Security Proofs for Quantum Key Distribution Protocols by Numerical Approaches

by

Jie Lin

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, 2017

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

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

Jie Lin

Abstract

This thesis applies numerical methods to analyze the security of quantum key distribution (QKD) protocols. The main theoretical problem in QKD security proofs is to calculate the secret key generation rate. Under certain assumptions, this problem has been formulated as a convex optimization problem and numerical methods [8, 41] have been proposed to produce reliable lower bounds for discrete-variable QKD protocols. We investigate the applicability of these numerical approaches and apply the numerical methods to study a variety of protocols, including measurement-device-independent (MDI) protocols, variations of the BB84 protocol with a passive countermeasure against Trojan horse attacks, and the phase-encoding BB84 protocol using attenuated laser sources without continuous phase randomization.

Acknowledgements

First of all, I would like to thank my supervisor Norbert Lütkenhaus who gave me the opportunity to pursue my Master of Science study in the Institute for Quantum Computing. I want to thank him for his support, helpful discussion and advices in the past two years.

Thanks to my colleagues in the OQCT research group and many members of IQC. I have learned so much from all of them. In particular, I would like to give my special thank to Patrick Coles for helpful discussion about the numerical approaches, both the dual problem approach and the primal problem approach. I would also like to thank Adam Winick for enlightening discussion about the primal problem approach, and choices of optimization algorithms. Without the help from them, I cannot complete the calculations for this thesis. I would also like to thank Yanbao Zhang, Michael Epping, Hao Qin and Poompong Chaiwongkhot for proofreading early versions of this thesis.

I also want to thank Steve Weiss for his technical support and arrangement of IQC Heavylift computers.

I would like to thank all my friends here at Waterloo. Thanks to Ace and Golson for being wonderful roommates and friends and for sharing a lot of helpful tips about Waterloo.

Finally, I would like to thank my family for their love, support and encouragement.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Since the invention of first quantum key distribution (QKD) protocol BB84 by Charles Bennett and Gilles Brassard in 1984 [2], over the past three decades, this field has advanced dramatically both in theory and in physical implementation [33].

Unlike conventional cryptographic schemes whose security is based on computational assumptions, QKD guarantees the security by the laws of quantum mechanics. In theory, QKD has been proven to be unconditionally secure [15, 18, 21, 28, 35]. However, the physical implementation of QKD deviates from the theoretical model in many aspects and the gap between implementation and theory is vulnerable to eavesdropping attacks. To close up the gap, from the theory side, the security proofs need to be modified by relaxing the assumptions and taking into account what can be achieved by the current technology. Analytical security proofs can be quite complicated and the key rate bound can be loose due to available proof techniques. On the other hand, the key rate calculation problem can be formulated as a convex optimization problem and therefore we can resort to computers to perform the key rate calculation. In this thesis, we will apply numerical approaches developed recently in Refs. [8, 41] to study various QKD protocols.

This thesis is organized as follows:

In chapter 2, we will review the basics of quantum mechanics, quantum key distribution, entropy, quantum optics and convex optimization.

In chapter 3, we will discuss the fundamental theoretical problem in QKD - the key rate problem. We will start with reviewing the theoretical frameworks developed previously, in particular, the universally composable security definition and general key rate formulas. Then we will discuss the particular key rate calculation problem we will focus on for this thesis and how this problem has been formulated as a convex optimization problem. Then we will discuss the numerical security proof techniques developed recently. We have been able to use a modified dual problem approach to tackle the key rate calculation of many protocols. We will briefly mention the advantages and disadvantages of this approach. We will also show some examples to illustrate how we treat each protocol in our numerical framework. Then we will discuss the primal problem approach and and the idea of obtaining a reliable lower bound from the primal problem. We end this chapter by discussing how we handle sifting in the numerical framework, in particular, within the primal problem approach.

In chapter 4, we will show the applications of the numerical approaches. In particular, we will consider the analysis of QKD protocols with some passive optical components acting as a countermeasure to the Trojan horse attacks. We will see how our numerical approaches give a better key rate bound. Our analysis considers various types of sources, including a single-photon source, phase-coherent laser source and phase-randomized laser source.

In chapter 5, we will apply numerical approaches to study phase-encoding BB84 protocols with an attenuated laser source. We analyze the phase-coherent source where the phase is known by Eve. We will also investigate the idea of phase randomization and present our numerical security proofs in the case of discrete phase randomization.

In chapter 6, we make some concluding remarks and give the outlook for future works.

Chapter 2

Background

2.1 Quantum mechanics

In this section, we will review the basic formulation of quantum mechanics that is relevant for understanding this thesis and also introduce some notations we will use. The section is mainly based on [31]. Readers can refer to it for details.

2.1.1 Quantum states

Given a physical system[1] of interest, every (pure) quantum state, denoted by a ket vector $|\psi\rangle$, lives in a complex Hilbert space $\mathcal{H}$, which we call the state space of this physical system. We will use subscripts to label different systems when our discussion involves multiple systems. For each ket vector $|\psi\rangle \in \mathcal{H}$, its dual vector $\langle\psi|$, a bra vector, lives in the dual space of $\mathcal{H}$, which is isomorphic to itself.[2] Then $\langle\phi|\psi\rangle \in \mathbb{C}$ denotes the inner product of two states $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, and the outer product $|\phi\rangle\langle\psi|$ is a linear map from $\mathcal{H}$ to itself. In particular, $|\phi\rangle\langle\phi|$ is a projector onto the state vector $|\phi\rangle$.

We may be interested in a bipartite system composed of two subsystems A and B with associated state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The composite system of both A and B has the state space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim \mathcal{H}_{AB} = d_A d_B$, where $d_A = \dim \mathcal{H}_A$ and

[1] In this thesis, we will also use the term register for the physical system of our interest. Formally speaking, a register is an abstraction of a physical device that stores quantum information.

[2] Mathematically, a dual vector $\langle\psi|$ is a linear functional from $\mathcal{H}$ to $\mathbb{C}$, and the dual space is the space of all bounded linear functionals, each of which maps every vector from $\mathcal{H}$ to a complex number.

$d_A = \dim \mathcal{H}_B$. In this thesis, most of the time we will deal with finite-dimensional Hilbert spaces unless stated otherwise.[3] If $\{|i\rangle_A\}_{i=1}^{d_A}$ is a basis for $\mathcal{H}_A$ and $\{|j\rangle_B\}_{j=1}^{d_B}$ is a basis for $\mathcal{H}_B$, then $\{|i\rangle_A \otimes |j\rangle_B\}_{i,j=1}^{d_A,d_B}$ is a basis for $\mathcal{H}_{AB}$. We sometimes write $|i\rangle_A \otimes |j\rangle_B$ as $|i\rangle_A |j\rangle_B$ or $|ij\rangle_{AB}$ for the ease of notation. We will drop the subscripts when the spaces in our discussion are clear.

The system can also be prepared in a statistical ensemble of pure states. In this case, such a state is called a mixed state and it cannot be described by a single ket vector. So, we resort to a more general mathematical description of the quantum states, that is, the density operator formulation. First, we define the density operators for pure states. The density operator associated to the state vector $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi|$. For a classical mixture of pure states $\{|\psi_i\rangle\}$ with a probability distribution $\{p_i\}$, the density operator is given by

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \,. \tag{2.1}$$

In a finite-dimensional Hilbert space, we can choose an orthonormal basis and then write every density operator in the matrix form, called the density matrix. We will use the words density operator and density matrix interchangeably.

We will also be interested in linear operators on $\mathcal{H}$. We denote $\mathcal{L}(\mathcal{H})$ as the set of all linear operators on $\mathcal{H}$. In particular, we will be interested in Hermitian operators and positive semi-definite operators. Here, we review the definitions of Hermitian operators, and positive semi-definite operators.

Definition 2.1. (Hermitian operator) A Hermitian operator X is a linear operator such that for every $|\psi\rangle \in \mathcal{H}$, $\langle\psi| X |\psi\rangle \in \mathbb{R}$. Equivalently, a linear operator X is Hermitian if $X = X^\dagger$, where $X^\dagger$ is its adjoint operator.[4] We denote the set of Hermitian operators on $\mathcal{H}$ as $Herm(\mathcal{H})$.

Definition 2.2. (Positive semidefinite operator) A positive semi-definite operator P is a linear operator such that for every $|\psi\rangle \in \mathcal{H}$, $\langle\psi| P |\psi\rangle \geq 0$. If P is positive semidefinite, we write $P \succeq 0$. The set of all positive semidefinite operators on $\mathcal{H}$ is denoted as $Pos(\mathcal{H})$.

It is clear from the definition that a positive semidefinite operator is also a Hermitian operator.

We now can give a general mathematical definition of density operators.

[3] Later, we will also discuss a particular infinite-dimensional Hilbert space, called Fock space.

[4] The adjoint operator $X^\dagger$ of X is defined as $\langle X^\dagger\phi|\psi\rangle = \langle\phi|X\psi\rangle$, where $|\psi\rangle$ and $|\phi\rangle$ are arbitrary state vectors.

Definition 2.3. (Density operator) A density operator ρ is a positive semidefinite operator such that $\mathrm{Tr}(\rho) = 1$. We denote the set of all density operators as $\mathcal{D}(\mathcal{H})$.

Because the density matrix ρ represents a state of the system and $\mathcal{H}$ is the state space, we will often say ρ in $\mathcal{H}$ even though formally $\rho \in \mathcal{D}(\mathcal{H})$.

Next, we discuss how to describe a subsystem. Suppose ρ_{AB} is the density operator for a bipartite system consisting of two subsystems A and B. If we are only interested in the subsystem A, then we can describe this subsystem by the reduced density operator $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ after tracing out the system B. Similarly, we can describe the subsystem B by ρ_B.

If the joint state ρ_{AB} is pure, by the following theorem, we then know that ρ_A and ρ_B share the same set of eigenvalues.

Theorem 2.4 (Schmidt decomposition)**.** *Let $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$ be a pure state in $\mathcal{H}_{AB}$. Then we can write*

$$|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\, |e_i\rangle_A \, |\tilde{e}_i\rangle_B \,, \tag{2.2}$$

$\rho_A := \mathrm{Tr}_B(\rho_{AB}) = \sum_i \lambda_i \, |e_i\rangle\langle e_i|_A$, and $\rho_B := \mathrm{Tr}_A(\rho_{AB}) = \sum_i \lambda_i \, |\tilde{e}_i\rangle\langle \tilde{e}_i|_B$, where $\{|e_i\rangle_A\}$ and $\{|\tilde{e}_i\rangle_B\}$ are orthonormal sets on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

In many scenarios, it is more convenient to deal with pure states than mixed states. The following theorem is helpful for converting an arbitrary mixed state in a smaller space to a pure state in a larger space.

Theorem 2.5 (Purification)**.** *Let ρ_A be a state in $\mathcal{H}_A$. Then there exists a reference space $\mathcal{H}_R$ with $\dim \mathcal{H}_R = \dim \mathcal{H}_A$, and a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R$ such that $\rho_A = \mathrm{Tr}_R(|\psi\rangle\langle\psi|)$.*

Such a purification can be constructed as the following:

We start with the orthogonal decomposition of $\rho_A = \sum_{i=1}^d p_i \, |i\rangle\langle i|_A$, where $\{|i\rangle_A\}_{i=1}^d$ is an orthonormal basis.[5] Then we introduce a reference system R such that $\dim \mathcal{H}_R = \dim \mathcal{H}_A = d$ and $\{|\tilde{i}\rangle_R\}_{i=1}^d$ is an orthonormal basis for $\mathcal{H}_R$. We then define a pure state $|\psi\rangle = \sum_{i=1}^d \sqrt{p_i}\, |i\rangle_A \, |\tilde{i}\rangle_R$. We notice that $\mathrm{Tr}_R(|\psi\rangle\langle\psi|) = \sum_{i=1}^d p_i \, |i\rangle\langle i|_A = \rho_A$. Therefore, $|\psi\rangle$ is a purification of ρ_A.

Finally, we end our discussion of quantum states with the definitions of separable states, entangled states and Bell states.

[5] Since ρ_A is also a Hermitian operator, such an orthogonal decomposition can be realized by its spectral decomposition.

Definition 2.6. (Separable state) A state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ of some physical system AB is separable if it can be written as a convex combination of product states:

$$\rho_{AB} = \sum_x p(x)\rho_A^x \otimes \rho_B^x.$$

Definition 2.7. (Entangled state) A state $\rho \in \mathcal{D}(\mathcal{H})$ is entangled if it is not separable.

Definition 2.8. (Bell states) The four Bell states are defined on a two-qubit Hilbert space as

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ \left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ \left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ \left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{2.3}$$

These four Bell states are maximally entangled states.

2.1.2 Measurements

Every physical measurement can be described by a positive operator-valued measure (POVM), which is defined below.

Definition 2.9. (POVM) An n-outcome POVM on a Hilbert space $\mathcal{H}$ is a set $\{E_i\}_{i=1}^n$ such that $E_i \succeq 0$ for each i and $\sum\limits_{i=1}^{n} E_i = \mathbb{1}$.

Also, every POVM can be realized by a physical measurement. Typically, one labels the outcomes of a measurement by the elements of the index set of its POVM. For a quantum state $\rho \in \mathcal{D}(\mathcal{H})$, and a physical measurement described by a POVM $\{F_j\}_{i=1}^m$, the probability for the outcome j of the measurement to occur is given by $\mathrm{Tr}(\rho F_j)$.

A POVM $\{F_j\}$ can be represented by a list of Kraus operators $\{M_i\}_{i\in I}$ acting on the Hilbert space $\mathcal{H}$ such that $\sum_{i\in I} M_i^\dagger M_i = \mathbb{1}$ for some index set I, where $\mathbb{1}$ is the identity operator. This representation is not unique and there can be several different lists of Kraus operators representing the same POVM. For a given list of Kraus operators, each POVM element F_j can be written as $F_j = \sum_{i \in I_j} M_i^\dagger M_i$, where the summation is over a subset I_j of the index set I. For a quantum state ρ, the probability p_k for the k-th outcome to occur is given by $p_k = \sum_{i \in I_k} \mathrm{Tr}\left(\rho M_i^\dagger M_i\right)$ and the post-measurement state conditioning on the outcome k is $\frac{\sum_{i \in I_k} M_i \rho M_i^\dagger}{p_k}$.

A special type of measurements that we will frequently encounter is projective measurements or projection-valued measure (PVM), where each measurement operator is a projection operator. A projection operator P is a positive semidefinite operator such that $P^2 = P = P^\dagger$.

A general POVM is not necessarily a projective measurement. However, we can construct a projective measurement from a given POVM. This can be done through Naimark dilation theorem. We state the Naimark dilation theorem in the form that is relevant to our discussion.

Theorem 2.10 (Naimark)**.** *Let $\{E_i\}_{i=1}^n$ be a POVM on $\mathcal{H}_A$. There exists a Hilbert space $\mathcal{H}_R$, an isometry $V : \mathcal{H}_A \to \mathcal{H}_A \otimes \mathcal{H}_R$ and a projective measurement $\{P_i\}_{i=1}^n$ such that $E_i = V^\dagger P_i V$ for each i.*

Here, we give an explicit construction of this isometry and the corresponding PVM. We first notice that for each positive semidefinite operator A, there exists a unique square-root operator B such that $B^2 = A$. Since E_i is positive semidefinite, we write $\sqrt{E_i}$ as its square-root operator. V can be constructed as $V = \sum_i \sqrt{E_i} \otimes |i\rangle_R$. We verify that V is an isometry since $V^\dagger V = \sum_i E_i = \mathbb{1}_A$. Each element of the desired PVM can be constructed as $P_i = \mathbb{1}_A \otimes |i\rangle\langle i|_R$, which is a projection onto one of the basis states of the new register system R.

2.1.3 Quantum channel

To define a quantum channel, we start with the definitions of completely positive (CP) maps and trace-preserving (TP) maps.

Definition 2.11. A map $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is completely positive if for every complex Euclidean space $\mathcal{Z}$, $\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathcal{Z})}$ is a positive map. Φ is trace-preserving if for every $X \in \mathcal{L}(\mathcal{H}_A)$, $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$.

Definition 2.12. (Quantum channel) A quantum channel $\mathcal{E}$ between two registers A and B with $\mathcal{H}_A$ and $\mathcal{H}_B$ is a map from $\mathcal{L}(\mathcal{H}_A)$ to $\mathcal{L}(\mathcal{H}_B)$ such that it is completely positive and trace-preserving (CPTP).

We notice that from the CPTP requirements, for $\rho \in \mathcal{D}(\mathcal{H}_A)$, we automatically have $\mathcal{E}(\rho) \in \mathcal{D}(\mathcal{H}_B)$.

An important representation of a quantum channel is its Kraus representation. A map $\mathcal{E}$ from $\mathcal{L}(\mathcal{H}_A)$ to $\mathcal{L}(\mathcal{H}_B)$ is CP if and only if there exists a set of operators $\{K_a\}$ such that $\mathcal{E}(X) = \sum\limits_a K_a X K_a^\dagger$ for every $X \in \mathcal{L}(\mathcal{H}_A)$. It is trace-preserving (TP) if and only if $\sum\limits_a K_a^\dagger K_a = \mathbb{1}_A$. The operators $\{K_a\}$ are called Kraus operators.

Before we end the discussion of quantum channels, we consider a particular channel of a qubit system, called depolarizing channel. This is a model for introducing noise to the system.

Definition 2.13. (Depolarizing channel) For a qubit system, a depolarizing channel $\mathcal{E} : \mathcal{L}(\mathbb{C}^2) \to \mathcal{L}(\mathbb{C}^2)$ is defined as $\mathcal{E}(\rho) = (1-p)\rho + p\frac{\mathbb{1}}{2}$ for every $\rho \in \mathcal{L}(\mathbb{C}^2)$, where p is the depolarizing probability.

Since for arbitrary ρ, we have $\frac{\mathbb{1}}{2} = \frac{\rho+\sigma_x\rho\sigma_x+\sigma_y\rho\sigma_y+\sigma_z\rho\sigma_z}{4}$, where σ_x, σ_y and σ_z are Pauli operators, we can write the depolarizing channel as $\mathcal{E}(\rho) = (1-\frac{3p}{4})\rho + \frac{p}{4}(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z)$. In the Kraus operator representation, the Kraus operators are $\sqrt{1-\frac{3p}{4}}\mathbb{1}$, $\frac{\sqrt{p}}{2}\sigma_x$, $\frac{\sqrt{p}}{2}\sigma_y$, and $\frac{\sqrt{p}}{2}\sigma_z$.

Sometimes, it is helpful to write an identity channel, which is the channel that does nothing but simply returns the input state as the output state. We denote the identity channel from $\mathcal{L}(\mathcal{H}_A)$ to $\mathcal{L}(\mathcal{H}_A)$ by $\mathcal{I}_A$.

2.2 Quantum key distribution

Quantum key distribution (QKD) allows two distant parties, the sender (commonly referred as Alice) and the receiver (Bob) in the presence of an eavesdropper (Eve) to establish a secret key for which Eve knows a negligible amount of information except the key length. Unlike conventional classical cryptographic schemes for key distribution, whose security is based on some computational assumptions, QKD in theory guarantees information-theoretical security solely based on the law of quantum physics. In this section, we start with reviewing general steps in a prepare-and-measure protocol and in an entanglement-based protocol, and then discuss some useful tools to prove security of a QKD protocol, namely, source-replacement schemes, and squashing models.

A QKD protocol consists of a quantum phase and a classical phase. The goal of Alice and Bob is to establish a secret key of ℓ bits. To do so, they use an insecure quantum channel to transmit N quantum signals and then communicate through an authenticated classical channel to perform classical post-processing procedures to distill ℓ-bit secure key.

2.2.1 Prepare-and-measure protocols

We now discuss the QKD protocols in the prepare-and-measure scheme, where Alice prepares some quantum states and sends them to Bob for measurements.

Quantum phase:

1. (Signal preparation) Alice prepares N quantum signals, each of which is chosen independently from the set of m distinct quantum states $\mathcal{S} = \{|\phi_1\rangle, \dots, |\phi_m\rangle\}$ according to *a priori* probability distribution $\{p_i\}_{i=1}^m$. Each quantum state $|\phi_i\rangle$ in a $d_{A'}$-dimensional Hilbert space $\mathcal{H}_{A'}$ encodes the information of the key.

2. (Signal transmission) Alice sends each of the N quantum signals to Bob and records the sequence of the states she sent.

3. (Measurement) Upon receiving the quantum states from Alice, Bob measures each state by a k-outcome POVM $\{M_B^j\}_{j=1}^k$ and records the measurement outcomes.

After all N signals have been transmitted to Bob and measured by Bob, they stop the quantum transmission and start the classical phase of the protocol.

Classical phase:

4. (Parameter estimation) They randomly choose a small portion of their data as a test set, which they use to estimate the amount of information leaked to Eve. For this test set, Alice tells Bob which states were prepared and Bob tells Alice what measurement outcomes he obtained via the classical channel. By doing so, they obtain a table of relative frequencies $f(i, j)$, where $i = 1, \dots m$, and $j = 1, \dots, k$, for all possible combinations of states sent and measurement outcomes. Then from $f(i, j)$, they decide whether they will be able to generate secret key from the remaining data. If not, they abort; otherwise, they continue.

5. (Announcement) For the remaining data, they can choose to make announcements based on their local data. By doing announcements, they may partition their data into subsets for further post-processing.

6. (Sifting) They may agree on which parts of the data are not suitable for generating secret key, and then discard those parts. For example, they may perform a basis sifting or discard rounds where Bob fails to detect the signals.

7. (Key map) Either Alice or Bob maps her (or his) remaining raw data into a key string of some predefined alphabet.[6] Although any alphabet is allowed, we consider binary alphabet below for the ease of our discussion. After this step, she (or he) now has an n-bit string,[7] where $n<N$. This n-bit string is usually called the raw key or sifted key.[8]

8. (Error correction) At the end of the previous step, Alice and Bob may have a pair of strings that are possibly only weakly correlated. To create a pair of perfectly correlated key strings, they then perform the error correction. One party sets his or her key as the reference key, and sends the error correction information to the other party. The other party corrects all errors to match with the reference key. If Alice (Bob) has the reference key, we sometimes call this procedure as direct (reverse) reconciliation. The error correction step leaks some amount of information to Eve, denoted by leak_{EC}.

9. (Privacy amplification) In order to eliminate Eve's information about their secret key, Alice and Bob then distill ℓ-bit key of their n-bit raw key ($\ell \leq n$) by applying privacy amplification. This can be done as follows. They first need to calculate ℓ. Then Alice randomly chooses a hash function $F : \{0,1\}^n \to \{0,1\}^\ell$ from the two-universal family of hash functions[9]. She applies F to her n-bit string X and sends Bob her choice of F. At the end of the protocol, Alice and Bob share an ℓ-bit string $F(X)$.

The above steps are generic for many protocols of our interests. Some variations are possible. In particular, we will only focus on discrete-variable QKD protocols. To give a concrete example, we briefly comment the specific setting in the case of the well-known BB84 protocol proposed by Charles Bennett and Gilles Brassard in 1984 [2]. For BB84, the set of signal states is $\mathcal{S} = \{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle\}$, where $\{\left|0\right\rangle, \left|1\right\rangle\}$ is referred as the Z-basis

[6] In many real-world implementations, the typical alphabet is binary even though there is no restriction on the choice of alphabet. Our discussion can be easily generalized to arbitrary alphabets.

[7] Without loss of generality, we assume one party obtains an n-bit string after this step and uses it as a reference key to which the other party needs to match his/her key later.

[8] In some older papers, raw key may refer to the one before the sifting step.

[9] A precise definition of two-university hashing is the definition 5.4.1 in [32]. This two-universal family of hash functions guarantees information-theoretical security.

(or computational basis) of a qubit system, and $\{|+\rangle, |-\rangle\}$ is called the X-basis, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The *a priori* probability for each of these four states is $\frac{1}{4}$. Bob's POVM consists of $\{\frac{1}{2}|0\rangle\!\langle 0|, \frac{1}{2}|1\rangle\!\langle 1|, \frac{1}{2}|+\rangle\!\langle +|, \frac{1}{2}|-\rangle\!\langle -|\}$. That is, Bob chooses randomly with an equal probability to measure the state in Z-basis or in X-basis. For the announcement step, they discard the rounds where Alice prepares in Z-basis, but Bob measures in X-basis, and the rounds where Alice prepares in X-basis, but Bob measures in Z-basis. We refer to $f(i,j)$ from the parameter estimation as the fine-grained statistics, and we can coarse-grain $f(i,j)$ by some classical processing, such as summing up some of the entries in the table $f(i,j)$ or taking average values. A single average error rate called quantum bit error rate (QBER) can be obtained for BB84 by coarse-graining $f(i,j)$. Alice and Bob then decide to abort the protocol if this error rate is above a certain threshold value. Other steps of the BB84 protocol are exactly what is described above.

We remark that in the case of infinitely long key limit ($N \to \infty$), the relative frequencies $f(i,j)$ can become a probability distribution $p(i,j)$. The number of secret bits ℓ that we can extract from the protocol depends on n (and therefore N). In the asymptotic key limit, the secret key generation rate per channel use $\frac{\ell}{N}$ is defined as $R^{\infty} := \lim\limits_{N\to\infty} \frac{\ell}{N}$, which we call the asymptotic key rate. Sometimes, we also talk about the key rate per sifted (or raw) key $\frac{\ell}{n}$ and asymptotic sifted key rate $r^{\infty} := \lim\limits_{n\to\infty} \frac{\ell}{n}$.

2.2.2 Entanglement-based protocols

Another major type of QKD protocols is the entanglement-based scheme. For the security proofs, entanglement-based protocols are usually more convenient to analyze. For the completeness of our presentation, we summarize the steps for the entanglement-based protocols. Later on, we will see, with regard to the security proofs, that there is an equivalence between prepare-and-measure and entanglement-based protocols. The main difference between a prepare-and-measurement protocol and an entanglement-based protocol is the quantum phase. We give a detailed description of the quantum phase for entanglement-based scheme and then comment on the classical phase.

Quantum Phase:

1'. (Signal preparation) An untrusted source prepares N quantum signals of a bipartite system. Ideally, the source emits N copies of the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or some noisy version of $|\Phi^+\rangle^{\otimes N}$. However, Eve can have access to the source or even prepare the states for Alice and Bob. She may prepare whatever states she wishes. She may instead prepare tripartite states, keep one system for herself and use the remaining two systems for the next step.

2'. (Signal transmission) The source sends one part of each of N bipartite states to Alice, and the other part to Bob.

3'. (Measurements) Alice performs her measurements on each of the states she receives by a POVM $\{M_A^i\}_{i=1}^m$ and records her measurement outcomes. Similarly, Bob performs his measurements on each of the states he receives by a POVM $\{M_B^j\}_{j=1}^k$ and records his measurement outcomes.

The classical phase of an entanglement-based protocol runs almost the same as the prepare-and-measure protocol. They perform parameter estimation to decide whether or not to abort the protocol, and if not aborting, they continue with other post-processing steps, error correction and privacy amplification as mentioned above. Some variations of these procedures can be done. For example, they can postpone their measurements until receiving all N states. Then they can perform random permutation on these N states, choose a subset of these states to perform their POVMs and use this subset as the test set for parameter estimation. If they do not abort after the parameter estimation, then for the remaining set of states, they can perform subsets of their POVMs. For instance, thank to the random permutation, for the remaining data set, they then are allowed to measure in the same basis (as in the case of BB84). By doing so, they avoid discarding more data in the sifting step due to basis mismatch.

2.2.3 Source-replacement scheme

In the entanglement-based picture, it is more natural to discuss the joint state shared by Alice and Bob (and Eve), and to quantify the amount of information leaked to Eve by some entropy measure on this joint state. Therefore, it is often easier to analyze an entanglement-based protocol. To analyze the security of a prepare-and-measure protocol, the first step is usually transforming it to an equivalent entanglement-based protocol. A canonical method to achieve this transformation is the source-replacement scheme [11].

We introduce an additional register A for Alice's system, whose state space is $\mathcal{H}_A$. If the set of signal states $\mathcal{S}$ contains m states, then $\dim \mathcal{H}_A = m$ and $\mathcal{H}_A$ has an orthonormal basis $\{|i\rangle\}_{i=1}^m$. Alice's source, instead of just sending the signal states to Bob, creates an entangled pair between the register A, which stores the information about the signal states prepared, and the register A' that holds the signal states. The source emits the following state for every signal transmission round:

$$|\Psi\rangle_{AA'} = \sum_{i=1}^{m} \sqrt{p_i}\, |i\rangle_A\, |\phi_i\rangle_{A'}\,. \tag{2.4}$$

Then Alice keeps the register A and sends the system A' to Bob through the insecure quantum channel. To establish the equivalence between the entanglement-based protocol based on the source replacement scheme and the original prepare-and-measure protocol, Alice performs a projective measurement $\{|j\rangle\langle j|\}_{j=1}^{m}$ on system A. With a probability p_a, this measurement outcome is a, and then the state sent to Bob is collapsed to the conditional state $|\phi_a\rangle$. Since Eve has no access to Alice's register A and this replaced source emits the same set of signal states with the same probability distribution as before, Eve cannot distinguish this new source and the original source. Therefore, the equivalence between the entanglement-based protocol with this source replacement and the original prepare-and-measure protocol is clear.

