The Security of Simplified Trusted Relays

by

William Spencer Stacey

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, 2014

Author's Declaration

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.

Abstract

This thesis examines the security of performing quantum key distribution (QKD) with a simplified trusted relay (STR). The protocol carries out the quantum phase of a conventional trusted relay, however, reduces the required complexity of the nodes by carrying out an altered classical phase. Rather than announcing the parity of the final keys, the simplified trusted relay announces the parity of the keys before error correction and privacy amplification. As a result, the majority of the post-processing is left to the end users.

Specifically, we examine the security of an STR protocol which carries out the quantum phase of the BB84 protocol. Through two different methods, we derive qubit key rates. For the first method, we require that the basis choice is equally weighted. Furthermore, we limit the relay to a single node. This proof has the benefit that it easily generalizes to an alternate protocol where a node may generate error correcting information. In the second security proof, we derive a key rate for an arbitrary number of nodes with an arbitrary basis weighting.

We further extend our analysis to realistic scenarios in which the legitimate parties use weak coherent pulses to transmit signal states over a lossy channel. We provide a framework for generalizing decoy state methods to STR protocols.

Acknowledgements

This research was carried out under the careful supervision of Norbert Lütkenhaus. I would like to thank him for making my time at the Institute for Quantum Computing possible and gratifying. By encouraging an open-door policy, he has taught me that a five minute meeting is worth a thousand emails. His support and guidance have made this project a reality. I would also like to thank the members of my advisory committee, Thomas Jennewein and Michele Mosca, for their time and support. It is well appreciated. Further thanks goes to Kevin Resch for participating in my defence committee.

I would like to thank my colleagues and coworkers both inside and outside the OQCT group. This work has greatly benefited from their insight and friendship: Razieh Annabestani, Juan Miguel Arrazola, Agnes Ferenczi, Oleg Gittsovich, David Luong, Ryo Namiki, Alf Pettersson, Marco Piani, Yanbao Zhang and many more.

Thanks to the Institute for Quantum Computing, and to all the individuals that make it a wonderful place to be. (I would list all of you here but this thesis has a page limit.)

Thanks to my family for the emotional, historical, financial, psychological, and on-going support.

And finally thanks Kendra for putting up with all this hoopla.

It will be true to you if you are true to it and you will never, never, ever become lost.

— *Alistair MacLeod, in reference to Highway 401*

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The emergence of quantum cryptography marks a shift in cryptographic paradigm. The security of most pre-quantum (or classical) cryptography stems from assumptions about the limited computational power of an adversary. Within a reasonable timespan, certain computational tasks are assumed to be outside the reach of an adversary. Quantum cryptography, on the other hand, offers provable security in the presence of a computationally unbounded adversary. The security of quantum cryptography arises from the fundamental principles of quantum mechanics.

While the first hints of quantum cryptography were published in 1983 [56], it was not until the development of quantum computing that the field attracted considerable attention. A number of computational problems which appear to be infeasible on classical computers, such as finding the prime factors of a large integer, have been shown to be feasible on a quantum computer. Quantum algorithms (such as Shor's factoring algorithm [46]) threaten to break several widely used classical cryptographic protocols (such as RSA public-key encryption). While quantum computing grows as a field, so does the need for quantum-safe cryptographic protocols.

Quantum key distribution (QKD) is a quantum-safe protocol that aims to establish two identical secret keys between spatially separated parties. Secret keys (strings of bits that are unknown to an adversarial party) are a valuable resource for many cryptographic tasks. One well-known example is the *one-time pad*, a classical protocol for unconditionally secure communication. The sender generates a maximally-entropic cryptogram by taking the bitwise parity of the original message and the secret key. The receiver similarly decodes the cryptogram. The one-time pad offers *information-theoretic secure* privacy,[1] provided

[1] Note that the one-time pad fails at other cryptographic objectives such as preserving data integrity.

two parties initially share a secret key. Given that QKD provides an information-theoretic secure method for establishing such a key, QKD in principle allows for the highest level of private communication.

QKD encompasses a variety of different protocols, all linked by their utilization of quantum mechanics to generate secret keys. In a typical QKD protocol, a legitimate party (conventionally called Alice) prepares non-orthogonal signal states and sends them over a quantum channel to a second legitimate party (Bob), who performs measurements on the states. Using an authenticated classical channel, Alice creates an asymmetry between Bob and any eavesdropper (Eve). This asymmetry is exploited to generate a secret key. The authenticated classical channel is not private; Eve can listen to any messages sent over the authenticated channel. However, the authenticated channel is assumed to preserve the integrity and authenticity of these messages. The security of QKD arises from Eve's inability to distinguish the quantum signals perfectly. By interacting with the signal states in a useful fashion, Eve has a non-zero probability of disturbing the states. Unlike protocols that exchange classical signals, Eve cannot acquire a complete transcript of the communication between the legitimate parties due to the quantum component of the communication. This is a direct result of the no-cloning theorem [57]. Disturbances introduced by Eve can be used by Alice and Bob to bound the correlation Eve may have with the key. Alice and Bob may then reduce Eve's correlation using classical privacy amplification, or simply abort the protocol entirely if the error rate is too high.

Note that QKD protocols require an authenticated classical channel between the legitimate parties. This prevents a *man-in-the-middle* attack. Message authentication is generally regarded as a distinct task from QKD; conventionally, an authenticated classical channel is simply treated as a resource required for the protocol.[2]

While other quantum-safe methods for key distribution have been suggested, they either rely upon unproven mathematical assumptions [10], or restrict the resources of an adversary [3]. If future developments in algorithms and computing power break these assumptions, the privacy of any historical communications that have relied upon these methods will be compromised. QKD, however, provides information-theoretic security, even in the presence of a computationally unbounded adversary; therefore, QKD remains secure in consideration of future advances.

The benefits of QKD are clear; however, several technical hurdles lie in the way of practical and wide-spread implementation. One challenge is achieving long-distance QKD.

[2]There exist unconditionally secure methods for message authentication which rely upon the legitimate parties sharing initial secret keys. Alternatively, public key authentication offers a practical method for message authentication in the presence of realistic eavesdroppers [49].

The limiting factor proves to be loss along the quantum channel connecting Alice and Bob. For *point-to-point protocols* the key rate is approximately upper-bounded by the single-photon transmittance of the channel [51]. The security of most implementations rely upon low-intensity signals; if signals are transmitted over an optical fibre, this leads to an exponential reduction in the number of detected signals. At long distances, the rate of dark counts surpasses the rate of signal counts, causing an apparent disturbance in the signal states. Unable to distinguish the disturbance from an eavesdropper, Alice and Bob necessarily abort the protocol. A second consequence of loss comes into play when considering small imperfections in the signal states. High loss may allow Eve additional leeway when exploiting these imperfections.

Both trusted quantum relays and quantum repeaters have been posited as methods for implementing long distance QKD. In the long term, quantum repeaters promise long-distance QKD by allowing the creation of entangled particles at arbitrary distances using a series of intermediate operations [1, 11]. However, practical quantum repeaters are still under development on a fundamental level and remain outside the reach of current technology.

Trusted relays [17] offer a more immediate method for implementing long-distance QKD. Trusted relays use a series of trusted nodes, each of which takes the role of two legitimate parties. Each node acts as both a pseudo-Alice, by preparing and sending signals, and a pseudo-Bob, by making measurements. In this manner, each node carries out a full QKD protocol with its nearest neighbours. If every node then publicly announces the bitwise parity of the two keys it holds, Bob can recover Alice's key by adding each parity announcement (bit-wise modulo) to his own. These announcements are of no use to Eve, as each node effectively encrypts one of the keys it holds using a one-time pad protocol. Trusted relays benefit from their simplicity; they are well within the reach of current technology, and have been demonstrated in several QKD network implementations [18, 37, 42]. However, trusted relays exhibit two major drawbacks. First, every node must be trusted, as any node could recover the final key held by Alice and Bob. Second, it is not always practical to carry out a full QKD protocol between every neighbour in a relay; most QKD protocols require significant computational resources and communication bandwidth.

This thesis examines an alternative version of the trusted relay that does not require a full QKD protocol to be carried out in each link of the relay [32]. For the remainder of this thesis, we will refer to this as the *simplified trusted relay* (STR). Rather than carrying out a full QKD protocol between adjacent nodes, each node simply carries out the first few steps of the QKD protocol, i.e. signal preparation, distribution and measurement. After some limited post-processing, the nodes map their raw measurements into bit strings and perform a parity announcement. If the error rate is low enough, Alice and Bob may distill

secret keys from the protocol using standard techniques — without further aid from the nodes. This reduces the required complexity of each node. Computationally cumbersome tasks (such as error correction and privacy amplification) are left to Alice and Bob.

How does the use of simplified nodes affect the security of a trusted relay? This thesis addresses this question. In the following pages, we review the principles in quantum information theory that are necessary for our analysis (Chapter 2). Further background on QKD, including the formalism behind security proofs, is detailed in Chapter 3. In Chapter 4 we examine the details of the STR protocol. As well, we present a rigorous examination of the security of the STR protocol.

Chapter 2

Background

The security of QKD arises from fundamental principles in quantum mechanics. In order to examine the security of an STR protocol, it is helpful to review several notions that lie at the heart of quantum mechanics. Equally important is the framework behind cryptography — information theory [15]. The intersection of these two scientific pillars, quantum information theory, provides the ideal structure for a rigorous examination of QKD.

2.1 Fundamental Principles in Quantum Mechanics

2.1.1 Basic Properties of Quantum States

Quantum systems are described by *Hilbert spaces* ($\mathcal{H}$). A quantum state, which is a particular physical realization of a quantum system, is described by an operator acting on that Hilbert space. Any normalized positive semidefinite operator, known as a *density matrix* (ρ), corresponds to a valid physical state of a quantum system. Quantum states with a two-dimensional Hilbert space play a special role in quantum information theory, as they represent the quantum analog of classical bits, known as *qubits*.

