimes E^A_{0,2}) \otimes \sigma_{0,2} \\ &+ (|1\rangle\langle 0|_R \otimes E^A_{2,0}) \otimes \sigma_{2,0} \\ &+ (|1\rangle\langle 1|_R \otimes E^A_{2,2}) \otimes \sigma_{2,2}\big] \otimes |0\rangle\langle 0|_{\widetilde{B}} \\ + \big[&(|0\rangle\langle 0|_R \otimes E^A_{1,1}) \otimes \sigma_{1,1} \\ &+ (|0\rangle\langle 1|_R \otimes E^A_{1,3}) \otimes \sigma_{1,3} \\ &+ (|1\rangle\langle 0|_R \otimes E^A_{3,1}) \otimes \sigma_{3,1} \\ &+ (|1\rangle\langle 1|_R \otimes E^A_{3,3}) \otimes \sigma_{3,3}\big] \otimes |1\rangle\langle 1|_{\widetilde{B}}\,, \end{aligned} \tag{E.11}$$

where $\sigma_{i,j} \coloneqq \mathcal{F}^B_{\alpha(i)} \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leq N_B})} \rho^{n,m}_{i,j} E_{n,m}\right) \mathcal{F}^B_{\alpha(i)} + \mathcal{F}^B_{\alpha(i)} \left(\sum_{k=1}^{28} c^k_{i,j} \widetilde{E}_{k,k}\right) \mathcal{F}^B_{\alpha(i)}$ with $\alpha(i) = i \bmod 2$. Apply the $\mathcal{Z}$ map to $\mathcal{G}(\rho_{AB})$ will get

$$\begin{aligned}\mathcal{Z}(\mathcal{G}(\rho_{AB})) = \big[&(|0\rangle\langle 0|_R \otimes E^A_{0,0}) \otimes \sigma_{0,0} \\ &+ (|1\rangle\langle 1|_R \otimes E^A_{2,2}) \otimes \sigma_{2,2}\big] \otimes |0\rangle\langle 0|_{\widetilde{B}} \\ + \big[&(|0\rangle\langle 0|_R \otimes E^A_{1,1}) \otimes \sigma_{1,1} \\ &+ (|1\rangle\langle 1|_R \otimes E^A_{3,3}) \otimes \sigma_{3,3}\big] \otimes |1\rangle\langle 1|_{\widetilde{B}}\,. \end{aligned} \tag{E.12}$$

Since Bob's basis announcement partitions $\mathcal{G}(\rho_{AB})$ into 2 orthogonal subspaces with the orthogonal projections and his quantum system B is further partitioned into 2 orthogonal subspaces (i.e. ($n \leq N_B$)-photon subspace and the flag-state subspace), $\mathcal{G}(\rho_{AB})$ as shown in Equation (E.11) can be broken down into 4 orthogonal subspaces.

Restricting to the image of map $\mathcal{G}$, matrices $\mathcal{G}(\rho_{AB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AB}))$ can be simplified

to

$$\mathcal{G}(\rho_{AB}) = \begin{pmatrix} \sigma_{0,0} & \sigma_{0,2} & 0 & 0 \\ \sigma_{2,0} & \sigma_{2,2} & 0 & 0 \\ 0 & 0 & \sigma_{1,1} & \sigma_{1,3} \\ 0 & 0 & \sigma_{1,3} & \sigma_{3,3} \end{pmatrix}, \tag{E.13}$$

$$\mathcal{Z}(\mathcal{G}(\rho_{AB})) = \begin{pmatrix} \sigma_{0,0} & 0 & 0 & 0 \\ 0 & \sigma_{2,2} & 0 & 0 \\ 0 & 0 & \sigma_{1,1} & 0 \\ 0 & 0 & 0 & \sigma_{3,3} \end{pmatrix}. \tag{E.14}$$

Recall the definition of relative entropy: $D(\rho||\sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma)$, which is finite if $\ker(\sigma) \subseteq \ker(\rho)$. We can restrict to non-zero subspaces and express the objective function as in Equation (E.17) below.

$$\mathrm{Tr}(\mathcal{G}(\rho_{AB}) \log \mathcal{G}(\rho_{AB})) = \sum_{i=0}^{1} \left[\mathrm{Tr}\left(\tau_i^{\leq N_B} \log \tau_i^{\leq N_B}\right) + \mathrm{Tr}\left(\tau_i^{\mathrm{flag}} \log \tau_i^{\mathrm{flag}}\right) \right], \tag{E.15}$$

$$\mathrm{Tr}(\mathcal{G}(\rho_{AB}) \log \mathcal{Z}(\mathcal{G}(\rho_{AB}))) = \sum_{i=0}^{1} \left[\mathrm{Tr}\left(\tau_i^{\leq N_B} \log \mathcal{P}(\tau_i^{\leq N_B})\right) + \mathrm{Tr}\left(\tau_i^{\mathrm{flag}} \log \mathcal{P}(\tau_i^{\mathrm{flag}})\right) \right], \tag{E.16}$$

$$\boxed{D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB}))) = \sum_{i=0}^{1} \left[D\left(\tau_i^{\leq N_B}||\mathcal{P}(\tau_i^{\leq N_B})\right) + D\left(\tau_i^{\mathrm{flag}}||\mathcal{P}(\tau_i^{\mathrm{flag}})\right) \right]}, \tag{E.17}$$