We want to highlight that in the source-replacement scheme, the source is in Alice's lab and is protected. This puts the constraint that the reduced density operator ρ_A on system A is unchanged before and after the signal transmission. Equivalently, we describe the quantum channel as a CPTP map $\mathcal{E}_{A'\to B} : \mathcal{D}(\mathcal{H}_{A'}) \to \mathcal{D}(\mathcal{H}_B)$ such that the state shared by Alice and Bob after the quantum transmission is $\rho_{AB} = (\mathcal{I}_A \otimes \mathcal{E}_{A'\to B})(|\Psi\rangle\langle\Psi|_{AA'})$. The additional requirement is $\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \mathrm{Tr}_{A'}(\rho_{AA'})$. Specifically,

$$\rho_A = \mathrm{Tr}_{A'}(|\Psi\rangle\langle\Psi|_{AA'}) = \sum_{j,k} \sqrt{p_j p_k}\, \langle\phi_k|\phi_j\rangle\, |j\rangle\langle k|\,. \tag{2.5}$$

2.2.4 Squashing model

Historically, QKD protocols were initially designed based on qubit systems and security proofs were first given assuming qubit systems, for example, see [35]. In reality, QKD protocols are implemented by quantum optical devices. In quantum optical implementations of QKD protocols, we deal with optical modes. Optical modes are described on infinite-dimensional Hilbert spaces, such as an infinite-dimensional Fock space. However, a finite-dimensional space is usually easier to study theoretically. It would be nice if we can make a reduction from an infinite-dimensional space to a finite-dimensional space, or even to a qubit. The idea of squashing model is to accomplish this reduction for the measurement devices. If such a squashing model exists for a QKD protocol, then we can think Bob's measurements on a higher-dimensional space by measurements on a lower-dimensional space. We now give a high-level overview of the basic ideas of squashing models since we only need to know whether such a squashing model exists for the protocol to be analyzed and if exists, then we can conveniently treat Bob's system on a low-dimensional Hilbert space. All technical details regarding how to search for a squashing map is beyond the scope of this thesis, and we direct readers to Refs. [1, 13, 38] for technical details.

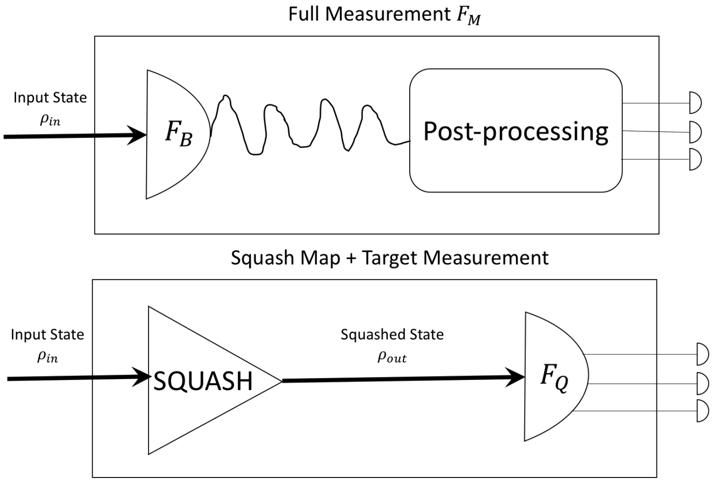

Figure 2.1: Schematics of squashing model, reproduced from the Fig. 1 of Ref. [13]. In reality, the measurement device may perform the POVM F_B. By applying an appropriate post-processing, the full measurement is now described by POVM F_M. If there exists a squashing map, then it allows us to think the measurement in terms of the target POVM F_Q on a lower-dimensional space.

As depicted in Fig. 2.1, we want to establish the equivalence of these two boxes. For the measurements in QKD, the physical measurement device B is described by the POVM F_B on the optical modes and the desired qubit measurement is given by the POVM F_Q. Since F_B is on a higher-dimensional Hilbert space and may have different numbers of outcomes from that of F_Q on a lower-dimensional space, a classical post-processing is needed for basic outcome events, and the full measurement including both F_B and the classical post-processing is then described by another POVM F_M. As we are typically interested in measurement outcomes and the statistics, we want to establish the equivalence of these two boxes in the sense that both boxes take the same general optical input ρ_{in} and output the same set of measurement outcome events with the same probability distribution. That is, these two boxes are statistically indistinguishable. Once this equivalence is established, even though the actual measurement we perform in the experiment is F_M, we can think in terms of F_Q and analyze the security with F_Q.

We remark that the essential step to find a squashing model is to show the existence of this squashing map Λ_B. Usually F_B is already defined by the protocol and fixed. In many circumstances when we study an optical implementation of a protocol, we may choose F_Q to be the measurements on the qubit version of the protocol with an additional flag for no detection in order to make connections to the security proofs of the qubit protocol. Our task is then to specify an appropriate post-processing procedure that may allow this squashing map to exist. Throughout this thesis, we will apply the squashing model, and the essential post-processing step is to map the double clicks to random bits. Fortunately, squashing models exist for the protocols studied here [1, 13, 38].

2.3 Entropy

In this section, we give a brief introduction to entropy based on the Ref. [31]. Entropy is a useful tool to quantify the amount of information. A traditional way to present this material is to start with the classical Shannon entropy and then to introduce the quantum analog. Roughly speaking, the Shannon entropy is defined for probability distributions, and in the quantum analog of Shannon entropy, which is called von Neumann entropy, the density operators replace the probability distributions. Now, we start to define them more formally.

Let X be a random variable taking values in a finite set of alphabet $\mathcal{X}$ with the probability $p(x)$ for $X = x$. Shannon entropy of X, denoted as $H(X)$ or $H(\{p(x)\})$ is defined as $H(X) = -\sum_x p(x) \log(p(x))$.[10] A nice interpretation of Shannon entropy is that $H(X)$ quantifies the uncertainty of X before we learn the value of X or the amount of information we gain after learning the value of X. Similarly, von Neumann entropy of a density operator ρ describing a physical system X is $H(\rho) = -\operatorname{Tr}(\rho \log(\rho))$, sometimes also denoted as $H(X)$. If λ's are eigenvalues of ρ, then $H(\rho) = -\sum_\lambda \lambda \log(\lambda)$. We remark that the von Neumann entropy is a generalization of the Shannon entropy. If the system is classical, then the density operator for this system can be written as a diagonal matrix, where the basis consists of all possible events and each diagonal entry corresponds to the probability of each event. In this case, the von Neumann entropy is the same as the Shannon entropy. That is, for $\rho = \sum_x p(x) |x\rangle\langle x|$, $H(\rho) = H(\{p(x)\})$. This is also the reason that we use the same notation for Shannon and von Neumann entropy. It should be clear that if a register is classical, then the von Neumann entropy reduces to the Shannon entropy.

For a pair of random variables X and Y with a joint probability distribution $p(x, y)$, we can define the joint entropy $H(XY)$ as $H(XY) = -\sum_{x,y} p(x, y) \log(p(x, y))$. Analogously,

[10] In this thesis, log is assumed to be in base 2, and $0 \log 0 = 0$. We will denote natural logarithm by ln.

for a bipartite system XY with a density operator ρ_{XY}, $H(XY) = H(\rho_{XY})$.

The conditional entropy $H(X|Y) = H(XY) - H(Y)$ tells us the remaining uncertainty of the pair (X, Y) after learning the value of Y. In the quantum case, for a density operator ρ_{XY}, $H(X|Y) = H(\rho_{XY}) - H(\rho_Y)$. In the classical picture, from the joint probability distribution $p(x, y)$, we can define the marginal probability for the random variable Y as $p(y) = \sum_x p(x, y)$. Then the conditional entropy $H(X|Y) = H(\{p(x, y)\}) - H(\{p(y)\})$.

The mutual information $I(X : Y) = H(X) + H(Y) - H(XY)$ quantifies how much information X and Y have in common. We remark that $I(X : Y) \geq 0$ in both classical and quantum cases.

These definitions are schematically represented in the Fig. 2.2.

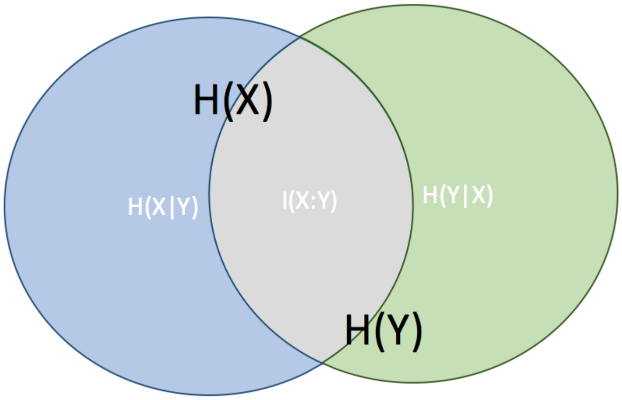

Figure 2.2: Schematic description of entropy. The left circle represents the amount of certainty for X, and the right circle represents the amount of uncertainty for Y. The blue area represents $H(X|Y)$; green area $H(Y|X)$ and grey area $I(X : Y)$.

The following is a useful theorem concerning the entropy of pure states:

Theorem 2.14. *If ρ_{AB} is a pure state, then $H(\rho_A) = H(\rho_B)$, where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$.*

Proof. This follows directly from the Schmidt decomposition of ρ_{AB} (Theorem 2.4). $\rho_{AB} = \sum\limits_i \sqrt{\lambda_i} \left|i\right\rangle_A \left|\tilde{i}\right\rangle_B$. $\rho_A = \sum\limits_i \lambda_i \left|i\right\rangle\!\left\langle i\right|_A$ and $\rho_B = \sum\limits_i \lambda_i \left|\tilde{i}\right\rangle\!\left\langle\tilde{i}\right|_B$, where λ_i's are eigenvalues of ρ_A and ρ_B. Since ρ_A and ρ_B have the same eigenvalues, $H(\rho_A) = H(\rho_B)$. □

Another useful quantity is the relative entropy. For two probability distribution $p(x)$ and $q(x)$ over the same index set x, the relative entropy, $D(p(x)||q(x)) = \sum_x p(x) \log \frac{p(x)}{q(x)}$, describes how the probability distribution $p(x)$ diverges from the other probability distribution $q(x)$. The quantum relative entropy is $D(\rho||\sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma)$. Since $H(\rho) = -\mathrm{Tr}(\rho \log \rho)$, we can also write $D(\rho||\sigma) = -\mathrm{Tr}(\rho \log \sigma) - H(\rho)$. A nice property of the relative entropy is the joint convexity, that is, $D(\sum_i p_i \rho_i || \sum_i p_i \sigma_i) \leq \sum_i p_i D(\rho_i||\sigma_i)$ for $\sum_i p_i = 1$ and $p_i \geq 0$.

2.4 Quantum optics

The physical realization of QKD protocols resorts to quantum optics. In this section, we give a short introduction to the relevant part of quantum optics based on [20].

2.4.1 Optical modes

A photon can be used as a carrier of information by encoding the information in some optical mode. In classical electrodynamics, optical modes refer to some orthonormal basis solutions to the Maxwell's Equations for the vector potential in the vacuum space. A general solution can be expressed as a linear combination of those modes. Since the basis choice is not unique, any solution can be defined as a mode. In quantum mechanics, through canonical quantization, the field amplitudes of orthonormal modes are promoted to mode operators. We describe those mode operators in terms of creation operator $\hat{a}^\dagger$ and annihilation operator $\hat{a}$. Since photons are excitations of the electromagnetic field, we say $\hat{a}^\dagger$ creates a photon in an optical mode, and $\hat{a}$ annihilates a photon. The associated Hilbert space that creation and annihilation operators of a mode act on has a convenient orthonormal basis, called Fock states, denoted as $|n\rangle$, where n represents the number of photons in a mode.[11] Mathematically, $\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle$, $\hat{a} |n\rangle = \sqrt{n} |n-1\rangle$ and $\hat{a} |0\rangle = 0$. We will use subscripts in the creation and annihilation operators to distinguish which mode they are associated with when we talk about several modes. The commutation relations between the creation and annihilation operators with several modes are $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$, where δ_{ij} is the Kronecker delta, that is, $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise.

[11] $|0\rangle$ of a mode means the vacuum state in this mode. Sometimes, to avoid confusion with the computational basis state $|0\rangle$ of a qubit, we will denote the vacuum state by $|\emptyset\rangle$. Otherwise, the meaning of the state should be clear from the context.

The Fock state $|n\rangle$ of one mode is the eigenstate of the Hamiltonian of this mode for the electromagnetic field. The Hamiltonian of one mode is $\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})$. The Hamiltonian of the whole system is then just the sum of the Hamiltonians of each mode, and the Fock state for several modes is just the tensor product of individual modes.

2.4.2 Coherent states

A laser source emits coherent states. A coherent state $|\alpha\rangle$ is an eigenstate of the annihilation operator $\hat{a}$ with a complex eigenvalue $\alpha = e^{i\phi}|\alpha|$. We can express a coherent state $|\alpha\rangle$ in the Fock state basis as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{2.6}$$

The number operator $\hat{N} := \hat{\alpha}^\dagger\hat{\alpha}$ measures the number of photons in a mode. For a coherent state $|\alpha\rangle$, the average photon number is $\mu := \langle\hat{N}\rangle = \langle\alpha|\,\hat{\alpha}^\dagger\hat{\alpha}\,|\alpha\rangle = |\alpha|^2$. The probability of finding n photons for a coherent state $|\alpha\rangle$ is given by $P_\mu(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2}\frac{|\alpha|^2}{n!}$, a Poissonian distribution.

Since the photon intensity is proportional to the mean photon number μ, we may use these two terms loosely when other parameters are assumed to be fixed and irrelevant for our discussion. When we say the coherent state with an intensity μ, we actually mean that the average photon number is μ. This is commonly found in the literature.

2.4.3 Linear optics

Linear optics are used to manipulate modes. Since each state can be written as some creation operators acting on the vacuum state $|0\rangle$, we can think the transformation of the state in terms of the transformations of creation and annihilation operators (that is, in the Heisenberg picture). We will use the subscripts to indicate the input modes and the output modes.

Phase shifter

A phase shifter (PS) changes the phase of the electromagnetic field. This can be realized by any device or material that changes the optical path, such as a delay line to change the length of the optical path, or some material with an index of refraction that can be changed by an applied voltage. The output mode and input mode are related by $\hat{a}^\dagger_{\text{out}} = e^{i\phi}\hat{a}^\dagger_{\text{in}}$ and $\hat{a}_{\text{out}} = e^{-i\phi}\hat{a}_{\text{in}}$.

Beam splitter

A beam splitter (BS) is an optical device that reflects some part of the incident light and transmitting the rest part. It is usually implemented by a semi-reflective mirror. It has two input ports and two output ports. We denote these two input modes in two input ports as $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$, and the two output modes as $\hat{a}_{\text{out}}$ and $\hat{b}_{\text{out}}$. Then $\hat{a}_{\text{out}} = \sqrt{t}\hat{a}_{\text{in}} + e^{i\varphi}\sqrt{r}\hat{b}_{\text{in}}$, and $\hat{b}_{\text{out}} = -e^{-i\varphi}\sqrt{r}\hat{a}_{\text{in}} + \sqrt{t}\hat{b}_{\text{in}}$, where t is the transmission probability and r is the reflection probability, $t + r = 1$, and φ is a phase shift introduced by the coating of the mirror.[12] This transformation can be compactly written as a unitary matrix in the vector notation as follows:

$$\begin{bmatrix} \hat{a}_{\text{out}} \\ \hat{b}_{\text{out}} \end{bmatrix} = \begin{bmatrix} \sqrt{t} & e^{i\varphi}\sqrt{r} \\ -e^{-i\varphi}\sqrt{r} & \sqrt{t} \end{bmatrix} \begin{bmatrix} \hat{a}_{\text{in}} \\ \hat{b}_{\text{in}} \end{bmatrix}. \tag{2.7}$$

For a 50/50 beam splitter, the transmission probability is the same as the reflection probability, that is, $t = r = \frac{1}{2}$, and the phase shift is $\varphi = 0$. Then,

$$\begin{bmatrix} \hat{a}_{\text{out}} \\ \hat{b}_{\text{out}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \hat{a}_{\text{in}} \\ \hat{b}_{\text{in}} \end{bmatrix}. \tag{2.8}$$

We can also express the input mode in terms of the output modes by the inverse of this unitary matrix. In the case of a 50/50 beam splitter, $\hat{a}_{\text{in}} = \frac{1}{\sqrt{2}}(\hat{a}_{\text{out}} - \hat{b}_{\text{out}})$, and $\hat{b}_{\text{in}} = \frac{1}{\sqrt{2}}(\hat{a}_{\text{out}} + \hat{b}_{\text{out}})$.

Polarization rotator

A polarization rotator (PR) changes the polarization of the input mode to its orthogonal polarization, and is physically realized by quarter- and half-wave plates. If we write $\hat{a}_{\text{in}}$ as $\hat{a}_x$, and $\hat{b}_{\text{in}}$ as $\hat{a}_y$, where x and y represent a set of orthogonal polarization directions, and write $\hat{a}_{\text{out}}$ as $\hat{a}_{x'}$, and $\hat{b}_{\text{out}}$ as $\hat{a}_{y'}$, where x' and y' represent another set of orthogonal polarization directions, then the transformation can be written as:

$$\begin{bmatrix} \hat{a}_{\text{x'}} \\ \hat{a}_{\text{y'}} \end{bmatrix} = \begin{bmatrix} \cos\theta & e^{i\varphi}\sin\theta \\ -e^{-i\varphi}\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \hat{a}_{\text{x}} \\ \hat{a}_{\text{y}} \end{bmatrix}, \tag{2.9}$$

[12] We only consider symmetric lossless beam splitters in this thesis.

where θ and φ are angles of rotation. We notice this transformation has the same form as the transformation of the beam splitter. From the unitary transformation, the equivalence between polarization and two-mode representation in a conceptual level can be established.

Polarizing beam splitter

A polarizing beam splitter (PBS) can separate modes with same spatial mode functions but orthogonal polarization into spatially different output modes. A PBS can be made to separate a preferred polarization mode decomposition. For example, if the PBS is designed to separate horizontal and vertical polarization, then such a transformation can be as follows for two input modes ($\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$):

$$\hat{a}_{\text{in,H}} \to \hat{a}_{\text{out,H}}, \hat{a}_{\text{in,V}} \to \hat{b}_{\text{out,V}}, \hat{b}_{\text{in,H}} \to \hat{b}_{\text{out,H}}, \hat{b}_{\text{in,V}} \to \hat{a}_{\text{out,V}},$$

where the subscript H indicates horizontal polarization and V vertical polarization.

A PBS can also be designed to separate other polarization directions, such as left-circular polarization (L) and right-circular polarization (R). In this case, the transformation is the same as listed above with the substitution H ↔ L and V ↔ R.

2.5 Convex optimization and semidefinite programming

Many problems in the field of quantum information can be formulated as mathematical optimization problems. In particular, if the problem can be expressed as a convex optimization problem, it means this problem can be efficiently solved numerically. With an aid of numerical optimization tools, we then are able to tackle many problems that are difficult to solve analytically. In this thesis, the focus of proving the security of QKD protocols resides on the calculation of secret key generation rate. Fortunately, the key rate calculation problem can be formulated as a convex minimization problem, as we will see later.

In this section, we briefly review some results from the theory of convex optimization, which will be useful for understanding the numerical approaches we adopt. We will also look at a specific type of convex optimization problems, semidefinite programming (SDP) problems. We direct readers to Ref. [3] for a detailed discussion of this topic.

We start with the basic definitions of convex functions and convex sets.

Definition 2.15. (Convex function) A function $f : \mathbb{R}^n \to \mathbb{R}$ is convex if for any $x_1, x_2 \in \mathbb{R}^n$ and $0 \leq p \leq 1$, $f(px_1 + (1-p)x_2) \leq pf(x_1) + (1-p)f(x_2)$.

Definition 2.16. (Convex set) A subset $C \subseteq \mathbb{R}^n$ is convex if for every $x_1, x_2 \in C$, and for any $0 \leq p \leq 1$, $px_1 + (1-p)x_2 \in C$.

We then state a convex optimization problem in the standard form

$$\begin{array}{ll} \text{minimize} & f_0(x) \\ \text{subject to} & f_i(x) \leq 0, \ i = 1, \dots, m. \\ & a_i^T x = b_i, \ i = 1, \dots, k, \end{array} \tag{2.10}$$

where $f_0, \dots, f_m$ are convex functions from $\mathbb{R}^n$ to $\mathbb{R}$, $a_i \in \mathbb{R}^n$ and $b_i \in \mathbb{R}$. We call the set of x that satisfies these constraints as the feasible set, denoted as $\mathfrak{D}$. We usually refer this problem as the primal problem.

For this optimization problem, we rewrite the equality constraints as $h_i(x) = a_i^T x - b_i$ and then we require $h_i(x) = 0$ for each i. With this rewriting, we then define the Lagrangian $\mathfrak{L} : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^k \to \mathbb{R}$ for this problem (2.10) as

$$\mathfrak{L}(x, \nu, \lambda) = f_0(x) + \sum_{i=1}^{m} \nu_i f_i(x) + \sum_{i=1}^{k} \lambda_i h_i(x). \tag{2.11}$$

We call the vectors ν and λ as the dual variables or Lagrange multiplier vectors associated with the problem.

For each optimization problem, there is an associated Lagrange dual problem, defined as below:

$$\begin{array}{ll} \text{maximize} & g(\nu, \lambda) \\ \text{subject to} & \nu \geq 0 \end{array}, \tag{2.12}$$

where $g(\nu, \lambda) := \inf\limits_{x \in \mathfrak{D}} \mathfrak{L}(x, \nu, \lambda) = \inf\limits_{x \in \mathfrak{D}} \Big(f_0(x) + \sum_{i=1}^{m} \nu_i f_i(x) + \sum_{i=1}^{k} \lambda_i h_i(x) \Big)$. We will use the superscript $*$ to indicate the optimal value of the variable.

Let p denote the primal objective function value and d denote the dual objective function value. An important relation between the optimal value p^* of the primal objective function and optimal function value d^* of the Lagrange dual problem is called weak duality, which states $d^* \leq p^*$. This weak duality holds even if the primal problem is not convex.

Weak duality tells us that the optimal value of the primal problem is always lower bounded by the optimal value of the dual problem, which in turn is lower bounded by any value of the dual problem objective function in the dual feasible set. If the gap between p^* and d^* is zero, then we call this relation $d^* = p^*$ strong duality. For convex optimization problems, the strong duality holds if Slater's condition is satisfied. Slater's condition is that there exists a point x inside the relative interior of the feasible set $\mathfrak{D}$ such that these inequality constraints $f_i(x)$ are strictly less than zero, and all the equality constraints are satisfied.

Another useful statement is that suppose a function f is differentiable, then f is convex if and only if $\textbf{dom}f$ (domain of f) is convex and

$$f(y) \geq f(x) + \nabla f(x)^T (y - x) \tag{2.13}$$

holds for all $x, y \in \textbf{dom}f$. This is called first-order condition. The right-hand side of this inequality is the first-order Taylor approximation of f near x. For convex functions, this first-order approximation is always a lower bound of the function value.

We end this section with a special class of convex optimization problems, where the objective function is linear and we only have linear constraints and matrix nonnegativity constraints. This class is called semidefinite programs (SDP).

The feasible set of an SDP problem is within a positive semidefenite cone, which we now define.

Definition 2.17. A subset $C \subseteq \mathbb{R}^n$ is called a cone if for every $x \in C$, and for any $p \geq 0$, $px \in C$. A cone C is called a convex cone if it is also convex.

It is straightforward to check the set of positive semidefinite matrices of size n by n is a cone, which we call positive semidefinite cone. In fact, this positive semidefinite cone is convex.

We now state the standard form of an SDP problem and its dual problem.

$$\begin{aligned} \underset{X}{\text{minimize}} \quad & \langle A, X \rangle \\ \text{subject to} \quad & \langle B_i, X \rangle = b_i,\ i = 1, \ldots, m. \\ & X \succeq 0 \end{aligned} \tag{2.14}$$

Here, $B_i \in Herm(\mathcal{H})$, $b_i \in \mathbb{R}$, and $\langle \cdot, \cdot \rangle$ denotes an inner product. In this thesis, we will use Hilbert-Schmidt inner product $\langle A, X \rangle = \mathrm{Tr}\big(A^\dagger X\big)$.

The dual problem is

$$\begin{aligned} \underset{y_1,\ldots,y_m}{\text{maximize}} \quad & \sum_{i=1}^{m} b_i y_i \\ \text{subject to} \quad & \sum_{i=1}^{m} y_i B_i \succeq A \\ & y_i \in \mathbb{R},\ i = 1, \ldots, m. \end{aligned} \tag{2.15}$$

Chapter 3

Key rate calculation problem

In this chapter, we will discuss the essential components for security proofs, review the key rate formulas, present the formulation of the key rate calculation problem as a convex optimization problem, summarize the numerical approaches we use to solve this problem and show some simple examples.

To prove the security of QKD, we first need a meaningful definition of security. In Section 3.1, we present the formal definition given by Renato Renner in his PhD. thesis [32]. In Section 3.2, we specify the framework for the security analysis, including any assumptions we have to impose, and then discuss possible attack models for Eve in Section 3.3. In analyzing QKD protocols, a main theoretical problem is to calculate the secret key generation rate. In Section 3.4, we discuss the formulation of the key rate calculation problem that we will focus on for this thesis. Finally, in Section 3.5 and Section 3.6, we will summarize the numerical approaches developed in [8, 41], which we will deploy for the following chapters of this thesis. In addition, we will give some simple examples that we have used to verify the numerical approaches. These examples now serve the purposes of illustrating the numerical methods.

3.1 Formal security definition

The secret key generated by QKD is usually used in other cryptographic applications, such as one-time pad encryption scheme. The universally composable security allows us to analyze the security of each cryptographic component separately. Among many security definitions, the definition given by Renato Renner in his PhD. thesis [32] fits into the framework of universal composability. Here, we restate this definition.

Definition 3.1. A key distillation protocol KD[1] with its description of the full protocol $\mathcal{E}_{ABE\to S_AS_BE'}$, which is a completely positive map, is said to be ϵ-secure on ρ_{ABE} if the trace distance[2] between the output state $\rho_{S_AS_BE'} := \mathcal{E}_{ABE\to S_AS_BE'}(\rho_{ABE})$ and the ideal state $\sigma_{S_AS_BE'}$ is less than ϵ, that is,

$$D(\rho_{S_AS_BE'}, \sigma_{S_AS_BE'}) := \frac{1}{2}||\rho_{S_AS_BE'} - \sigma_{S_AS_BE'}||_1 \leq \epsilon,$$

where the ideal state $\sigma_{S_AS_BE'} := \sum\limits_{s\in\mathcal{S}} \frac{1}{|\mathcal{S}|} |s\rangle\langle s|_{S_A} \otimes |s\rangle\langle s|_{S_B} \otimes \rho_{E'}$ satisfies correctness, secrecy and uniform randomness, and $\{|s\rangle\}$ is a set of orthonormal vectors representing the values of the key space $\mathcal{S}$. Furthermore, this protocol is ϵ-fully secure if it is ϵ-secure on all density operators $\rho_{ABE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$.

We want to make several remarks here to give a more intuitive understanding of this definition.

Remark 3.2. $\mathcal{E}_{ABE\to S_AS_BE'}$ is not trace-preserving. In fact, the trace of the output state $\rho_{S_AS_BE'}$ is the probability that the protocol does not abort. We also notice that $\rho_{S_AS_BE'} = \sum\limits_{s,s'} p(s,s') |s\rangle\langle s|_{S_A} \otimes |s'\rangle\langle s'|_{S_B} \otimes \rho_{E'}^{(s,s')}$.

Remark 3.3. We can interpret this security definition from an operational point of view. We consider the joint probability that the protocol does not abort and the key S from this state $\rho_{S_AS_BE'}$ is not the same as the perfectly secure key U from the ideal state $\sigma_{S_AS_BE'}$. This joint probability is upper bounded by ϵ.

3.2 Framework for security proofs

Unlike classical cryptography, the security of QKD is not based on some computational assumptions. Here, Eve is only limited by the laws of quantum physics. In her possession, she has unlimited computational powers. She also has access to quantum computers and quantum memories, as well as any other advanced technology that is physically allowed.[3] To say a QKD protocol is secure, we want it to be secure not only against currently available

[1] A key distillation protocol is a generalization of a key distribution protocol.

[2] The 1-norm of a linear operator A is $||A||_1 = \mathrm{Tr}(|A|) = \mathrm{Tr}\left(\sqrt{AA^\dagger}\right)$ and the trace distance of two linear operators A and B is $D(A,B) = \frac{1}{2}||A-B||_1$.

[3] To name a few, perfect photon-number resolving devices, lossless channels.

technology, but also against future technology. QKD in theory is unconditionally secure, that is, information-theoretically secure. However, there are still explicit or even implicit assumptions in many security proofs of QKD, especially when it connects to physical implementations. Eve may exploit any gap between theory and real QKD devices, and launch so-called side-channel attacks. To prevent side-channel attacks, this gap has to be closed up either by revising the theory or improving the physical implementations, such as, adding countermeasures.

Before we proceed to analyze any QKD protocols, we briefly discuss the framework for security proofs. We review some of the common assumptions in QKD security proofs and comment on the feasibility of each assumption.

1. Eve can listen to the classical channel, but she cannot tamper the message transmitted through this classical channel since this classical channel is authenticated.
2. Eve is physically isolated from Alice's and Bob's laboratories. Eve cannot access any devices in Alice's and Bob's laboratories.
3. Alice's and Bob's physical devices behave as modeled.

The first assumption is feasible due to the development of classical cryptography. There exist information-theoretical secure message authentication schemes. Also, this classical channel is only required to be authenticated before the secret key can be generated. This authentication requires two parties to share a short secret key before they start communication. In this sense, QKD is said to be a key growing protocol. From a practical point of view, the initial secret key for authentication can also be generated by classical cryptography, such as post-quantum algorithms, since this key is only needed for a very short amount of time before any secure key from QKD can be generated [29]. Once a secure key is generated from one session of QKD, a small portion of the secret key can be used for authenticating the classical channel in the next session of QKD. Since to attack a QKD system, Eve needs to attack in real time and she cannot do it retrospectively, the security of QKD is still guaranteed if the security of the initial key cannot be broken in the required short amount of time.

The second assumption requires that Eve cannot directly learn Alice's and Bob's random bits used for preparing signals or making measurement choices or even the key itself. If such information is leaked to Eve, then Eve can break the security of the protocol. This assumption can be broken in a realistic setup through side-channel attacks. In particular, so-called Trojan horse attacks, which we will discuss more in Chapter 4, explore such a side channel. Therefore, a countermeasure is needed to prevent or minimize the information leakage, and revised security proofs might be needed to address this problem. If we can quantify the amount of the information leaked from the side channel, then we might still be able to generate secret key by applying appropriate privacy amplification.