Quantum states can be categorized as *pure* or *mixed*. A finite-dimensional pure quantum state is most readily described by a complex unit vector, typically represented in *ket*-notation ($|\phi\rangle$). For a pure state, the density matrix can be constructed by taking the product of the corresponding unit vector with its own complex conjugate transpose,

$$|\phi\rangle \longrightarrow \rho_{\text{pure}} = |\phi\rangle\langle\phi| \tag{2.1}$$

where conventional notation defines $\langle\phi| := (|\phi\rangle)^\dagger$. Pure states therefore correspond to rank-one density matrices. For a given orthonormal basis spanning a finite-dimensional Hilbert space, $\{|a_1\rangle, \ldots, |a_n\rangle\}$, any pure state on that Hilbert space may be expressed as

$$|\phi\rangle = \sum_{i=1}^{n} c_i |a_i\rangle \tag{2.2}$$

where $c_i = \langle a_i|\phi\rangle$ is a complex scalar. Normalization ensures that $\sum_{i=1}^{n} |c_i|^2 = 1$. The state $|\phi\rangle$ is said to be in a superposition of the basis states $\{|a_i\rangle\}$.

Any density operator which cannot be represented as a pure state is known as *mixed*. Intuitively, it may help to think of mixed states representing incomplete knowledge of a quantum state. As the name suggests, mixed states can be described by probabilistic mixtures of pure states, although they lack a unique representation.

It is natural to pose questions involving numerous quantum systems. The tensor product operation ($\otimes$) gives us a mathematical approach for forming composite quantum systems. We define $\mathcal{D}(\mathcal{H})$ to be the set of all density operators on the Hilbert space $\mathcal{H}$. If ρ_A and ρ_B are quantum states on $\mathcal{D}(\mathcal{H}_A)$ and $\mathcal{D}(\mathcal{H}_B)$ respectively, the joint state ρ_{AB} exists on $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The state ρ_{AB} is said to be bipartite, while a state existing on more than two Hilbert spaces is generally said to be multipartite. If $\{|a_1\rangle, \ldots, |a_n\rangle\}$ and $\{|b_1\rangle, \ldots, |b_m\rangle\}$ are two sets of orthonormal basis states spanning $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then the set $\{|a_i\rangle \otimes |b_j\rangle\}$, where $1 \leq i \leq n$ and $1 \leq j \leq m$, forms a basis for the joint Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. Note that when referring to the tensor product of two pure states in ket-notation, it is common to use the shorthand notation $|a\rangle|b\rangle := |a\rangle \otimes |b\rangle$.

In contrast to the tensor product, the partial trace function allows us to consider subsystems of a larger quantum system. Examining the bipartite state ρ_{AB}, the reduced state ρ_A is found by taking the partial trace over system B, i.e. $tr_B\{\rho_{AB}\} = \rho_A$. Similarly, ρ_B is obtained by taking the partial trace over system A.

It is useful to note that any mixed state may be expressed as a pure state on a larger Hilbert space. The quantum state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be a *purification* of $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ if ρ_{AB} is pure and $tr_B\{\rho_{AB}\} = \rho_A$.

2.1.2 Entanglement and Bell States

Entanglement is a quantum phenomenon in which multipartite quantum states exhibit stronger correlations than allowed clasically. Entanglement is fundamental to quantum information theory, and lies at the heart of many quantum technologies.

Similar to mixed states, entangled states are defined by what they are *not*. Specifically, an entangled state is any state that cannot be expressed as a probabilistic mixture of product states. On the contrary, states which *can* be expressed this way are known as *separable* states. For two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a general separable state can be represented as

$$\rho_{AB}^{\text{separable}} = \sum_{i=1}^{n} p_i \rho_A^i \otimes \rho_B^i \tag{2.3}$$

for some set of states $\{\rho_A^1, \rho_B^1, \ldots, \rho_A^n, \rho_B^n\}$, a probability distribution $\mathbf{p} = \{p_1, \ldots, p_n\}$, and some n. Any state that cannot be written in this manner is said to be entangled.

The *Bell states* are an important set of entangled two-qubit quantum states. For qubits, it is common to represent the *canonical basis* with the orthonormal vectors $|0\rangle$ and $|1\rangle$ (reminiscent of classical bits "0" and "1"). Adopting this notation, the four Bell states are explicitly given by

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{2.4}$$

$$|\Phi^-\rangle := \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \tag{2.5}$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \tag{2.6}$$

$$|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \tag{2.7}$$

The Bell states form an orthonormal basis for two-qubit states. It is useful to express the Bell states using a compact notation:

$$|\Phi_{a,b}\rangle := \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{ak} |k\rangle|k \oplus b\rangle \tag{2.8}$$

where $a, b \in \{0, 1\}$. Here $\oplus$ denotes modulo-2 addition. For the remainder of this thesis, $|\Phi_{a,b}\rangle$ will denote the four Bell states.

2.1.3 Quantum Channels

A *quantum channel* is a general description of any discrete change in a quantum state. Formally, quantum channels are linear mappings from one Hilbert space, $\mathcal{H}_A$, to another

Hilbert space, $\mathcal{H}_B$. In order for the channel to be physically realizable, the mapping must be completely positive and trace preserving. These two conditions ensure that density operators are mapped to density operators.

There exist several useful characterizations of a quantum channel. For the purpose of this thesis, we introduce both the *Stinespring representation* and the *Kraus representation*. Any quantum system, ρ_A, may be viewed as part of a composite pure quantum system, ρ_{AE}, where $\rho_E = tr_A\{\rho_{AE}\}$ represents the environment. The dynamics of the entire system are described by unitary evolution; however, the dynamics of ρ_A are described by a more general quantum channel.

This intuition motivates the Stinespring dilation theorem, which states that any quantum channel may be expressed as a linear isometry on a dilated Hilbert space. Recall that unitary mappings are a special case of linear isometries. Let us denote the set of operators on a Hilbert space $\mathcal{H}$ by $\mathcal{L}(\mathcal{H})$. If $\psi(X)$ is a quantum channel of the form $\psi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$, then there exists a pure state $|e\rangle$ on another Hilbert space $\mathcal{H}_E$ and a linear isometry $U : \mathcal{H}_{AE} \to \mathcal{H}_{BE}$ such that

$$\psi(\rho) = tr_E\{U(\rho \otimes |e\rangle\langle e|)U^\dagger\} \tag{2.9}$$

for all $\rho \in \mathcal{L}(\mathcal{H}_A)$. The Stinespring representation is useful for QKD when considering the action of Eve on a quantum channel between Alice and Bob.

We may wish to consider the action of a channel without considering a larger Hilbert space. In this case, the Kraus representation provides an alternate but equivalent description of a quantum channel. If we trace out system E in Eq. 2.9, we find that the channel is equivalently described by a set of linear operators $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, where $\mathcal{A}_i : \mathcal{H}_A \to \mathcal{H}_B$:

$$\psi(\rho) = \sum_{i=1}^{n} \mathcal{A}_i \rho \mathcal{A}_i^\dagger. \tag{2.10}$$

The operators $\mathcal{A}_i$ are known as Kraus operators. In consideration of the Stinespring representation, the Kraus operators can be written in terms of U and $|e\rangle$ from Eq. 2.9:

$$\mathcal{A}_i = (\mathbb{1}_B \otimes \langle e_i|)U(\mathbb{1}_A \otimes |e\rangle) \tag{2.11}$$

where $\{|e_1\rangle, \ldots, |e_n\rangle\}$ is an orthonormal basis state spanning $\mathcal{H}_E$. We use $\mathbb{1}$ to denote the identity operator. Note that the choice of basis $|e_i\rangle$ is not unique, therefore the Kraus operators do not have a unique representation.

The trace preserving property of quantum channels enforces the condition $\sum_i \mathcal{A}_i^\dagger \mathcal{A}_i = \mathbb{1}_A$. Any set of Kraus operators satisfying this condition corresponds to a physical channel.

2.1.4 Measurements

In quantum mechanics, a quantum state is not directly accessible to an observer. Instead, an observer may interact with a quantum system through an external system (such as a measurement device) in order to derive classical information. Intuitively, and formally, measurements may be understood as a quantum channel in which the measurement outcome is stored in a classical register. For the purpose of this thesis, we introduce a different but equivalent formalization, known as the *measurement operator* formalism.

Any measurement may be described by a collection of *measurement operators*, $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, each associated with a particular measurement outcome. Measuring a quantum state ρ, we find that the outcome ρ_x with probability p_x, where ρ and p_x are given by

$$p_x = tr\{\mathcal{A}_x \rho \mathcal{A}_x^\dagger\} = tr\{\mathcal{A}_x^\dagger \mathcal{A}_x \rho\} \tag{2.12}$$

$$\rho_x = \frac{1}{p_x} \mathcal{A}_x \rho \mathcal{A}_x^\dagger. \tag{2.13}$$

In order to be physical, the measurement operators must satisfy the completeness relation $\sum_i \mathcal{A}_i^\dagger \mathcal{A}_i = \mathbb{1}$. This ensures $\sum_x p_x = 1$.

Often, the final state of the quantum system is of little interest. Rather, our interest lies in the probability that each measurement outcome is observed. In this case *Positive Operator-Valued Measure* (POVM) formalism proves to be a useful tool. By considering the product of measurement operators, $M_i := \mathcal{A}_i^\dagger \mathcal{A}_i$, we may define a set of positive semidefinite operators, $\{M_1, \ldots, M_n\}$. M_i is referred to as a *POVM element*, while the set $\{M_1, \ldots, M_n\}$ is a POVM. Note that the completeness relation for measurement operators enforces $\sum_i M_i = \mathbb{1}$. In this case, the probability of outcome x is simply $p_x = tr\{M_x \rho\}$.