$$\tau_i^{\beta} \coloneqq \begin{pmatrix} \sigma_{i,i}^{\beta} & \sigma_{i,i+2}^{\beta} \\ \sigma_{i+2,i}^{\beta} & \sigma_{i+2,i+2}^{\beta} \end{pmatrix}, \quad \mathcal{P}(\tau_i^{\beta}) \coloneqq \begin{pmatrix} \sigma_{i,i}^{\beta} & 0 \\ 0 & \sigma_{i+2,i+2}^{\beta} \end{pmatrix} \quad \text{with } \beta \in \{\leq N_B, \mathrm{flag}\}, \tag{E.18}$$

where we define the matrices $\sigma_{i,j}^{n \leq N_B} \coloneqq \mathcal{F}_{\alpha(i)}^{B} \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n \leq N_B})} \rho_{i,j}^{n,m} E_{n,m} \right) \mathcal{F}_{\alpha(i)}^{B}$ and $\sigma_{i,j}^{\mathrm{flag}} \coloneqq \mathcal{F}_{\alpha(i)}^{B} \left(\sum_{k=1}^{28} c_{i,j}^{k} \widetilde{E}_{k,k} \right) \mathcal{F}_{\alpha(i)}^{B}$.

The objective function in (E.17) only requires diagonalisation and the logarithms of the smaller matrices τ_i^{β} and $\mathcal{P}(\tau_i^{\beta})$ for $i \in \{0, 1\}$ and $\beta \in \{n \leq N_B, \mathrm{flag}\}$. Therefore, the expression in (E.17) can be computed much quicker than if we directly calculate the relative entropy with the full matrices $\mathcal{G}(\rho_{AB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AB}))$.

E.4 Speedup in evaluating the perturbed objective function

In the step of linearising the convex optimisation problem, the gradient of the objective function has to be evaluated at the suboptimal point obtained from the first step [2]. As pointed out in Section 3.2 of Ref. [2], the gradient is undefined if the matrix $\mathcal{G}(\rho_{AB})$ is not full rank. Besides, due to the finite numerical precision of a computer, the computed matrix $\mathcal{G}(\rho_{AB})$ may have negative eigenvalues for which the objective function is undefined. In these cases, we perform a perturbation on the matrix $\mathcal{G}(\rho_{AB})$ by applying a depolarising channel which gives the perturbed map $\mathcal{G}_\epsilon(\rho_{AB})$, as defined in Ref. [2],

$$\begin{aligned}\mathcal{G}_\epsilon(\rho_{AB}) &\coloneqq (1-\epsilon)\mathcal{G}(\rho_{AB}) + \frac{\epsilon}{d'}\mathbb{1}_{d'} \\ &= (1-\epsilon)\mathcal{G}(\rho_{AB}) + \frac{\epsilon}{d'}\mathbb{1}|_{\mathrm{Im}(\mathcal{G})} + \frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\ ,\end{aligned} \tag{E.19}$$

where $\epsilon > 0$ is the perturbation parameter and $d' = \dim(\mathcal{G}(\rho_{AB}))$. Applying the $\mathcal{Z}$ map to (E.19) results in

$$\mathcal{Z}(\mathcal{G}_\epsilon(\rho_{AB})) = (1-\epsilon)\mathcal{Z}(\mathcal{G}(\rho_{AB})) + \frac{\epsilon}{d'}\mathbb{1}|_{\mathrm{Im}(\mathcal{G})} + \frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\ . \tag{E.20}$$

The new objective function $D(\mathcal{G}_\epsilon(\rho_{AB})||\mathcal{Z}(\mathcal{G}_\epsilon(\rho_{AB})))$ is the relative entropy of the two perturbed matrices (E.19) and (E.20). We now show that the evaluation of the relative entropy can be restricted to the image of the map $\mathcal{G}$. We evaluate the matrix logarithms

$$\log \mathcal{G}_\epsilon(\rho_{AB}) = \log\left[(1-\epsilon)\mathcal{G}(\rho_{AB}) + \frac{\epsilon}{d'}\mathbb{1}|_{\mathrm{Im}(\mathcal{G})}\right] + \log\left(\frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\right), \tag{E.21}$$

$$\log \mathcal{Z}(\mathcal{G}_\epsilon(\rho_{AB})) = \log\left[(1-\epsilon)\mathcal{Z}(\mathcal{G}(\rho_{AB})) + \frac{\epsilon}{d'}\mathbb{1}|_{\mathrm{Im}(\mathcal{G})}\right] + \log\left(\frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\right). \tag{E.22}$$

and define $\widetilde{\mathcal{G}}_\epsilon(\rho_{AB}) \coloneqq \Pi_{\mathrm{Im}(\mathcal{G})}\mathcal{G}_\epsilon(\rho_{AB})\Pi_{\mathrm{Im}(\mathcal{G})}$ to obtain

$$\begin{aligned} D(\mathcal{G}_\epsilon(\rho_{AB})||\mathcal{Z}(\mathcal{G}_\epsilon(\rho_{AB}))) &= \mathrm{Tr}\{\mathcal{G}_\epsilon(\rho_{AB})\left[\log \mathcal{G}_\epsilon(\rho_{AB}) - \log \mathcal{Z}(\mathcal{G}_\epsilon(\rho_{AB}))\right]\} && \text{(E.23)} \\ &= \mathrm{Tr}\{\widetilde{\mathcal{G}}_\epsilon(\rho_{AB})[\log \widetilde{\mathcal{G}}_\epsilon(\rho_{AB}) - \log \mathcal{Z}(\widetilde{\mathcal{G}}_\epsilon(\rho_{AB}))]\} && \text{(E.24)} \\ &= D(\widetilde{\mathcal{G}}_\epsilon(\rho_{AB})||\mathcal{Z}(\widetilde{\mathcal{G}}_\epsilon(\rho_{AB}))). && \text{(E.25)}\end{aligned}$$