The feasibility of the third assumption depends on the specific assumptions used in security proofs. Many security proofs may involve the characterization of these physical devices. Then if the physical implementation deviates from what is modeled, it is likely to open up a side channel for Eve to attack. Some security proofs leave the devices uncharacterized, for example, in measurement-device-independent QKD (MDI-QKD) [23], the measurement devices are not characterized, and no assumptions are put on these devices. There are also active research activities in device-independent QKD (DI-QKD), where both the sources and the measurement devices are not characterized or trusted (see, for example, Ref. [40]). Even in the DI-QKD, one may still need to impose some minimal assumptions, for example, the device does not directly leak the measurement outcomes that are used for generating secret keys to Eve through a side channel.

With regard to the optical implementation of QKD protocols using dim laser sources instead of single-photon sources, it is usually assumed that the phase of the coherent states emitted by the source is continuously randomized. This assumption about the phase randomization needs to be verified carefully. When the phase of the coherent states from the laser source is fully randomized, since Eve does not know the phase, we can prove the security in terms of the Fock states and Poisson distributions. In practice, this phase-randomization assumption may not hold. If the phase is not randomized at all, then Eve might be able to learn this phase information and then launch more powerful attacks. The key rate in this case has been shown in Ref. [24] to be much lower than that with a continuously phase-randomized source. The phase randomization can be achieved either passively or actively. For the passive phase randomization, a common assumption is that after each switch on and off of the laser source, the coherent state from the source acquires a new random phase. On the one hand, this assumption lacks a rigorous justification. On the other hand, switching on and off the laser can be a slow process to prevent the source from operating at a high clock rate. An active phase randomization process is to use an additional phase modulator to actively changing the phase of coherent states. However, a phase modulator cannot have an infinite number of settings. This might cause some deviation from the continuous phase-randomized picture. Fortunately, one can perform discrete phase randomization with just a few choices of phase to obtain almost the same key rate as with continuous phase randomization in the asymptotic case [5]. We will discuss more in Chapter 5.

This list is not exhausted. When we study security proofs, it is crucial to understand the underlying assumptions. The gap between theoretical security proofs and the physical implementations has to be closed up by relaxing those unfeasible assumptions besides improving the current technology.

3.3 Eavesdropping strategies

Historically, three categories of eavesdropping strategies have been considered in the security analysis of QKD protocols. We summarize these categories.

Individual attacks

When Alice sends the system A' that contains the signal to Bob, Eve interacts with each individual signal using the same strategy. For each signal, she may attach an ancillary system E to the system A', and then perform a unitary operator U to both the signal system A' and her system E. Then she sends A' to Bob and stores her system E in a quantum memory. At the time of her choosing, she measures her system E to gain some information about the raw key, and applies any post-processing procedures of her wish, possibly the same classical post-processing procedures as Alice and Bob. Individual attacks are weaker than collective attacks and coherent attacks.

Collective attacks

Eve interacts with each signal in the same way as in individual attacks. However, Eve has a quantum memory to store all the ancillary systems E's and then makes a collective measurement on them. She can wait until after listening to the classical communication between Alice and Bob. She uses the additional information learned from the classical communication to decide how to make her collective measurements on her systems E's and then obtain her version of the raw key. Under the assumption of collective attacks, the bipartite system between Alice and Bob after N signal transmission ρ_{AB}^N has a tensor product structure, that is, $\rho_{AB}^N = \rho_{AB}^{\otimes N}$.

Coherent attacks

Coherent attacks are the most general type of attacks. Instead of interacting with each signal individually, Eve interacts with all signals coherently. She may have one ancillary system E attached to all the signals and then make a coherent measurement at any time of her choosing.

3.4 Key rate calculation problem formulation

In this section, we will review some important steps to reduce the calculation of secret key generation rate to a convex optimization problem.

3.4.1 Reduction from coherent attacks to collective attacks

To prove the security of a QKD protocol, we need to prove it secure against the coherent attacks. On the other hand, under the assumption of the collective attacks, the density operator ρ_{AB}^{N} has a simplified structure, which is easier to analyze. Fortunately, one can simplify the security proofs against the most general attacks to the security proofs against collective attacks by entropic uncertainty principle approach [37], post-selection technique [6] or quantum de Finetti theorem [32]. For a generic QKD protocol, we can invoke the quantum de Finetti representation theorem to make such a connection. Roughly speaking, for the system composed of N rounds, if the system is invariant under permutation of subsystems corresponding to each round, then coherent attacks are not stronger than collective attacks. This means we can prove the security against collective attacks and then the proof generalizes to the coherent attacks easily.

More precisely, quantum de Finetti representation theorem states that any density operator ρ^n on $\mathcal{H}^{\otimes n}$ that is infinitely exchangeable can be written as a statistical mixture of product states $\sigma^{\otimes n}$. Infinitely exchangeable means that ρ^n is the partial state of a permutation-invariant operator ρ^{n+k} on $n+k$ subsystems, where k is arbitrary. The extension of quantum de Finetti representation theorem to the finite case has been presented in Ref. [32].

With this powerful representation theorem, we can focus our calculation under the assumption of collective attacks. Since the real state is just statistical mixture of product states, the key rate under the coherent attacks is upper bounded by the key rate of the worst-case product states under the collective attacks as we replace the statistical mixture by the state that gives Eve the most information in the mixture.

3.4.2 Finite key rate and infinite key rate formulas

After transmitting N quantum signals, Alice and Bob are able to obtain an n-bit raw key, from which they can distill an ℓ-bit secret key. The value of ℓ is given by the key rate formula.

In the case that N is finite, the finite key rate formula under the assumption of collective attacks is given as follows in Ref. [4]:

$$\frac{\ell}{N} = \frac{n}{N}\left[\min_{\mathcal{C}_\xi} H(X|E) - 7\sqrt{\frac{\log\left(\frac{2}{\bar{\epsilon}}\right)}{n}} - \frac{2}{n}\log\left(\frac{1}{\epsilon_{\text{PA}}}\right) - \frac{\delta_{\text{leak}}}{n}\right], \tag{3.1}$$

where $\mathcal{C}_\xi$ is the set containing all ρ_{AB} that are compatible with the observed data during parameter estimation, except of the probability ϵ_{PE}, X is the classical register that stores the result of key map, $\bar{\epsilon}$ is the smoothing parameter for the smooth min-entropy, ϵ_{PA} is the failure probability of the privacy amplification, and δ_{leak} is the amount of information leaked during error correction step. The total security parameter ϵ is then given by

$$\epsilon = (\epsilon_{\text{EC}} + \bar{\epsilon} + n_{\text{PE}}\epsilon_{\text{PE}} + \epsilon_{\text{PA}})(N+1)^{d^2-1},$$

where ϵ_{EC} is the failure probability that the error correction step fails to correct all errors, n_{PE} is the number of parameters that need to be estimated, and d is the dimension of single-copy signals. We also notice that the factor $(N+1)^{d^2-1}$ comes from the post-selection technique described in the Ref. [6] to generalize the security against collective attacks to coherent attacks.

By the Corrollay 6.3.5 of Ref. [32], one can bound δ_{leak} in the case of ideal error correction performed at the Shannon limit by

$$\frac{1}{n}\delta_{\text{leak}} \leq H(X|Y) + \log(5)\sqrt{\frac{3\log\left(\frac{2}{\epsilon_{EC}}\right)}{n}}, \tag{3.2}$$

where Y is the classical register that stores Bob's raw key.[4] Then the number of distillable secret bits can be chosen to be

$$\frac{\ell}{N} = \frac{n}{N}\left[\min_{\mathcal{C}_\xi} H(X|E) - 7\sqrt{\frac{\log\left(\frac{2}{\bar{\epsilon}}\right)}{n}} - \frac{2}{n}\log\left(\frac{1}{\epsilon_{\text{PA}}}\right) - H(X|Y) - \log(5)\sqrt{\frac{3\log\left(\frac{2}{\epsilon_{\text{EC}}}\right)}{n}}\right], \tag{3.3}$$

[4] We assume without loss of generality that Alice holds the register X.

We observe that these terms $7\sqrt{\frac{\log\left(\frac{2}{\bar{\epsilon}}\right)}{n}}$, $\frac{2}{n}\log\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right)$ and $\log(5)\sqrt{\frac{3\log\left(\frac{2}{\epsilon_{\mathrm{EC}}}\right)}{n}}$ in Eq. (3.3) all vanish when n (and N) goes to infinity. These terms are related to the finite-size effects since when N is smaller, their influences on the key rate become more visible. Also, they are all related to the number of signals transmitted in one QKD session, and the security parameters of individual sub-protocols used in QKD. In the finite-size key scenario, a careful analysis of these terms is needed to in order to calculate ℓ. We remark here that the study of finite-size effects is also an active research area in the field of QKD, for example, see [34]. Unfortunately, under the scope of this thesis, we won't discuss more.

In the case that N is infinite, $\frac{n}{N}$ becomes the probability that the initial signal leads to the generation of raw key, which we may also call the sifting probability or sifting factor, denoted by q. We do not need to worry about the statistical fluctuation in the parameter estimation. The relative frequencies $f(i,j)$ become the probability distribution $p(i,j)$, and the set $\mathcal{C}_\xi$ becomes the set $\mathcal{C}$ of all density matrices ρ_{AB} compatible with the observed data. Then, the infinite key rate formula becomes

$$R^\infty = q[\min_{\mathcal{C}} H(X|E) - H(X|Y)]. \tag{3.4}$$

Notice that this equation is derived under the assumption of collective attacks. We may use subscripts to indicate this. The calculation of asymptotic key rate is an important step for security proofs of QKD protocols, which allows us to compare the performance of QKD protocols and also provides an upper bound of the finite-size key rate. In this thesis, we will limit ourselves to the calculation of the asymptotic key rate.

Before we proceed to discuss how to calculate this key rate, we shoud make several comments on this formula. First of all, the asymptotic key rate formula under the collective attacks has been given by the Devetak-Winter formula in Ref. [9] as

$$r^\infty_{coll} = I(X:Y) - \chi(X:E), \tag{3.5}$$

where the definitions of X, Y and E are the same as above, and χ is the Holevo quantity. Here, we denote this key rate by r since it is the key rate per raw key (or taking the sifting factor $q=1$). The Holevo quantity is just the quantum mutual information $\chi(X:E) = H(X) + H(E) - H(XE)$. Since $I(X:Y) = H(X) + H(Y) - H(XY)$, Eq. (3.5) can also be written as

$$\begin{aligned} r^\infty_{coll} &= I(X:Y) - \chi(X:E) \\ &= H(X) + H(Y) - H(XY) - H(X) - H(E) + H(XE) \\ &= H(X|E) - H(X|Y). \end{aligned} \tag{3.6}$$

This formula is valid if we know the exact state shared by Alice and Bob. But in reality, there might be multiple states that are compatible with the parameter estimation data. Then, we need to consider the worst-case scenario in order to guarantee security. Therefore, we need to do a minimization of this key rate formula over all possible states. The key rate formula is then

$$r^{\infty}_{coll} = \min_{\rho_{AB} \in \mathcal{C}} [H(X|E) - H(X|Y)]. \tag{3.7}$$

This is exactly what we have derived in Eq. (3.3) up to the sifting factor q. In this equation (as well as in Eq. (3.3)), these conditional entropies are evaluated for the state

$$\rho_{XYE} = \sum_{j,k} p(j,k) \, |j\rangle\langle j|_X \otimes |k\rangle\langle k|_Y \otimes \rho_E^{(j,k)}.$$

Let $\{Z_A^j\}$ be the POVM that Alice uses to obtain her raw key, and $\{Z_B^k\}$ be Bob's POVM for deriving his raw key. Then $p(j,k) = \mathrm{Tr}\big(\rho_{AB} Z_A^j \otimes Z_B^k\big)$. Since the registers X and Y store the outcomes of measurements Z_A, and Z_B, respectively, we may also denote $H(X|E)$ by $H(Z_A|E)$ and $H(X|Y)$ by $H(Z_A|Z_B)$.

A final comment is that the term $H(X|Y)$ is directly determined by the observed data, and therefore can be taken outside the minimization. This term is related to the cost of error correction. Since we invoke Eq. (3.2) to derive this term, we should notice the assumption behind this term is that the error correction can be performed efficiently at the Shannon limit. In reality, this might not be possible. Then we replace this term by $f_{\mathrm{EC}} H(X|Y)$, where f_{EC} is the efficiency (or inefficiency) of the error correction and $f_{\mathrm{EC}} \geq 1$.

3.4.3 Transformation to a convex optimization problem

From the key rate formula, we have an optimization problem. The set of ρ_{AB} we need to minimize over is $\mathcal{C} = \{\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB}) : \mathrm{Tr}(\rho_{AB}\Gamma_i) = \gamma_i, i = 1, \ldots, m\}$, where m is the total number of observables in the parameter estimation sub-protocol, Γ_i's are Hermitian operators corresponding to the observables, and γ_i's are corresponding observed data. These constraints that ρ_{AB} needs to satisfy are linear constraints. The requirement that ρ_{AB} is a density matrix is decoupled into two constraints, that is, $\rho_{AB} \succeq 0$ and $\mathrm{Tr}(\rho_{AB}) = 1$. The first constraint restricts our minimization to the positive semidefinite cone, which is a convex set. The second constraint is a linear constraint, for which we can define $\Gamma_0 = \mathbb{1}_{AB}$ and $\gamma_0 = 1$. We can then rewrite the set as $\mathcal{C} = \{\rho_{AB} \in Pos(\mathcal{H}_{AB}) : \mathrm{Tr}(\rho_{AB}\Gamma_i) = \gamma_i, i = 0, 1, \ldots, m\}$.

Therefore, the optimization problem we have is of the form:

$$\begin{aligned} \underset{\rho_{AB}}{\text{minimize}} \quad & H(Z_A|E) \\ \text{subject to} \quad & \operatorname{Tr}(\rho_{AB}\Gamma_i) = \gamma_i \; i = 0, \ldots, m. \\ & \rho_{AB} \succeq 0. \end{aligned} \tag{3.8}$$

At this moment, we still need to show that the objective function $H(Z_A|E)$ is a convex function and express it without the unknown Eve's conditional state. The transformation from this optimization problem to a convex optimization problem without involving Eve's conditional state has been done in Ref. [8], which is based on Ref. [7].

The essential part of this transformation is to apply the Theorem 1 in Ref. [7]. We restate the relevant part of this theorem here.

Theorem 3.4. *Let ρ_{ABE} be a pure state and $Z = \{Z_A^j\}$ be a set of orthogonal projectors such that $\mathbb{1}_A = \sum_j Z_A^j$. We define $\tilde{\rho}_{M_zABE} := V_Z\rho_{ABE}V_Z^\dagger$ and $\tilde{\rho}_{M_ZE} = \operatorname{Tr}_{AB}(\tilde{\rho}_{M_zABE})$, where $V_Z = \sum\limits_j |j\rangle_{M_z} \otimes Z_A^j$ is an isometry used to model this Z measurement on system A, which stores the measurement outcomes in a register system M_z. Then*

$$H(Z|E) := H(\tilde{\rho}_{M_ZE}) - H(\rho_E) = D(\rho_{AB}||\sum_j Z_A^j\rho_{AB}Z_A^j). \tag{3.9}$$

The original proof can be found in Appendix C of Ref. [7]. We present this proof with more explanations here for the completeness of our discussion since this is an important result to allow us to formulate the key rate calculation problem as a convex optimization problem.

Proof. Since ρ_{ABE} is a pure state and V_Z is an isometry, $\tilde{\rho}_{M_zABE} := V_Z\rho_{ABE}V_Z^\dagger$ is also pure. Then $H(\tilde{\rho}_{M_zE}) = H(\tilde{\rho}_{AB})$ and $H(\rho_E) = H(\rho_{AB})$ directly follow from Theorem 2.14. We will use the following two observations. First,

$$\begin{aligned} \tilde{\rho}_{AB} &:= \operatorname{Tr}_{M_ZE}(\tilde{\rho}_{M_ZABE}) = \operatorname{Tr}_{M_ZE}(\sum_{j,k} |j\rangle\langle k|_{M_Z} \otimes Z_A^j\rho_{ABE}Z_A^k) \\ &= \sum_j \operatorname{Tr}_E(Z_A^j\rho_{ABE}Z_A^j) = \sum_j Z_A^j\rho_{AB}Z_A^j. \end{aligned} \tag{3.10}$$

Second, $\sum_j Z_A^j(\log\tilde{\rho}_{AB})Z_A^j = \log\tilde{\rho}_{AB}$ since Z_A^j commutes with $\tilde{\rho}_{AB} = \sum_k Z_A^k\rho_{AB}Z_A^k$ by direct computation (using the fact $\{Z_A^j\}$ are orthogonal projectors), and thus Z_A^j commutes with $\log\tilde{\rho}_{AB}$. Also, $\sum_j Z_A^jZ_A^j = \sum_j Z_A^j = \mathbb{1}_A$.

Now, putting everything together:

$$\begin{aligned}
H(Z|E) &= H(\tilde{\rho}_{M_Z E}) - H(\rho_E) && \text{(definition of } H(Z|E)\text{)}\\
&= H(\tilde{\rho}_{AB}) - H(\rho_{AB}) && \text{(from Theorem 2.14)}\\
&= -\operatorname{Tr}(\tilde{\rho}_{AB}\log\tilde{\rho}_{AB}) - H(\rho_{AB}) && \text{(definition of } H\text{)}\\
&= -\operatorname{Tr}\left(\sum_j Z_A^j \rho_{AB} Z_A^j \log\tilde{\rho}_{AB}\right) - H(\rho_{AB}) && \text{(first observation, Eq. (3.10))}\\
&= -\operatorname{Tr}\left(\rho_{AB}\sum_j Z_A^j (\log\tilde{\rho}_{AB}) Z_A^j\right) - H(\rho_{AB}) && \text{(cyclic property of trace)}\\
&= -\operatorname{Tr}(\rho_{AB}\log\tilde{\rho}_{AB}) - H(\rho_{AB}) && \text{(second observation above)}\\
&= D(\rho_{AB}||\tilde{\rho}_{AB}) = D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j) && \text{(definitions).}
\end{aligned}$$

□

The application of this theorem to QKD key rate problem is straightforward. First of all, we restrict ourselves to the protocols where $\{Z_A^j\}$ is a PVM in order to apply this theorem. We remark that for a general POVM, we can obtain a PVM by Naimark's Theorem (Theorem 2.10). Also, when we consider prepare-and-measure protocols, we usually obtain a PVM for Alice after the source-replacement scheme. Moreover, for each ρ_{AB} in the minimization, in the worst-case, Eve holds a purification of ρ_{AB}, which leads to a pure state ρ_{ABE} shared by Alice, Bob and Eve. We directly see $H(Z_A|E) = D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j)$. Now, we can write the key rate formula as

$$r_{coll}^{\infty} = \min_{\rho_{AB}\in\mathcal{C}} [D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j)] - H(Z_A|Z_B). \tag{3.11}$$

A nice property of the quantum relative entropy, as we mentioned in Section 2.3, is the joint convexity. A direct application of joint convexity implies $D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j)$ is a convex function of ρ_{AB}. In summary, we now have a convex optimization problem:

$$\begin{aligned}
\underset{\rho_{AB}}{\text{minimize}} \quad & D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j)\\
\text{subject to} \quad & \operatorname{Tr}(\rho_{AB}\Gamma_i) = \gamma_i \; i = 0, \ldots, m.\\
& \rho_{AB} \succeq 0.
\end{aligned} \tag{3.12}$$

This is the first term in the asymptotic key rate formula (Eq. (3.11)), and the second term is directly calculated from experimental data. When we refer Eq. (3.12) as our key rate calculation problem, we implicitly mean subtracting the term $H(Z_A|Z_B)$ from the optimal value obtained in this optimization problem to derive the asymptotic key rate. Since the asymptotic key rate calculation problem has been formulated as a convex optimization problem, it means this problem can be efficiently solved by computers. However, in the context of QKD security proofs, there is an additional requirement, that is, the key rate that we obtain should have a security guarantee. This means, we are interested in a reliable lower bound of the key rate, which is the physically achievable key rate, instead of an upper bound of the key rate. Unfortunately, since computers have finite-precision in representing real numbers, optimization algorithms will stop when the solution is close enough to the optimal point by some tolerance parameter. Virtually no algorithms can find the exact minimum. Since this convex optimization in Eq. (3.12) is a constrained minimization problem, by solving this problem directly, we can only obtain an upper bound of the key rate if all constraints are satisfied. Moreover, again due to the numerical imprecision, these equality constraints cannot be satisfied exactly. From our experience of tackling this problem directly, the positivity constraint on ρ_{AB} is also hard to be fulfilled as we desire. This is because in theory, ρ_{AB} can have zero eigenvalues and numerically, the minimum eigenvalue of ρ_{AB} can be slightly negative. If these constraints are not satisfied, then we do not have any good interpretation of the number output from the computer.

In the next two sections, we will discuss how to bypass these issues or how to address them directly in a rigorous way. In Section 3.5, the approach is to solve the simplified version of the Lagrange dual problem of this convex optimization problem in Eq. (3.12), which is an unconstrained maximization problem. This is the approach we adopted initially. Later on, we discovered some limitations of this approach. In Section 3.6, we then solve the primal problem via a two-step procedure, and the issues mentioned above are dealt in the second step. In the end, we obtain a reliable lower bound.

Before we discuss the numerical methods to solve Eq. (3.12), we comment on the constraints we can put in the problem. In a QKD protocol, Alice and Bob perform their measurements using POVMs $\{M_A^j\}$ and $\{M_B^k\}$, respectively. In the case of entanglement-based protocols, we have fine-grained constraints $p(i,j) = \mathrm{Tr}\big(\rho_{AB} M_A^i \otimes M_B^j\big)$, corresponding to all possible measurement outcomes. One may reduce the number of constraints by coarse-graining. A coarse-grained constraint is obtained by some post-processing of the data, such as, taking the average value or sum of a subset of observed data. We notice that by using coarse-grained constraints, the calculated key rate can only be smaller or equal to the optimal value of the calculation with fine-grained constraints since the minimization is now done with a larger set of density operators. One may use the coarse-grained constraints if the calculation can be sped up by using fewer constraints. For prepare-and-measure protocols, as we discussed in Section 2.2.3, when we use the source-replacement scheme to transform a prepare-and-measure protocol to its equivalent entanglement-based protocol, we also need to constrain ρ_A as unchanged by Eve. Therefore, in addition to the probability distribution, we constrain ρ_A by additional linear constraints. Let $\{\Omega_i\}$ be a Hermitian basis of $Herm(\mathcal{H}_A)$. We then impose additional $\Gamma'_k = \Omega_k \otimes \mathbb{1}_B$ with the expectation value $\gamma'_k = \mathrm{Tr}(\rho_A \Omega_k)$.

3.5 Dual problem approach

As we have already discussed previously, the convex optimization problem in Eq. (3.12) does not give us a lower bound for numerical reasons, and therefore cannot serve the purpose of security proofs. In this section, we summarize the dual problem approach proposed in [8].

3.5.1 Formulation of optimization problem

The main result is Theorem 1 in Ref. [8]. We restate this theorem here.

Theorem 3.5. *The minimization problem in Eq. (3.11) is lower bounded by the following maximization problem:*

$$r^{\infty}_{coll} \geq \frac{\Theta}{\ln 2} - H(Z_A|Z_B), \tag{3.13}$$

where

$$\Theta := \max_{\vec{\lambda}} \Big(- || \sum_j Z_A^j R(\vec{\lambda}) Z_A^j ||_\infty - \vec{\lambda} \cdot \vec{\gamma} \Big), \tag{3.14}$$

and

$$R(\vec{\lambda}) := \exp\Big(-\mathbb{1} - \vec{\lambda} \cdot \vec{\Gamma} \Big), \tag{3.15}$$

The infinity norm $||M||_\infty$ is defined as $||M|| = \sup_{||v||=1} ||Mv||$. When M is positive semidefinite, this norm is the same as the maximum eigenvalue of M. $\vec{\lambda}$ is the vector of dual variables λ_j from the Lagrange dual problem of Eq. (3.12) (see Section 2.5). $\vec{\Gamma}$ and $\vec{\gamma}$ are just a compact way to write Γ_i's and γ_i's.

We only describe the proof idea of this theorem here, and direct the reader to Ref. [8] for technical details. We refer the convex optimization problem in Eq. (3.12) as the primal problem. The $\ln(2)$ factor in this theorem is due to rescaling of log to ln. We denote $\alpha := \min_{\rho_{AB}\in\mathcal{C}} D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j)$ as the optimal value of the objective function and define $\hat{\alpha} = \alpha \ln(2)$. This rescaling is helpful to change all logarithms in the relative entropy to natural logarithms. As defined in Eq. (2.11), the Lagrangian function associated with the rescaled optimization problem is $\mathcal{L}(\rho_{AB}, \vec{\lambda}) = \ln(2) D(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j)) + \sum_{i=0}^m \lambda_i(\mathrm{Tr}(\rho_{AB}\Gamma_i) - \gamma_i)$. According to Eq. (2.12), the Lagrange dual problem is then

$$\max_{\vec{\lambda}} \inf_{\rho_{AB}\in Pos(\mathcal{H}_{AB})} \mathcal{L}(\rho_{AB}, \vec{\lambda}). \tag{3.16}$$

We denote the optimal value of Eq. (3.16) as $\hat{\beta}$.

Specifically, this minimization $\inf\limits_{\rho_{AB}\in Pos(\mathcal{H}_{AB})} \mathcal{L}(\rho_{AB}, \vec{\lambda})$ can be rewritten as

$$\min_{\sigma_{AB}\in\mathcal{D}(\mathcal{H}_{AB})} \min_{\rho_{AB}\in Pos(\mathcal{H}_{AB})} \left[\ln(2) D(\rho_{AB}||\sum_j Z_A^j \sigma_{AB} Z_A^j)) + \sum_{i=0}^m \lambda_i(\mathrm{Tr}(\rho_{AB}\Gamma_i) - \gamma_i) \right].$$

The inner minimization problem can be solved analytically and the optimal ρ^*_{AB} is given by $\exp\Big(-\mathbb{1}_{AB} - \vec{\lambda}\cdot\vec{\Gamma} + \ln\Big(\sum_j Z_A^j \sigma_{AB} Z_A^j\Big)\Big)$. The optimal value of this inner minimization is $-\mathrm{Tr}(\rho^*_{AB}) - \vec{\lambda}\cdot\vec{\gamma}$. Until this moment, no approximation has been introduced. To perform the outer minimization to simplify the expression, Ref. [8] applied the Golden-Thompson inequality to obtain a lower bound on the dual problem. The Golden-Thompson inequality states that for two Hermitian matrices A and B, $\mathrm{Tr}(\exp(A+B)) \leq \mathrm{Tr}(\exp(A)\exp(B))$. After using Golden-Thompson inequality to rewrite $\mathrm{Tr}(\rho^*_{AB})$, the optimization over σ_{AB} can be easily performed. In the end, the desired result of the theorem is obtained. We denote the optimal value of this simplified version of dual problem using the Golden-Thompson inequality as $\hat{\beta}'$. So, $\hat{\beta} \geq \hat{\beta}'$. Ref. [8] also shows strong duality holds. In the end, we have $\hat{\alpha} = \hat{\beta} \geq \hat{\beta}'$.

We have implemented MATLAB code to perform the key rate calculation using this approach. We adopted two-round procedure in general. In the first round, we apply the MATLAB built-in fmincon function with either the interior point method or the sequential quadratic programming (SQP) method to perform a coarse-grained search. The set of dual variables as a result of the first round is fed into the second round. In the second round, we then apply amoeba method [30] to do a refined optimization. We notice this optimization problem in Eq. (3.14) is an unconstrained maximization. The advantage of this dual problem approach is that we are guaranteed to have a reliable lower bound even if the computer terminates before reaching the optimal point. Also, the number of optimization

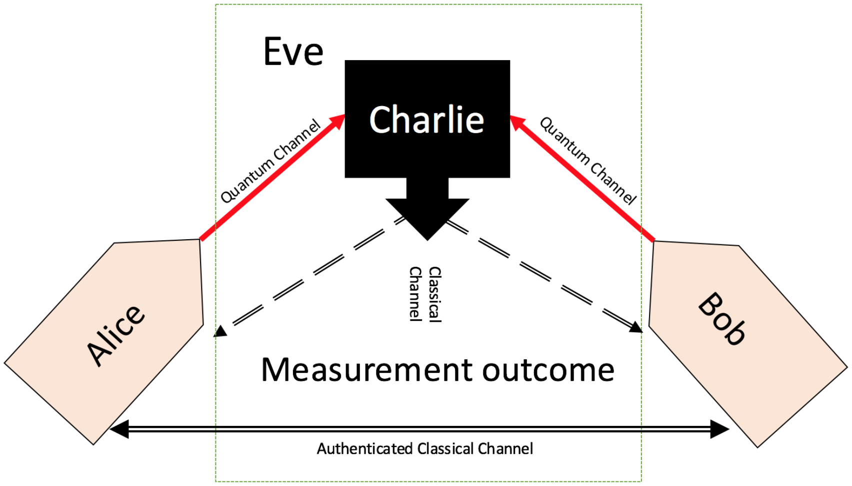

Figure 3.1: Schematic description of MDI protocols. Alice and Bob both prepare signal states and send to an untrusted third party Charlie. Charlie performs a joint measurement on both signals in a black box (from Alice and Bob's perspective) and publicly announces the measurement outcomes. In this setup, Eve can control both quantum channels and Charlie, as well as listening to the communication in the classical channel.

variables is the cardinality of $\vec{\lambda}$, which is equal to the number of constraints. Due to the non-convexity of the objective function in Eq. (3.14) as a result of the Golden-Thompson inequality, we typically perform an initial point optimization.