2.2 Information Theory

2.2.1 Shannon Entropy

Shannon entropy is an important notion in information theory, providing a method to quantify uncertainty. Consider a source emitting a random variable $X \in \{x_1, \ldots, x_n\}$ with probability distribution $\mathbf{p} = \{p_1, \ldots, p_n\}$. The Shannon entropy of the source is given by

$$H(X) = H(\mathbf{p}) := -\sum_{i=1}^{n} p_i \log p_i. \tag{2.14}$$

Note that the Shannon entropy is a function *only* of the probability distribution, and not of the values of the random variable. Shannon entropy may be interpreted as the average information content of X, i.e. a measure of how much information is gained, on average, when the value of X is revealed. Conventionally, Shannon entropy is measured in bits and the above logarithm is understood to be base two. For the remainder of this thesis, we will adopt this convention. When $n = 2$, the Shannon entropy is also known as the binary entropy function. We define this case as a special function, $h(p) := -p \log p - (1-p)\log(1-p)$.

Considering two random variables X and Y with a joint probability distribution $\mathbf{p}_{X,Y} = \{p_{i,j}\}$, we can consider the *conditional Shannon entropy*, defined by

$$H(X|Y) := -\sum_{i,j} p_{i,j} \log \frac{p_{i,j}}{p_j}. \tag{2.15}$$

The conditional Shannon entropy plays an important role in error correction. Consider two different strings of length n, arising from X and Y. There exists a lower bound on the amount of information that must be exchanged in order to correct differences between the strings. Explicitly, this bound is given $nH(X|Y)$ [45]. Note that this limit is only achievable as the length of each string approaches infinity. Stricter bounds exist for the case of finite strings [52].

From the Shannon entropy and the conditional Shannon entropy, we can define a measure of the correlation between X and Y, known as the mutual information. The mutual information is defined as

$$I(X:Y) = I(\mathbf{p}_{X,Y}) := H(X) - H(X|Y) = H(Y) - H(Y|X). \tag{2.16}$$

2.3 Quantum Information Theory

2.3.1 Von Neumann Entropy

The *von Neumann entropy* serves as a generalization of the Shannon entropy. While the Shannon entropy was limited to classical variables, the von Neumann entropy acts as an entropic measure for quantum states. The von Neumann entropy of a state ρ is given by

$$S(\rho) := -tr\{\rho \log \rho\}. \tag{2.17}$$

When considering the eigenvalues of ρ, denoted by $\lambda_1, \ldots, \lambda_n$, the von Neumann entropy more closely resembles the Shannon entropy:

$$S(\rho) = -\sum_{i=1}^{n} \lambda_i \log \lambda_i. \tag{2.18}$$

2.3.2 Holevo Bound

In cryptography, it is natural to ask how correlated two systems are. In quantum cryptography, this question typically arises when Alice holds a classical system (X), and Eve holds a quantum system (E). We refer to such a state as a *cq-state*. A general cq-state can be written as

$$\rho_{XE} = \sum_{i=1}^{n} p_i |i\rangle\langle i| \otimes \rho_E^i \tag{2.19}$$

for some probability distribution $\mathbf{p} = \{p_1, \ldots, p_n\}$ and an orthonormal basis $\{|1\rangle, \ldots, |n\rangle\}$ spanning $\mathcal{H}_A$. Here we use $\{\rho_E^1, \ldots, \rho_E^n\}$ to denote an arbitrary set of quantum states on $\mathcal{H}_E$.

The *Holevo bound* provides a useful limit on the correlation between the classical system X and the quantum system E. More precisely, let us imagine Eve chose to measure her system, obtaining the variable Z. For any choice of Eve's measurement,

$$I(X:Z) \leq \chi(X:E) := S\left(\sum_{i=1}^{n} p_i \rho_E^i\right) - \sum_{i=1}^{n} p_i S\left(\rho_E^i\right). \tag{2.20}$$

The quantity on the right hand side is known as the *Holevo quantity*. In this thesis, the Holevo quantity is considered largely for its cryptographic implications; however, the Holevo quantity plays a vital role in many areas of quantum information theory.

Chapter 3

Quantum Key Distribution

Since the first QKD protocol was published in 1984, QKD has grown to encapsulate a variety of protocols — all linked by their exploitation of quantum mechanics to derive a secret and shared key. In this chapter, we will review a class of QKD protocols known as *prepare-and-measure protocols*. We will further review a common framework for dealing with the security of these schemes. Finally, we examine the prototypical QKD scheme, the BB84 protocol [8].

3.1 Prepare and Measure Protocols

The most common class of QKD protocol is known as a prepare-and-measure protocol. Alice, with some probability, chooses a signal state from a predetermined set of signal states. Over a public quantum channel, Alice sends the signal state to Bob, who performs a measurement on the system. This process is repeated until Alice and Bob have a suitably large data set. Alice and Bob then perform post-processing using an authenticated classical channel to distill secret keys. Given this structure, prepare-and-measure schemes are typically divided into a quantum phase (signal preparation and measurement) followed by a classical phase (post-processing).

The security of QKD protocols relies on several assumptions about Alice, Bob and Eve. In Section 3.2 we will mention assumptions about Eve; however, let us first list the assumptions that are commonly made about Alice and Bob in a prepare-and-measure protocol:

- In addition to the quantum channel, the legitimate parties have access to an authenticated classical channel.
- Alice and Bob's labs are inaccessible to Eve.
- The source and measurement apparatus are completely characterized.[1]

With these assumptions in mind, let us look in detail at the steps of a typical prepare-and-measure protocol:

Quantum Phase

1. *State Preparation*: Let $\mathcal{H}_S$ be a d-dimensional Hilbert space. Alice chooses a signal state $|\phi_x\rangle \in \mathcal{H}_S$ from a predetermined set of signal states, $\{|\phi_1\rangle, \ldots, |\phi_n\rangle\}$, with probability p_x. Alice then sends the signal state to Bob, using an untrusted quantum channel. Alice repeats this process N times.
2. *Measurement:* Bob measures each signal state independently, corresponding to a POVM $\mathbf{M}_B = \{M_{B,y}\}$, and records the result. This results in an overall joint probability distribution, $p_{x,y}$.

Classical Phase

1. *Parameter Estimation:* While the quantum phase of prepare-and-measure protocols has a clear ordering, the ordering of the classical phase is less definitive. Most protocols begin with some form of parameter estimation and end with error correction and privacy amplification. Parameter estimation is a critical step as it allows Alice and Bob to detect the presence of an eavesdropper. Alice and Bob choose a random subset of their measurement events and publicly reveal the results over an authenticated channel. This allows Alice and Bob to faithfully estimate $p_{x,y}$.
2. *Continuation Decision:* Given the observed probability distribution, Alice and Bob abort the protocol if it is possible that an eavesdropper is significantly correlated with their data. Otherwise they continue with the protocol. Typically, the full probability distribution $p_{x,y}$ is not considered here. Instead, some linear combination of observed quantities (such as error rates) is used to simplify the analysis.

[1] Generally speaking, this is not a reasonable assumption. Realistic implementations vary significantly from theoretical models. Locating security loopholes introduced by the physical implementation of a protocol (known as *side channels*) is an active subject in QKD [27, 33, 43]. Currently, robust theoretical frameworks for incorporating general side channels into a security proof have not been developed; however, several QKD protocols have been developed which reduce their reliance upon device characterization [2, 9, 28].

3. *Data Processing:* This step includes any two-way post-processing. A common example of data processing is *sifting*. During sifting, Alice and Bob postselect on highly correlated data. (We will examine sifting in Sections 3.3 and 3.6.) Another common example of data processing is the removal of events in which Bob's detector did not detect an event.

4. *Key Map:* Alice and Bob locally map their data into strings of bits, known as a *raw key*.

5. *Error Correction:* At this point, Alice and Bob each hold a bit-string. In general, we must assume that the strings differ due to errors introduced in the protocol. In order to correct the strings, Alice and Bob carry out error correction, or *reconciliation*, over the public channel. The most common choice for error correction uses one-way communication. If Alice sends error correcting information to Bob, this is known as *direct reconciliation*, while Bob sending information to Alice is known as *reverse reconciliation*. Alternatively, Alice and Bob may use two-way communication for error correction. This approach can tolerate higher error rates [22] but the security of such protocols is less well understood. Any realistic error correction protocol comes with a finite probability of failure. In this case the protocol aborts.

6. *Privacy Amplification:* If error correction has succeeded, Alice and Bob hold identical keys; however, the keys are still potentially correlated with a third party. If the potential correlation is weak enough, Alice and Bob may locally map their keys into shorter keys, cutting any correlation with a third party. If privacy amplification fails, the protocol is aborted.

3.2 An Eavesdropper's Interaction

QKD offers provable security in the presence of a computationally unbounded eavesdropper. However, the proof of such security relies on several assumptions about an eavesdropper:

- Eve is assumed to be bound by the laws of quantum mechanics. This prohibits Eve from implementing attacks such as a perfect quantum cloner [57]. Eve is allowed any physical interaction with the quantum channel.

- In adherence to *Kerckhoff's principle*, all aspects of the protocol are assumed to be known by Eve, including a full characterization of the experimental apparatus. Eve, however, does not have the power to alter the devices.

- Eve receives a perfect transcript of any classical communication sent over the authenticated channel but cannot alter the message.

Note that these assumptions are not common to all QKD protocols (for example, see Ref. [4]). For the purpose of this thesis, we will work with these assumptions.