The step going from (E.23) to (E.24) comes from the fact that Equation (E.21) minus (E.22) results in the zero operator in the kernel of map $\mathcal{G}$. Now that we only have to

consider the image of $\mathcal{G}$ in (E.25), we can use the decomposition described in Equation (E.17) but with the matrices τ_i^β and $\mathcal{P}(\tau_i^\beta)$ replaced by $\widetilde{\tau}_i^\beta$ and $\mathcal{P}(\widetilde{\tau}_i^\beta)$ respectively, which are defined as

$$\widetilde{\tau}_i^\beta \coloneqq (1-\epsilon)\tau_i^\beta + \frac{\epsilon}{d'}(\mathbb{1}_\beta \oplus \mathbb{1}_\beta), \tag{E.26}$$

$$\mathcal{P}(\widetilde{\tau}_i^\beta) \coloneqq (1-\epsilon)\mathcal{P}(\tau_i^\beta) + \frac{\epsilon}{d'}(\mathbb{1}_\beta \oplus \mathbb{1}_\beta) \tag{E.27}$$

with $\beta \in \{n \leq N_B, \text{flag}\}$. Since we can break down the evaluation of the perturbed objective function into calculations on restricted subspaces, the speedup described in Appendix E.3 applies here.

Appendix F

Simulated Statistics with a Loss-only Channel

In this appendix, we will derive Bob's measurement outcome probabilities from an experimental simulation that has the quantum channel as a loss-only channel. Suppose that Alice sends out the 2-mode coherent signal state of choice x (see Equation (4.9))

$$|\psi_x^{\theta=0}(\alpha)\rangle_{A'} = |\sqrt{\xi}\alpha, \sqrt{1-\xi}e^{-i\phi_x}\alpha\rangle. \tag{F.1}$$

We ignore the phase randomisation here since it does not affect Bob's measurement outcome statistics. The loss-only channel is effectively a beam splitter with transmissivity η. When it is applied to the signal state $|\psi_x^{\theta=0}(\alpha)\rangle_{A'}$, the output is another 2-mode coherent state with a reduced overall amplitude

$$|\alpha', \beta\rangle \coloneqq |\sqrt{\eta\xi}\alpha, \sqrt{\eta(1-\xi)}e^{-i\phi_x}\alpha\rangle. \tag{F.2}$$

We first calculate the overlap between the 2-mode coherent state $|\alpha', \beta\rangle$ with a general 4-mode (in spatial-temporal modes before Bob's detectors) state

$$\begin{aligned}
&\langle\alpha', \beta|(b_{t_1}^\dagger)^i(b_{t_3}^\dagger)^j(b_{2,\phi_B}^\dagger)^k(b_{5,\phi_B}^\dagger)^m|0,0\rangle \\
=&\langle\alpha', \beta|(\sqrt{\xi}\ a_1^\dagger)^i(\sqrt{1-\xi}\ a_2^\dagger)^j(\sqrt{\frac{1-\xi}{2}}\ a_1^\dagger - e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\ a_2^\dagger)^k(\sqrt{\frac{1-\xi}{2}}\ a_1^\dagger + e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\ a_2^\dagger)^m|0,0\rangle \\
=&(\sqrt{\xi}\alpha'^*)^i(\sqrt{1-\xi}\beta^*)^j(\sqrt{\frac{1-\xi}{2}}\alpha'^* - e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^k(\sqrt{\frac{1-\xi}{2}}\alpha'^* + e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^m\langle\alpha', \beta|0,0\rangle \\
=&(\sqrt{\xi}\alpha'^*)^i(\sqrt{1-\xi}\beta^*)^j(\sqrt{\frac{1-\xi}{2}}\alpha'^* - e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^k(\sqrt{\frac{1-\xi}{2}}\alpha'^* + e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^m e^{-\frac{|\alpha'|^2+|\beta|^2}{2}}
\end{aligned} \tag{F.3}$$

With the expression (F.3), we can derive all of Bob's **dark count free** outcome probabilities conditioned on Alice chooses signal x in the following:

- Ideal no-click probability:

$$p(0|x) = |\langle \alpha', \beta|0,0\rangle|^2 = e^{-(|\alpha'|^2+|\beta|^2)} = e^{-(\eta\xi+\eta(1-\xi))|\alpha|^2} = e^{-\eta|\alpha|^2} \tag{F.4}$$

- Ideal single-click probabilities:

$$\begin{aligned}
p(2,\phi_B|x) &= \langle \alpha', \beta| \left(p(\phi_B) \sum_{n=1}^{\infty} \frac{1}{n!} (b^\dagger_{2,\phi_B})^n |0,0\rangle\langle 0,0| b^n_{2,\phi_B} \right) |\alpha', \beta\rangle \\
&= p(\phi_B) \sum_{n=1}^{\infty} \frac{1}{n!} |\langle \alpha', \beta| (b^\dagger_{2,\phi_B})^n |0,0\rangle|^2 \\
&= p(\phi_B) \sum_{n=1}^{\infty} \frac{1}{n!} \left| \left(\sqrt{\frac{1-\xi}{2}} \alpha'^* - e^{-i\phi_B} \sqrt{\frac{\xi}{2}} \beta^* \right)^n e^{-\frac{|\alpha'|^2+|\beta|^2}{2}} \right|^2 \\
&= p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=1}^{\infty} \frac{1}{n!} \left| \sqrt{\frac{1-\xi}{2}} e^{i\phi_B} \alpha'^* - \sqrt{\frac{\xi}{2}} \beta^* \right|^{2n} \\
&= p(\phi_B) e^{-\eta|\alpha|^2} \left(\exp \left| \sqrt{\frac{1-\xi}{2}} e^{i\phi_B} \sqrt{\eta\xi} \alpha^* - \sqrt{\frac{\xi}{2}} \sqrt{\eta(1-\xi)} e^{i\phi_x} \alpha^* \right|^2 - 1 \right) \\
&= p(\phi_B) e^{-\eta|\alpha|^2} \left[\exp \left(\frac{\eta\xi(1-\xi)}{2} |\alpha|^2 |e^{i\phi_B} - e^{i\phi_x}|^2 \right) - 1 \right] \\
&= p(\phi_B) e^{-\eta|\alpha|^2} \left[\exp \left(\frac{\eta\xi(1-\xi)}{2} |\alpha|^2 (2 - e^{i(\phi_B-\phi_x)} - e^{-i(\phi_B-\phi_x)}) \right) - 1 \right] \\
&= p(\phi_B) e^{-\eta|\alpha|^2} (e^{\eta\xi(1-\xi)|\alpha|^2(1-\cos(\phi_B-\phi_x))} - 1).
\end{aligned} \tag{F.5}$$

Similarly, by turning the minus sign in $b^\dagger_{2,\phi_B}$ into a plus in $b^\dagger_{5,\phi_B}$ gets us

$$\begin{aligned}
p(5,\phi_B|x) &= p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=1}^{\infty} \frac{1}{n!} \left| \sqrt{\frac{1-\xi}{2}} e^{i\phi_B} \alpha'^* + \sqrt{\frac{\xi}{2}} \beta^* \right|^{2n} \\
&= p(\phi_B) e^{-\eta|\alpha|^2} \left[\exp \left(\frac{\eta\xi(1-\xi)}{2} |\alpha|^2 |e^{i\phi_B} + e^{i\phi_x}|^2 \right) - 1 \right] \\
&= p(\phi_B) e^{-\eta|\alpha|^2} (e^{\eta\xi(1-\xi)|\alpha|^2(1+\cos(\phi_B-\phi_x))} - 1),
\end{aligned} \tag{F.6}$$

$$p(t_1|x) = \langle\alpha',\beta|\left(\sum_{n=1}^{\infty}\frac{1}{n!}(b_{t_1}^{\dagger})^n|0,0\rangle\langle 0,0|b_{t_1}^n\right)|\alpha',\beta\rangle$$
$$= e^{-(|\alpha'|^2+|\beta|^2)}\sum_{n=1}^{\infty}\frac{(\xi|\alpha'|^2)^n}{n!}$$
$$= e^{-\eta|\alpha|^2}(e^{\xi|\alpha'|^2}-1) = e^{-\eta|\alpha|^2}(e^{\eta\xi^2|\alpha|^2}-1), \tag{F.7}$$

$$p(t_3|x) = \langle\alpha',\beta|\left(\sum_{n=1}^{\infty}\frac{1}{n!}(b_{t_3}^{\dagger})^n|0,0\rangle\langle 0,0|b_{t_3}^n\right)|\alpha',\beta\rangle$$
$$= e^{-(|\alpha'|^2+|\beta|^2)}\sum_{n=1}^{\infty}(1-\xi)^n\frac{|\beta|^{2n}}{n!}$$
$$= e^{-\eta|\alpha|^2}(e^{(1-\xi)|\beta|^2}-1) = e^{-\eta|\alpha|^2}(e^{\eta(1-\xi)^2|\alpha|^2}-1). \tag{F.8}$$

- Ideal double-click probabilities:

$$p(t_1,t_3|x) = \sum_{n=2}^{\infty}\sum_{k=1}^{n-1}\frac{1}{(n-k)!k!}|\langle\alpha',\beta|(b_{t_1}^{\dagger})^{n-k}(b_{t_3}^{\dagger})^k|0,0\rangle|^2$$
$$= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}\sum_{k=1}^{n-1}\binom{n}{k}(\xi|\alpha'|^2)^{n-k}[(1-\xi)|\beta|^2]^k$$
$$= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}[(\xi|\alpha'|^2+(1-\xi)|\beta|^2)^n-(\xi|\alpha'|^2)^n-((1-\xi)|\beta|^2)^n]$$
$$= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}(\eta|\alpha|^2)^n[(\xi^2+(1-\xi)^2)^n-\xi^{2n}-(1-\xi)^{2n}]$$
$$= e^{-\eta|\alpha|^2}(e^{\eta|\alpha|^2(\xi^2+(1-\xi)^2)}-e^{\eta|\alpha|^2\xi^2}-e^{\eta|\alpha|^2(1-\xi)^2}+1), \tag{F.9}$$