3.5.2 Examples: MDI QKD protocols

To test the practicality of this approach, I have applied this approach to many protocols. Now we discuss simple examples that I calculated to illustrate how to apply this numerical optimization to study a real QKD protocol. We can apply this approach to study measurement-device-independent (MDI) QKD protocols [23]. The schematic setup of this protocol is depicted in Fig. 3.1.

In each round during signal transmission, each of Alice and Bob chooses randomly and independently a signal from a set of signal states $\{|\phi_i\rangle\}$ and sends it to an untrusted third party Charlie, who then performs a joint measurement on both signals. After the measurement, Charlie publicly announces the measurement outcomes to both Alice and Bob. In MDI protocols, measurement devices are not characterized nor trusted. Since Charlie is not trusted, it could be Eve who acts as Charlie and performs any measurements of her wish. What Charlie (Eve) has to do is to make an announcement for each transmission. In MDI protocols, there are still assumptions on the sources. Both Alice's and Bob's sources are trusted and protected such that Eve cannot access them. The security of this protocol is based on post-selected entanglement. In each round, Alice prepares $|\phi_i\rangle$ for some i, Bob prepares $|\phi_j\rangle$ for some j and Charlie announces the outcome k. Then in the parameter estimation step, Alice and Bob can obtain the joint probability distribution $p(i, j, k)$ (in the asymptotic limit). From this probability distribution, Alice and Bob can verify whether they can generate secure key bits. To calculate the asymptotic key rate for MDI protocols, we apply the source-replacement schemes to both Alice and Bob. If the number of different signal states that they can choose is d_A, then the dimension of Alice's (Bob's) register A (B) is d_A. We also have the constraint that ρ_{AB} is fixed from the source-replacement scheme. Alice's source prepares an entangled state $|\Psi\rangle_{AA'} = \sum_j \sqrt{p_j}\, |j\rangle_A |\phi_j\rangle_{A'}$. Bob's source prepares the similar entangled state $|\Psi\rangle_{BB'} = \sum_j \sqrt{p_j}\, |j\rangle_B |\phi_j\rangle_{B'}$. After reordering of the systems A' and B, the initial state prepared from Alice and Bob is

$$|\Psi\rangle_{ABA'B'} = \sum_{i,j} \sqrt{p_i p_j}\, |i\rangle_A |j\rangle_B |\phi_i\rangle_{A'} |\phi_j\rangle_{B'} . \tag{3.17}$$

ρ_{AB} has the form

$$\rho_{AB} = \sum_{i,j,k,l} \sqrt{p_i p_j p_k p_l}\, \langle\phi_j|\phi_i\rangle_{A'} \langle\phi_l|\phi_k\rangle_{B'} |i\rangle\langle j|_A \otimes |k\rangle\langle l|_B . \tag{3.18}$$

MDI BB84

For simplicity, we consider the MDI QKD protocol with BB84 signal states using a perfect single-photon source.

Each of Alice and Bob prepares BB84 signal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, which are Z-basis states and X-basis states. For the normal behavior of the protocol without the intervention of Eve, Charlie is supposed to perform a Bell-state-measurement (BSM), that is, projecting onto one of the four Bell states in Eq. (2.3). Table 3.1 lists the state of the register A (similarly B) and the corresponding signal state sent to Charlie in the register A' (B') after the source-replacement scheme for this protocol. It also lists the basis choice and the bit value after applying a specific key map. This key map maps the qubit states $|0\rangle$ and $|+\rangle$ to bit value 0 and the qubit states $|1\rangle$ and $|-\rangle$ to bit value 1. We assume the implementation of the efficient BB84 protocol [22] in the MDI setting, in which one of the two bases is chosen with a high probability. By doing so, the sifting factor can be made

state of $A(B)$	state of $A'(B')$	basis choice	key bit value
$\|0\rangle$	$\|0\rangle$	Z	0
$\|1\rangle$	$\|1\rangle$	Z	1
$\|2\rangle$	$\|+\rangle$	X	0
$\|3\rangle$	$\|-\rangle$	X	1

Table 3.1: A table for this MDI QKD protocol with BB84 signal states, showing the relation between the state in Alice's (Bob's) register A (B) and the signal state prepared as well as the basis choice and bit value after applying a key map.

very close to 1. By applying the biased basis choice, we do not need to perform explicit sifting since most of the states will be prepared in the same basis. We take into account that the cost of error correction would be slightly higher than that in the case with sifting since the error rate is higher and Alice and Bob also need to correct the errors when they actually use different bases.

We performed this calculation with the dual problem approach using the two-round procedure described before with the fmincon function and the amoeba method. The set of constraints we put is the fine-grained constraints $p(i, j, k)$. To use this dual problem approach, in reality, one performs the experiments and collects the data to obtain the joint probability distribution in the asymptotic case. For our calculation, we simulate the quantum channel to produce this probability distribution. For this protocol, we vary the observed error rate and calculate the asymptotic key rate to compare with the known analytical key rate formula. We modeled the quantum channel as a depolarizing channel, which introduces noises. As for the measurements, Charlie announces which of the four Bell states he obtains during the measurement. So, we introduce a classical register C to store the announcements. This register C has a 4-dimensional state space with four orthonormal basis states corresponding to four announcement outcomes. To simulate the probability distribution, we choose the quantum channel to be composed of a depolarizing channel for each of two quantum channels depicted in Fig. 3.1 and the Bell-state measurements performed on Charlie.

Specifically, let $\mathcal{E}^{\text{dp}}_{A'B'}$ be the depolarizing channels with depolarizing probability ϵ. Then in the Kraus operator representation,

$$\tilde{\rho}_{ABA'B'} = \mathcal{I}_{AB} \otimes \mathcal{E}^{\text{dp}}_{A'B'}(\rho_{ABA'B'}) = \sum_{r,s=0}^{3} q_r q_s (\mathbb{1}_{AB} \otimes \sigma_r \otimes \sigma_s)\rho_{ABA'B'}(\mathbb{1}_{AB} \otimes \sigma_r \otimes \sigma_s),$$

where $q_0 = 1 - \frac{3\epsilon}{4}$, $q_1 = q_2 = q_3 = \frac{\epsilon}{4}$, and $\sigma_0 = \mathbb{1}_2$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$ and $\sigma_3 = \sigma_z$.

We then simulate the statistics

$$p(i,j,k) = \mathrm{Tr}(\tilde{\rho}_{ABA'B'} \left|i\right\rangle\!\left\langle i\right|_A \otimes \left|j\right\rangle\!\left\langle j\right|_B \otimes \left|\Phi_k\right\rangle\!\left\langle \Phi_k\right|_{A'B'}),$$

where $\{\left|i\right\rangle_A\}$, $\{\left|j\right\rangle_B\}$ are standard bases for systems A and B, and Φ_k are these four Bell states in Eq. (2.3) after relabeling.

After simulation, we perform the optimization with the following constraints for ρ_{ABC} of Alice, Bob and the classical announcement outcomes:

$$\begin{aligned} \Gamma^{obs}_{ijk} &= \left|i\right\rangle\!\left\langle i\right|_A \otimes \left|j\right\rangle\!\left\langle j\right|_B \left|k\right\rangle\!\left\langle k\right|_C, & \gamma^{obs}_{ijk} &= p(i,j,k) \\ \Gamma^{\rho}_{ij} &= \Omega_i \otimes \Omega_j \otimes \mathbb{1}_C, & \gamma^{\rho}_{ij} &= \mathrm{Tr}(\rho_{AB}\Omega_i \otimes \Omega_j), \end{aligned}$$

where $\{\Omega_i\}$ is a Hermitian basis of $Herm(\mathcal{H}_A)$ (as well a Hermitian basis of $Herm(\mathcal{H}_B)$), and ρ_{AB} is from Eq. (3.18).

Therefore, we have $\vec{\Gamma} = [\Gamma^{obs}_{ijk}, \Gamma^{\rho}_{sr}, \mathbb{1}_{ABC}]^T$, where each of i,j,k runs from 0 to 3 since $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = \dim(\mathcal{H}_C) = 4$, and each of s,r runs from 1 to 16 since $\dim(Herm(\mathcal{H}_A)) = 4^2 = 16$. The corresponding expectation values are $\vec{\gamma} = [\gamma^{obs}_{ijk}, \gamma^{\rho}_{sr}, 1]^T$. In total, we had 321 constraints in this case. We find that reducing the number of constraints of ρ_{AB} by only constraining the eigenvalues of ρ_{AB} gave us effectively the same results. In this case, we only had 81 constraints, which sped up the calculation.

To perform the numerical calculation, we also need to specify the key map elements $\{Z^j_A\}$. In this case, we have two elements

$$\begin{aligned} Z^0_A &= (\left|0\right\rangle\!\left\langle 0\right|_A + \left|2\right\rangle\!\left\langle 2\right|_A), \\ Z^1_A &= (\left|1\right\rangle\!\left\langle 1\right|_A + \left|3\right\rangle\!\left\langle 3\right|_A). \end{aligned}$$

In the simulation, we vary the parameter ϵ of the depolarizing channel. This parameter is related to the observed error rate Q. We calculate this error rate Q by defining the total error operator E_Q such that $Q = \mathrm{Tr}(\tilde{\rho}_{ABA'B'}E_Q)$. The exact expression of E_Q is quite long, but the way to construct E_Q is simple to describe. After projecting onto one of the Bell state, we can identify the situations where Alice and Bob would have an error. For example, conditioning on projecting onto $\left|\Phi^+\right\rangle$ state, Table 3.2 lists the situations that they would have an error. This corresponds to a term in E_Q, that is, $(\left|01\right\rangle\!\left\langle 01\right|_{AB} + \left|10\right\rangle\!\left\langle 10\right|_{AB} + \left|23\right\rangle\!\left\langle 23\right|_{AB} + \left|32\right\rangle\!\left\langle 32\right|_{AB} + \left|03\right\rangle\!\left\langle 03\right|_{AB} + \left|30\right\rangle\!\left\langle 30\right|_{AB} + \left|12\right\rangle\!\left\langle 12\right|_{AB} + \left|21\right\rangle\!\left\langle 21\right|_{AB}) \otimes \left|\Phi^+\right\rangle\!\left\langle \Phi^+\right|$. We can similarly construct the terms related to $\left|\Phi^-\right\rangle$, $\left|\Psi^+\right\rangle$ and $\left|\Psi^-\right\rangle$.

In Fig. 3.2, we show the result of this calculation. Since we only investigate how the key rate depends on the error rate due to depolarizing noises, the theoretical key rate is

State of AB	$\|01\rangle$	$\|10\rangle$	$\|23\rangle$	$\|32\rangle$	$\|03\rangle$	$\|30\rangle$	$\|12\rangle$	$\|21\rangle$
State of $A'B'$	$\|01\rangle$	$\|10\rangle$	$\|+-\rangle$	$\|-+\rangle$	$\|0-\rangle$	$\|-0\rangle$	$\|1+\rangle$	$\|+1\rangle$

Table 3.2: The list of situations that would lead to an error, conditioning on that Charlie announces the measurement outcome corresponding to $|\Phi^+\rangle$. The first row lists the state of AB after measurements of Alice and Bob. The second row lists the corresponding states they prepare for Charlie. The interpretation of these states is listed in Table 3.1.

$1 - 2h(Q)$, the same as prepare-and-measure BB84, where h is the binary entropy.[5] Our calculation using this dual problem approach reproduces the theoretical results.

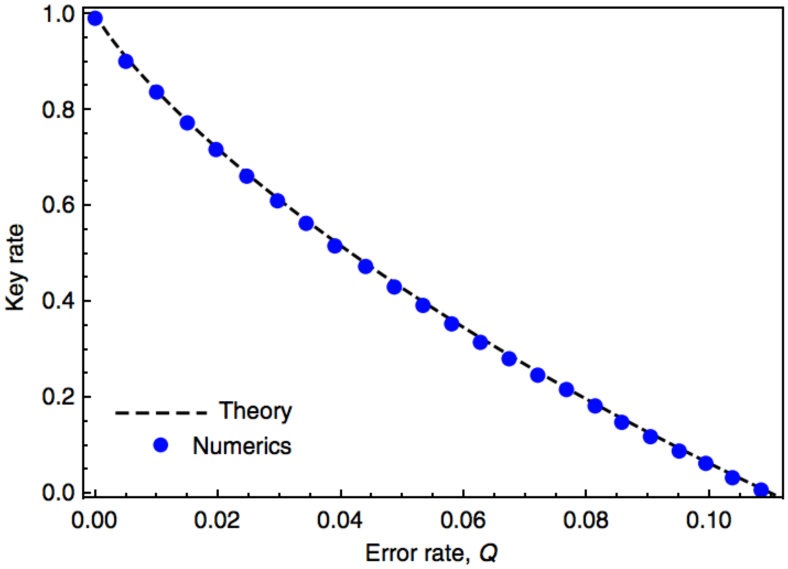

Figure 3.2: Key rate for MDI protocol with BB84 signal states using a single-photon source. This plot shows the asymptotic key rate of MDI BB84 as a function of the observed error rate Q. Blue solid dots are our numerical results using the dual problem approach described in Theorem 3.5, and black dashed line is the theoretical key rate, which is $1 - 2h(Q)$ in this case.

[5] $h(p) = -p \log(p) - (1-p)\log(1-p)$.

MDI B92

Here, we give another example to demonstrate this dual problem approach. One purpose of this example is to show how we can handle post-selection. In this protocol, instead of using a perfect single-photon source, we can use a dim laser to emit weak coherent states. The schematic setup is the same as depicted in Fig. 3.1. Instead of preparing BB84 signal states, Alice and Bob choose B92-type signal states, that is, they send one of two non-orthogonal states. Alice and Bob prepare coherent states $|+\alpha\rangle$ or $|-\alpha\rangle$.

In this protocol, Charlie (or Eve) is supposed to make announcements, chosen from the set of announcement choices that an ideal measurement can give. In a practical implementation of this protocol, Charlie ideally can perform a joint unambiguous state discrimination (USD) measurement.[6] In this joint USD, Charlie (or Eve) must distinguish between the correlated joint state $\rho^+$and anti-correlated joint state ρ^-:

$$\rho^+ = \frac{1}{2}(|\alpha,\alpha\rangle\langle\alpha,\alpha| + |-\alpha,-\alpha\rangle\langle-\alpha,-\alpha|)$$

$$\rho^- = \frac{1}{2}(|\alpha,-\alpha\rangle\langle\alpha,-\alpha| + |-\alpha,\alpha\rangle\langle-\alpha,\alpha|)$$

From these measurements, Charlie is supposed to announce one of three possible outcomes, which we denote them by " + ", " − " and "?". " + " and " − " correspond to successful discrimination of one of these two states ρ^+ and ρ^-. However, since these two states are not orthogonal, this USD measurement cannot distinguish them perfectly. There will be events when Charlie fails to discriminate, which he announces "?".

In the security proof, there is no assumption on how the measurements are actually done. We only need to have a predefined set of possible announcements. We prove the security based on the observed data. In this protocol, the possible announcements are " + ", " − " and "?". The observed data corresponding to USD measurement has the following properties: there is no error in Alice and Bob's data and there is non-zero probability for this "?" announcement. For our simulation and investigation of the performance of this protocol, we simulated the data by assuming optimal USD measurement, where the success probability is optimal allowed by quantum mechanics.

This optimal success probability is given by $1 - |\langle\alpha|-\alpha\rangle| = 1 - e^{-2|\alpha|^2}$, which has been reported in Ref. [10].

[6] The optical implementation of joint USD is straightforward and involves only beamsplitters and single-photon threshold detectors, although it is not necessarily the best measurements that could lead to the optimal key rate of this protocol. We consider this case for the ease of implementation and simplicity of simulation.

To make things even simpler, we simulated the data assuming no loss in the quantum channel. Our simulated statistics gives us the observed error rate $Q = 0$ and the probability of "?" announcement $p(\text{"?"}) = |\langle\alpha|-\alpha\rangle| = e^{-2|\alpha|^2}$.

We performed the key rate calculation with these simulated data using both the fmincon function and the amoeba method. We used coarse-grained constraints in the calculation, by only constraining the eigenvalues of ρ_{AB}, the error rate and $p(\text{"?"})$, in addition to normalization constraint on ρ_{ABC}. Here, $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = 2$ and $\dim(\mathcal{H}_C) = 3$. For the register C, $|1\rangle$ corresponds to " + ", $|2\rangle$ corresponds to " − " and $|3\rangle$ corresponds to "?". The operator corresponding to the error rate is $(|01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}) \otimes |1\rangle\langle 1|_C + (|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}) \otimes |2\rangle\langle 2|_C$. And the operator corresponds to $p(\text{"?"})$ is $\mathbb{1}_{AB} \otimes |3\rangle\langle 3|_C$. In total, we had only 7 constraints (4 of which are constraints for eigenvalues of ρ_{AB}.).

Now, we discuss the post-selection for this protocol. Since when the announcement "?" is made, there is no correlation between Alice and Bob's signals for this round, Alice and Bob have to discard this round. This post-selection corresponds to a CP map $\mathcal{G}$ such that $\tilde{\rho}_{ABC} = \frac{\mathcal{G}(\rho_{ABC})}{\mathrm{Tr}(\mathcal{G}(\rho_{ABC}))} = \frac{1}{p_{\text{pass}}}(|1\rangle\langle 1|_C\, \rho_{ABC}\, |1\rangle\langle 1|_C + |2\rangle\langle 2|_C\, \rho_{ABC}\, |2\rangle\langle 2|_C)$, where $p_{\text{pass}} = \mathrm{Tr}(\mathcal{G}(\rho_{ABC})) = p(\text{" + "}) + p(\text{" − "})$. So, if we could know what ρ_{ABC} is, we then could transform ρ_{ABC} according to this CP map and plug $\tilde{\rho}_{ABC}$ into the relative entropy expression in Eq. (3.11). The complication is that since we are dealing with the dual variables λ_i's, we need to express this CP map in terms of the dual variables. Ref. [8] provides a framework to perform this transformation, but it is slightly more involved. Here, we discuss another approach we actually used to simplify the post-selection step.

This post-selection can be done by carefully choosing Alice's key map POVM $\{Z_A^j\}$ such that all signals corresponding to the inconclusive "?" announcement will not contribute to the value of the relative entropy $D(\rho_{ABC}||\sum_j Z_A^j \rho_{ABC} Z_A^j)$. This smart choice of key map allows us to directly proceed with our dual problem.

The key map POVM $\{Z_A^j\}$ in this case actually acts on both A and C and has three elements:

$$\begin{aligned} Z^0_{ABC} &= |0\rangle\langle 0|_A \otimes \mathbb{1}_B \otimes (|1\rangle\langle 1|_C + |2\rangle\langle 2|_C), \\ Z^1_{ABC} &= |1\rangle\langle 1|_A \otimes \mathbb{1}_B \otimes (|1\rangle\langle 1|_C + |2\rangle\langle 2|_C), \\ Z^2_{ABC} &= \mathbb{1}_{AB} \otimes |3\rangle\langle 3|_C\,. \end{aligned} \tag{3.19}$$

Here we explicitly write out the identity operator on the register B, and denote them as Z^j_{ABC} instead of Z^j_A, while before implicit identity operators are assumed for BC. In Appendix A, we show the equivalence between this post-selection approach and the canonical way to perform post-selection mentioned above.

In Fig. 3.3, we showed how the asymptotic key rate of this protocol depends on the choice of coherent state. For convenience, we plot the key rate against the amplitude of the coherent state. This scenario has also been studied analytically in Ref. [10], which gives the following key rate expression:

$$R^{\infty}_{USD} = (1 - |\langle\alpha|{-\alpha}\rangle|)\left[1 - h(\frac{1 + |\langle\alpha|{-\alpha}\rangle|}{2})\right]. \tag{3.20}$$

By using only 7 constraints, our numerical calculation can reproduce the analytical result.

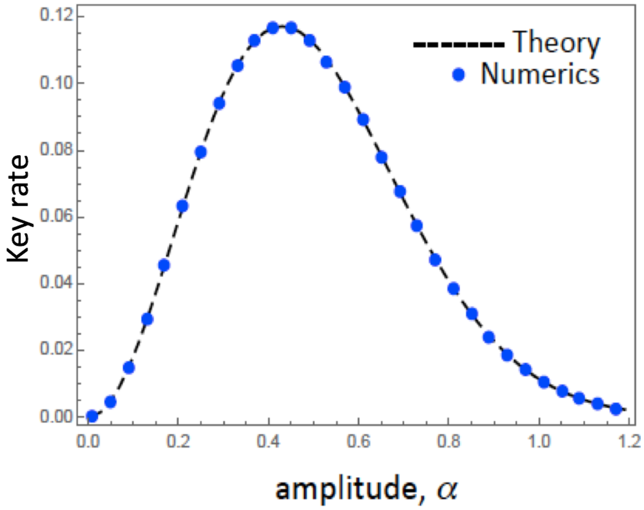

Figure 3.3: Key rate for MDI protocol with B92 signal states $|{+\alpha}\rangle$ and $|{-\alpha}\rangle$. This plot shows the asymptotic key rate of MDI B92 as a function of the amplitude of the coherent state. Blue solid dots are our numerical results using the dual problem approach described in Theorem 3.5, and black dashed line is the analytically calculated key rate in Ref. [10].

3.5.3 Limitations of this approach

The advantage of this approach is that it always gives us a reliable lower bound. For many entanglement-based protocols, especially for high-dimensional protocols, this approach can solve the key rate calculation problem efficiently since the number of optimization variables is just the number of constraints, and we can choose coarse-grained constraints such that the number of variables does not scale up with the dimension of the protocol. On the other hand, for prepare-and-measure protocols, since we need to impose ρ_A constraints, this optimization problem scales up as the number of signal states increases.

The primal problem (Eq. (3.12)) is a convex optimization problem and thus the Lagrange dual problem (Eq. (3.16)) is also convex. However, in the simplification of the dual problem to make it implementable in computers, the convexity property of the simplified version (Eq. 3.14) is lost due to Golden-Thompson inequality. In addition, this lower bound is not necessarily tight because of this inequality. In fact, when we applied this approach to protocols with more signal states, we encountered the the problem of looseness. Also due to the non-convexity of this simplified dual problem, we then have to perform some initial point optimization to try to improve the key rate, which renders the problem inefficient in this situation.

Since we deal with dual variables, it is not easy (if not impossible) to obtain a corresponding density operator that gives rise to the output key rate. Since the optimal density operator ρ_{AB} gives us some information about the optimal eavesdropping attacks, in this dual problem approach, we do not obtain such information.

In summary, this numerical method offers some advantages in solving the key rate calculation problem. However, it has its own limitations.

3.6 Primal problem approach

We now describe another approach to solve the key rate calculation problem presented in Eq. (3.11). We refer this approach as primal problem approach since we first directly solve the primal minimization problem and then derive a lower bound. This approach and its technical details are presented in Ref. [41]. In this section, we describe the general ideas.

3.6.1 Formulation of optimization problem

Fig. 3.4 depicts the essential idea behind this approach to solve the key rate calculation problem in Eq. (3.12) by thinking of a 1-dimensional abstraction. This approach involves a two-step procedure. In the first step, we try to solve this convex optimization primal problem (Eq. (3.12)) directly. As we mentioned in Section 3.4.3, there are two main issues. First, the computer is most likely to stop at a suboptimal point due to the finite precision. Then we may end up with an upper bound of the key rate, which has no security guarantee. Secondly, it is likely that this suboptimal point is actually outside the feasible region since constraints are only satisfied up to some predefined precision.

Nevertheless, the first step is to try to solve this minimization problem as good as possible. Then, in the second step, we take into account of these numerical issues to obtain a reliable lower bound. To achieve this goal, one can take the linearization from the suboptimal point. This linearization is actually the first-order Taylor approximation of the objective function at that point. Since we have a convex optimization problem, if the objective function is differentiable, and defined on a convex set, then by the first-order condition in Eq. (2.13), this linearization always gives us a lower bound. A technical detail is that the objective function that we have is not differentiable at every point in the domain. To remedy, a perturbation is introduced such that the perturbed objective function is always differentiable and the difference between the original objective function and the perturbed one is small enough. To solve this linearization problem, which is actually formulated as an SDP minimization problem (see Eq. (2.14)), we actually solve the dual problem since the dual problem is a maximization problem (see Eq. (2.15)). In such a way, we can obtain a lower bound of the optimal value, thereby giving a security guarantee in the context of QKD. So far, our discussion has ignored the issue of feasibility of the suboptimal point. If the suboptimal point is actually outside the feasible region of the primal problem, we then enlarge the set that we optimize with and take care of the issue in the formulation of the second step optimization.

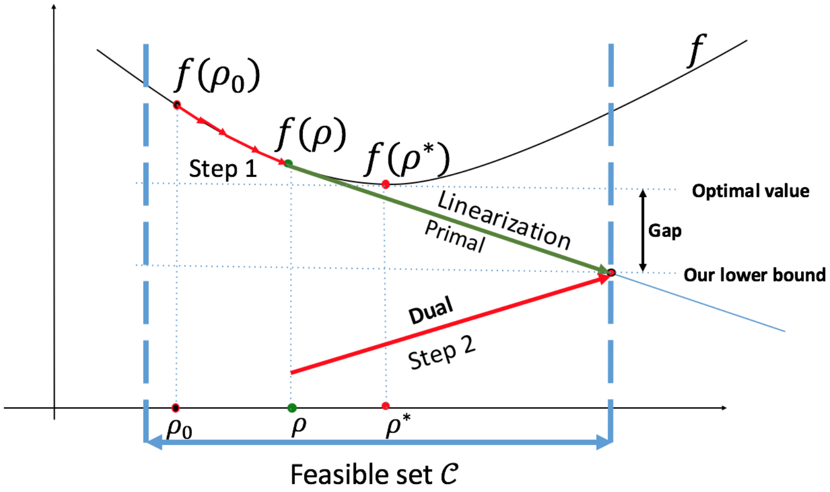

Figure 3.4: Illustration of the numerical method in a 1-dimensional abstraction. The gap between our lower bound and the optimal value can be made smaller by finding ρ closer to the optimal ρ^*. Red arrows indicate the optimizations we actually perform.

For simplicity of our discussion, we present the algorithm used in our MATLAB code and state the main theorem from Ref. [41] that allows us to perform the second step calculation.

Step 1: Finding suboptimal solution

Now, we describe the algorithm that we choose to solve the first step. In theory, we are free to choose any algorithm to obtain a suboptimal point since the security guarantee comes from the second step. However, as depicted in the Fig. 3.4, one can imagine that if we solve the first step poorly, then we need to sacrifice more in the second step. In the end, the gap between the lower bound we obtain and the true optimal value of the primal problem will be large. From a practical point of view, the key rate lower bound obtained in this situation would be too loose to have any significance. Therefore, we need to try as best as we can. For our MATLAB implementation, we adapt the Frank-Wolfe algorithm [12], which is an iterative first-order optimization algorithm. We now describe some details of applying this algorithm to our particular problem.

For the ease of notation, we define $f(\rho) := \ln(2)D(\rho|| \sum_j Z_A^j \rho Z_A^j)$, the rescaled objective function.[7] By matrix calculus, we can have an analytical expression for the gradient of f as $\nabla f(\rho) = [\ln(\rho)]^T + [\ln\Big(\sum_j Z_A^j \rho Z_A^j\Big)]^T$.

We restate the primal problem in Eq. (3.12) here.

$$\begin{aligned} \underset{\rho_{AB}}{\text{minimize}} \quad & f(\rho) \\ \text{subject to} \quad & \text{Tr}(\rho_{AB}\Gamma_i) = \gamma_i \; i = 0, \ldots, m. \\ & \rho_{AB} \succeq 0. \end{aligned}$$

We first remove these linear equality constraints by implicitly imposing these constraints into the decomposition of ρ_{AB}. Since we have a set of Hermitian operators $\{\Gamma_i\}$, we first apply the Gram-Schmidt process to obtain an orthonormal set of Hermitian operators $\{\bar{\Gamma}_k\}$ ($k \leq m$) with respect to the Hilbert-Schmidt norm. Correspondingly, we have renormalized expectation values $\bar{\gamma}_i = \langle \bar{\Gamma}_k \rangle$. Then, we can extend this set to an orthonormal basis of $Herm(\mathcal{H}_{AB})$ by finding an orthonormal basis $\{\Omega_j\}$ of the orthogonal complementary space of span($\{\bar{\Gamma}_k\}$). We then can express ρ_{AB} in this orthonormal basis $\{\bar{\Gamma}_k\} \cup \{\Omega_j\}$, and incorporate the linear equality constraints into the coefficients of $\bar{\Gamma}_k$'s. The feasible set $\mathcal{C}$ of our convex optimization contains ρ_{AB} of the form

$$\rho_{AB} = \sum_k \bar{\gamma}_k \bar{\Gamma}_k + \sum_j \omega_j \Omega_j, \tag{3.21}$$

[7] As we will see in Section B.1, if we impose any post-selection by a CP map $\mathcal{G}$, then the actual definition of our objective function is $f(\rho) = \ln(2)D(\mathcal{G}(\rho)|| \sum_j Z_A^j \mathcal{G}(\rho) Z_A^j)$. In this case, $[\nabla f(\rho)]^T = \mathcal{G}^\dagger(\ln(\mathcal{G}(\rho))) + \mathcal{G}^\dagger(\ln\Big(\sum_j Z_A^j \mathcal{G}(\rho) Z_A^j\Big))$, where $\mathcal{G}^\dagger$ is the adjoint map of $\mathcal{G}$. We do not worry about all technical details here, and just give some intuitive understanding of how this approach works.

and $\rho_{AB} \succeq 0$. $\bar{\gamma}_k$'s are fixed to make sure these linear equality constraints are satisfied. ω_j's are the variables we need to optimize with. A direct observation is that the more constraints we have for the primal problem, the fewer optimization variables we have. This is in contrast with the situation in the dual problem approach mentioned in previous section. To speed up calculation, we desire to use fine-grained constraints in this step.

Next, we define ϵ_{th} be some small non-negative number, representing the threshold value for the stopping condition of the iterations.