The characterization of Eve's attack is motivated by the Stinespring representation of quantum channels. In the worst case scenario, Eve has complete control of the quantum channel linking Alice and Bob. This is realized by allowing Eve to attach an ancilla system E' to the n signal states. Eve then applies a unitary map taking $S^{\otimes N}E'$ to $B^{\otimes N}E$, keeping the system E for herself and delivering $B^{\otimes N}$ to Bob. This is referred to as a *coherent attack* or a *general attack*.

Often, it is convenient to consider a weaker form of attack, known as a *collective attack*. Rather than performing one large unitary, Eve attaches an individual ancilla to each signal state. Eve then applies the same unitary to each signal/ancilla pair. At the end of the protocol, after Eve has received any classical communication exchanged between Alice and Bob, Eve may perform a collective measurement on her systems. If a protocol is proven to be secure against collective attacks, methods exist for extending the security to coherent attacks [13, 14].

3.2.1 Source-Replacement Picture

The *source-replacement picture* is a common technique used to simplify the security analysis of prepare-and-measure protocols [9]. The technique provides a simple method for characterizing the action of an eavesdropper's attack.

In Section 3.1, we did not specify how Alice prepares the signal states. Let us imagine a hypothetical protocol where Alice generates the signal states by first creating the bipartite entangled state

$$|\Phi\rangle_{AS} = \sum_{x=1}^{n} \sqrt{p_x}|i_x\rangle_A|\phi_x\rangle_S. \tag{3.1}$$

Here $\{|i_x\rangle\}$ denote an orthonormal basis on an n-dimensional Hilbert space, $\mathcal{H}_A$. Alice could now prepare the signal state $|\phi_x\rangle$ by measuring system A. Given that the channel does not act on system A, Alice may in fact delay her measurement until after sending the system S along the channel. Due to the fact that Alice's measurement commutes with the action of the channel, this hypothetical protocol is functionally equivalent to the original protocol.

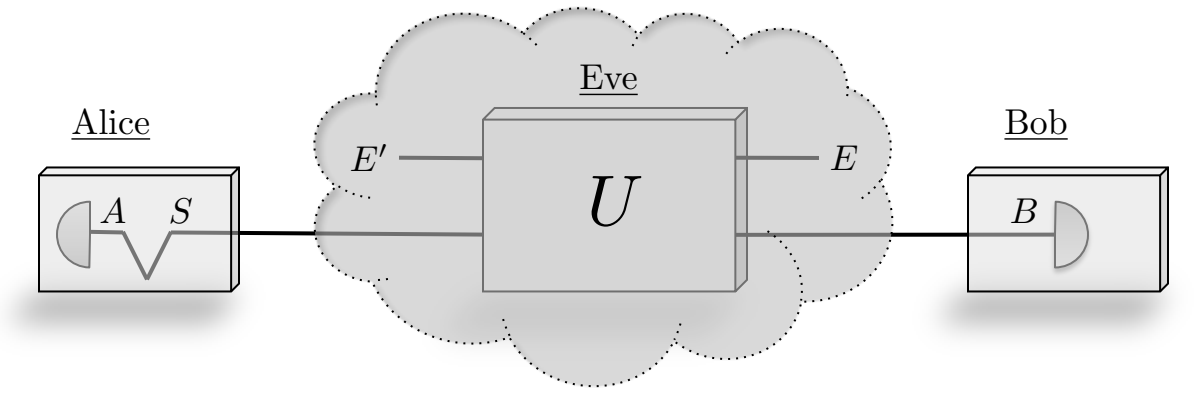

Figure 3.1: A depiction of a collective attack on a prepare-and-measure protocol. The figure shows the source-replacement picture in which Alice generates a bipartite state ρ_{AS} on the joint system AS. Eve applies the operation $U : \rho_{AS} \otimes \rho_{E'} \rightarrow \rho_{ABE}$.

After distributing N signal states, Alice and Bob share a large multipartite state, ρ_{AB}^{N}, consisting of $2N$ systems. If we consider only collective attacks, this state takes a product form, $\rho_{AB}^{N} = \rho_{AB}^{\otimes N}$. If Bob's measurements also adhere to a tensor product structure, this effectively allows us to consider each signal state individually. If Alice and Bob hold the bipartite state ρ_{AB}, Eve's control over the unitary channel allows her to generate any purification $|\Phi\rangle_{ABE}$, subject to the restriction that $tr_{BE}\{|\Phi\rangle\langle\Phi|_{ABE}\} = tr_{S}\{|\Phi\rangle\langle\Phi|_{AS}\}$. Note that when considering a lossy channel, Eve has access to strategies that preferentially block certain signal states, potentially altering the probability distribution of the detected signals. If Alice and Bob postselect on detected events, the above restriction cannot be applied to the detected events. Eve's ability to alter the probability distribution of the detected events can be accounted for by updating the original probability distribution p_x in Eq. 3.1, or by recasting the source-replacement picture (see Section 3.6.2 for example).

A collective attack in the source-replacement picture is depicted in Figure 3.1.

3.2.2 Limiting an Eavesdropper's Attack

In theory, by specifying the precise form of the tripartite state, $|\Phi\rangle_{ABE}$, Alice and Bob could fully characterize Eve's attack. Considering the source-replacement picture, the observed probability distribution between Alice and Bob is given by

$$p_{x,y} = tr_{AB}\{|i_x\rangle\langle i_x| \otimes M_{B,y}\ \rho_{AB}\}. \tag{3.2}$$

Note that this is not enough to uniquely specify Eve's attack; it merely classifies which attacks were possible and which were not. Considering the Hilbert space shared by the three parties, $\mathcal{H}_{ABE}$, we make the following definition,

Definition 1. *Let Γ_0 be the set of all tripartite states $|\Phi\rangle_{ABE} \in \mathcal{H}_{ABE}$ that are consistent with the probability distribution $p_{x,y}$, and have the reduced state $\rho_A = tr_{BE}\{|\Phi\rangle\langle\Phi|_{ABE}\}$.*

Intuitively, if Alice and Bob can show that their protocol is secure against all attacks in the set Γ_0, they can prove that their protocol is secure. In Section 3.4 we address how this is done in practice.

3.3 Announcements and Postselection

In the data processing step of a QKD protocol, it is common for Alice and Bob to discard subsets of their data. This process of postselection is aided by public announcements. A common example is *basis sifting* (for example, see the BB84 protocol in Section 3.6). In such protocols, Alice typically prepares basis states from two or more bases. Bob randomly picks a measurement basis. During the data processing step, the corresponding basis for each signal state is announced. Whenever Alice and Bob's basis choices do not coincide, the data are discarded. By doing so, Alice and Bob increase correlations in their data sets. Public announcements and postselection have non-trivial effects on the security of a protocol. To analyze these effects, we will adopt the announcement and postselection formalism presented in Ref. [19].

Conventionally, announcements and postselection are dealt with simultaneously. For illustrative purposes, let us first deal with announcements. Let us look at an announcement model where Alice and Bob's announcements are related to their data, x and y, by a function ξ such that $\xi(x) = u_A$ and $\xi(y) = u_B$ are publicly announced. In the case of basis sifting, u_A and u_B are simply Alice and Bob's basis choice.

During announcements, Alice and Bob measure the joint state ρ_{ABE} with the POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$, then make the corresponding public announcement. This process may be equivalently described by first applying a map $\Psi_{\text{ann.}}$ to ρ_{ABE}, then performing new basis dependent measurements ($\mathbf{M}_A^u$ and $\mathbf{M}_B^u$) on the state. The announcements are represented by a classical register C, held by Alice, Bob and Eve. Specifically, the map has the form

$$\Psi_{\text{ann.}}(\rho_{ABE}) = \sum_{u_A,u_B} p_{u_A,u_B} \psi_{\text{ann.}}^{u_A,u_B}(\rho_{ABE}) \otimes |u_A,u_B\rangle\langle u_A,u_B|_C. \tag{3.3}$$

Here $\psi_{\text{ann.}}^{u_A,u_B}(\rho_{AB})$ is the state conditioned on each announcement combination, and p_{u_A,u_B} is the associated probability.

By announcing particular values of u, the legitimate parties effectively partition the original POVMs into subsets containing the POVM elements corresponding to u. Let us denote these subsets by $\mathbf{m}^{u_A} := \{M_{A,x} : \xi(x) = u_A\}$ and $\mathbf{m}^{u_B} := \{M_{B,y} : \xi(y) = u_B\}$. New measurements, $\mathbf{M}_A^{u_A}$ and $\mathbf{M}_B^{u_B}$ are made on the conditional states $\psi_{\text{ann.}}^{u_A,u_B}(\rho_{AB})$, where the conditional state is given explicitly by the mapping

$$\psi_{\text{ann.}}^{u_A,u_B}(\rho_{ABE}) = \frac{\mathcal{A}_{A,u_A} \otimes \mathcal{A}_{B,u_B} \otimes \mathbb{1}_E \rho_{ABE} (\mathcal{A}_{A,u_A} \otimes \mathcal{A}_{B,u_B} \otimes \mathbb{1}_E)^\dagger}{tr_{AB}\{\mathcal{A}_{A,u_A} \otimes A_{B,u_B} \rho_{AB} (\mathcal{A}_{A,u_A} \otimes \mathcal{A}_{B,u_B})^\dagger\}}, \tag{3.4}$$

where the $\mathcal{A}_{A,u_A}$ and $\mathcal{A}_{B,u_B}$ are Kraus operators given by

$$\mathcal{A}_{A,u_A} := \sqrt{\sum_{\mathbf{m}^{u_A}} M_{A,x}} \tag{3.5}$$

$$\mathcal{A}_{B,u_B} := \sqrt{\sum_{\mathbf{m}^{u_B}} M_{B,x}}. \tag{3.6}$$

This formalism yields the interpretation that Alice and Bob first measure ρ_{ABE} to ascertain the basis information, then perform updated measurements on the conditional states. The new measurements ensure that measuring ρ_{AB} with the original POVMs yields the same results, as measuring $\psi_{\text{ann.}}^{u_A,u_B}(\rho_{AB})$ with the updated POVMs $\mathbf{M}_A^{u_A}$ and $\mathbf{M}_B^{u_B}$. The updated POVMs are given by

$$\mathbf{M}_A^{u_A} := \{M_{A,x}^{u_A}\} = \{\mathcal{A}_{A,u_A}^{-1} M_{A,x}^{u_A} \mathcal{A}_{A,u_A}^{-1\dagger} : M_{A,x}^{u_A} \in \mathbf{m}^{u_A}\} \tag{3.7}$$

$$\mathbf{M}_B^{u_B} := \{M_{B,x}^{u_B}\} = \{\mathcal{A}_{B,u_B}^{-1} M_{B,x}^{u_B} \mathcal{A}_{B,u_B}^{-1\dagger} : M_{B,x}^{u_B} \in \mathbf{m}^{u_B}\}. \tag{3.8}$$

Note that the inverses of $\mathcal{A}_{A,u_A}$ and $\mathcal{A}_{B,u_B}$ are defined for non-zero subspaces only.