$$\langle\alpha',\beta|(b_{2,\phi_B}^{\dagger})^{n-k}(b_{5,\phi_B}^{\dagger})^k|0,0\rangle$$
$$=\left(\sqrt{\frac{1-\xi}{2}}\alpha'^{*}-e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*\right)^{n-k}\left(\sqrt{\frac{1-\xi}{2}}\alpha'^{*}+e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*\right)^{k}e^{-\frac{|\alpha'|^2+|\beta|^2}{2}}$$
$$=e^{-\frac{\eta|\alpha|^2}{2}}\frac{(\sqrt{\eta\xi(1-\xi)}\alpha^*)^n}{\sqrt{2^n}}\sum_{j=0}^{n-k}\binom{n-k}{j}e^{i\phi_B(n-k-j)}(-e^{i\phi_x})^j\sum_{r=0}^{k}\binom{k}{r}e^{i\phi_B(k-r)}e^{i\phi_x r}$$
$$=e^{-\frac{\eta|\alpha|^2}{2}}(\alpha^*\sqrt{\eta\xi(1-\xi)/2})^n(e^{i\phi_B}-e^{i\phi_x})^{n-k}(e^{i\phi_B}+e^{i\phi_x})^k, \tag{F.10}$$

$$
\begin{aligned}
p(2,5,\phi_B|x) &= \sum_{n=2}^{\infty}\sum_{k=1}^{n-1}\frac{p(\phi_B)}{(n-k)!k!}|\langle\alpha',\beta|(b_{2,\phi_B}^{\dagger})^{n-k}(b_{5,\phi_B}^{\dagger})^{k}|0,0\rangle|^2 \\
&= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{p(\phi_B)}{n!}\left(\frac{\eta\xi(1-\xi)}{2}|\alpha|^2\right)^n\sum_{k=1}^{n-1}\binom{n}{k}|e^{i\phi_B}-e^{i\phi_x}|^{2(n-k)}|e^{i\phi_B}+e^{i\phi_x}|^{2k} \\
&= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{p(\phi_B)}{n!}\left(\eta\xi(1-\xi)|\alpha|^2\right)^n\left[2^n-(1-\cos(\phi_B-\phi_x))^n-(1+\cos(\phi_B-\phi_x))^n\right] \\
&= p(\phi_B)e^{-\eta|\alpha|^2}[e^{2\eta\xi(1-\xi)|\alpha|^2}-e^{\eta\xi(1-\xi)|\alpha|^2(1-\cos(\phi_B-\phi_x))}-e^{\eta\xi(1-\xi)|\alpha|^2(1+\cos(\phi_B-\phi_x))}+1],
\end{aligned}
\tag{F.11}
$$

$$
\begin{aligned}
\langle\alpha',\beta|(b_{t_1}^{\dagger})^{n-k}(b_{2,\phi_B}^{\dagger})^{k}|0\rangle &= (\sqrt{\xi}\alpha'^{*})^{n-k}(\sqrt{\frac{1-\xi}{2}}\alpha'^{*}-e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^{*})^{k}e^{-\frac{|\alpha'|^2+|\beta|^2}{2}} \\
&= e^{-\frac{\eta|\alpha|^2}{2}}\sqrt{\xi}^{2n-k}\sqrt{\frac{1-\xi}{2}}^{k}(\sqrt{\eta}\alpha^{*})^{n}\sum_{r=0}^{k}\binom{k}{r}e^{i\phi_B(k-r)}(-e^{i\phi_x})^{r} \\
&= e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^{*})^{n}\sqrt{\xi}^{2n-k}\sqrt{\frac{1-\xi}{2}}^{k}(e^{i\phi_B}-e^{i\phi_x})^{k},
\end{aligned}
\tag{F.12}
$$

$$
\begin{aligned}
p(t_1,2,\phi_B|x) &= \sum_{n=2}^{\infty}\sum_{k=1}^{n-1}\frac{p(\phi_B)}{(n-k)!k!}|\langle\alpha',\beta|(b_{t_1}^{\dagger})^{n-k}(b_{2,\phi_B}^{\dagger})^{k}|0\rangle|^2 \\
&= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{p(\phi_B)}{n!}\left(\eta\xi|\alpha|^2\right)^n\sum_{k=1}^{n-1}\binom{n}{k}\xi^{n-k}[(1-\xi)\frac{|e^{i\phi_B}-e^{i\phi_x}|^2}{2}]^k \\
&= e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{p(\phi_B)}{n!}\left(\eta\xi|\alpha|^2\right)^n\sum_{k=1}^{n-1}\binom{n}{k}\xi^{n-k}[(1-\xi)(1-\cos(\phi_B-\phi_x))]^k \\
&= p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}\left(\eta\xi|\alpha|^2\right)^n\{(\xi+(1-\xi)\cos(\phi_B-\phi_x))^n-\xi^n \\
&\qquad\qquad -[(1-\xi)(1-\cos(\phi_B-\phi_x))]^n\} \\
&= p(\phi_B)e^{-\eta|\alpha|^2}[e^{\eta\xi(\xi+(1-\xi)\cos(\phi_B-\phi_x))|\alpha|^2}-e^{\eta\xi^2|\alpha|^2}-e^{\eta\xi(1-\xi)|\alpha|^2(1-\cos(\phi_B-\phi_x))}+1].
\end{aligned}
\tag{F.13}
$$