The algorithm runs as follows:

0. Set the iteration counter k to be 0.

1. Find a good initial point ρ_0.

   By varying optimization variables ω_j's, find $\rho_0 \in Pos(\mathcal{H}_{AB})$, where $\rho_0 = \sum_k \bar{\gamma}_k \bar{\Gamma}_k + \sum_j \omega_j \Omega_j$.

2. Solve the direction-finding subproblem.

   For the kth iteration, find the optimal $\Delta\rho$ from the following SDP problem:

$$\begin{aligned} \underset{\Delta\rho}{\text{minimize}} \quad & \operatorname{Tr}\big[(\Delta\rho)^T \nabla f(\rho_k)\big] \\ \text{subject to} \quad & \rho_k + \Delta\rho \geq 0, \end{aligned}$$

   where $\Delta\rho = \sum_j \omega_j \Omega_j$ due to our decomposition.

3. Check whether stopping criterion is satisfied:

$$|\operatorname{Tr}\big(\rho_k^T \nabla f(\rho_k)\big) - \operatorname{Tr}\big((\rho_k + \Delta\rho)^T \nabla f(\rho_k)\big)| \leq \epsilon_{\text{th}}$$

   If so, stop. Otherwise, continue.

4. Determine the step-size t.

   Find t that minimizes $f(\rho_k + t\Delta\rho)$ and $0 \leq t \leq 1$

5. Update and repeat.

   Set $\rho_{k+1} = \rho_k + t\Delta\rho$.

   Increment the counter k and go back to step 2.

Step 2: Obtaining a reliable lower bound

Once the step 1 is done, we obtain a suboptimal point ρ^{sub}. Let us denote the optimal point as ρ^*. From the first-order condition in Eq. (2.13), we have

$$f(\rho^*) \geq f(\rho^{\text{sub}}) + \operatorname{Tr}\big([\nabla f(\rho^{\text{sub}})]^T(\rho^* - \rho^{\text{sub}})\big). \tag{3.22}$$

Since we do not know what ρ^* is, we need to rewrite this equation. We notice that

$$\operatorname{Tr}\big(\nabla f(\rho^{\text{sub}})(\rho^* - \rho^{\text{sub}})^T\big) \geq \min_{\sigma\in\mathcal{C}} \operatorname{Tr}\big[(\sigma - \rho^{\text{sub}})^T \nabla f(\rho^{\text{sub}})\big],$$

since $\rho^* \in \mathcal{C}$.

Therefore,

$$\begin{aligned} f(\rho^*) &\geq f(\rho^{\text{sub}}) + \min_{\sigma\in\mathcal{C}} \operatorname{Tr}\big[(\sigma - \rho^{\text{sub}})^T \nabla f(\rho^{\text{sub}})\big] \\ &= f(\rho^{\text{sub}}) - \operatorname{Tr}\big[(\rho^{\text{sub}})^T \nabla f(\rho^{\text{sub}})\big] + \min_{\sigma\in\mathcal{C}} \operatorname{Tr}\big(\sigma^T \nabla f(\rho^{\text{sub}})\big) \end{aligned} \tag{3.23}$$

We observe that $f(\rho^{\text{sub}}) - \operatorname{Tr}\big[(\rho^{\text{sub}})^T \nabla f(\rho^{\text{sub}})\big]$ can be directly calculated after step 1 is done, and $\min_{\sigma\in\mathcal{C}} \operatorname{Tr}\big(\sigma^T \nabla f(\rho^{\text{sub}})\big)$ is a standard linear SDP problem (see Eq. (2.14)). Then, the task of the step 2 is to perform the following optimization

$$\begin{aligned} \underset{\sigma}{\text{minimize}} \quad & \operatorname{Tr}\big[\sigma^T \nabla f(\rho^{\text{sub}})\big] \\ \text{subject to} \quad & \operatorname{Tr}(\sigma\Gamma_i) = \gamma_i, i = 1, \ldots, m, \\ & \sigma \succeq 0. \end{aligned} \tag{3.24}$$

This minimization problem can be lower bounded by its dual problem (see Eq. (2.15)).

$$\begin{aligned} \underset{\vec{y}}{\text{maximize}} \quad & \vec{\gamma} \cdot \vec{y} \\ \text{subject to} \quad & \sum_i y_i \Gamma_i^T \preceq \nabla f(\rho^{\text{sub}}), \\ & \vec{y} \in \mathbb{R}^n. \end{aligned} \tag{3.25}$$

Strong duality holds for this SDP problem [41]. Therefore, the optimal objective function value of Eq. (3.24) is equal to the optimal objective function value of Eq. (3.25).

So far, we have ignored the issue that the objective function is not always differentiable. To remedy, one can define a perturbed version of the objective function $f_\epsilon(\rho) = f[(1-\epsilon)\rho + \epsilon\frac{\mathbb{1}}{d}]$, where d is the dimension of $\mathcal{H}_{AB}$ and ϵ is some small positive number that determines the perturbation.[8] Ref. [41] shows f_ϵ is always differentiable and its domain is a convex set. Then we can apply the first-order condition. It is also shown $|f(\rho) - f_\epsilon(\rho)| \leq 2\epsilon(d-1)\ln\frac{d}{\epsilon(d-1)}$.[9] Another issue to address is that the computer representations of Γ_i's and γ_i's are not precise so that the constraints are not satisfied to any arbitrary precision. To take everything into account, Ref. [41] presents the theorem that allows us to perform the step 2 calculation and to obtain a reliable lower bound. For completeness of our discussion, we present this reliable lower bound expression but without proof here.

We start with defining all relevant terms in this lower bound. Let n be the number of constraints, and let $\tilde{\Gamma}_i$, $\tilde{\gamma}_i$ be the numerical representations of the constraint Γ_i and γ_i, respectively. Let ϵ' be the tolerance of linear constraints, that is,

$$\left|\mathrm{Tr}\Big(\rho\tilde{\Gamma}_i\Big) - \tilde{\gamma}_i\right| \leq \epsilon'. \tag{3.26}$$

We define the following quantities:

$$L_\epsilon(\sigma) := f_\epsilon(\sigma) - \mathrm{Tr}\big(\sigma^T \nabla f_\epsilon(\sigma)\big) \tag{3.27}$$

$$\begin{aligned} M_{\epsilon\epsilon'}(\sigma) := \quad & \max_{\vec{y}} (\vec{\tilde{\gamma}}^T + \epsilon', -\vec{\tilde{\gamma}}^T + \epsilon')^T \cdot \vec{y} \\ \text{subject to} \quad & \sum_{i=1}^{n} y_i (\tilde{\Gamma}_i^+)^T + \sum_{i=1}^{n} y_{i+n} (\tilde{\Gamma}_i^-)^T \preceq \nabla \tilde{f}_\epsilon(\sigma), \\ & \vec{y} \in \mathbb{R}^{2n}, \end{aligned} \tag{3.28}$$

where $\tilde{\Gamma}_i^+ := \mathrm{diag}(\tilde{\Gamma}_i, \delta_{i1}, \delta_{i2}, \ldots, \delta_{in}, \vec{0}^T)$, $\tilde{\Gamma}_i^- := \mathrm{diag}(-\tilde{\Gamma}_i, \vec{0}^T, \delta_{i1}, \delta_{i2}, \ldots, \delta_{in})$, $\nabla\tilde{f}_\epsilon(\sigma) = \mathrm{diag}(\nabla f_\epsilon(\sigma), \vec{0}^T)$, where δ_{ij} is the Kronecker delta and $\vec{0}$ denotes a vector with an appropriate number of zero's such as all these three matrices are of size $2n+d$ by $2n+d$. The expansion of dimension from d to $2n+d$ is related to converting those n inequality constraints in Eq. (3.26) to $2n$ equality constraints with $2n$ slack variables.

Finally, we state the lower bound expression without proof

$$f(\rho^*) \geq L_\epsilon(\rho^{\mathrm{sub}}) + M_{\epsilon\epsilon'}(\rho^{\mathrm{sub}}) - \zeta_\epsilon, \tag{3.29}$$

[8] With the post-selection CP map $\mathcal{G}$, we define $f(\rho) = f[(1-\epsilon)\mathcal{G}(\rho) + \epsilon\frac{\mathbb{1}}{d'}]$, where d' is the dimension of $\mathcal{G}(\mathcal{H}_{AB})$.

[9] $|f(\rho) - f_\epsilon(\rho)| \leq 2\epsilon(d'-1)\ln\frac{d'}{\epsilon(d'-1)}$ in the case of post-selection.

where $\zeta_\epsilon = 2\epsilon(d-1)\ln\frac{d}{\epsilon(d-1)}$.[10]

In the limit $\epsilon \to 0$ and $\epsilon' \to 0$, we actually have an equality in Eq. (3.29).

For all the SDP subproblems, we use CVX, a package for specifying and solving convex programs [16]. We typically use the underlying solvers SDPT3 [36] and Mosek.

3.6.2 Examples

We now show simple examples to illustrate how to use this primal problem approach.

Sifting in BB84

In this primal problem approach, we directly deal with the density operators in the step 1. This allows us to manipulate the density operator with post-selection CP map. A general framework to deal with post-selection is described in Ref. [41], and a slight variation is explained in Appendix B.

In this example, we discuss how to do sifting in BB84 with polarization encoding. From source-replacement scheme, Alice's register A corresponds to a four-dimensional system. The correspondence between the state in A and the signal state in A' is the same as in Table 3.1. Suppose in this protocol, Alice prepares Z basis states with a probability p_z and X basis states with probability $1-p_z$. For simplicity of our discussion, suppose Bob has the same *a priori* probability of measurement basis choice. As shown in Ref. [1], there exists a squashing model for this protocol. This allows us to think that Bob's measurements are actually done on the Fock space restricted to vacuum and single photon. So, we model Bob's system as a qutrit, a three-dimensional system, corresponding to a qubit system and a flag that indicates no detection. We write Bob's target POVM as $M_B = \{p_z\left|0\right\rangle\!\left\langle 0\right|, p_z\left|1\right\rangle\!\left\langle 1\right|, (1-p_z)\left|+\right\rangle\!\left\langle +\right|, (1-p_z)\left|-\right\rangle\!\left\langle -\right|, \left|2\right\rangle\!\left\langle 2\right|\}$, where the state $\left|2\right\rangle$ indicates the detection of vacuum.

We then write the Kraus operators for sifting. These Kraus operators introduce a new register system R to store the basis choices. R has four orthogonal basis states corresponding to four possible combinations of Alice's and Bob's basis choices, which we

[10] $\zeta_\epsilon = 2\epsilon(d'-1)\ln\frac{d'}{\epsilon(d'-1)}$ in the case of post-selection.

denote as $|zz\rangle_R$, $|zx\rangle_R$, $|xz\rangle_R$, $|xx\rangle_R$. We define the following Kraus operators.

$$\begin{aligned}
K_{zz} &= \sqrt{(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A)} \otimes \sqrt{p_z(|0\rangle\langle 0|_B + |1\rangle\langle 1|_B)} \otimes |zz\rangle_R\,,\\
K_{zx} &= \sqrt{(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A)} \otimes \sqrt{(1-p_z)(|+\rangle\langle +|_B + |-\rangle\langle -|_B)} \otimes |zx\rangle_R\,,\\
K_{xz} &= \sqrt{(|2\rangle\langle 2|_A + |3\rangle\langle 3|_A)} \otimes \sqrt{p_z(|0\rangle\langle 0|_B + |1\rangle\langle 1|_B)} \otimes |xz\rangle_R\,,\\
K_{xx} &= \sqrt{(|2\rangle\langle 2|_A + |3\rangle\langle 3|_A)} \otimes \sqrt{(1-p_z)(|+\rangle\langle +|_B + |-\rangle\langle -|_B)} \otimes |xx\rangle_R
\end{aligned} \tag{3.30}$$

Then after the basis announcement, we transform the state ρ_{AB} by the announcement CP map $\mathcal{E}^{\text{ann}}$, $\rho^{\text{ann}}_{ABR} = \mathcal{E}^{\text{ann}}(\rho_{AB}) = \sum_{s,r} K_{sr}\rho_{AB}K^{\dagger}_{sr}$, where $s, r \in \{z, x\}$. We note that this CP map (and these Kraus operators) can be thought of as an isometry from Naimark's Theorem (Theorem 2.10) that turns the original POVM to a PVM acting on the extra register R, and then a decoherence in the register R to make it classical and public.

During sifting, Alice and Bob only keep the data when they measure in the same basis. The sifting procedure is then projecting the register R onto the subspace spanned by $\{|zz\rangle, |xx\rangle\}$. This projection operator is $\Pi = |zz\rangle\langle zz|_R + |xx\rangle\langle xx|_R$.[11] The state after sifting is $\rho^{sift}_{ABR} = \Pi\rho^{ann}_{ABR}\Pi$. In the end, the post-selection CP map $\mathcal{G}$ is just a composition of $\mathcal{E}^{\text{ann}}$ and the projection Π, that is, $\mathcal{G}(\rho_{AB}) = \Pi\mathcal{E}^{\text{ann}}(\rho_{AB})\Pi$.

The procedure of simulation can be the same as discussed in MDI examples. For simplicity, we show how the key rate depends on the error rate Q and the choice of p_z using this numerical approach. Instead of using the fine-grained constraints, we just use coarse-grained constraints, like error rate in each basis.

In Fig. 3.5, we show the key rate plot of single-photon BB84 protocol in the situation where there is no loss in transmission. In this situation, we can actually model Bob's system as a qubit system. As we vary the *a priori* probability p_z, we see how the key rate depends on the error rate Q in each case. Theoretically, we expect the key rate as $R^{\infty}_{\text{BB84}} = (p_z^2 + (1-p_z)^2)(1 - 2h(Q))$. Our numerical calculation using this primal problem approach and post-selection CP map reproduces the theoretical results.

In Fig. 3.6, we show the key rate plot of single-photon BB84 protocol in the situation where there is loss in transmission. Let η be the single-photon transmission probability. Theoretically, we expect the key rate as $R^{\infty}_{\text{BB84,loss}} = \eta(p_z^2 + (1-p_z)^2)(1 - 2h(Q))$. Our numerical calculation with this primal problem approach and post-selection CP map reproduces the theoretical results for each choice of error rate Q and *a priori* probability.

In both $\eta = 1$ and $\eta = 0.8$ scenarios, our numerical key rate bounds are tight.

[11] Identity operators on unspecified spaces are implicitly assumed.

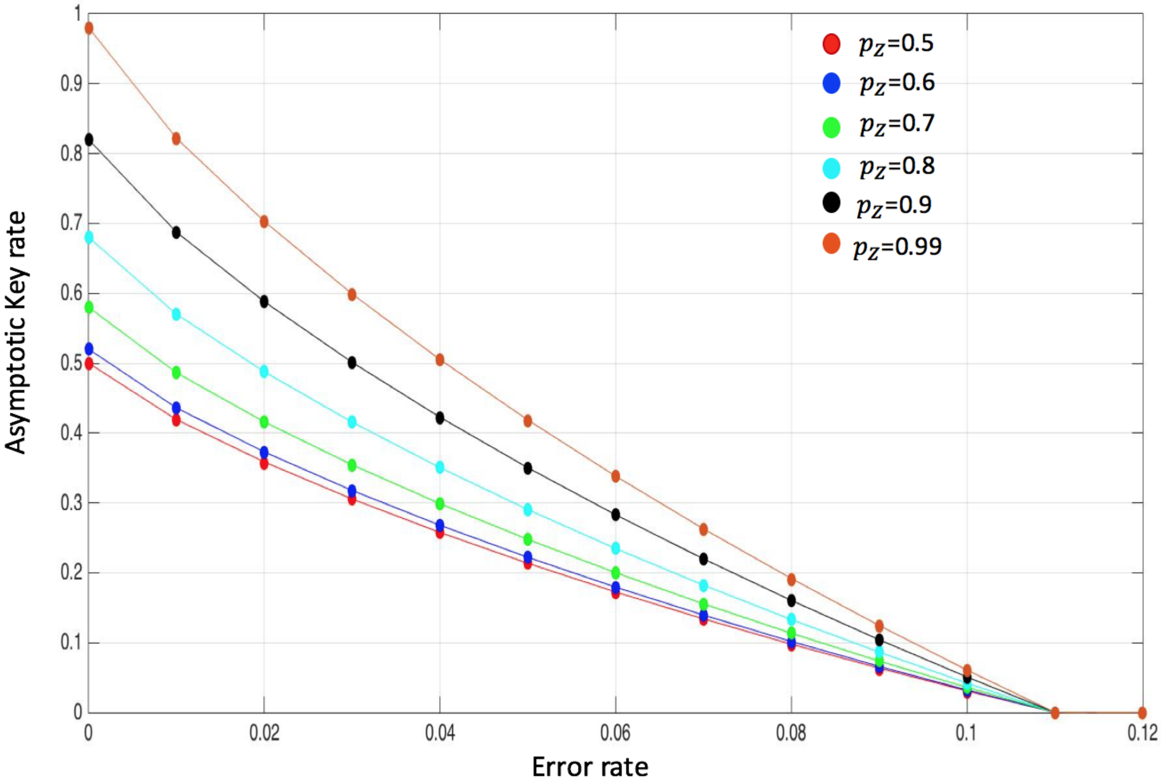

Figure 3.5: Key rate as a function of observed error rate Q for single-photon BB84 with single-photon transmission probability $\eta = 1$. The solid dots are our numerical results using the primal problem approach and the lines are given by the analytical key rate expression $R^{\infty}_{\text{BB84}} = (p_z^2 + (1-p_z)^2)(1-2h(Q))$. Different curves correspond to different *a priori* probabilities for basis choice. This is a demonstration of handling sifting in the numerical framework.

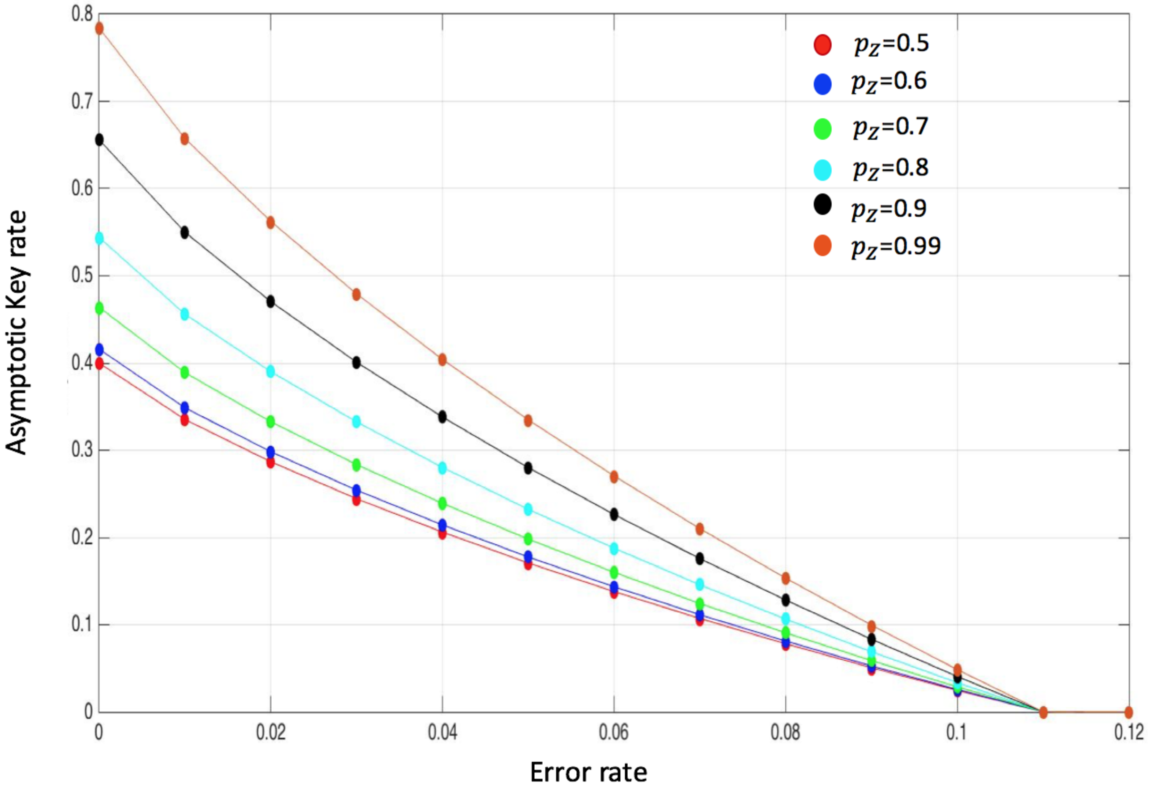

Figure 3.6: Key rate as a function of observed error rate Q for single-photon BB84 with single-photon transmission probability $\eta = 0.8$. The solid dots are our numerical results using the primal problem approach and the lines are given by the analytical key rate expression $R^{\infty}_{\text{BB84,loss}} = \eta(p_z^2 + (1-p_z)^2)(1-2h(Q))$. This figure is similar to Fig. 3.5.

We remark here that the set of Kraus operators in Eq. (3.30) applies for other variations of BB84 protocols as long as there exists a squash map that allows the reduction of Bob's measurements to target qubit measurements. We will apply the same idea described here to other suitable scenarios.

Chapter 4

Numerical security analysis for Trojan horse attacks

In this chapter, we apply the numerical approaches described in the previous chapter to analyze the security of protocols with passive optical components that act as countermeasures to prevent the so-called Trojan horse attacks.

4.1 Preliminary

In a QKD system, Alice has an encoding device to write the information of her secret random bits into some degree of freedom of photons emitted by a source.

A common assumption in many security proofs is that Eve cannot access devices in Alice's laboratory. In particular, Eve has no information about the setting of the encoding device in each round. However, since the signal needs to exit from Alice's laboratory and goes to Bob through a quantum channel, Eve can potentially inject strong lights through this quantum channel into Alice's encoding device. These lights will also go through the same encoding device and carry the same encoded information as the signal prepared by Alice. Some portion of these lights will be reflected back to Eve. Eve can perform some measurements on these back-reflected lights. Through the measurements, she can learn some information about the setting of this encoding device, which may help her unambiguously discriminate the transmitted states. In the end, Eve can end up with the same key as Alice and Bob have after the classical post-processing. If there is no mechanism to prevent the back-reflected lights, then the security of QKD can be completely compromised through this side-channel attack. This is called Trojan horse attacks(THA), as Eve intrudes the presumably secure and protected area, Alice's encoding device.

Since it was initially described in Ref. [39], many countermeasures have been proposed. However, the security analysis has not been derived for a lot of those countermeasures. Recently, Ref. [25] analyzed a passive architecture to counteract the Trojan horse attacks. I apply the numerical approaches to quantify the information leakage due to THA given this specific countermeasure.

The purpose of our calculation is two-fold. First, we want to demonstrate the applicability of the numerical approaches and have a better understanding of the advantages and disadvantages of the numerical methods. This helps for the future development of the numerical approaches. The vision we have is to develop an efficient, reliable approach to solve key rate problems, which are difficult to solve analytically. Second, since the analytical security bound in Ref. [25] can be loose due to the underlying proof techniques, we want to tighten up the key rate bound. The intuition behind this argument is that to make problems solvable by available analytical tools, analytical proofs usually resort to pessimistic lower bound, such as entropic uncertainty relation, which can make the key rate bound loose. On the other hand, our numerical methods, especially the primal problem approach described in the previous chapter, in principle, can be very tight. We know the difference between the loose lower bound and the exact key rate formula is due to the proof techniques, not because of the information leakage to Eve. Many efforts in QKD community have been devoted to improving the key rate from both theoretical point of view and from physical implementation perspectives. With a better proof technique, we can give a tighter lower bound on the key rate. From a practical point of view, this tighter lower bound allows us to distill more secure key bits than we previously thought.

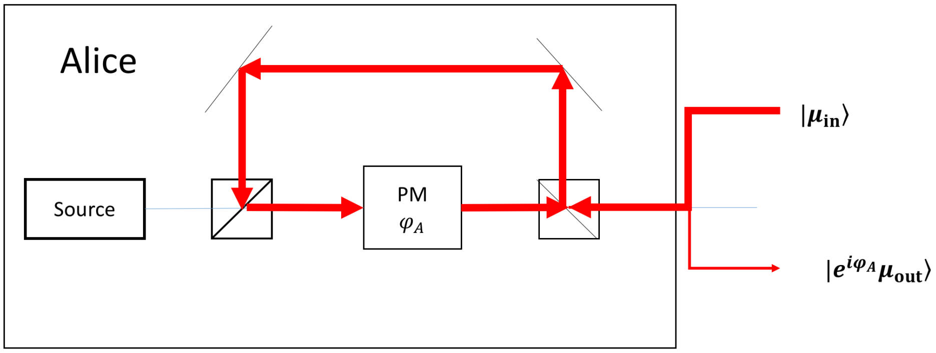
Alice
Source
PM
φ_A
$|\mu_{\text{in}}\rangle$
$|e^{i\varphi_A}\mu_{\text{out}}\rangle$

Figure 4.1: Schematics of Trojan horse attacks on Alice's devices. Eve injects a coherent light into Alice's system to probe the encoding device's setting. Some part of the light is reflected back to carry the information about the secret information. By measuring the back-reflected lights, Eve can break the security of QKD.

To make our discussion more concrete, we will focus on the unidirectional QKD setup depicted in Fig. 4.1. Here, after the source emits a pulse, it will be split into a reference pulse and a signal pulse. The photons traveling in the short arm of the interferometer will go through a phase modulator that acts as an encoding device. This phase modulator writes the phase information onto this signal pulse. Then both pulses will be transmitted to Bob. We also restrict our attentions to BB84 protocols. However, our study can be adapted to many other protocols with slight changes. Our restriction is mostly helpful for the purpose of data simulation and for dimension reduction.

A small caveat is that the numerical calculation can only handle finite-dimensional matrices. In dual problem approach, we need to make the measurement operators Γ_i finite-dimensional and in the primal problem approach, we need to make the density operator ρ_{AB} finite-dimensional. In fact, Γ_i and ρ_{AB} should have the same size to allow the calculation $\text{Tr}(\rho_{AB}\Gamma_i)$.

To be able to calculate within a suitable amount of time and with a limited computational power, it would be desirable to make Bob's dimension as small as possible so that the size of ρ_{AB} is small. On the other hand, in reality, measurements are usually done on optical modes, which live on infinite-dimensional Fock spaces. As we discussed before, we can apply an analytical tool, the squashing model, to reduce the dimension of Bob's measurements if there exists a squashing map for this connection. Other techniques, such as truncation of the infinite-dimensional space to a finite one, may also work, but may require a lot of analysis, such as the effects of truncation on the security proof. For simplicity, we restrict our attentions to the situations where we know the squashing model applies. Due to this reason, our analysis below can be generalized to protocols where a squashing map exists with a slight modification. Generalization to protocols without a squashing map may require more research.

Due to the limitation mentioned above, we need to impose some assumptions on Bob's system. We focus on the detection scheme based on two-mode interference and assume both detectors have the same efficiency (or all detectors in a passive detection scheme have the same efficiency). In reality, this assumption can be fulfilled by calibrating and setting the detector efficiency of two detectors to lower one. For this type of protocols, it has been proven in Ref. [1] that a squashing map exists, if we apply appropriate post-processing. In particular, we need to map double-click events (simultaneous clicks of both detectors) to the basis events of the target measurements. A reasonable post-processing randomly assigns a bit value for a double-click event.

4.2 Countermeasure

The study of each countermeasure requires both analyzing the behaviors of the physical devices and then quantifying the information leakage with some conditions imposed by physical devices. Within the scope of this thesis, we choose to focus on quantifying the information leakage and base our calculation on the physical properties of the countermeasure described in Ref. [25], which uses the laser induced damage threshold (LIDT) of passive optical components, such as optical fiber. Our work deviates from this existing work by using a different approach to quantify the information leakage. Nevertheless, we summarize some essential properties of this countermeasure mechanism that are relevant for our security analysis.

To limit Eve's action, this countermeasure relies on physical properties of the common optical components in a fiber-based QKD system. We can consider an optical fiber as a concrete example. The physical mechanism behind this countermeasure is that if Eve uses a laser with a sufficiently high power to probe Alice's encoding device, a lot of energy is accumulated in a small region of an optical fiber, which will increase the temperature and induce the fiber thermal damage. This damage threshold is characterized by the LIDT.

The LIDT for our purpose can be quantified by the maximum number of Trojan horse photons per second N such that Eve does not cause a permanent damage on the optical components. To effectively restrict Eve's attacks, a suitable estimation of this LIDT of

Alice's system is crucial for bounding Eve's information. In our analysis, we will see the value of LIDT affects the key generation rate.

To proceed with our security analysis, suppose N is determined by carefully examining the optical components of Alice's devices. As the phase modulator operates at some certain clock rate f_A, to maximize the amount of information Eve can learn, the best eavesdropping attack is to send Trojan horse photons at the same frequency f_A to probe each setting of the phase modulator. To probe the setting of i-th round within a second, Eve sends one coherent state $\left|\sqrt{\mu_i}\right\rangle$ with some mean photon number μ_i. Then $\sum_{i=1}^{f_A} \mu_i = f_A \mu_{\text{in}} \leq N$, where μ_{in} is the overall mean photon number. As we will show later (also shown in Ref. [25]), it is better for Eve to evenly distribute the Trojan horse photons in each round, that is, $\mu_i = \mu_{\text{in}}$. Since the maximum number of photons per second N is bounded by the physical mechanism of this countermeasure, μ_{in} is also bounded. As Alice's transmitting unit has the optical isolation factor γ such that $\mu_{\text{out}} = \gamma\mu_{\text{in}}$, to reduce the information leakage, Alice can also choose this optical isolation factor γ to limit μ_{out} in addition to reducing the LIDT value N.

For our security analysis, we have the following setup: after Eve injects a coherent state $\left|\sqrt{\mu_{\text{in}}}\right\rangle$ into Alice's system, this coherent state is modulated by the phase modulator and acquires a phase φ_A. After back-reflection, Eve obtains a coherent state $\left|e^{i\varphi_A}\sqrt{\mu_{\text{out}}}\right\rangle$. μ_{out} can be upper bounded by this countermeasure mechanism. We can think that Alice's system, not only emits the signal states she prepares, but also sends this additional coherent state to Eve. We will investigate how the value of μ_{out} influences the key rate.