The process of postselection follows simply from the announcement structure. As an example, let us examine basis sifting, where data are only kept when $u := u_A = u_B$. In practice, the effect of announcements and postselection on the original state ρ_{ABE} are described by a single mapping

$$\Psi(\rho_{ABE}) := \sum_u p_u \psi^u(\rho_{ABE}) \otimes |u\rangle\langle u|_C \tag{3.9}$$

where for simplicity we have defined $\psi^u(\rho_{ABE}) := \psi^{u_A=u,u_B=u}(\rho_{ABE})$, and

$$p_u = \frac{p_{u_A=u,u_B=u}}{\sum_i p_{u_A=i,u_B=i}}. \tag{3.10}$$

3.4 Security

The description of a typical protocol in Section 3.1 should leave a skeptical reader wanting. What does it mean for a protocol to be secure, and how do we quantify this? What condition triggers Alice and Bob to abort their protocol? How likely is a protocol to fail? These questions are all addressed by a thorough security analysis. In this thesis, we use the security framework developed by Refs. [38, 26, 39]. As before, we consider collective attacks. Additionally, we examine the limit where the number of signals approaches infinity.

3.4.1 Security Definition

The final product of any QKD protocol is either two keys, held by legitimate parties, or a null string, signifying the protocol has aborted. A protocol is considered to have failed if the protocol did not abort *and* the keys are not ideal. (By ideal, we specifically mean the keys are identical, secret and evenly distributed.)

We can formalize this notion. If a protocol does not abort, the final state held between Alice, Bob and Eve can be described by two classical registers (held by Alice and Bob) and a quantum register (held by Eve). This state is referred to as a *ccq-state*. Any general output can be written as

$$\rho_{ccq} = \sum_{k_A,k_B} p_{k_A,k_B} |k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \rho_E^{k_A,k_B}. \tag{3.11}$$

The ideal output is uncorrelated with an eavesdropper ($\rho_E^{k_A,k_B} = \rho_E$ for all k_A, k_B) and produces evenly distributed and identical keys ($p_{k_A,k_B} = \delta_{k_A,k_B}/|\mathcal{K}|$):

$$\rho_{ideal} = \frac{1}{|\mathcal{K}|} \left(\sum_k |k\rangle\langle k| \otimes |k\rangle\langle k| \right) \otimes \rho_E. \tag{3.12}$$

Here $|\mathcal{K}|$ is the size of the key space.

With these tools, we introduce the security definition given in Ref. [38]:

Theorem 1. *A QKD protocol is said to be ϵ-secure if there exists a density matrix ρ_{ideal} of the form of Eq. 3.12 such that*

$$\frac{1}{2} \left\| \rho_{ccq} - \rho_{ideal} \right\|_1 \leq \epsilon \tag{3.13}$$

where $\left\| . \right\|_1$ denotes the trace norm.

The security parameter ϵ represents the probability that the protocol will not abort *and* the key will not be ideal. Importantly, the security definition provides composability [36]. This ensures that if the final key is used in another cryptographic protocol, or if a QKD protocol relies upon a message authentication protocol, the total protocol remains secure. Note that an ϵ-secure protocol is not necessarily a useful protocol. A protocol that aborts every time has $\epsilon = 0$. Perhaps worse, a protocol with $\epsilon \approx 0$ may produce an insecure key every time it does not abort.

In the limit of an infinite number of signal states, ϵ can be made to approach zero; however, for a finite number of signal states ϵ is generally finite. How a protocol's security is affected by using a finite number of signals (known as *finite size effects*) is an active area of research in QKD (see for example Ref. [44]).

3.4.2 Key Rate Formula

The final step in most QKD protocols is to perform privacy amplification, where n raw key bits are mapped into a shorter string of l key bits, using *two-universal hash functions* [38]. In order to cut correlations with a third party, l must be sufficiently small. Let us define the *key rate* to be

$$r = \lim_{n\to\infty} \frac{l}{n}. \tag{3.14}$$

Note that the key rate will be dependent both on the protocol employed, and an eavesdropper's attack. For clarity, let us define l to be the maximum length of the final key for which any correlation with a third party is removed. In practice, proof techniques only lower bound the key rate. Any protocol operating at or below this bound is known to be ϵ-secure.

For a given collective attack, the key rate formula derived by Refs. [26, 38, 39] is given by

$$r \geq H(K_A) - \delta^{EC}_{\text{leak}} - \chi(K_A : E). \tag{3.15}$$

From left to right, $H(K_A)$ is the entropy of Alice's key data, $\delta^{EC}_{\text{leak}}$ is an upper bound on the amount of information leaked during error correction, and $\chi(K_A : E)$ is the Holevo quantity between Alice's key data and Eve's quantum states. Typically, Eve's attack is not uniquely specified by Alice and Bob's measurements. In this case, a common method for lower bounding Eq. 3.15 is to maximize the Holevo quantity with respect to the set Γ_0 (introduced in Section 3.2.2). The Holevo quantity is given by

$$\chi(K_A : E) = S\left(\sum_k p_k \tilde{\rho}^k_E\right) - \sum_k p_k S(\tilde{\rho}^k_E), \tag{3.16}$$

where $\tilde{\rho}_E^k$ is Eve's total state (after the announcement and postselection map Ψ) conditioned on the key bit k.

We introduce two theorems for simplifying the above expression. For ease, let us use the notation presented in Ref. [19]. Recall that we previously introduced $\mathbf{M}^u$ in Section 3.3, denoting a measurement conditioned on some public announcement u. For most protocols, each outcome in the conditional measurement $\mathbf{M}^u$ is associated with a definite key bit. For this thesis, we will assume that this is the case. This provides a natural interpretation for the definition $\chi(\Psi(\rho_{ABE}), \mathbf{M}_A^u) := \chi(K_A : E)$, and allows us to define the following theorems. Note that the form of the key map is now implicit in $\chi(\Psi(\rho_{ABE}), \mathbf{M}_A^u)$; for more general key maps, the following theorems cannot be assumed to hold.

Theorem 2. *Consider the set of bipartite density matrices ρ_{AE}^u and the probability distribution $\boldsymbol{p}_U = \{p_u\}$. If the measurements $\boldsymbol{M}_A^u$ result in the probability distribution $\boldsymbol{p}_{U,K} = \{p_{u,k}\}$, it holds that*

$$\chi\left(\sum_u p_u \rho_{AE}^u \otimes |u\rangle\langle u|, \boldsymbol{M}_A^u\right) = \sum_u p_u \chi(\rho_{AE}^u, \boldsymbol{M}_A^u) + I(\boldsymbol{p}_{U,K}) \tag{3.17}$$

where $|u\rangle$ denotes an orthonormal basis, and $I(\boldsymbol{p}_{U,K})$ is the mutual information between the announcement and the final key bit.

The proof for this theorem is found in Appendix A.1. The mutual information can be expressed in terms of Shannon entropies:

$$I(\mathbf{p}_{U,K}) = H(K_A) - \sum_u p_u H(K_A^u). \tag{3.18}$$

where $H(K_A^u) := -\sum_k p_{k|u} \log p_{k|u}$. Using Thm. 2 and the specific form of the postselection mapping Ψ, it follows that

$$H(K_A) - \chi(\Psi(\rho_{ABE}), \mathbf{M}_A^u) = \sum_u p_u \Big(H(K_A^u) - \chi(\psi^u(\rho_{ABE}), \mathbf{M}_A^u) \Big). \tag{3.19}$$

Next, we introduce a theorem which can be used to upper bound the Holevo quantity:

Theorem 3. *Consider a measurement $\boldsymbol{M}_A$ acting on system A of the tripartite pure state $|\Phi\rangle_{AEE'}$, resulting in the conditional state $\rho_{AEE'}^k$ with probability p_k. If the conditional states $\rho_{AEE'}^k$ are pure, it holds that*

$$\chi(\rho_{AE}, \boldsymbol{M}_A) \leq S(\rho_A) - \sum_k p_k S(\rho_A^k). \tag{3.20}$$

The proof for this theorem is found in Appendix A.2. Note that if the measurement in the above theorem is a rank-one projective measurement, the condition required for Theorem 3 is satisfied. If Theorem 3 is satisfied, the above two theorems can often be used to express the key rate without explicit reference to Eve's conditional states.

3.5 Symmetry in Security Proofs

In this section, we review a method that may be used to maximize the Holevo quantity [19, 26]. The method utilizes symmetries within a protocol to show that, in specific circumstances, Eve's optimal attack belongs to a symmetric subset of attacks.