Again, by turning the minus sign in $b_{2,\phi_B}^{\dagger}$ into a plus in $b_{5,\phi_B}^{\dagger}$ (i.e. $e^{i\phi_B}-e^{i\phi_x}\to e^{i\phi_B}+e^{i\phi_x}$):

$$
p(t_1,5,\phi_B|x) = p(\phi_B)e^{-\eta|\alpha|^2}[e^{\eta\xi(1-\xi\cos(\phi_B-\phi_x))|\alpha|^2}-e^{\eta\xi^2|\alpha|^2}-e^{\eta\xi(1-\xi)|\alpha|^2(1+\cos(\phi_B-\phi_x))}+1].
\tag{F.14}
$$

$$\begin{aligned}\langle\alpha',\beta|(b_{t_3}^\dagger)^{n-k}(b_{2,\phi_B}^\dagger)^k|0\rangle &= (\sqrt{1-\xi}\beta^*)^{n-k}(\sqrt{\frac{1-\xi}{2}}\alpha'^* - e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^k e^{-\frac{|\alpha'|^2+|\beta|^2}{2}} \\ &= e^{in\phi_x}e^{-\frac{\eta|\alpha|^2}{2}}\sqrt{1-\xi}^{2n-k}\sqrt{\frac{\xi}{2}}^k(\sqrt{\eta}\alpha^*)^n\sum_{r=0}^{k}\binom{k}{r}e^{i(\phi_B-\phi_x)r}(-1)^{k-r} \\ &= e^{in\phi_x}e^{-\frac{\eta|\alpha|^2}{2}}\sqrt{1-\xi}^{2n-k}\sqrt{\frac{\xi}{2}}^k(\sqrt{\eta}\alpha^*)^n[e^{i(\phi_B-\phi_x)}-1]^k, \qquad \text{(F.15)}\end{aligned}$$

$$\begin{aligned}p(t_3,2,\phi_B|x) &= \sum_{n=2}^{\infty}\sum_{k=1}^{n-1}\frac{p(\phi_B)}{(n-k)!k!}|\langle\alpha',\beta|(b_{t_3}^\dagger)^{n-k}(b_{2,\phi_B}^\dagger)^k|0\rangle|^2 \\ &= p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}\left(\eta(1-\xi)|\alpha|^2\right)^n\sum_{k=1}^{n-1}\binom{n}{k}(1-\xi)^{n-k}\left(\xi\frac{|e^{i(\phi_B-\phi_x)}-1|^2}{2}\right)^k \\ &= p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}\left(\eta(1-\xi)|\alpha|^2\right)^n\sum_{k=1}^{n-1}\binom{n}{k}(1-\xi)^{n-k}[\xi(1-\cos(\phi_B-\phi_x))]^k \\ &= p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=2}^{\infty}\frac{1}{n!}\left(\eta(1-\xi)|\alpha|^2\right)^n\{(1-\xi\cos(\phi_B-\phi_x))^n-(1-\xi)^n \\ &\qquad -[\xi(1-\cos(\phi_B-\phi_x))]^n\} \\ &= p(\phi_B)e^{-\eta|\alpha|^2}[e^{\eta(1-\xi)(1-\xi\cos(\phi_B-\phi_x))|\alpha|^2}-e^{\eta(1-\xi)^2|\alpha|^2}-e^{\eta\xi(1-\xi)|\alpha|^2(1-\cos(\phi_B-\phi_x))}+1]. \qquad \text{(F.16)}\end{aligned}$$

Again, by turning the minus sign in $b_{2,\phi_B}^\dagger$ into a plus in $b_{5,\phi_B}^\dagger$ (i.e. $e^{i\phi_B}-e^{i\phi_x}\to e^{i\phi_B}+e^{i\phi_x}$):

$$p(t_3,5,\phi_B|x) = p(\phi_B)e^{-\eta|\alpha|^2}[e^{\eta(1-\xi)(1+\xi\cos(\phi_B-\phi_x))|\alpha|^2}-e^{\eta(1-\xi)^2|\alpha|^2}-e^{\eta\xi(1-\xi)|\alpha|^2(1+\cos(\phi_B-\phi_x))}+1]. \qquad \text{(F.17)}$$

- Ideal triple-click probabilities:

$$\begin{aligned}&\langle\alpha',\beta|(b_{t_1}^\dagger)^{n-k-j}(b_{t_3}^\dagger)^k(b_{2,\phi_B}^\dagger)^j|0\rangle \\ =&(\sqrt{\xi}\alpha'^*)^{n-k-j}(\sqrt{1-\xi}\beta^*)^k\left(\sqrt{\frac{1-\xi}{2}}\alpha'^*-e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*\right)^j e^{-\frac{|\alpha'|^2+|\beta|^2}{2}} \\ =&e^{ik\phi_x}e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^*)^n\frac{1}{\sqrt{2^j}}\sqrt{\xi}^{2(n-k)-j}\sqrt{1-\xi}^{2k+j}\sum_{r=0}^{j}\binom{j}{r}e^{i\phi_B(j-r)}(-e^{i\phi_x})^r \\ =&e^{ik\phi_x}e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^*)^n\frac{1}{\sqrt{2^j}}\sqrt{\xi}^{2(n-k)-j}\sqrt{1-\xi}^{2k+j}(e^{i\phi_B}-e^{i\phi_x})^j. \qquad \text{(F.18)}\end{aligned}$$