4.3 Single-photon source

4.3.1 Problem setup

We first calculate the key rate when the source is an ideal single-photon source using the primal problem approach with CVX and the SDPT3 solver.

In the BB84 protocol, the set of signal states emitted from Alice's system is the following:

$$\begin{aligned}
\left|\phi_{0X}\right\rangle_{A'E} &= \left|0_X\right\rangle_{A'} \left|+\sqrt{\mu_{\text{out}}}\right\rangle_E \\
\left|\phi_{1X}\right\rangle_{A'E} &= \left|1_X\right\rangle_{A'} \left|-\sqrt{\mu_{\text{out}}}\right\rangle_E \\
\left|\phi_{0Y}\right\rangle_{A'E} &= \left|1_Y\right\rangle_{A'} \left|+i\sqrt{\mu_{\text{out}}}\right\rangle_E \\
\left|\phi_{1Y}\right\rangle_{A'E} &= \left|0_Y\right\rangle_{A'} \left|-i\sqrt{\mu_{\text{out}}}\right\rangle_E
\end{aligned} \tag{4.1}$$

Suppose Alice prepares states in the X basis with a probability p_x and in the Y basis with a probability $1 - p_x$. To analyze this protocol, we first apply the source-replacement scheme (see Section 2.2.3) to transform it into its equivalent entanglement-based protocol. Then, from Eq. (2.5), we have to constrain ρ_A to be the following

$$\rho_A = \begin{bmatrix} \frac{p_x}{2} & 0 & \frac{\sqrt{p_x(1-p_x)}}{2}V & \frac{\sqrt{p_x(1-p_x)}}{2}V^* \\ 0 & \frac{p_x}{2} & \frac{\sqrt{p_x(1-p_x)}}{2}V^* & \frac{\sqrt{p_x(1-p_x)}}{2}V \\ \frac{\sqrt{p_x(1-p_x)}}{2}V^* & \frac{\sqrt{p_x(1-p_x)}}{2}V & \frac{1-p_x}{2} & 0 \\ \frac{\sqrt{p_x(1-p_x)}}{2}V & \frac{\sqrt{p_x(1-p_x)}}{2}V^* & 0 & \frac{1-p_x}{2} \end{bmatrix}, \tag{4.2}$$

where $V = \frac{1+i}{2}e^{-(1+i)\mu_{\text{out}}}$ and V^* is the complex conjugate of V.

Now we compare the constraints we have in the numerical optimization between two scenarios. One scenario is that there are Trojan horse photons coming from Alice's laboratory due to Eve's attack. The other scenario is that the Trojan horse photons are not present when this side channel is assumed to be completely blocked. Since Trojan horse attacks explore the side channel, in the worst-case scenario, we assume Eve can split off this back-reflected light without introducing any additional disturbance. This means, Alice and Bob would observe the same statistics during parameter estimation in both scenarios. Translating into the language of our numerical framework, we notice that the constraints from the joint probability distribution are the same for these two situations. On the other hand, with this LIDT countermeasure mechanism, we can think that the source actually emits one of the four states in Eq. (4.1) in the first scenario and normal BB84 signals in the second scenario. Different signal state structures will result in different ρ_A as shown in Eq. (2.4). Since ρ_A has to be of the form in Eq. (4.6) in the first situation, we notice that constraints on ρ_A reflect the influences of Trojan horse photons. This is the main difference between the two optimization problems associated to these two scenarios.

To perform our numerical optimization, we put constraints on ρ_A in addition to coarse-grained constraints on observed statistics, such as the error rate in each basis and total detection probability.

We first investigate how the key rate depends on the mean photon number μ_{out} of Eve's coherent light. While Eve may use different intensities for different probe of Alice's phase modulation, we assume for this moment, that Eve will use the same intensity of light for each probe. From our numerical results, we will see this is actually the best strategy for her.

To compare our numerical results with the existing key rate bound, we briefly discuss the analytical key rate bound derived in Ref. [25].

Their key rate expression derives from the refinement of the "GLLP" approach [15] done by Koashi [19]. It is assumed that the efficient BB84 protocol [22] is implemented and the key is generated from the X basis. The asymptotic key rate under collective attacks is then given by

$$R^{\infty} = Q_x[1 - h(e'_Y) - f_{EC}h(e_X)], \tag{4.3}$$

where Q_X is the single-photon detection rate in the X basis, f_{EC} is the error correction efficiency, e_X is the single-photon quantum bit error rate (QBER) measured in the X basis, and e'_Y is the single-photon phase error rate, which is given by

$$\begin{aligned}
e'_Y &= e_Y + 4\Delta'(1-\Delta')(1-2e_Y) + 4(1-2\Delta')\sqrt{\Delta'(1-\Delta')e_Y(1-e_Y)},\\
\Delta' &= \frac{\Delta}{\mathcal{Y}},\\
\Delta &= \frac{1}{2}[1 - \exp(-\mu_{\text{out}})\cos(\mu_{\text{out}})],\\
\mathcal{Y} &= \min[\mathcal{Y}_X, \mathcal{Y}_Y],
\end{aligned} \tag{4.4}$$

where e_Y is the observed single-photon quantum bit error rate in the Y basis, $\mathcal{Y}_X$ and $\mathcal{Y}_Y$ are the single-photon yields[1] in the X and Y bases, respectively.

Without explaining a lot of details, we want to point out how the analytical expression changes with or without Trojan horse photons. Δ quantifies the imbalance between X-basis state and Y-basis state in the sense that the source leaks some information about which basis is used. This is because when averaged over the bit value, the state prepared in the X basis might not be the same as the state prepared in the Y basis. With an ideal single-photon source, in the absence of Trojan horse photons, these two states are actually identical. This can be seen that $\Delta = 0$ in the limit $\mu_{\text{out}} = 0$. With the presence of Trojan horse attacks, these two states become more distinguishable.

4.3.2 Numerical result

We first restrict our attention to some ideal situation, where the detector has no dark count rate and operates with the perfect efficiency, and the channel is lossless. We vary the intensity of back-reflected lights and calculate the asymptotic key rate for different observed error rates. We show this result in Fig. 4.2. Since the LIDT threshold value N

[1] The single-photon yield is the conditional probability that Bob's detectors gets a click conditioned on Alice sending a single-photon pulse.

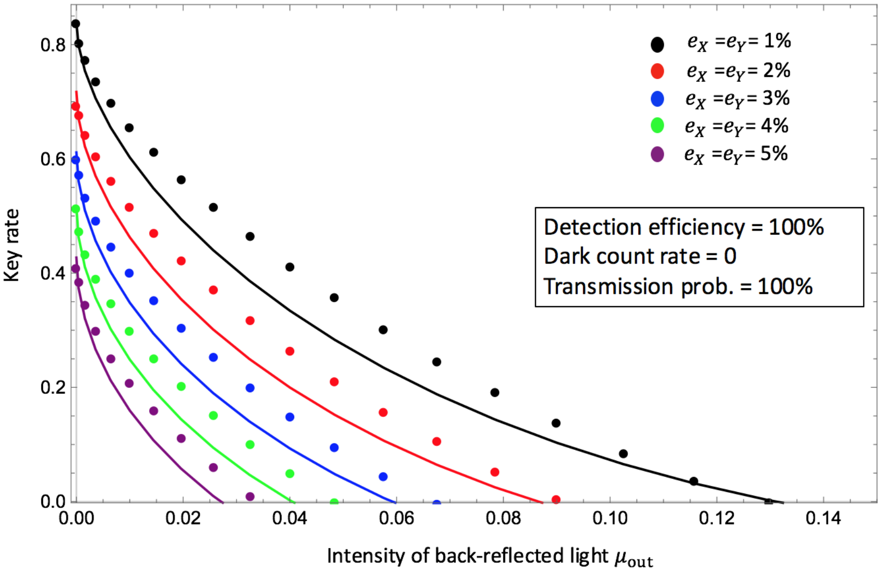

Figure 4.2: Asymptotic key rate versus the intensity of back-reflected Trojan horse light μ_{out} for different observed error rates. Solid dots are our numerical results and lines are given by Eq. (4.3). Parameters are listed in the figure. We consider ideal parameters for simplicity. We numerically observe the key rate is a convex function of μ_{out}.

is determined, Alice can choose the optical isolation factor γ to limit the intensity of back-reflected light. A plot like this can tell Alice how to choose γ. We also plot the key rate from the analytical expression in Eq. (4.3) for comparison. We directly see our numerical key rate bound is tighter than the analytical bound. Another direct observation is that the key rate is a convex function of μ_{out}. This means the best eavesdropping strategy for Eve is to send the same intensity of lights for each probe and to choose the intensity to be slightly below $\frac{N}{f_A}$, where f_A is again the clock rate of Alice's phase modulator. Also, since in this situation of ideal parameters, we know when μ_{out} is zero, the analytical bound is tight. Our numerical results reproduce the expected analytical results in this special scenario. Finally, we point out that for this specific figure shown here, we applied the dual problem approach with the fmincon function and amoeba method. However, we can also obtain similar results with the primal problem approach using CVX and the SDPT3 solver.

Moving away from the ideal parameters, we then use the set of parameters reported in Ref. [25], as shown in Table 4.1 for data simulation. We investigate how the key rate

Dark count (P_e)	1×10^{-5}
Error correction efficiency (f_{EC})	1.2
Attenuation coefficient (α)	0.2 dB/km
Detector efficiency (η_{Bob})	12.5%
Detector error probability (e_d)	0.01

Table 4.1: Parameters used in the data simulation for the key rate calculation in the case of Trojan horse attacks. Those parameters are taken from Ref. [25].

depends on the transmission distance for various back-reflected intensities.

In Fig. 4.3, we show how the key rate varies with the transmission distance for different intensities μ_{out} of back-reflected Trojan horse photons. The key rate is plotted in logarithmic scale. This calculation was done with the primal problem approach using CVX and the SDPT3 solver. We first observe that our numerical results are higher than the analytical bound for each choice of μ_{out}. As μ_{out} becomes smaller and closer to zero, the analytical key rate reaches the tight theoretical key rate bound. We see the difference between our numerical key rate values and the analytical ones become smaller as μ_{out} becomes smaller. Our numerical results agree with our expectation in the limiting cases. When μ_{out} becomes larger, the analytical key rate lower bound in Eq. (4.3) is more pessimistic in estimating the key rate. Since our numerical methods produce reliable lower bounds, we see the numerical calculation gives tighter bounds here. We also want to point out that when μ_{out} is 10^{-8}, the key rate is almost the same as that in the absence of Trojan horse attacks.

4.4 Phase-coherent laser source

Now, we consider that the source is an attenuated laser since it is commonly used in QKD. A laser emits coherent states with some intensity μ, which can be fixed for all signals. We consider the situation where the global phase of the coherent state is not randomized. We call this source a phase-coherent laser source. In particular, this phase is fixed and can be assumed to be known by Eve. Our analysis can proceed by changing the states in Eq. (4.1) to the following:

$$\begin{aligned}
|\phi_{0X}\rangle_{A'E} &= |{+}\sqrt{\mu}\rangle_{A'} \, |{+}\sqrt{\mu_{\text{out}}}\rangle_E \\
|\phi_{1X}\rangle_{A'E} &= |{-}\sqrt{\mu}\rangle_{A'} \, |{-}\sqrt{\mu_{\text{out}}}\rangle_E \\
|\phi_{0Y}\rangle_{A'E} &= |{+}i\sqrt{\mu}\rangle_{A'} \, |{+}i\sqrt{\mu_{\text{out}}}\rangle_E \\
|\phi_{1Y}\rangle_{A'E} &= |{-}i\sqrt{\mu}\rangle_{A'} \, |{-}i\sqrt{\mu_{\text{out}}}\rangle_E
\end{aligned} \tag{4.5}$$

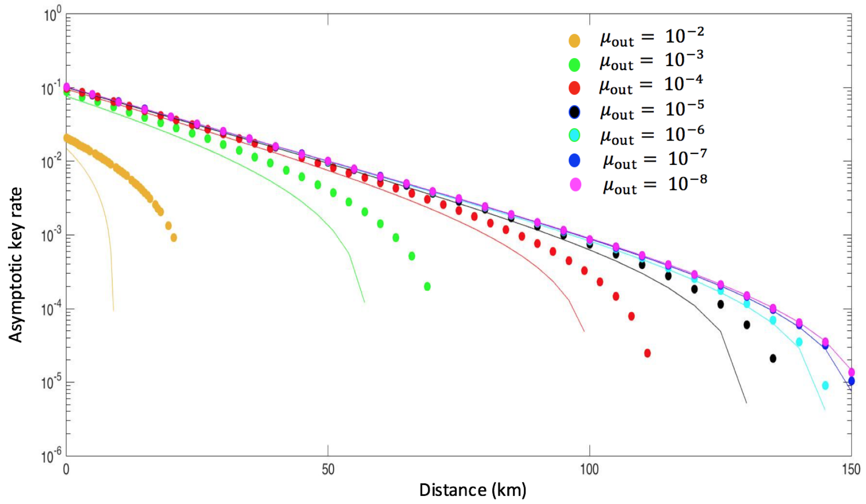

Figure 4.3: Asymptotic key rate versus the transmission distance for various intensities of back-reflected Trojan horse light $\mu_{\rm out}$. Solid dots are our numerical results and lines are given by Eq. (4.3). Parameters are listed in the Table 4.1.

Then ρ_A has the following form:

$$\rho_A = \begin{bmatrix} \frac{p_x}{2} & \frac{p_x}{2}U & \frac{\sqrt{p_x(1-p_x)}}{2}W & \frac{\sqrt{p_x(1-p_x)}}{2}W^* \\ \frac{p_x}{2}U & \frac{p_x}{2} & \frac{\sqrt{p_x(1-p_x)}}{2}W^* & \frac{\sqrt{p_x(1-p_x)}}{2}W \\ \frac{\sqrt{p_x(1-p_x)}}{2}W^* & \frac{\sqrt{p_x(1-p_x)}}{2}W & \frac{1-p_x}{2} & \frac{1-p_x}{2}U \\ \frac{\sqrt{p_x(1-p_x)}}{2}W & \frac{\sqrt{p_x(1-p_x)}}{2}W^* & \frac{1-p_x}{2}U & \frac{1-p_x}{2}, \end{bmatrix} \tag{4.6}$$

where $U = e^{-2(\mu+\mu_{\rm out})}$ and $W = e^{-(1+i)(\mu+\mu_{\rm out})}$.

Again, we compare the constraints in the presence of THA with that in the absence of THA. In particular, we consider how the constraints change from the case without THA to the case with THA. As we will discover in the end, for this type of source, the analysis for the presence of THA is simply the analysis of the protocol in the absence of THA, but with a different set of parameters. To clarify what this means, let us suppose that there exists a key rate function $R_{\rm noTHA}$ for the protocol in the absence of THA. In fact, for the purpose of our discussion, this function takes two parameters as its input, specifically, the intensity of coherent light coming out of Alice's laboratory and the single-photon transmission probability for the quantum channel between Alice and Bob. We will show that in the presence of THA, the key rate can be calculated by using the same key rate function with a different choice of values for these input parameters.

First, we look at the reduced density matrix ρ_A. As shown in Eq. (4.6), when μ_{out} becomes nonzero, we notice that in the presence of Trojan horse photons, the density matrix ρ_A associated with the signal intensity μ is replaced by the one associated with intensity $\mu + \mu_{\text{out}}$. Secondly, since the μ_{out} part of the coherent light exiting from Alice's laboratory is split off by Eve, and only μ part is sent to Bob, we can think that the single-photon transmission probability changes from η to $\eta\frac{\mu}{\mu+\mu_{\text{out}}}$ when Trojan horse photons are present. In other word, we can think that in the presence of THA, the source emits a coherent state with intensity $\mu + \mu_{\text{out}}$ and then the single photon transmission probability becomes $\eta\frac{\mu}{\mu+\mu_{\text{out}}}$ so that in the end, the intensity of light arriving at Bob's side is still $\eta\mu$. Since Bob's measurement outcomes depend on the intensity $\eta\mu$ of the arriving light, the observed statistics would be same for both the case that the source sends lights of intensity μ and the transmission probability is η and the case that the source sends lights of intensity $\mu+\mu_{\text{out}}$ and the transmission probability is $\eta\frac{\mu}{\mu+\mu_{\text{out}}}$. Since the optimization depends on the constraints on ρ_A and the constraints from the observed statistics, by thinking in terms of how constraints change in the presence of THA, we are able to find the key rate function in the presence of THA, which we denote as R_{THA} with the same set of input parameters. In summary, $R_{\text{THA}}(\mu, \eta) = R_{\text{noTHA}}(\mu + \mu_{\text{out}}, \eta\frac{\mu}{\mu+\mu_{\text{out}}})$.

Even though this equivalence can be argued in terms of constraints, we can verify it numerically. We have implemented MATLAB codes to perform both optimization problems, which effectively give us R_{THA} and R_{noTHA}. In Fig. 4.4, we show the key rate versus the intensity of Alice's signal μ for this phase-coherent protocol and we set $\mu_{\text{out}} = 10^{-3}$ to be fixed. We first see that the presence of THA decreases the key rate, compared to the protocol without THA for the same set of parameters. Also, we numerically verify that $R_{\text{THA}}(\mu, \eta) = R_{\text{noTHA}}(\mu + \mu_{\text{out}}, \eta\frac{\mu}{\mu+\mu_{\text{out}}})$. We will discuss more about this protocol without THA and the calculation of R_{noTHA} in Section 5.1. We postpone the analysis until then.

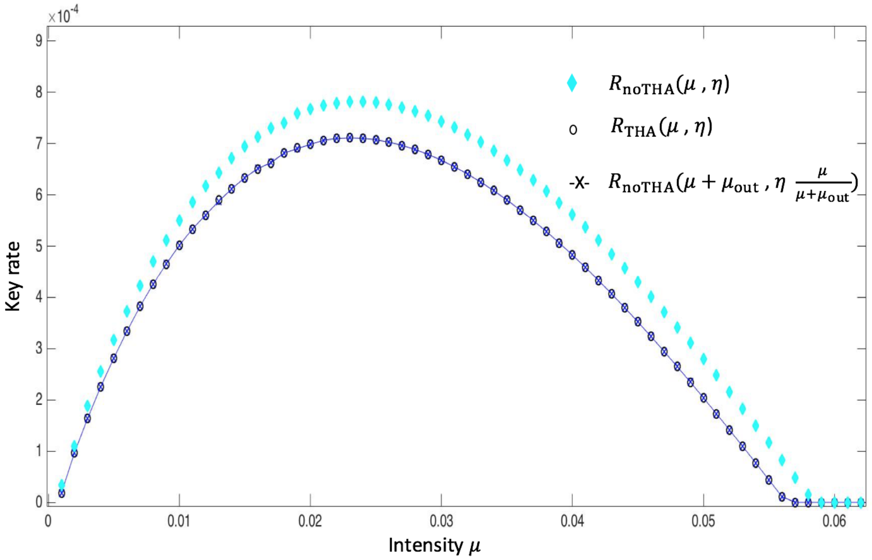

Figure 4.4: Asymptotic key rate versus the transmission distance for various intensities of Alice's signal intensity μ. $\eta = 12.5\%$. Blue diamond curve represents the key rate in the situation if we assume Trojan horse photons are completely blocked. Black circle curve represents the key rate in the case the Trojan horse photons are of intensity $\mu_{\mathrm{out}} = 10^{-3}$. The connected line represents the calculation if we assume Trojan horse photons are completely blocked, but the intensity of lights coming out from Alice's laboratory is actually $\mu + \mu_{\mathrm{out}} = \mu + 10^{-3}$ and the transmission probability is actually $\eta\frac{\mu}{\mu+\mu_{\mathrm{out}}}$. Other parameters are listed in the Table 4.1.

4.5 Phase-randomized laser source

4.5.1 Problem setup

If the laser emits a phase-randomized coherent state, that is, a state from a statistical ensemble $\{p(\theta), \left|\sqrt{\mu}e^{i\theta}\right\rangle\}$, without the information about the phase θ, Eve sees the state

$$\rho = \frac{1}{2\pi}\int_0^{2\pi} d\theta \left|\sqrt{\mu}e^{i\theta}\middle\rangle\!\middle\langle\sqrt{\mu}e^{i\theta}\right| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\left|n\middle\rangle\!\middle\langle n\right|, \tag{4.7}$$

where $p(\theta)$ is uniformly distributed. Then we can think that the source emits a Fock state $|n\rangle$ with a Poisson distribution $p_n^\mu = e^{-\mu}\frac{\mu^n}{n!}$.

For Eve, she can choose her attack strategy according to the number of photons in the signal pulse since Eve can first perform quantum non-demolition measurements for each signal pulse to obtain the number of photons in the pulse. Since in multi-photon pulses, each photon carries the same secret information, Eve can launch so-called photon-number-splitting (PNS) attack [26]. For $n \geq 2$, Eve can split out just one photon to forward to Bob and keep the remaining $n-1$ photons in her quantum memory. She then postpones her measurements until listening to the communication during the classical phase of the protocol. In this way, she is able to measure these photons in the same basis as Alice or Bob. Thus, for multi-photon pulses, Eve learns every single bit value without introducing any disturbance. In summary, multi-photon pulses leak complete information to Eve and no secure bits can be generated.

On the other hand, Alice does not know exactly which of her pulses contain single photons and which contain multiple photons. She can only estimate the contribution of multi-photon pulses and assume Eve knows everything about these pulses. Then she needs to apply appropriate privacy amplification to reduce Eve's information to a negligible amount. In the security analysis, the idea of tagging is helpful.

We can think the signals coming from Alice live in a seven-dimensional space. All multi-photon signals ($n \geq 2$) leak complete information to Eve so that multi-photon signals can be represented by four orthogonal states. We denote them by $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$. Since they are four orthogonal states, Eve can perfectly discriminate them.

Without Trojan horse attacks, we would model Alice's system A as a nine-dimensional space since she would send one of these 9 states listed in Table 4.2.

With Trojan horse attacks, since Eve's Trojan horse photons can still carry some information about the setting of phase modulator even if Alice's source emits a vacuum state. Eve can use this information. For example, if she successfully learns the phase information, then she can prepare a photon with this phase information for Alice and send to Bob. In this way, she can block more parts of the single-photon contribution where she fails to learn the phase information to discriminate the states unambiguously. Since Alice does not know how many photons her pulse contains, by doing this, Eve can learn more information. Therefore, it is important to distinguish these four states even if Alice sends a vacuum. With Trojan horse photons, there are actually 12 signal states listed in Table 4.3.

Again, since Alice does not know how many photons her pulse contains, each observation has three contributing components, vacuum, single-photon and multi-photon. This

state	*a priori* probability	meaning of the state
$\vert\emptyset\rangle$	p_0^μ	vacuum state
$\vert 0_X\rangle$	$p_1^\mu \frac{p_x}{2}$	state 0 in X basis for single-photon component
$\vert 1_X\rangle$	$p_1^\mu \frac{p_x}{2}$	state 1 in X basis for single-photon component
$\vert 0_Y\rangle$	$p_1^\mu \frac{1-p_x}{2}$	state 0 in Y basis for single-photon component
$\vert 1_Y\rangle$	$p_1^\mu \frac{1-p_x}{2}$	state 1 in Y basis for single-photon component
$\vert H\rangle$	$p_{\text{multi}}^\mu \frac{p_x}{2}$	state 0 in X basis for multi-photon component
$\vert V\rangle$	$p_{\text{multi}}^\mu \frac{p_x}{2}$	state 1 in X basis for multi-photon component
$\vert D\rangle$	$p_{\text{multi}}^\mu \frac{1-p_x}{2}$	state 0 in Y basis for multi-photon component
$\vert A\rangle$	$p_{\text{multi}}^\mu \frac{1-p_x}{2}$	state 1 in Y basis for multi-photon component

Table 4.2: Signal states and *a priori* probability distribution for the phase-randomized laser source. By using the idea of tagging, we can think that the source emits one of these nine states. p_0^μ is the probability of emitting vacuum state from a Poisson distribution with mean photon number μ. Similarly, p_1^μ is the probability of emitting single photons, and p_{multi}^μ for multi-photons.

Alice's register state	signal state	*a priori* probability	basis	bit value
$\vert 0\rangle$	$\vert\emptyset\rangle \left\vert +\sqrt{\mu_{\text{out}}}\right\rangle$	$p_0^\mu \frac{p_x}{2}$	X	0
$\vert 1\rangle$	$\vert\emptyset\rangle \left\vert -\sqrt{\mu_{\text{out}}}\right\rangle$	$p_0^\mu \frac{p_x}{2}$	X	1
$\vert 2\rangle$	$\vert\emptyset\rangle \left\vert +i\sqrt{\mu_{\text{out}}}\right\rangle$	$p_0^\mu \frac{1-p_x}{2}$	Y	0
$\vert 3\rangle$	$\vert\emptyset\rangle \left\vert -i\sqrt{\mu_{\text{out}}}\right\rangle$	$p_0^\mu \frac{1-p_x}{2}$	Y	1
$\vert 4\rangle$	$\vert 0_X\rangle \left\vert +\sqrt{\mu_{\text{out}}}\right\rangle$	$p_1^\mu \frac{p_x}{2}$	X	0
$\vert 5\rangle$	$\vert 1_X\rangle \left\vert -\sqrt{\mu_{\text{out}}}\right\rangle$	$p_1^\mu \frac{p_x}{2}$	X	1
$\vert 6\rangle$	$\vert 0_Y\rangle \left\vert +i\sqrt{\mu_{\text{out}}}\right\rangle$	$p_1^\mu \frac{1-p_x}{2}$	Y	0
$\vert 7\rangle$	$\vert 1_Y\rangle \left\vert -i\sqrt{\mu_{\text{out}}}\right\rangle$	$p_1^\mu \frac{1-p_x}{2}$	Y	1
$\vert 8\rangle$	$\vert H\rangle$	$p_{\text{multi}}^\mu \frac{p_x}{2}$	X	0
$\vert 9\rangle$	$\vert V\rangle$	$p_{\text{multi}}^\mu \frac{p_x}{2}$	X	1
$\vert 10\rangle$	$\vert D\rangle$	$p_{\text{multi}}^\mu \frac{1-p_x}{2}$	Y	0
$\vert 11\rangle$	$\vert A\rangle$	$p_{\text{multi}}^\mu \frac{1-p_x}{2}$	Y	1

Table 4.3: Source-replacement states for phase-randomized laser source. By using the idea of tagging, we can think the source emits one of these 12 states. The meaning of probabilities is the same as in Table 4.2. Since multi-photon states are orthogonal to each other, there is no need to attach Trojan horse pulses because Eve has complete knowledge.

means, for the measurement operators M_A, for example, if she wants to project onto the 0 state of X basis, the corresponding measurement operator is defined as $M_A^{0X} = |0\rangle\langle 0| + |4\rangle\langle 4| + |8\rangle\langle 8|$. On Bob's side, since we assume both detectors have the same efficiency, there exists a squashing model such that Bob's measurements can be treated as measurements on a qutrit system as discussed before. In the end, we optimize ρ_{AB} of size 36 by 36.

4.5.2 Numerical result

We performed the calculation with the primal problem approach using CVX and the SDPT3 solver. In Fig. 4.5, we see that first of all, compared with the single-photon source (Fig. 4.3), the key rate drops dramatically. This is expected from the difference between single-photon BB84 and weak-coherent-pulse BB84 in the absence of THA. Also, as expected, as the Trojan horse intensity μ_{out} becomes stronger, the key rate decreases because Eve can learn more information with stronger back-reflected lights. For $\mu_{\text{out}} = 10^{-5}$ and $\mu_{\text{out}} = 10^{-6}$, the difference is small. Without decoy states, the maximum transmission distance is limited. We plan to have a calculation with decoy state methods. If we assume that Eve can also attack the phase modulator, but not the intensity modulator used for the decoy-state setting, then the analysis can be generalized to the calculation with decoy states straightforwardly. In our numerical optimization, we then impose additional inequality constraints for the single-photon error rate and single-photon yield from the decoy-state method. The extension to Trojan horse attacks on both the intensity modulator and the phase modulator requires a significant modification of our problem setup. We expect to solve this problem once we are able to deal with decoy states directly in our numerical framework.

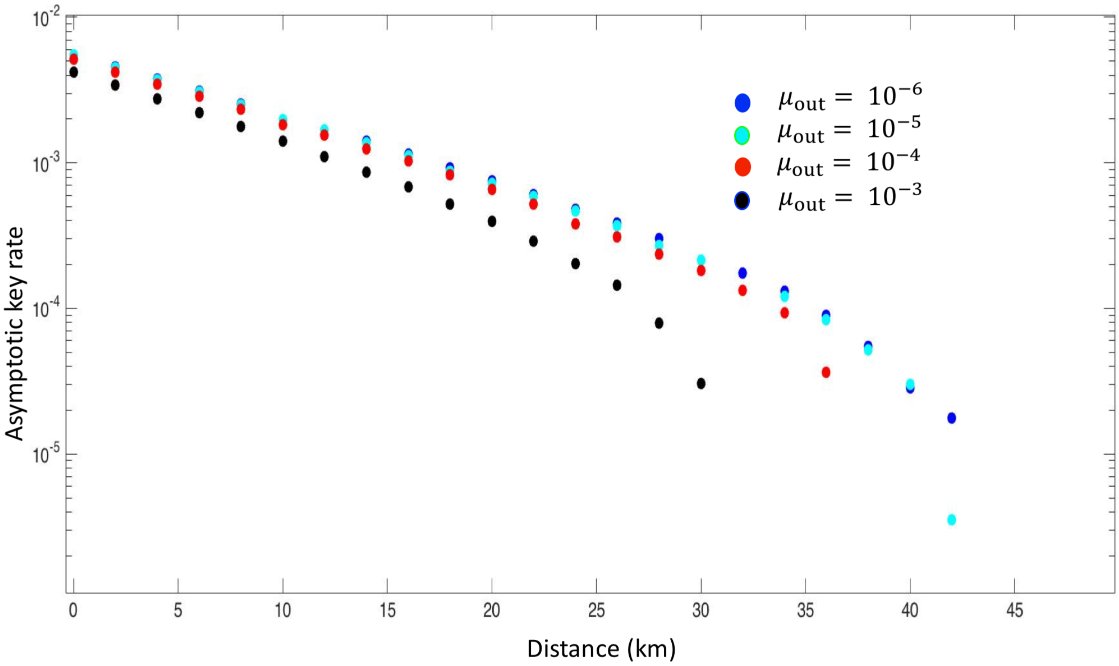

Figure 4.5: The asymptotic key rate versus the transmission distance for a phase-randomized coherent state source for different intensities of back-reflected lights μ_{out}. Solid dots are our numerical results.