In order to limit the form of Eve's interaction, the legitimate parties may use the set Γ_0 (Def. 1). In general, optimizing over the set Γ_0 is difficult due to the large number free parameters. The number of free parameters may be reduced if the legitimate parties relax the constraints on Γ_0. For this purpose, the legitimate parties instead rely on a set of linear functions of the probability distribution, denoted by e^i. Let use define Γ to be the set of all states consistent with e^i that have the same reduced density matrix ρ_A. In practice, the quantities e^i are often error rates.

The process of deriving a key rate may be simplified, if a set of states $\{\rho_1, \ldots, \rho_N\}$ can be found that satisfy the following properties:

1. The states result in the same quantities e^i.
2. The states have the same postselected Holevo quantity as the original state:[2]

$$\chi(\Psi(\rho_{ABE}), \mathbf{M}_A^u) = \chi(\Psi(\rho_i), \mathbf{M}_A^u) \quad \forall i. \tag{3.21}$$

3. The composition of the postselection map and the Holevo quantity is concave:

$$\frac{1}{N}\sum_i \chi(\Psi(\rho_i), \mathbf{M}_A^u) \leq \chi\left(\Psi\left(\frac{1}{N}\sum_i \rho_i\right), \mathbf{M}_A^u\right) \tag{3.22}$$

[2]Strictly speaking, it is only required that $\chi(\Psi(\rho_{ABE}), \mathbf{M}_A^u) \leq \chi(\Psi(\rho_i), \mathbf{M}_A^u)$ for all i; however, in practice the case of equality is typically proven.

Given the above properties, it follows that

$$\max_{\Gamma} \chi(\Psi(\rho_{ABE}), \mathbf{M}_A^u) \leq \max_{\Gamma} \chi\left(\Psi\left(\frac{1}{N}\sum_i \rho_i\right), \mathbf{M}_A^u\right). \tag{3.23}$$

In practice, it is often possible to find such a set of states that drastically reduces the number of free parameters involved in maximizing the Holevo quantity. These states are commonly found by exploiting symmetries inherent in the protocol. We will make use of this approach in Section 4.4.

3.6 An Example: the BB84 Protocol

The BB84 protocol [8] is the prototypical QKD protocol. Published in 1984, the BB84 protocol, and variations thereof, are still implemented and studied. In this section, we will review the fundamental steps of the BB84 protocol, and provide basic results on the security of the protocol.

3.6.1 Protocol Outline

The BB84 protocol follows the basic steps of a prepare-and-measure protocol, outlined in Section 3.1. With some probability, p_u, Alice selects a basis, $u_A \in \{X, Z\}$. Alice then chooses a bit value $r \in \{0, 1\}$ with equal probability. She then follows one of two encoding rules:

X-basis: Alice creates a qubit from the X-basis $\{|+\rangle, |-\rangle\}$, using $r \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^r|1\rangle)$.

Z-basis: Alice creates a qubit from the Z-basis $\{|0\rangle, |1\rangle\}$, using $r \to |r\rangle$.

For the remainder of this thesis, we will define the states $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Making note of the basis and bit value, Alice sends the state to Bob.

Upon receiving the state, Bob carries out the following POVM measurement

$$\mathbf{M}_B := \{p_{u=Z}|0\rangle\langle 0|, p_{u=Z}|1\rangle\langle 1|, p_{u=X}|+\rangle\langle +|, p_{u=X}|-\rangle\langle -|\}. \tag{3.24}$$

Using the postselection formalism from Section 3.3, Bob could equivalently select a basis $u_B \in \{X, Z\}$ with probability p_u, then measure the quantum state with the corresponding POVM, $\mathbf{M}_B^{u=X}$ or $\mathbf{M}_B^{u=Z}$:

$$\mathbf{M}_B^{u=X} := \{M_{B,y=0}^{u=X}, M_{B,y=1}^{u=X}\} = \{|+\rangle\langle+|, |-\rangle\langle-|\} \tag{3.25}$$

$$\mathbf{M}_B^{u=Z} := \{M_{B,y=0}^{u=Z}, M_{B,y=1}^{u=Z}\} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}. \tag{3.26}$$

For the BB84 protocol, the new measurement POVM elements are simply rescaled versions of the old POVM elements. Similarly, it can be shown that the postselected states $\psi^u(\rho_{AB}) = \rho_{AB}$. This is typical when announcements are based solely on local randomness. Alice and Bob continue the preparation and measurement process until they have built up a sufficient set of data.

If the protocol is not aborted during parameter estimation, Alice and Bob carry out *sifting* during the data processing step. Sifting provides Alice and Bob a method to increase correlations in their data by postselecting on events where they have respectively prepared and measured in the same basis. In order to do this, Alice and Bob first announce their basis choice over the authenticated channel. Any events in which Alice and Bob did not measure in the same basis are discarded.

Alice and Bob then reverse the original encoding process to derive a raw key. This process is known as a key map. The basis information is no longer needed; only the bit value r is kept. Using error correction and privacy amplification, Alice and Bob refine their raw keys to produce two identical secret keys.

3.6.2 Source-Replacement for the BB84 Protocol

For the BB84 protocol, it is helpful to recast the canonical source-replacement technique, as introduced in Section 3.2.1. In order to generate the signal states, let us imagine that Alice generates the Bell state

$$|\Phi_{0,0}\rangle_{AS} := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{3.27}$$

In order to prepare the signal states for Bob, Alice measures $|\Phi_{0,0}\rangle_{AS}$ with the POVM measurement, defined by

$$\mathbf{M}_A := \{p_{u=Z}|0\rangle\langle 0|, p_{u=Z}|1\rangle\langle 1|, p_{u=X}|+\rangle\langle+|, p_{u=X}|-\rangle\langle-|\}. \tag{3.28}$$

Note that $\mathbf{M}_A$ and $\mathbf{M}_B$ have the same POVM elements. Importantly, by recasting the source-replacement picture, it turns out we no longer require that Alice's reduced density

matrix ρ_A be kept constant. Instead, the restrictions are accounted for in Alice's POVM measurement.

3.6.3 Security of the BB84 Protocol

Recall that the key rate formula introduced in Section 3.4.2 (Eq. 3.15) is given by

$$r \geq H(K_A) - \delta^{EC}_{\text{leak}} - \max_{\Gamma_0} \chi(\Psi(\rho_{ABE}), \mathbf{M}^u_A). \tag{3.29}$$

In practice, the entropy of Alice's key data, $H(K_A)$, and the information lost during error correction, $\delta^{EC}_{\text{leak}}$, are easily bounded from observed quantities.

The maximization of the Holevo quantity proves difficult to analytically calculate, even for basic protocols. Conventional approaches place a lower bound on the key rate by loosening restrictions on the shared state $|\Phi\rangle_{ABE}$. For the BB84 protocol, only the error rates in the Z- and X-basis are typically considered.

Definition 2. *Let $\bar{\Gamma}$ be the set of all tripartite states $|\Phi\rangle_{ABE} \in \mathcal{H}_{ABE}$ that are consistent with the basis dependent error rates $e^{u=X}$ and $e^{u=Z}$.*

Note that Γ_0 is a subset of $\bar{\Gamma}$. The error rates place restrictions upon the joint state ρ_{AB}. The relation is given explicitly by

$$e^u = \sum_{x \neq y} tr_{AB}\{M^u_x \otimes M^u_y \rho_{AB}\}. \tag{3.30}$$

Using the techniques outlined in Ref. [47], an upper bound can be placed on the Holevo quantity:

$$\begin{aligned} \max_{\Gamma_0} \chi(\Psi(\rho_{ABE}), \mathbf{M}^u_A) &\leq \max_{\bar{\Gamma}} \chi(\Psi(\rho_{ABE}), \mathbf{M}^u_A) && (3.31) \\ &\leq p_{u=Z} h(e^{u=X}) + p_{u=X} h(e^{u=Z}). && (3.32) \end{aligned}$$

Here $h(x)$ is the binary entropy function. If error correction is carried out in the Shannon limit, the above key rate becomes independent of p_u. Explicitly,

$$r \geq H(K_A) - h(e^{u=X}) - h(e^{u=Z}). \tag{3.33}$$

Chapter 4

Simplified Trusted Relays

Most *point-to-point* QKD protocols (in which Alice sends quantum signals directly to Bob) are severely limited by distance. For any protocol in which signals are sent over a lossy channel, the infinite key rate is approximately bounded by the single-photon transmittance [51]. For optical fibre, this results in an exponential reduction of the key rate, limiting useful key rates to a few hundred kilometres. In free space, dispersion places similar limitations on the distance between Alice and Bob. The maximum distance is ultimately limited by detector dark counts. If the rate of dark counts is equal to or greater than the rate of signal counts, Alice and Bob cannot establish a secret key, due to the possibility of an *intercept-resend attack*.

Practical methods for implementing long-distance QKD are an active area of research. In this chapter, we review a simple approach that allows QKD to be extended to arbitrary distances, provided Alice and Bob have access to a series of trusted intermediate nodes. This approach is known as a *trusted quantum relay* [17], or simply a trusted relay. Trusted relays form the basis for a number of quantum networks [18, 37, 42] and satellite-based QKD implementations [34, 53, 58].