Using the substitutions for index $r = j + k$ and the variable $C \coloneqq \cos(\phi_B - \phi_x)$,

$$
\begin{aligned}
& p(t_1, t_3, 2, \phi_B|x) \\
=& \sum_{n=3}^{\infty} \sum_{k=1}^{n-2} \sum_{j=1}^{n-k-1} \frac{p(\phi_B)}{(n-k-j)!k!j!} |\langle \alpha', \beta| (b_{t_1}^\dagger)^{n-k-j} (b_{t_3}^\dagger)^k (b_{2,\phi_B}^\dagger)^j |0\rangle|^2 \\
=& p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=3}^{\infty} \frac{(\eta|\alpha|^2)^n}{n!} \sum_{r=2}^{n-1} \binom{n}{r} \xi^{2(n-r)} (1-\xi)^{2r} \sum_{j=1}^{r-1} \binom{r}{j} (\frac{\xi}{1-\xi} \cdot \frac{|e^{i\phi_B} - e^{i\phi_x}|^2}{2})^j \\
=& p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=3}^{\infty} \frac{(\eta|\alpha|^2)^n}{n!} \sum_{r=2}^{n-1} \binom{n}{r} \xi^{2(n-r)} (1-\xi)^{2r} \sum_{j=1}^{r-1} \binom{r}{j} [\frac{\xi}{1-\xi} (1 - \cos(\phi_B - \phi_x)]^j \\
=& p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=3}^{\infty} \frac{(\eta|\alpha|^2)^n}{n!} \sum_{r=2}^{n-1} \binom{n}{r} \xi^{2(n-r)} (1-\xi)^{2r} \{[1 + \frac{\xi(1-C)}{1-\xi}]^r - [\frac{\xi(1-C)}{1-\xi}]^r - 1\} \\
=& p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=3}^{\infty} \frac{(\eta|\alpha|^2)^n}{n!} \sum_{r=2}^{n-1} \binom{n}{r} \xi^{2(n-r)} (1-\xi)^{r} \{(1-\xi C)^r - [\xi(1-C)]^r - (1-\xi)^r\} \\
=& p(\phi_B) e^{-\eta|\alpha|^2} \sum_{n=3}^{\infty} \frac{(\eta|\alpha|^2)^n}{n!} \{[\xi^2 + (1-\xi)(1-\xi C)]^n - [(1-\xi)(1-\xi C)]^n \\
& \qquad - [\xi^2 + \xi(1-\xi)(1-C)]^n + [\xi(1-\xi)(1-C)]^n \\
& \qquad - [\xi^2 + (1-\xi)^2]^n + \xi^{2n} + (1-\xi)^{2n}\} \\
=& p(\phi_B) e^{-\eta|\alpha|^2} [e^{\eta[\xi^2 + (1-\xi)(1-\xi C)]|\alpha|^2} - e^{\eta(1-\xi)(1-\xi C)|\alpha|^2} - e^{\eta[\xi^2 + \xi(1-\xi)(1-C)]|\alpha|^2} \\
& \qquad + e^{\eta\xi(1-\xi)(1-C)|\alpha|^2} - e^{\eta[\xi^2 + (1-\xi)^2]|\alpha|^2} + e^{\eta\xi^2|\alpha|^2} + e^{\eta(1-\xi)^2|\alpha|^2} - 1]. \qquad \text{(F.19)}
\end{aligned}
$$

Again, by turning the minus sign in $b_{2,\phi_B}^\dagger$ into a plus in $b_{5,\phi_B}^\dagger$ (i.e. $e^{i\phi_B} - e^{i\phi_x} \to e^{i\phi_B} + e^{i\phi_x}$):

$$
\begin{aligned}
p(t_1, t_3, 5, \phi_B|x) = p(\phi_B) e^{-\eta|\alpha|^2} & [e^{\eta[\xi^2 + (1-\xi)(1+\xi C)]|\alpha|^2} - e^{\eta(1-\xi)(1+\xi C)|\alpha|^2} - e^{\eta[\xi^2 + \xi(1-\xi)(1+C)]|\alpha|^2} \\
& + e^{\eta\xi(1-\xi)(1+C)|\alpha|^2} - e^{\eta[\xi^2 + (1-\xi)^2]|\alpha|^2} + e^{\eta\xi^2|\alpha|^2} + e^{\eta(1-\xi)^2|\alpha|^2} - 1]. \qquad \text{(F.20)}
\end{aligned}
$$

$$
\begin{aligned}
&\langle\alpha',\beta|(b_{t_1}^\dagger)^{n-k-j}(b_{2,\phi_B}^\dagger)^k(b_{5,\phi_B}^\dagger)^j|0\rangle\\
=&(\sqrt{\xi}\alpha'^*)^{n-k-j}(\sqrt{\frac{1-\xi}{2}}\alpha'^*-e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^k(\sqrt{\frac{1-\xi}{2}}\alpha'^*+e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^j e^{-\frac{|\alpha'|^2+|\beta|^2}{2}}\\
=&e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^*)^n\sqrt{\xi}^{2n-k-j}\sqrt{\frac{1-\xi}{2}}^{k+j}\sum_{s=0}^{k}\binom{k}{s}e^{i\phi_B(k-s)}(-e^{i\phi_x})^s\sum_{r=0}^{j}\binom{j}{r}e^{i\phi_B(j-r)}e^{i\phi_x r}\\
=&e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^*)^n\sqrt{\xi}^{2n-k-j}\sqrt{\frac{1-\xi}{2}}^{k+j}(e^{i\phi_B}-e^{i\phi_x})^k(e^{i\phi_B}+e^{i\phi_x})^j, \qquad \text{(F.21)}
\end{aligned}
$$