Chapter 5

Numerical security analysis of coherent-state BB84 protocols

Unconditional security of the QKD protocols was first proven for single-photon sources [21, 28, 35]. However, even to date, no efficient and reliable single-photon source with a high clock rate is commerically available. Experimental implementations of QKD and commercial QKD devices commonly use attenuated laser sources instead of single-photon sources since lasers with integrated circuits can make clock rates in the order of GHz possible. A laser source emits coherent states, which has a non-zero probability to emit multi-photon pulses. Multi-photon pulses are vulnerable to photon number splitting attacks. Fortunately, the unconditional security of QKD with laser sources has also been proven [15, 18].

The physical implementation of a QKD protocol can deviate from the theory in many aspects, intentionally or unintentionally. An assumption in security proofs [15, 18] is that the phase of coherent states is totally random such that Eve has no *a priori* information about the phase. As we discussed before, if the phase is truly random, the laser source effectively prepares photon number Fock states with a Poisson distribution. However, this assumption may not hold in many implementations. For example, for protocols with a strong reference pulse, the phase of this reference pulse can be correctly measured and may be correlated with the phase of the signal pulse. Also, even for weak pulses, if the same global phase is used for many pulses, the phase information may also be determined unambiguously. While the phase randomization can be achieved by active phase randomization using an additional phase modulator, some implementations in favor of high clock rate may avoid this additional phase modulator and also maintain the phase coherence. Even for the active phase randomization, since the phase modulator has a finite number of settings, the phase is not random enough to allow us to obtain a Fock state picture. In this chapter, I apply the numerical methods to study a protocol with the phase information known by Eve and to study discrete-phase-randomization. We will also compare our numerical results with other existing analytical or semi-analytical analysis.

For concrete discussions, we consider BB84 protocols with phase-encoding. Specifically, the pulse emitted from a laser will be split into a reference pulse and a signal pulse by an interferometer. We will focus on the protocols where the reference pulse has the same intensity as the signal pulse. We remark that an extension to strong reference protocols can be obtained straightforwardly in our numerical framework.

5.1 Phase-coherent laser source

We consider the phase-encoding BB84 protocol with a phase-coherent laser source. A similar version of this protocol was proposed in Ref. [17]. The schematic setup of this protocol is shown in Fig. 5.1.

5.1.1 Problem setup

The source emits a coherent state with an intensity of 2μ. After the first 50/50 beam splitter, each of the signal pulse and the reference pulse has an intensity of μ. Since the information is encoded in the relative phase between a signal pulse and a reference pulse, we consider a two-mode representation of the signals. Effectively, Alice prepares one of the following BB84 states:

$$\begin{aligned} |0_Z\rangle_{A'} &= |{+\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \,, \\ |1_Z\rangle_{A'} &= |{-\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \,, \\ |0_X\rangle_{A'} &= |{+i\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \,, \\ |1_X\rangle_{A'} &= |{-i\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \,, \end{aligned} \tag{5.1}$$

where we denote the signal pulse by a subscript s and the reference pulse by r.

We consider the measurements with an active basis choice. For a double-click event, Bob randomly assigns the bit value 0 or 1. A squashing map exists for this protocol as shown in Ref [1]. We model Bob's measurements as qubit measurements with an additional flag for the detection of vacuum. Then we can describe Alice and Bob's joint state ρ_{AB} by a 12×12 matrix.

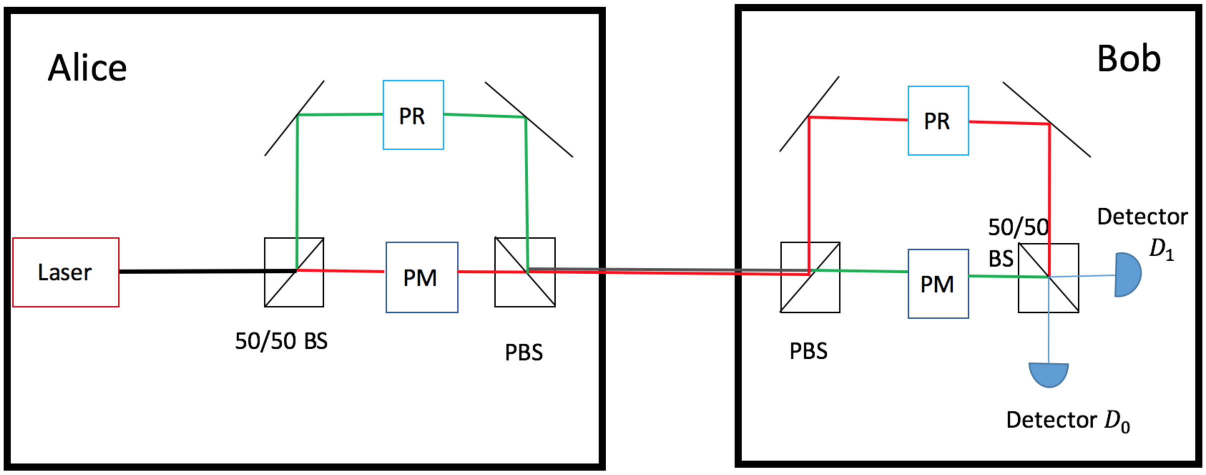

Figure 5.1: Schematics of the phase-encoding BB84 protocol: the attenuated laser source emits a coherent state, which is split by the 50/50 beam splitter (BS) into a reference pulse and a signal pulse. A phase modulator (PM) is used to encode the information about the secret key in the signal pulse. Both the signal pulse and the reference pulse are transmitted through the same fiber to Bob. One may use polarization rotators (PR) and polarizing beam splitters (PBS) to pack the signal and reference pulses for transmission. (Or one can apply adjustable time delay to the pulses such that they arrive at the same time at the interferometer in Bob's lab.) In Bob's lab, he applies 0 or $\frac{\pi}{2}$ phase shift to the reference pulse via a phase modulator (PM). This allows him to choose the measurement basis. The signal pulse and the reference pulse will then interfere at the 50/50 beam splitter and trigger one of the detectors.

Dark count rate (P_e)	8.5×10^{-7}
Error correction efficiency (f_{EC})	1.16
Detector efficiency (η_{Bob})	0.045
Detector error probability (e_d)	0.033
Attenuation coefficient (α)	0.2 dB/km

Table 5.1: Simulation parameters for this BB84 protocol with phase-encoding using a phase-coherent laser source.

In our data simulation, we characterize some imperfection of detectors. Specifically, we adopt parameters from the experiment reported in Ref. [14]. We assume two detectors have the same efficiency η_{Bob}. In addition, we consider background noises, such as dark count and stray light. P_e is the probability of an error count per clock cycle of a single detector due to the background noise. For simplicity of our simulation, we use the same background noise probability for both detectors. From the listed parameters, we can simulate the joint probability distribution $p(x, y)$ that we would observe from the test set during the parameter estimation if we actually ran an experiment with these parameters. Since the number of free variables in the first step of the primal problem approach is the number of free variables in the operator space to describe a density matrix, the more linearly independent constraints on the density matrix ρ_{AB} we have, the fewer free variables we have and then the faster the first-step calculation will be. In reality, this corresponds to Alice and Bob disclosing all available information about the test sets during the parameter estimation and applying a fine-grained analysis.

For the error correction term, the error correction efficiency is assumed to be 1.16 for all error rates. The cost of error correction is directly computed from observed statistics, in particular, the observed error rate of the key-generating basis, E_μ. Therefore, $\text{leak}_{EC} = f_{\text{EC}} h(E_\mu)$ in our calculation.

We briefly mention some statistics from our simulation here. The total detection probability Q_μ has two contributing factors, background noise and detection of signals. We use $Q_\mu = 2P_e + (1 - e^{-\eta\mu})$, where we ignore higher-order terms in P_e. η is the total transmission probability for single-photons. For a distance L measured in km, $\eta = 10^{-\frac{\alpha L}{10}} \eta_{\text{Bob}}$. We assume the click due to the background noise is random so that the error rate for this event is $\frac{1}{2}$. Then $E_\mu = \frac{P_e + (1-e^{-\eta\mu})e_d}{Q_\mu}$.

Ref. [24] has analyzed this protocol based on the "GLLP" framework. The analytical key rate formula is as follows:

$$R^\infty = Q_\mu[1 - f_{\text{EC}}(E_\mu)h(E_\mu) - h(E_\mu^{\text{ph}})], \tag{5.2}$$

where we take the sifting factor to be 1 and E_{μ}^{ph} is the phase error rate given by the following equations:

$$
\begin{aligned}
E_{\mu}^{\text{ph}} &= E_{\mu} + 4\Delta'(1-\Delta')(1-2E_{\mu}) + 4(1-2\Delta')\sqrt{\Delta'(1-\Delta')E_{\mu}(1-E_{\mu})},\\
\Delta' &= \frac{\Delta}{Q_{\mu}},\\
\Delta &= \frac{1}{2}[1-e^{-\frac{\mu}{2}}(\cos\Big(\frac{\mu}{2}\Big)+\sin\Big(\frac{\mu}{2}\Big))].
\end{aligned}
\tag{5.3}
$$

We will compare our numerical results with this anaytical key rate formula.

5.1.2 Numerical results

In Fig. 5.2, we plot the asymptotic key rate versus the intensity μ of the signal pulse for the parameters in Table 5.1. In this figure, we show two transmission distances $L = 0$ km and $L = 5$ km for illustration. If we look at the highest key rate value in the plot corresponding to an optimal μ, our numerical results give roughly three times higher key rate than analytical results. Also, for each distance plotted here, the optimal μ from our numerical results is larger than the optimal value given by the analytical result. For example, for $L = 0$ ($\eta = 0.045$), the optimal intensity μ from the numerical result is roughly 0.008, while with the same intensity, the analytical key rate is zero. We believe this discrepancy is due to pessimistic estimation in the analytical formula. We notice that the analytical key rate formula in Eq. (5.2) requires an estimation of the phase error rate, which cannot be observed directly from the experiments. The phase error rate expression in Eq. (5.3) is an upper bound estimation of the actual phase error rate. To have a sense of those numbers, with $\mu = 0.008$ and $\eta = 0.045$, we observe that $\Delta \approx 8 \times 10^{-6}, Q_{\mu} \approx 3.62 \times 10^{-4}$ and $E_{\mu} \approx 0.035$. This gives us $\Delta' \approx 0.022$. Then the estimation of the phase error rate by Eq. (5.3) is roughly 21.8%. From our numerical results, we believe this phase error rate estimation is too loose when the transmission probability is low.

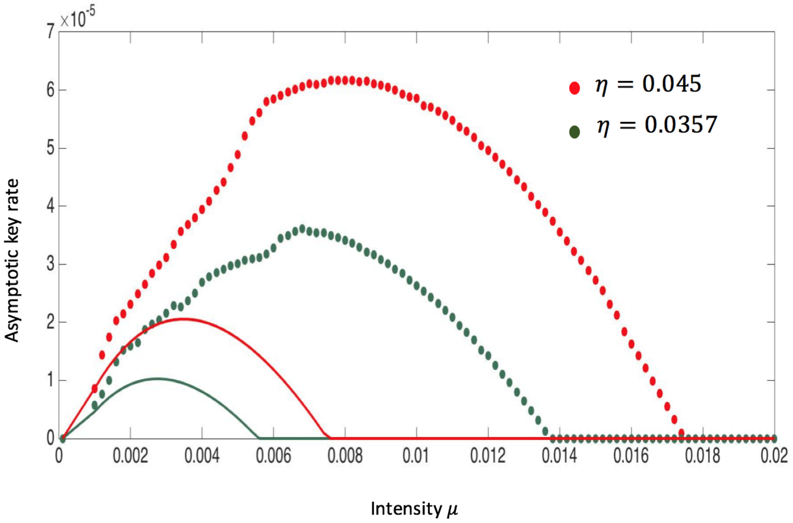

Figure 5.2: The asymptotic key rate versus the intensity μ of the signal pulse for this phase-encoding BB84 protocol using phase-coherent laser source for different transmission probabilities $\eta = 0.045$ ($L = 0$ km) and $\eta = 0.0357$ ($L = 5$ km) for the parameters listed in Table 5.1. The phase information is assumed to be known by Eve. Solid dots are our numerical results and lines are given by the analytical expression in Ref. [24].

We remark that the non-smoothness of the curve in Fig. 5.2 is due to the numerical instability. This figure was generated using the primal problem approach with CVX and the Mosek solver. As we discussed in Section 3.6, the gap between our lower bound and the optimal value depends on how close the suboptimal point from the first step is to the optimal point. Potentially, the curve can be smoothed by an improved first step calculation of the primal problem approach to obtain a better ρ_{AB} that is closer to the optimal ρ^*_{AB} for each point. Nevertheless, we have seen that the numerical method gives a tighter key rate bound than the analytical bound.

We also consider some ideal parameters by setting the dark count rate to zero, detector efficiency to 100% and the detector error rate to 0. In Fig. 5.3, we plot the asymptotic key rate versus the intensity μ of the signal for $\eta = 1$ and $\eta = 0.8$. We notice that in this ideal parameter region, the difference between the analytical results and numerical results is less dramatic. We do not observe a region of intensities where the analytical result is zero, but the numerical result is significantly non-zero.

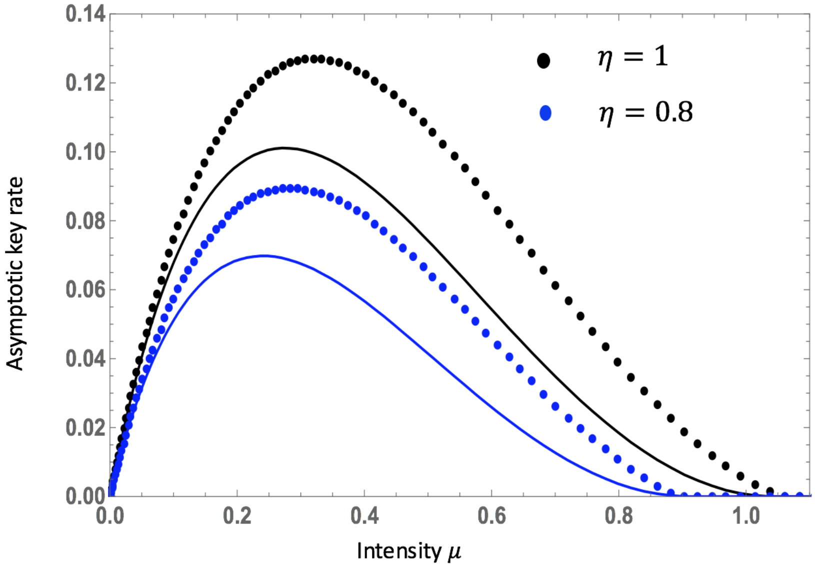

Figure 5.3: The asymptotic key rate versus the intensity μ of the signal pulse for this phase-encoding BB84 protocol using phase-coherent laser source for two values of total transmission probability $\eta = 1$ and $\eta = 0.8$. The phase information is assumed to be known by Eve. Other simulation parameters, such as dark count rate, are ideal as described in the main text. Solid dots are our numerical results and lines are given by the analytical expression in Ref. [24].

5.2 Discrete phase randomization

We notice that if the phase is known by Eve, the key rate is significantly lower than the key rate with phase-randomized coherent states. It is important to verify this phase randomization assumption in the realistic QKD devices. The phase randomization in some setups is assumed to be done passively. For the passive phase randomization, it is usually believed that after each switch on and off of the laser, the phase coherence is destroyed. However, there is no rigorous argument to prove this phase is actually random and to show that there is no residual correlation between the phases of two consecutive pulses. Any residual correlation may leak some information to Eve. In this section, we focus on the active phase randomization scenario. The active phase randomization uses an additional phase modulator to change the phase of coherent states. It is inserted immediately after the laser source as shown in Fig. 5.4. By actively modulating the phase of the coherent state from the source before it is split into a reference and a signal pulse, both pulses acquire the same global phase. A realistic phase modulator cannot create an infinitely many choices of phase to be applied to the coherent pulses from the source. With the active phase modulation, we cannot achieve the continuous phase randomization. Instead, we need to consider the number of possible random phases is finite. Also, to be more practical, these random phases are chosen from a prescribed finite set of phases. Since adding more phases into the settings of the phase modulator imposes higher demand on the precision and control of the phase modulator, it is more desired to use a small number of phases. In this section, I apply the numerical methods, in particular, the primal problem approach, to study the effects of discrete phase randomization.

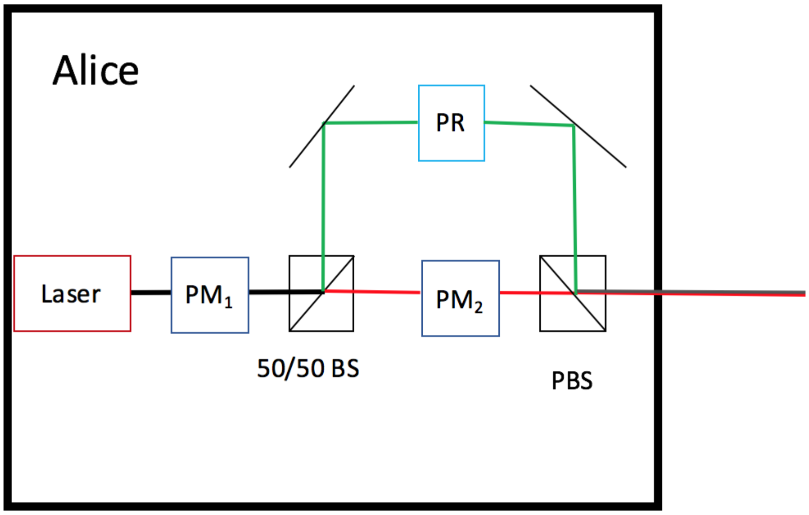

Figure 5.4: The schematics of Alice's device. Compared with Fig. 5.1, an additional phase modulator (PM$_1$) is inserted immediately after the source to randomize the phase of coherent states. This phase modulator randomly applies one of the N possible choices of phase to each coherent state before it is split into a reference pulse and a signal pulse.

5.2.1 Problem setup

If the source is only discretely phase-randomized, it deviates from the behaviors of a continuous phase-randomized source. This deviation may leak some information to Eve. We need to quantify the information leakage and to see how the key rate is affected. Suppose the phase modulator PM_1 in the Fig. 5.4 has N possible settings. Then the laser source and this phase modulator together effectively create a discrete-phase-randomized source. This discrete-phase-randomized source emits a coherent state whose phase is chosen uniformly randomly from N possible choices. A natural choice of those N possible phases is to let these N phases be evenly distributed in $[0, 2\pi)$. Each phase is chosen with a probability $\frac{1}{N}$. For our concrete discussion, we assume the phase is an integer multiple of $\frac{2\pi}{N}$ between 0 and 2π. We remark here that other choices are possible and for each different choice, we simply rerun our calculation with the simple modification of the signal states. However, an inappropriate choice may leak more information to Eve and thus results in a lower key rate.

For my calculation, I take the signal states to have the following general structure

$$\left|\sqrt{\mu}e^{i(\theta+\phi)}\right\rangle_s \left|\sqrt{\mu}e^{i\theta}\right\rangle_r \tag{5.4}$$

where $\phi \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ and $\theta = \frac{2\pi k}{N}$ for $k = 0, 1, \ldots, N-1$. ϕ encodes the secret information and the four choices correspond to four BB84 signal states. θ is the introduced random phase for both the signal pulse and the reference pulse. In the case of N choices of phases, we see Alice prepares $4N$ different signal states.

The data simulation for observed statistics is done with the same parameters listed in Table 5.1. This is also the set of parameters used in Ref. [5]. Using the same set of parameters allows us to directly compare our results with the existing semi-analytical results. We briefly summarize the analysis in Ref. [5]. In the case of discrete phase randomization, since we cannot think the signal states in terms of the Fock states, Ref. [5] considers approximated Fock states with N phases. When N goes to infinity, these approximated Fock states become the actual Fock states. It then quantifies the information leakage from the source due to imbalance of Z-basis signals and X-basis signals, and applies the "GLLP" approach to calculate the key rate. It performs a minimization of the key rate formula subject to a few parameters, such as, the single-photon error rate and the single-photon yield since the observed statistics can only constrain the range of those parameters. Due to the combination of the analytical analysis and the numerical optimization, we refer the results in Ref. [5] as semi-analytical results. We also want to point out that when N is small, these approximated Fock states deviate significantly from the Fock states.

5.2.2 Numerical results

For our calculation, we use the fine-grained constraints. It is important to notice that in the parameter estimation step, Alice can also disclose the information about the value of θ for each pulse since she can record this information. By doing so, Alice and Bob can perform a refined analysis. They can obtain a probability distribution for each phase and then use all the information together to bound Eve's information.

In Fig. 5.5, we plot our numerical results for $N = 1, 2, 3$ and 4 along with the results reported in Ref. [5]. The key rate is plotted in the logarithmic scale. This figure was generated using the primal problem approach with CVX. The first-step calculation in the primal problem approach was done with the SDPT3 solver and the second-step was done with the Mosek solver. We show how the key rate changes with the transmission distance. By comparing the curves for $N = 1$ and $N = 2$, our results show that there is a big jump in the key rate when the number of phases is increased to two. This is in contrast to the previous result. We believe that two phases should have a significant impact on the key rate. The intuition behind this is that if the phase is known to Eve, then Eve can launch more powerful attacks, like unambiguous state discrimination in conjunction with intercept and resend attacks. One possibility is that Eve tries to discriminate these four BB84 signal states for the signal pulse. Another possibility is that for each transmission, for the signal pulse, Eve tries to discriminate the Z-basis states from the X-basis states and upon the successful discrimination, Eve can measure the signal pulse in the correct basis as it is prepared by Alice. Another less favorable situation is that since those signals will be mapped to 0's and 1's, Eve may try to discriminate the signal states that will be mapped to 0 from the signal states that will be mapped to 1. In all these scenarios, Eve can attack on the signal pulse only. If the channel loss is high enough, whenever she fails to discriminate, she can block the transmission, and hide her attacks by the channel loss. In the case that she successfully discriminates, she can then prepare corresponding states to Bob.

$$\begin{aligned}
|0_Z, \theta = 0\rangle &= |{+\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \\
|1_Z, \theta = 0\rangle &= |{-\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \\
|0_X, \theta = 0\rangle &= |{+i\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r \\
|1_X, \theta = 0\rangle &= |{-i\sqrt{\mu}}\rangle_s \, |\sqrt{\mu}\rangle_r
\end{aligned} \tag{5.5}$$

$$
\begin{aligned}
\left|0_Z, \theta = \pi\right\rangle &= \left|-\sqrt{\mu}\right\rangle_s \left|-\sqrt{\mu}\right\rangle_r \\
\left|1_Z, \theta = \pi\right\rangle &= \left|+\sqrt{\mu}\right\rangle_s \left|-\sqrt{\mu}\right\rangle_r \\
\left|0_X, \theta = \pi\right\rangle &= \left|-i\sqrt{\mu}\right\rangle_s \left|-\sqrt{\mu}\right\rangle_r \\
\left|1_X \theta = \pi\right\rangle &= \left|+i\sqrt{\mu}\right\rangle_s \left|-\sqrt{\mu}\right\rangle_r
\end{aligned}
\tag{5.6}
$$

Intuitively, we expect that those attack strategies become less possible when an additional phase is introduced. To see this, we observe that in the case $N = 2$, Alice effectively prepares these two sets of signals given in Eq. (5.5) and Eq. (5.6).If Eve only tries to discriminate from the signal pulse, then without knowing the global phase, even if she successfully discriminates the four states for the signal pulse, she cannot determine the bit value. This is because without the information about θ, for example, $\left|+\sqrt{\mu}\right\rangle_s$ can be mapped to 0 if the phase θ is 0 and it can also mapped to 1 if θ is π. Therefore, by only discriminating the signal pulse, she is equally likely to guess 0 and 1 for each round. In order to learn the bit information, she may also need to discriminate the reference pulse in order to determine whether she is in the first scenario given by Eq. (5.5) or in the second scenario given by Eq. (5.6). Then the success probability for the unambiguous state discrimination decreases significantly once a second phase is introduced. While the success probability continues to decrease with the introduction of the third phase or more, we do not expect the decrease is as significant as the case from $N = 1$ to $N = 2$. From this intuition, we expect there is a significant improvement from $N = 1$ to $N = 2$ and small improvement from $N = 2$ to $N = 3$ or more. Our numerical results match with this intuition.

We observe the significant increase in the key rate from $N = 1$ to $N = 2$. Our numerical results show a marginal improvement from 2 to 3 phases and from 3 to 4 phases. The results with 3 and 4 phases basically reproduce the key rate of a continuously phase-randomized source. We also notice that for long distances (above 35 km), our numerical results give loose bound. We expect the discrepancy for long distances between our numerical results and the results reported in Ref. [5] can be explained by the numerical instability. We may be able to improve our numerical results for those points with better numerical solvers. In this study, we do not consider the decoy-state methods. In the future work, we want to also include decoy states.

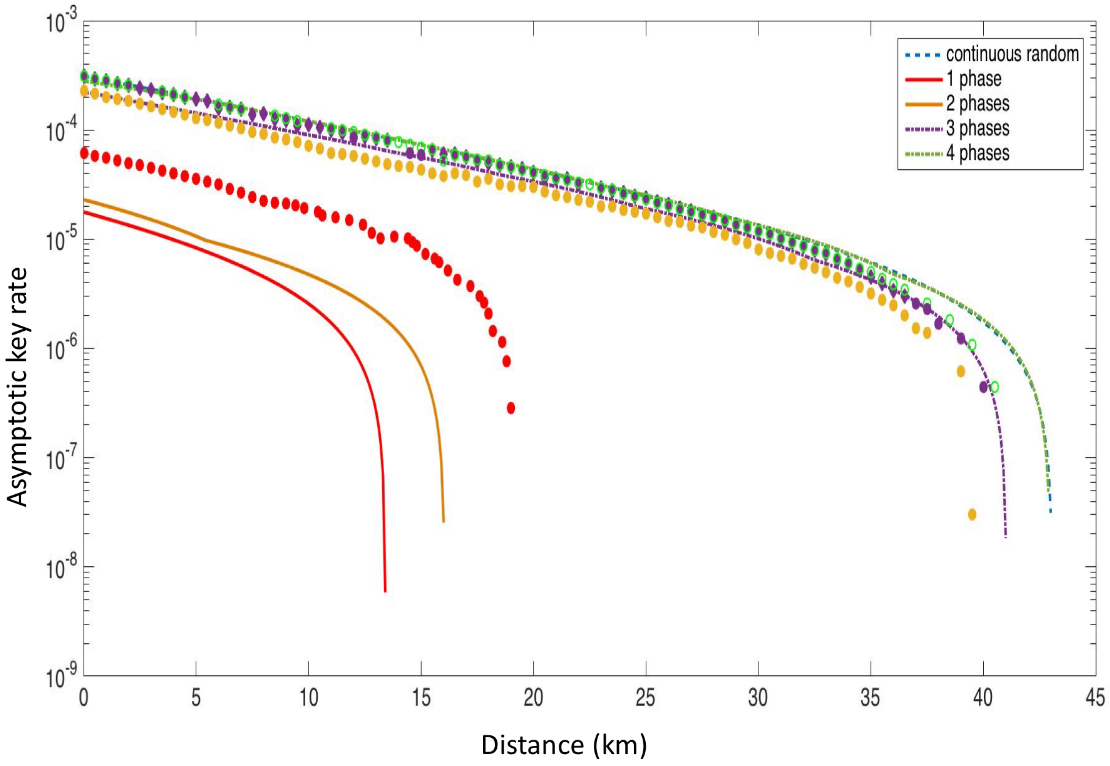

Figure 5.5: The asymptotic key rate versus the transmission distance in the case of discrete phase randomization without decoy states. The key rate is plotted in the logarithmic scale. Solid dots are our numerical results in the case $N = 1, 2, 3, 4$. We compare our numerical results with the results (lines) reported in Ref. [5]. Red curves and dots are for $N = 1$; yellow for $N = 2$; purple for $N = 3$ and green for $N = 4$. The blue dashed line is the key rate with a continuous phase-randomized source.

Chapter 6

Concluding remarks and future work

QKD in theory comes with the unconditional security. However, the physical implementations of QKD open up a lot of loopholes. The gap between the theory and implementations makes QKD vulnerable to quantum hacking. In order to remedy, we need to bridge the gap between the theory and experiments. From the theory side, we need to revise our security proofs by removing unrealistic assumptions subject to current technology.

It is usually difficult to prove the security analytically. Also, analytical proofs may involve some approximation in order to proceed, which in turns makes the key rate bound loose. On the other hand, since the key rate calculation problem can be stated as a convex optimization problem, we can resort to numerical tools. We have demonstrated how to apply numerical methods to study the security of QKD protocols. Since the numerical methods we discuss here produce reliable lower bounds of the asymptotic key generation rate per channel use under the assumptions of collective attacks, each of our calculation can turn into a security proof, with appropriate justifications.

Nevertheless, the numerical approaches we have so far are still limited in several aspects. First, we want to extend our study to decoy-state methods. Second, we cannot deal with infinite-dimensional spaces directly. To be applicable to protocols like continuous-variable (CV) QKD, we need analytical tools to reduce the dimension of the space and measurements. It may also require some modification of the numerical approaches to work with CV QKD. Third, these two methods discussed in this thesis do not consider finite-size effects. An extension of those numerical approaches to finite-key scenario is desirable. Finally, we want to make our implementation of numerical methods stable and reliable such that we can make the gap between our lower bound and the optimal value small enough.