The focus of this chapter (and this thesis) is a novel variation of the trusted quantum relay which seeks to simplify the intermediate nodes (a *simplified trusted relay*, or an *STR*) [32, 48]. As we will show, STRs cannot naively be extended to an arbitrary distance; however, they are promising tools for realistic QKD networks. We focus on a particular STR protocol which implements the quantum phase of the BB84 protocol. Two separate security proofs for the protocol are provided. The first proof (Section 4.4) follows a conventional method for calculating the key rate, however, fails to generalize to an arbitrary number of nodes. Our second proof (Section 4.5) can be generalized to any number of

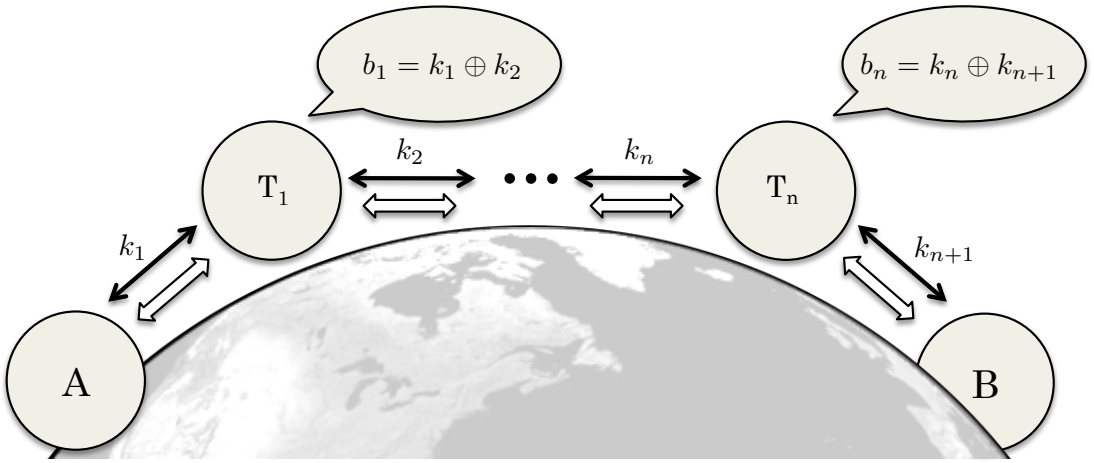

Figure 4.1: A trusted relay with n nodes. In the first link, the node (T_1) acts as a pseudo-Bob. Quantum signals (black arrows) are used to establish raw data $\{d_A, d_{T_1}\}$, which is transformed into the secret key k_1 using classical post-processing (white arrows). In the second link, the same node takes the role of Alice, establishing the secret key k_2 with the second node (T_2). Bob corrects his key by adding the parity announcements to his key.

nodes but requires the protocol to be stricter in how error correction is accomplished.

4.1 Trusted Relays

If Alice and Bob are spatially separated by a long distance, loss prohibits most naive point-to-point QKD implementations. Other times, it is simply impractical to connect Alice and Bob with a quantum channel. Trusted relays provide a simple method to overcome distance limitations, without significantly increasing the complexity of the QKD architecture. The primary drawback of trusted relays is their reliance upon a series of intermediate nodes. Importantly, these nodes must be trusted. In a basic implementation, if any one node in a relay is compromised, the entire relay is compromised. The number of trusted nodes required for a relay increases linearly with the distance between Alice and Bob.

Each node in a trusted relay functions as a pseudo-Alice and a pseudo-Bob, and carries out a point-to-point QKD protocol with its nearest neighbours. Each link in the relay runs a protocol in parallel, generating a secret key. Note that any QKD protocol may be run in each link, so long as a secure key is generated. The specific manner in which the keys are

established is irrelevant, so long as each pair of neighbours shares a secret key. A protocol involving n nodes will generate $n+1$ secret keys; each node possesses two secret keys (see Figure 4.1). Bob recovers Alice's key with two final steps:

1. *Parity Announcement:* Each node publicly announces the parity (bitwise modulo) of the two keys in its possession (denoted by b_n).
2. *Parity Announcement Processing:* Bob recovers Alice's key by adding each parity announcement (bitwise modulo) to his own key.

It is simple to show that by carrying out the parity announcement processing step, Bob recovers Alice's key:

$$\begin{aligned}(b_1 \oplus b_2 \oplus \cdots \oplus b_n) \oplus k_{n+1} &= (k_1 \oplus k_2) \oplus (k_2 \oplus k_3) \oplus \cdots \oplus (k_n \oplus k_{n+1}) \oplus k_{n+1} \\ &= k_1 \oplus (k_2 \oplus k_2) \oplus \cdots \oplus (k_{n+1} \oplus k_{n+1}) \\ &= k_1.\end{aligned} \tag{4.1}$$

Despite generating $n+1$ secret keys, n keys are consumed during the parity announcement. Effectively, each key in the relay is encrypted using the next key in the relay in the fashion of a one-time pad. After carrying out the parity announcement and processing steps, Alice and Bob are left with a single secret and shared key.

4.2 Simplified Trusted Relay Protocols

Simplified trusted relays (STRs) are an alternative to trusted relays. In the case of a trusted relay, it may not always be practical to carry out a full QKD protocol between each node. Error correction and privacy amplification have large computation and communication overheads, typically requiring substantial computational power and communication bandwidth. STR protocols have the advantage that they do not require the nodes to participate in error correction and privacy amplification. Instead, these tasks are left to Alice and Bob. In situations where computational power or communication bandwidth are limited (such as satellites or network hubs) STRs have the potential to outperform conventional trusted relays.

The primary difference between trusted relays and STRs is the timing of the parity announcement and processing steps. For a trusted relay, these are the final two steps

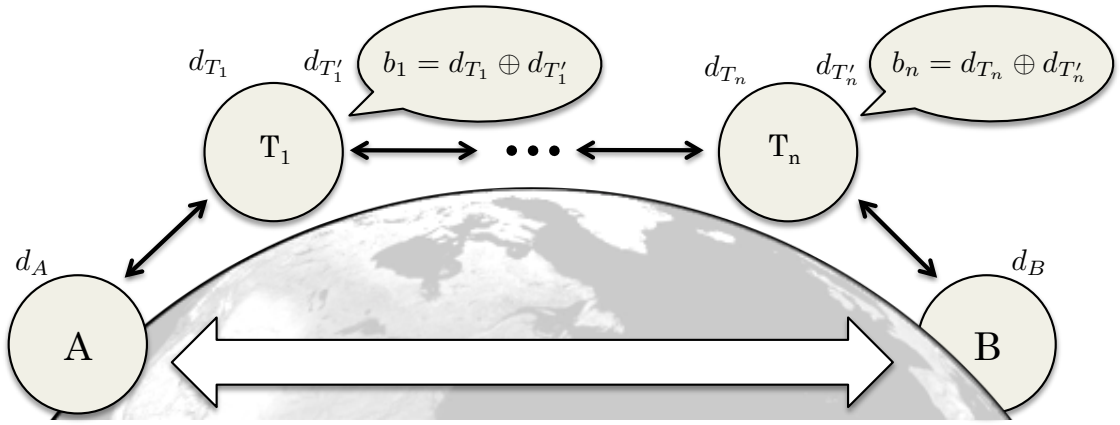

Figure 4.2: An STR with n nodes. For ease of notation alone, we have split each node into two parties (pseudo-Alice and pseudo-Bob). The legitimate parties establish a set of raw data using quantum signals (black arrows). From this raw data, they perform a key map to establish raw keys, d. Each node announces the parity (bitwise modulo) of the two keys that it holds. Bob adds each parity announcement to his own key to derive a new raw key d'_B. In the absence of errors the raw keys match in each link (i.e. $d_A = d_{T_1}$) and $d'_B = d_A$. Alice and Bob carry out the majority of the classical post-processing (white arrow).

in the protocol. In an STR, the nodes perform the parity announcement directly after sifting. In general, the nodes are not required to participate in error correction or privacy amplification. These tasks are performed by Alice and Bob, after Bob has corrected his data using the parity announcements. We visually depict the protocol in Figure 4.2. Note the two main differences to the conventional trusted relay: 1) the nodes announce the parity of raw keys, not secret keys, and 2) Alice and Bob carry out the majority of the classical post-processing.

Recall that STRs (and conventional trusted relays) require the intermediate nodes to be trusted. Any malicious node can obtain the final key shared by Alice and Bob. Methods exist for relaxing this trust assumption [5, 41]; however, the basic framework of trusted relays requires a minimal level of trust in the intermediate nodes. If the nodes are assumed to be *honest-but-curious*[1] the final key can be protected by encrypting the public announcements.

[1] An honest-but-curious adversary (also known as a *passive adversary*) is a party that faithfully carries out the protocol, however, attempts to learn as much as possible from any exchange of communication during the protocol.

There are many possible variations of the general STR protocol. In this thesis, we will examine an STR protocol in which the individual links carry out the quantum phase of the BB84 protocol. To avoid confusion with the general class of STR protocols, we will refer to this specific implementation as the *BB84 STR protocol*. Note that our analysis will directly apply to many variations of this protocol. Moreover, the analysis may be extended in a straightforward manner to include protocols such as the *6-state protocol* [12, 7]. For clarity, let us list the individual steps below:

Quantum Phase — All Parties

1. *State Preparation & Distribution:* Alice chooses a basis $u_A \in \{Z, X\}$ with probability p_u, then selects a bit value $x \in \{0, 1\}$ with uniform probability and prepares the corresponding BB84 qubit state $|\phi_x^{u_a}\rangle$. Alice records the state she created, then sends the signal to the nearest trusted node. Alice carries out this process N times, where N is suitably large. Similarly, each node prepares signals and sends them to the next node in the relay. The last node sends signals to Bob.

2. *Measurement:* Each node (and Bob) locally select a basis $u \in \{Z, X\}$ with probability p_u and perform a projective measurement in that basis, denoted by the positive operator valued measure (POVM) $\mathbf{M}^u$. To distinguish between the two roles each node plays, we use u_{T_j} to denote the j-th node's measurement basis, while $u_{T'_j}$ denotes the j-th node's state preparation basis. The choice of basis in each link is independent, i.e. u_{T_j} is independent of $u_{T'_j}$. Bob and the nodes record their measurement outcome, as well as the basis in which they measured.

Classical Phase Part I — All Parties

1. *Sifting:* The legitimate parties reveal their measurement and preparation bases. In each link, data are kept only when an event was detected and the basis choices coincided. All other data are discarded, reducing the data strings from size N to m. The basis in the first link is then $u_1 := u_A = u_{T_1}$. Similarly, we define the basis in the i-th link to be u_i.