$$
\begin{aligned}
&p(t_1,2,5,\phi_B|x)\\
=&\sum_{n=3}^{\infty}\sum_{k=1}^{n-2}\sum_{j=1}^{n-k-1}\frac{p(\phi_B)}{(n-k-j)!k!j!}|\langle\alpha',\beta|(b_{t_1}^\dagger)^{n-k-j}(b_{2,\phi_B}^\dagger)^k(b_{5,\phi_B}^\dagger)^j|0\rangle|^2\\
=&p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=3}^{\infty}\frac{(\eta\xi|\alpha|^2)^n}{n!}\sum_{r=2}^{n-1}\binom{n}{r}\xi^{n-r}(\frac{1-\xi}{2})^r\sum_{j=1}^{r-1}\binom{r}{j}|e^{i\phi_B}-e^{i\phi_x}|^{2(r-j)}|e^{i\phi_B}+e^{i\phi_x}|^{2j}\\
=&p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=3}^{\infty}\frac{(\eta\xi|\alpha|^2)^n}{n!}\sum_{r=2}^{n-1}\binom{n}{r}\xi^{n-r}(\frac{1-\xi}{2})^r\sum_{j=1}^{r-1}\binom{r}{j}2^r(1-C)^{r-j}(1+C)^j\\
=&p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=3}^{\infty}\frac{(\eta\xi|\alpha|^2)^n}{n!}\sum_{r=2}^{n-1}\binom{n}{r}\xi^{n-r}(1-\xi)^r[2^r-(1-C)^r-(1+C)^r]\\
=&p(\phi_B)e^{-\eta|\alpha|^2}\sum_{n=3}^{\infty}\frac{(\eta\xi|\alpha|^2)^n}{n!}\{[\xi+2(1-\xi)]^n-[2(1-\xi)]^n\\
&\qquad\qquad -[\xi+(1-\xi)(1-C)]^n+[(1-\xi)(1-C)]^n\\
=&p(\phi_B)e^{-\eta|\alpha|^2}[e^{\eta\xi(2-\xi)|\alpha|^2}-e^{2\eta\xi(1-\xi)|\alpha|^2}-e^{\eta\xi[1-(1-\xi)C]|\alpha|^2}+e^{\eta\xi(1-\xi)(1-C)|\alpha|^2}\\
&\qquad -e^{\eta\xi[1+(1-\xi)C]|\alpha|^2}+e^{\eta\xi(1-\xi)(1+C)|\alpha|^2}+e^{\eta\xi^2|\alpha|^2}-1]. \qquad \text{(F.22)}
\end{aligned}
$$

$$
\begin{aligned}
&\langle\alpha',\beta|(b_{t_3}^\dagger)^{n-k-j}(b_{2,\phi_B}^\dagger)^k(b_{5,\phi_B}^\dagger)^j|0\rangle\\
=&(\sqrt{1-\xi}\beta^*)^{n-k-j}(\sqrt{\frac{1-\xi}{2}}\alpha'^*-e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^k(\sqrt{\frac{1-\xi}{2}}\alpha'^*+e^{-i\phi_B}\sqrt{\frac{\xi}{2}}\beta^*)^j e^{-\frac{|\alpha'|^2+|\beta|^2}{2}}\\
=&e^{i\phi_x(n-k-j)}e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^*)^n\sqrt{1-\xi}^{2n-k-j}\sqrt{\frac{\xi}{2}}^{k+j}\sum_{s=0}^{k}\binom{k}{s}e^{i\phi_B s}(-e^{i\phi_x})^{k-s}\sum_{r=0}^{j}\binom{j}{r}e^{i\phi_B r}e^{i\phi_x(j-r)}\\
=&e^{i\phi_x(n-k-j)}e^{-\frac{\eta|\alpha|^2}{2}}(\sqrt{\eta}\alpha^*)^n\sqrt{1-\xi}^{2n-k-j}\sqrt{\frac{\xi}{2}}^{k+j}(e^{i\phi_B}-e^{i\phi_x})^k(e^{i\phi_B}+e^{i\phi_x})^j. \qquad \text{(F.23)}
\end{aligned}
$$

As we see by switching from $b_{t_1}^\dagger$ to $b_{t_3}^\dagger$, we are simply swapping $\xi \leftrightarrow 1-\xi$ compared with Equation (F.21) and adding a global phase to the overlap, so

$$
\begin{aligned}
p(t_3,2,5,\phi_B|x) = p(\phi_B)e^{-\eta|\alpha|^2}[&e^{\eta(1-\xi)(1+\xi)|\alpha|^2}-e^{2\eta\xi(1-\xi)|\alpha|^2}-e^{\eta(1-\xi)(1-\xi C)|\alpha|^2}+e^{\eta\xi(1-\xi)(1-C)|\alpha|^2}\\
&-e^{\eta(1-\xi)(1+\xi C)|\alpha|^2}+e^{\eta\xi(1-\xi)(1+C)|\alpha|^2}+e^{\eta(1-\xi)^2|\alpha|^2}-1]. \qquad \text{(F.24)}
\end{aligned}
$$

- Ideal all-click probabilities:

$$
\begin{aligned}
&p(t_1,t_3,2,5,\phi_B|x)\\
=&p(\phi_B)[1-p(0|x)-p(t_1|x)-p(t_3|x)-p(t_1,t_3|x)]-p(2,\phi_B|x)-p(5,\phi_B|x)\\
&-p(t_1,2,\phi_B|x)-p(t_1,5,\phi_B|x)-p(t_3,2,\phi_B|x)-p(t_3,5,\phi_B|x)-p(2,5,\phi_B|x)\\
&-p(t_1,2,5,\phi_B|x)-p(t_3,2,5,\phi_B|x)-p(t_1,t_3,2,\phi_B|x)-p(t_1,t_3,5,\phi_B|x). \qquad \text{(F.25)}
\end{aligned}
$$