References

[1] N. J. Beaudry, T. Moroder, and N. Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008.

[2] C. H. Bennett and G. Brassard. Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE.

[3] S. Boyd and L. Vandenberghe. *Convex Optimization.* Cambridge University Press, Cambridge, UK, 2004.

[4] R. Y Q Cai and V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.*, 11:045024, 2009.

[5] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.*, 17:053014, 2015.

[6] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, 2009.

[7] P. J. Coles. Unification of different views of decoherence and discord. *Phys. Rev. A*, 85:042103, 2012.

[8] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nat. Commun.*, 7:11712, 2016.

[9] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society A*, volume 461, pages 207–235, 2005.

[10] A. Ferenczi. *Security proof methods for quantum key distribution protocols.* PhD thesis, University of Waterloo, 2013.

[11] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85:052310, 2012.

[12] M. Frank and P. Wolfe. An algorithm for quadratic programming. *Naval Research Logistics Quarterly.*, 3:95–110, 1956.

[13] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, Alvarez, T. Moroder, and N. Lütkenhaus. Squashing model for detectors and applications to quantum-key-distribution protocols. *Phys. Rev. A*, 89:012325, 2014.

[14] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.*, 84:3762, 2004.

[15] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.*, 5:325–360, 2004.

[16] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. http://cvxr.com/cvx, Mar. 2014.

[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863, 1995.

[18] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D*, 41:599, 2007.

[19] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.*, 11:045018, 2009.

[20] Pieter Kok. Five lectures on optical quantum computing. *Lecture Notes in Physics*, 787:187–229, 2009, arXiv:0705.4193.

[21] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.

[22] H.-K. Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution shceme and a proof of its unconditional security. *J. Cryptol.*, 18:133–165, 2004.

[23] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:200501, 2012.

[24] H.-K. Lo and J. Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Inf. Comput.*, 7:431, 2007.

[25] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields. Practical security bounds aganist the trojan-horse attack in quantum key distribution. *Phys. Rev. X.*, 5:031030, 2015.

[26] N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon number statistics in the photon number splitting attack. *New J. Phys.*, 4:44, 2002.

[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, 2005.

[28] D. Mayers. Unconditional security in quantum cryptography. *JACM*, 48:351–406, 2001.

[29] M. Mosca, D. Stebila, and B. Ustaoglu. Quantum key distribution in the classical authenticated key exchange framework. 2012, arXiv:1206.6150.

[30] J. A. Nelder and R. Mead. A simplex method for function minimization. *Computer Journal*, 7:308–313, 1965.

[31] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 2000.

[32] R. Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zürich, 2005.

[33] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The security of pratical quantum key distribution. *Rev. Mod. Phys.*, 81:1301, 2009.

[34] V. Scarani and R. Renner. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:093601, 2008.

[35] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441, 2000.

[36] K.C. Toh, M.J. Todd, and R.H. Tütüncü. SDPT3 — a matlab software package for semidefinite programming. *Optimization Methods and Software*, 11:545–581, 1999.

[37] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nat. Commun.*, 3:634, 2012.

[38] T. Tsurumaru and K. Tamaki. Security proof for QKD systems with threshold detectors. *Phys. Rev. Lett.*, 78:032302, 2008.

[39] A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum crytography. *J. Mod. Opt.*, 48:2023–2038, 2001.

[40] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, 2014.

[41] A. Winick, N. Lütkenhaus, and P. J. Coles. Reliable numerical key rates for quantum key distribution. 2017, arXiv:1710.05511.

APPENDICES

Appendix A

Key map with post-selection

In Section 3.5.2, we mentioned that the post-selection step corresponds to a CP map $\mathcal{G}$ acting on the density matrix ρ_{ABC}. Then the key rate formula in the Eq. (3.11) becomes

$$r_{\text{coll}}^{\infty} = \min_{\rho_{ABC}\in\mathcal{C}} D(\mathcal{G}(\rho_{ABC})||\sum_j Z_A^j \mathcal{G}(\rho_{ABC}) Z_A^j) - H(Z_A|Z_B). \tag{A.1}$$

However, in the dual problem framework, we deal with Lagrange multipliers λ's rather than the density matrix ρ_{ABC} directly. It is more complicated to relate this CP map to λ's. Instead, we can choose the key map POVM in a clever way to effectively perform the desired post-selection. This allows us to apply the dual problem approach directly without modification of the objective function or constraints. In this appendix, we will show why the choice of key map in Eq. (3.19) is able to accomplish the post-selection in the MDI B92 example. This idea can be generalized to many other examples, and is not restricted to the dual problem framework, as we will see.

Recall that the post-selection CP map is

$$\mathcal{G}(\rho_{ABC}) = |1\rangle\langle 1|_C \, \rho_{ABC} \, |1\rangle\langle 1|_C + |2\rangle\langle 2|_C \, \rho_{ABC} \, |2\rangle\langle 2|_C \, . \tag{A.2}$$

Appendix B discusses how to handle post-selection steps in general and how we obtain such a CP map.

Recall that the choice of key map given in Eq. (3.19) is

$$\begin{aligned} Z_{ABC}^0 &= |0\rangle\langle 0|_A \otimes \mathbb{1}_B \otimes (|1\rangle\langle 1|_C + |2\rangle\langle 2|_C), \\ Z_{ABC}^1 &= |1\rangle\langle 1|_A \otimes \mathbb{1}_B \otimes (|1\rangle\langle 1|_C + |2\rangle\langle 2|_C), \\ Z_{ABC}^2 &= \mathbb{1}_{AB} \otimes |3\rangle\langle 3|_C \, . \end{aligned} \tag{A.3}$$

For the ease of notation, we write $\mathcal{Z}(\rho_{ABC}) = \sum_j Z^j_{ABC}\rho_{ABC}Z^j_{ABC}$.

We want to show

$$D(\rho_{ABC}||\mathcal{Z}(\rho_{ABC})) = D(\mathcal{G}(\rho_{ABC})||\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC})), \tag{A.4}$$

where $\tilde{\mathcal{Z}}(\rho) = \sum_{k=0}^{1} \tilde{Z}^k_A \rho \tilde{Z}^k_A$ and $\tilde{Z}^0_A = |0\rangle\langle 0|_A \, , \tilde{Z}^1_A = |1\rangle\langle 1|_A$.

The first observation is that since the register C is classical, ρ_{ABC} has a block diagonal structure with respect to the classical register C. This observation allows us to rewrite ρ_{ABC} as

$$\rho_{ABC} = p_1\rho^1_{AB} \otimes |1\rangle\langle 1|_C + p_2\rho^2_{AB} \otimes |2\rangle\langle 2|_C + p_3\rho^3_{AB} \otimes |3\rangle\langle 3|_C \, , \tag{A.5}$$

where ρ^i_{AB} is the corresponding block with respect to $|i\rangle\langle i|_C$, and $p_1 = p(\text{“+”})$, $p_2 = p(\text{“−”})$, $p_3 = p(\text{“?”})$.

Due to the block diagonal structure of ρ_{ABC}, we can find eigenvalues λ^i_k and eigenvectors $|v^i_k\rangle$ for each ρ^i_{AB} such that $|v^i_k\rangle \otimes |i\rangle_C$ form an eigenbasis of ρ_{ABC} and $p_i\lambda^i_k$ are eigenvalues of ρ_{ABC}. Then,

$$\begin{aligned} \operatorname{Tr}(\rho_{ABC}\log(\rho_{ABC})) &= \sum_i p_i \sum_k \lambda^i_k \log\bigl(p_i\lambda^i_k\bigr) \\ &= \sum_i p_i \operatorname{Tr}\bigl(\rho^i_{AB}\log\bigl(\rho^i_{AB}\bigr)\bigr) - H(\{p_i\}) \end{aligned} \tag{A.6}$$

The second observation is

$$\log(\mathcal{Z}(\rho_{ABC})) = \mathcal{Z}(\log(\mathcal{Z}(\rho_{ABC}))). \tag{A.7}$$

since Z^j_{ABC} commutes with $\mathcal{Z}(\rho_{ABC})$. This observation allows us to rewrite the term $\operatorname{Tr}(\rho_{ABC}\log(\mathcal{Z}(\rho_{ABC})))$ as

$$\begin{aligned} \operatorname{Tr}(\rho_{ABC}\log(\mathcal{Z}(\rho_{ABC}))) &= \operatorname{Tr}(\rho_{ABC}\mathcal{Z}(\log(\mathcal{Z}(\rho_{ABC})))) \\ &= \operatorname{Tr}[\mathcal{Z}(\rho_{ABC})\log(\mathcal{Z}(\rho_{ABC}))] \\ &= p_1 \operatorname{Tr}\Bigl(\tilde{\mathcal{Z}}(\rho^1_{AB})\log\Bigl(\tilde{\mathcal{Z}}(\rho^1_{AB})\Bigr)\Bigr) + p_2 \operatorname{Tr}\Bigl(\tilde{\mathcal{Z}}(\rho^2_{AB})\log\Bigl(\tilde{\mathcal{Z}}(\rho^2_{AB})\Bigr)\Bigr) \\ &\quad + p_3 \operatorname{Tr}\bigl(\rho^3_{AB}\log\bigl(\rho^3_{AB}\bigr)\bigr) - H(\{p_i\}), \end{aligned} \tag{A.8}$$

where we slightly abuse the notation of $\tilde{\mathcal{Z}}$.[1]

[1] Recall $\tilde{\mathcal{Z}}(\rho) = \sum_{k=0}^{1} \tilde{Z}^k_A \rho \tilde{Z}^k_A$. Since $\tilde{Z}^k_A$ only acts on the register A, we allow ρ to be a density operator of registers A and B or a density operator of registers A, B and C. By doing so, we implicitly add the appropriate identity operators to $\tilde{Z}^k_A$.

Then,

$$\begin{aligned}D(\rho_{ABC}||\mathcal{Z}(\rho_{ABC})) &= \mathrm{Tr}(\rho_{ABC}\log(\rho_{ABC})) - \mathrm{Tr}(\rho_{ABC}\mathcal{Z}(\rho_{ABC}))\\
&= \sum_{i=1}^{3} p_i \,\mathrm{Tr}\big(\rho^i_{AB}\log\big(\rho^i_{AB}\big)\big) - H(\{p_i\})\\
&- p_1\,\mathrm{Tr}\Big(\tilde{\mathcal{Z}}(\rho^1_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^1_{AB})\Big)\Big) - p_2\,\mathrm{Tr}\Big(\tilde{\mathcal{Z}}(\rho^2_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^2_{AB})\Big)\Big)\\
&- p_3\,\mathrm{Tr}\big(\rho^3_{AB}\log\big(\rho^3_{AB}\big)\big) + H(\{p_i\})\\
&= \sum_{i=1}^{2} p_i\Big[\mathrm{Tr}\big(\rho^i_{AB}\log\big(\rho^i_{AB}\big)\big) - \mathrm{Tr}\Big(\tilde{\mathcal{Z}}(\rho^i_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^i_{AB})\Big)\Big)\Big]\\
&= \sum_{i=1}^{2} p_i\Big[\mathrm{Tr}\big(\rho^i_{AB}\log\big(\rho^i_{AB}\big)\big) - \mathrm{Tr}\Big(\rho^i_{AB}\log\Big(\tilde{\mathcal{Z}}(\rho^i_{AB})\Big)\Big)\Big]\\
&= \sum_{i=1}^{2} p_i D(\rho^i_{AB}||\tilde{\mathcal{Z}}(\rho^i_{AB})).\end{aligned} \tag{A.9}$$

Similarly, we want to show $D(\mathcal{G}(\rho_{ABC})||\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC})) = \sum_{i=1}^{2} p_i D(\rho^i_{AB}||\tilde{\mathcal{Z}}(\rho^i_{AB}))$.

First, we notice

$$\begin{aligned}\mathcal{G}(\rho_{ABC}) &= |1\rangle\langle 1|_C\,\rho_{ABC}\,|1\rangle\langle 1|_C + |2\rangle\langle 2|_C\,\rho_{ABC}\,|2\rangle\langle 2|_C\\
&= p_1\rho^1_{AB}\otimes|1\rangle\langle 1|_C + p_2\rho^2_{AB}\otimes|2\rangle\langle 2|_C\,.\end{aligned} \tag{A.10}$$

This allows us to rewrite two terms in the expression of $D(\mathcal{G}(\rho_{ABC})||\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC}))$ as

$$\begin{aligned}\mathrm{Tr}(\mathcal{G}(\rho_{ABC})\log(\mathcal{G}(\rho_{ABC}))) =& p_1\,\mathrm{Tr}\big(\rho^1_{AB}\log\big(\rho^1_{AB}\big)\big) + p_2\,\mathrm{Tr}\big(\rho^2_{AB}\log\big(\rho^2_{AB}\big)\big)\\
&+ p_1\log(p_1) + p_2\log(p_2),\end{aligned} \tag{A.11}$$

and

$$\begin{aligned}\mathrm{Tr}\left[\mathcal{G}(\rho_{ABC})\log\Big(\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC}))\Big)\right] &= \mathrm{Tr}\left[\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC}))\log\Big(\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC}))\Big)\right]\\
&= p_1\,\mathrm{Tr}\Big(\tilde{\mathcal{Z}}(\rho^1_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^1_{AB})\Big)\Big) + p_2\,\mathrm{Tr}\Big(\tilde{\mathcal{Z}}(\rho^2_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^2_{AB})\Big)\Big)\\
&+ p_1\log(p_1) + p_2\log(p_2).\end{aligned} \tag{A.12}$$

Then

$$\begin{aligned}
D(\mathcal{G}(\rho_{ABC})||\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC})) &= \operatorname{Tr}(\mathcal{G}(\rho_{ABC})\log(\mathcal{G}(\rho_{ABC}))) - \operatorname{Tr}\left[\mathcal{G}(\rho_{ABC})\log\Big(\tilde{\mathcal{Z}}(\mathcal{G}(\rho_{ABC}))\Big)\right] \\
&= p_1 \operatorname{Tr}\big(\rho^1_{AB}\log\big(\rho^1_{AB}\big)\big) + p_2 \operatorname{Tr}\big(\rho^2_{AB}\log\big(\rho^2_{AB}\big)\big) \\
&+ p_1\log(p_1) + p_2\log(p_2) \\
&- p_1 \operatorname{Tr}\Big(\tilde{\mathcal{Z}}(\rho^1_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^1_{AB})\Big)\Big) - p_2 \operatorname{Tr}\Big(\tilde{\mathcal{Z}}(\rho^2_{AB})\log\Big(\tilde{\mathcal{Z}}(\rho^2_{AB})\Big)\Big) \\
&- p_1\log(p_1) - p_2\log(p_2) \\
&= \sum_{i=1}^{2} p_i D(\rho^i_{AB}||\tilde{\mathcal{Z}}(\rho^i_{AB})).
\end{aligned} \tag{A.13}$$

From Eq. (A.9) and Eq. (A.13), we have shown that Eq. (A.4) holds. Therefore, we have shown that this choice of key map effectively does the post-selection since the block corresponding to the announcement "?" does not contribute to the objective function.

This idea can be generalized to other protocols with a specific type of post-selection. In the post-selection step, if Bob announces "keep" or "discard" for each round, where Alice and Bob will only distill secret keys from the "keep" events, then we can introduce a classical register C to store the announcement outcomes. By doing so, we transform Alice and Bob's joint state ρ_{AB} to ρ_{ABC}. Since C is a classical register, we can apply this clever choice of key map to perform the post-selection.

Appendix B

Post-selection

In this appendix, we will discuss how to deal with the post-selection in the numerical framework. We will start with the general procedure and then discuss possible simplifications.

In the first section, we will discuss the general procedure without any assumptions on Alice's and Bob' POVMs. We remark that the general procedure we describe here is a slight variation of the procedure described in Ref. [41]. Here, we try to follow the steps in a generic QKD protocol and show how we can transform the density operator in each step. In the second section, we will present a simplified version if POVMs are actually PVMs. The simplified version allows us to speed up the numerical calculation since the dimension of the density matrix in the optimization problem is made as small as possible. In the protocols discussed in this thesis, when we combine the ideas of source-replacement schemes and squashing models, we happen to have PVMs that allows us to do this simplification.

B.1 General framework

In a QKD protocol, Alice has a POVM $\{M_A^x\}_{x=1}^m$ for her measurements[1] and Bob has a POVM $\{M_B^y\}_{y=1}^k$.

After parameter estimation, Alice and Bob constrain the set $\mathcal{C}$ of ρ_{AB} compatible with their observations. For each ρ_{AB}, as we notice before, the worse-case scenario is that Eve holds a purification of ρ_{AB}. We will construct a CP map for post-processing of ρ_{AB} (in

[1] For prepare-and-measure protocols, we will use the source-replacement scheme, and Alice's POVM is the projective measurements onto the basis of her system A.

particular, steps that lead to a raw key). Since Eve can listen to the classical communication during the classical post-processing, Eve should have all information leaked during the classical communication. This means, if we have a classical register to store announcements, Eve should have a copy of that register as well.

Before we start to discuss how to make announcements, it is convenient to introduce extra registers X and Y to Alice and Bob, respectively, such that their POVMs become PVMs on these extra registers. We want to transform ρ_{AB} to ρ'_{XYAB} in such a way that doing projective measurements $|x\rangle\langle x|_X$ or $|y\rangle\langle y|_Y$ on the state ρ'_{XYAB} recovers the probabilities $\mathrm{Tr}(M_A^x \rho_{AB})$ or $\mathrm{Tr}(M_B^y \rho_{AB})$, respectively. The transformation from ρ_{AB} to ρ'_{XYAB} can be done via an isometry V_1 by Naimark's Theorem (Theorem 2.10). That is, $V_1 = \sum\limits_{x,y} |x\rangle_X \otimes |y\rangle_Y \otimes \sqrt{M_A^x} \otimes \sqrt{M_B^y}$. Then since

$$\begin{aligned} \mathrm{Tr}(\rho_{AB} M_A^x \otimes M_B^y) &= \mathrm{Tr}\Big[\rho_{AB}(V_1^\dagger \, |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \, V_1)\Big] \\ &= \mathrm{Tr}\Big[(V_1 \rho_{AB} V_1^\dagger) \, |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y\Big], \end{aligned} \tag{B.1}$$

we can define $\rho'_{XYAB} = V_1 \rho_{AB} V_1^\dagger$ such that $\mathrm{Tr}(\rho_{AB} M_A^x \otimes M_B^y) = \mathrm{Tr}[\rho'_{XYAB} \, |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y]$.

In the classical phase, Alice and Bob will communicate through the classical channel to post-process their local data stored in registers X and Y. Let $\mathtt{X} = \{1, \ldots, m\}$ denote possible outcomes for the register X and $\mathtt{Y} = \{1, \ldots, k\}$ for the register Y. Based on their local data, Alice and Bob choose announcement strategies. For simplicity, we will only consider announcement strategies that are deterministic functions of their local data. Any probabilistic announcement strategy is then just a statistical combination of those deterministic functions. Under the assumption of the deterministic functions, all announcements they made (including any data they will discard later) in this step correspond to a partition of all possible combinations of their data in X and Y, that is, a partition of the set $(\mathtt{X}, \mathtt{Y}) := \mathtt{X} \times \mathtt{Y} = \{1, \ldots, m\} \times \{1, \ldots, k\}$.

Let $\mathbf{S}$ be the set of all announcements they made. Each $s \in \mathbf{S}$ corresponds to a set $\gamma_s \subseteq (\mathtt{X}, \mathtt{Y})$. We define $E_s = \sum_{(x,y) \in \gamma_s} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y$. Notice that $\sum_{s \in \mathbf{S}} E_s = \mathbb{1}_{XYAB}$ and $E_s \succeq 0$ for each $s \in \mathbf{S}$. This means that $\{E_s\}$ is a POVM. We want to store the announcement results in a register S such that by measuring this register S, we recover the desired probabilities. This can be accomplished by an isometry $V_2 = \sum_s \sqrt{E_s} \otimes |s\rangle_S$ from Naimark's Theorem. However, since the announcements are public, we want to make this register classical such that the purifying system has a copy of this register. Therefore, we decohere S as well. We now have

$$\rho^{ann}_{XYABS} = \sum_{s \in \mathbf{S}} |s\rangle\langle s|_S \, V_2 \rho'_{XYAB} V_2^\dagger \, |s\rangle\langle s|_S \,. \tag{B.2}$$

Then Alice and Bob will decide which parts of data to discard after announcements $\mathbf{S}$. Let $\mathbf{S}_{keep}$ denote the set of announcements they will keep. This sifting procedure corresponds to a projection onto the subspace of $\mathcal{H}_S$ spanned by $\{|s\rangle : s \in \mathbf{S}_{keep}\}$ for the register S. We define the projector $\Pi = \sum_{s\in\mathbf{S}_{keep}} |s\rangle\langle s|_S$. The post-processed state is then

$$\rho^{sift}_{XYABS} = \frac{\Pi\rho^{ann}_{XYABS}\Pi}{p_{pass}}, \tag{B.3}$$

where $p_{pass} = \mathrm{Tr}(\Pi\rho^{ann}_{XYABS})$.

After sifting, Alice will apply a key map to map her data to key symbols $\mathcal{X} = \{0, 1, \dots, N-1\}$.[2] Let $g : \mathtt{X} \times \mathbf{S}_{keep} \to \mathcal{X}$ represent such a mapping. We define $G_i = \sum_{(x,s):g(x,s)=i} |x\rangle\langle x|_X \otimes |s\rangle\langle s|_S$. The results of the key map are stored in the register R. The isometry V_3 in this case is $V_3 = \sum_i |i\rangle_R \otimes \sqrt{G_i}$. Then we have the state

$$\rho^{key}_{RXYABS} = V_3\rho^{sift}_{XYABS}V_3^\dagger. \tag{B.4}$$

By doing a projective measurement $\{|j\rangle\langle j|_R\}_{j=0}^{N-1}$ on the register R, Alice obtains the result of key map.

Now, we define one CP map $\mathcal{G}$ that transforms ρ_{AB} to ρ^{key}_{RXYABS} by putting everything together. We notice

$$\begin{aligned}
\rho^{key}_{RXYABS} &= V_3\rho^{sift}_{XYABS}V_3^\dagger \\
&= \frac{1}{p_{pass}}V_3\Pi\rho^{ann}_{XYABS}\Pi V_3^\dagger \\
&= \frac{1}{p_{pass}}V_3\Pi\sum_{s\in\mathbf{S}} |s\rangle\langle s|_S V_2\rho'_{XYAB}V_2^\dagger |s\rangle\langle s|_S \Pi V_3^\dagger \\
&= \frac{1}{p_{pass}}\sum_{s\in\mathbf{S}} V_3\Pi |s\rangle\langle s|_S V_2V_1\rho_{AB}V_1^\dagger V_2^\dagger |s\rangle\langle s|_S \Pi V_3^\dagger
\end{aligned} \tag{B.5}$$

Therefore, we define a Kraus operator $K_s = V_3\Pi |s\rangle\langle s|_S V_2V_1$. This CP map is defined as $\mathcal{G}(\rho_{AB}) := \sum_{s\in\mathbf{S}} K_s\rho_{AB}K_s^\dagger = p_{pass}\rho^{key}_{RXYABS}$.

B.2 Simplification in special cases

We now consider some special cases where we are able to simplify the general procedure of post-selection without introducing many extra registers. In many protocols, especially

[2] Usually, the set of key symbols is $\{0, 1\}$.

in the protocols considered in this thesis, sifting is usually performed. In the sifting step, Alice and Bob will discard rounds where they measure in different bases and rounds where Bob fails to detect a signal. Here, we restrict our attention to the situation where the post-selection step only involves basis announcements and sifting. More specifically, we consider a prepare-and-measure BB84 protocol.

For prepare-and-measure protocols, after applying the source-replacement scheme, Alice's measurements become projections onto the standard basis of her register A. We now consider the case that Alice's POVM is actually projective measurements. On Bob's side, we know if there exists a squashing model, then we can think of Bob's measurements in terms of target qubit measurements with an additional flag that indicates the detection of vacuum. For the measurements in BB84, Bob has the following POVM $M_B = \{p_z \left|0\middle\rangle\!\middle\langle 0\right|, p_z \left|1\middle\rangle\!\middle\langle 1\right|, (1-p_z)\left|+\middle\rangle\!\middle\langle +\right|, (1-p_z)\left|-\middle\rangle\!\middle\langle -\right|, \left|2\middle\rangle\!\middle\langle 2\right|\}$, where $\left|0\right\rangle, \left|1\right\rangle$ are qubit Z-basis states, $\left|+\right\rangle, \left|-\right\rangle$ are qubit X-basis states, and $\left|2\right\rangle$ represents detection of vacuum (no detection).[3] These POVM elements are projection onto four BB84 signal states or the no-detection flag up to some normalization factor. p_z is the probability of measuring Z-basis.

We define

$$\begin{aligned} E_{zz} &= (\left|0\middle\rangle\!\middle\langle 0\right|_A + \left|1\middle\rangle\!\middle\langle 1\right|_A) \otimes (\left|0\middle\rangle\!\middle\langle 0\right|_B + \left|1\middle\rangle\!\middle\langle 1\right|_B) \\ E_{zx} &= (\left|0\middle\rangle\!\middle\langle 0\right|_A + \left|1\middle\rangle\!\middle\langle 1\right|_A) \otimes (\left|+\middle\rangle\!\middle\langle +\right|_B + \left|-\middle\rangle\!\middle\langle -\right|_B) \\ E_{xz} &= (\left|2\middle\rangle\!\middle\langle 2\right|_A + \left|3\middle\rangle\!\middle\langle 3\right|_A) \otimes (\left|0\middle\rangle\!\middle\langle 0\right|_B + \left|1\middle\rangle\!\middle\langle 1\right|_B) \\ E_{xx} &= (\left|2\middle\rangle\!\middle\langle 2\right|_A + \left|3\middle\rangle\!\middle\langle 3\right|_A) \otimes (\left|+\middle\rangle\!\middle\langle +\right|_B + \left|-\middle\rangle\!\middle\langle -\right|_B) \\ E_{\emptyset} &= \mathbb{1}_A \otimes \left|2\middle\rangle\!\middle\langle 2\right|_B \end{aligned} \tag{B.6}$$

We notice that registers X and Y are redundant in this situation since the information is in registers A and B and measuring registers A and B after basis announcements can recover the desired probabilities. Without introducing registers X and Y, the basis announcements are realized by the following Kraus operators according to the general framework in the previous section:

$$\begin{aligned} K_{zz} &= \sqrt{p_z E_{zz}} \otimes \left|zz\right\rangle_S, \\ K_{zx} &= \sqrt{(1-p_z)E_{zx}} \otimes \left|zx\right\rangle_S, \\ K_{xz} &= \sqrt{p_z E_{xz}} \otimes \left|xz\right\rangle_S, \\ K_{xx} &= \sqrt{(1-p_z)E_{xx}} \otimes \left|xx\right\rangle_S, \\ K_{\emptyset} &= \sqrt{E_{\emptyset}} \otimes \left|\emptyset\right\rangle_S, \end{aligned} \tag{B.7}$$

[3] $\left|0\right\rangle, \left|1\right\rangle$ and $\left|2\right\rangle$ form an orthonormal basis for Bob's 3-dimensional space. $\left|\pm\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle \pm \left|1\right\rangle$.

where $|zz\rangle, |zx\rangle, |xz\rangle, |xx\rangle$ and $|\emptyset\rangle$ denote five orthonormal basis states for the register S, indicating the basis choices for Alice and Bob or the no-detection event.

The post-announcement state is then

$$\begin{aligned}\rho_{ABS}^{\text{ann}} &= K_{zz}\rho_{AB}K_{zz}^{\dagger} + K_{zx}\rho_{AB}K_{zx}^{\dagger} + K_{xz}\rho_{AB}K_{xz}^{\dagger} + K_{xx}\rho_{AB}K_{xx}^{\dagger} + K_{\emptyset}\rho_{AB}K_{\emptyset}^{\dagger}\\ &= p_z E_{zz}\rho_{AB}E_{zz} \otimes |zz\rangle\langle zz|_S\\ &+ (1-p_z)E_{zx}\rho_{AB}E_{zx} \otimes |zx\rangle\langle zx|_S\\ &+ p_z E_{xz}\rho_{AB}E_{xz} \otimes |xz\rangle\langle xz|_S\\ &+ (1-p_z)E_{xx}\rho_{AB}E_{xx} \otimes |xx\rangle\langle xx|_S\\ &+ E_{\emptyset}\rho_{AB}E_{\emptyset} \otimes |\emptyset\rangle\langle\emptyset|_S\end{aligned} \tag{B.8}$$

Bob's POVM becomes two sets of POVMs: Z-basis measurements $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$ and X-basis measurements $\{|+\rangle\langle +|, |-\rangle\langle -|, |2\rangle\langle 2|\}$.

Then the sifting step corresponds to a projection $\Pi = |zz\rangle\langle zz|_S + |xx\rangle\langle xx|_S$ since only rounds where Alice and Bob measure in the same basis and Bob detects a signal will be kept.

$$\begin{aligned}\rho_{ABS}^{\text{sift}} &= \frac{1}{p_{\text{pass}}}\Pi\rho_{ABS}^{\text{ann}}\Pi\\ &= \frac{1}{p_{\text{pass}}}(p_z E_{zz}\rho_{AB}E_{zz} \otimes |zz\rangle\langle zz|_S + (1-p_z)E_{xx}\rho_{AB}E_{xx} \otimes |xx\rangle\langle xx|_S),\end{aligned} \tag{B.9}$$

where $p_{\text{pass}} = (p_z^2 + (1-p_z)^2)P_{\text{det}}$, and P_{det} is the probability of detection.

Due to the projective measurements for Alice, we do not need to introduce an additional register R to store the result of key map. In the end, we only need to introduce a two-dimensional register S that stores the announcement results kept after sifting.