2. *Key Map:* The legitimate parties map their data into classical bit strings (raw keys, d), by mapping the BB84 states they have sent and/or measured into raw bits using the rule $|\phi_x^u\rangle \to$ "x", where $x \in \{0, 1\}$. Alice now holds the raw key $d_A = \{x_1, \ldots, x_m\}$. For clarity, we denote Bob's raw key as $d_B = \{y_1, \ldots, y_m\}$, where y denotes Bob's measurement outcome. Similarly, the j-th node holds the raw keys $d_{T_j} = \{t_{j,1}, \ldots, t_{j,m}\}$ and $d_{T'_j} = \{t'_{j,1}, \ldots, t'_{j,m}\}$.

3. *Parity Announcement & Processing:* Each node announces the bitwise parity of the two raw keys that it holds, $b_j = \{t_{j,1} \oplus t'_{j,1}, \ldots, t_{j,m} \oplus t'_{j,m}\}$. Bob adds each parity announcement to his own raw key to obtain a new raw key d'_B. In the absence of errors, $d'_B = d_A$ and Bob recovers Alice's raw key.

Classical Phase Part II — End Users

1. *Parameter Estimation & Continuation Decision:* Alice and Bob determine the error rate for each basis combination (analogous to calculating the X- and Z-basis error rates in the BB84 protocol). If the error is suitably low, they continue the protocol. Otherwise, they abort. We will define the exact meaning of *suitably low* in the following sections.

2. *Error Correction & Privacy Amplification:* If the protocol is not aborted, Alice and Bob carry out one-way error correction and privacy amplification to obtain secure keys.[2]

Again, the primary difference between the STR protocol and the conventional trusted relay is the timing of the parity announcement and processing step. Note that after the parity announcement, the nodes are no longer required to participate in the protocol.

4.3 Motivating the Security of the BB84 STR Protocol

In this section, we apply the security proof formalism from Chapter 3 to the BB84 STR protocol in order to derive the key rate for the protocol. In further sections, we examine different methods to analytically bound this key rate.

We begin our analysis by examining the ideal case where qubit signal states are exchanged over lossless channels. Furthermore, we examine the asymptotic limit where the legitimate parties exchange a large number of signals. In this limit, we can consider Eve to make collective attacks without loss of generality [14]. In this context, collective attacks are defined for each group of signals that are matched by the parity announcements. We

[2] In order to extend our security analysis from collective to general attacks, we require that privacy amplification is executed in a *permutation invariant* fashion (see Section 4.6.1). It remains an open question whether this restriction is necessary.

will justify this definition is Section 4.6.1. For simplicity, we begin by examining the case where the BB84 STR protocol contains a single node. In Section 4.5.3, the case of multiple nodes is examined.

The source-replacement scheme can be extended to the STR protocol. In this thought set-up, each source generates the Bell state $|\Phi_{0,0}\rangle \in \mathcal{H}_{SS'}$, where $|\Phi_{0,0}\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$.[3] Instead of sending a signal state, the source then sends the second half of the entangled system (S'). Using a POVM $\mathbf{M}^u$ chosen with probability p_u, the legitimate party which has prepared the entangled state, performs a projective measurement on the remaining system S, preparing S'. The source-replacement picture reveals an important property: in each link the roles of state creation and measurement may be interchanged without affecting the qubit-level security. Alternatively, the parties could carry out an entanglement-based protocol (in which all parties perform measurements) [9] or a measurement-device independent protocol (in which all parties send signal states) [28].

4.3.1 Announcements and Postselection

In the STR protocol, the legitimate parties in each link postselect on data where the basis choices (u) matched. In order to do so, they publicly announce the basis in which states were prepared or measured. Any events in which the basis choice did not coincide are discarded. Additionally, the node announces the parity of the raw keys that it holds. Given that we are examining collective attacks on a single node, the parity announcement is given by a single bit, $b := b_1 \in \{0, 1\}$.

After distributing the signal states, the legitimate parties hold the joint system ρ_{ATB}. Due to the fact that the node sends and receives signal states, the system T is described by the tensor product of two qubit spaces. In order to ensure that Eve is limited only by the laws of quantum mechanics, we allow Eve complete control over the purification $|\Phi\rangle_{ATBE}$. As outlined in Section 3.3, the quantum treatment of postselection is represented by a completely positive trace-preserving map. The announcements are represented by a classical register C held by the legitimate parties and Eve. The postselected state is therefore block-diagonal, given explicitly by

$$\Psi(\rho_{ATBE}) = \sum_{u_1,u_2,b} p_{u_1} p_{u_2} p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |u_1, u_2, b\rangle\langle u_1, u_2, b|_C. \tag{4.2}$$

Here p_u represents the probability of each basis announcement and $p_{b|u_1,u_2}$ is the conditional probability associated with the parity announcement. Furthermore, $\psi^{u_1,u_2,b}(\rho_{ATBE})$ is the

[3] Note that we change the labelling of the subsystems from Section 3.2.1 to reflect that each source in the relay generates a Bell state, not just Alice.

state held by the legitimate parties, conditioned on a given combination of announcements. Note that the basis announcements are determined by local randomness. As a result, the state conditioned on u_1 and u_2 alone is the same as the original state. The parity announcement is determined by a measurement outcome. Using the previously outlined postselection formalism, the effect proves to be non-trivial. Explicitly,

$$\psi^{u_1,u_2,b}(\rho_{ATBE}) := \frac{1}{p_{b|u_1,u_2}} \left(\mathbb{1}_A \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes \mathbb{1}_{BE} \right) \rho_{ATBE} \left(\mathbb{1}_A \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes \mathbb{1}_{BE} \right)^\dagger \quad (4.3)$$

$$\mathcal{F}_T^{u_1,u_2,b} := \sum_{t=0}^{1} M_{T,t}^{u_1} \otimes M_{T,t\oplus b}^{u_2} \quad (4.4)$$

where $M_{T,t}^u$ denote the node's POVM elements. For the BB84 STR protocol, these are the same as Alice and Bob's POVM elements (see Eqs. 3.25-3.26).

The key rate is

$$r \geq H(K_A) - \delta_{\text{leak}}^{EC} - \max_{\Gamma_0} \chi(\Psi(\rho_{ATBE}), \mathbf{M}_A^{u_1}) \quad (4.5)$$

where Γ_0 is defined to be the set all states ρ_{ATBE} consistent with all observables measured by the legitimate parties.

4.3.2 Parameter Estimation and Error Rates

In order to derive an analytic key rate, we do not consider all possible observables. Conventionally, error rates are used. For each basis combination, the error rate between Alice's raw key, d_A, and Bob's corrected raw key, d'_B, is given by

$$e^{u_1,u_2} = \sum_b p_{b|u_1,u_2} \sum_{x \neq y \oplus b} tr_{ATBE}(M_{A,x}^{u_1} \otimes \mathbb{1}_T \otimes M_{B,y}^{u_2} \otimes \mathbb{1}_E \psi^{u_1,u_2,b}(\rho_{ATBE})) \quad (4.6)$$

$$= \sum_b \sum_{x \neq y \oplus b} tr_{ATB}\{M_{A,x}^{u_1} \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes M_{B,y}^{u_2} \rho_{ATB}\} \quad (4.7)$$

where $M_{A,x}^{u_1}$ and $M_{B,y}^{u_2}$ denote Alice and Bob's POVM elements.

From the above quantities, we can define a superset of Γ_0:

Definition 3. *Let Γ_{e^u} be the set of all states ρ_{ATBE} consistent with the set of basis-dependent error rates e^{u_1,u_2}.*

Given that $\Gamma_0 \subseteq \Gamma_{e^u}$, we may safely lower-bound the key rate by replacing the maximization over Γ_0 in Eq. 4.5, with a maximization over Γ_{e^u}. In the following section, we will use symmetries to reduce the size of Γ_{e^u}.

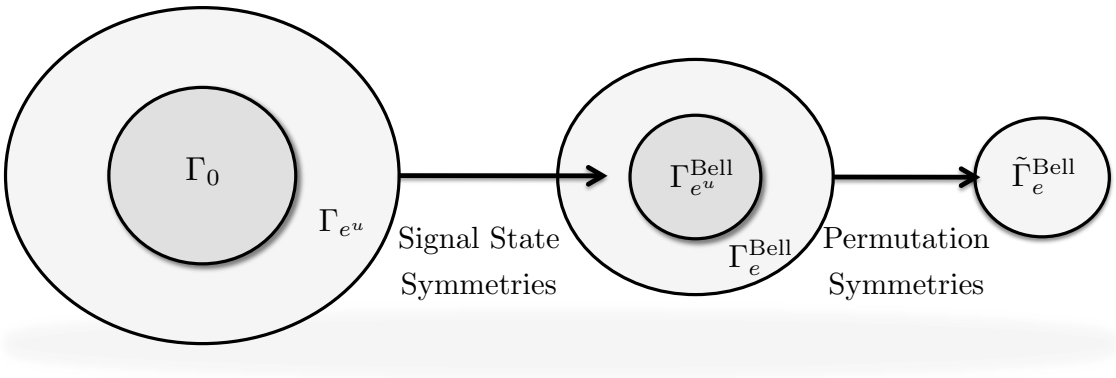

Figure 4.3: By relaxing the restrictions on the joint state ρ_{ATB} the set of possible attacks is increased; however, the complexity of the key rate calculation is reduced. By considering only the basis-dependent error rate, Γ_0 is expanded to Γ_{e^u}. In Section 4.4.1, symmetries are then used to restrict Γ_{e^u}. This process is repeated in Section 4.4.2; the set $\Gamma_{e^u}^{\text{Bell}}$ is first expanded to Γ_e^{Bell}, then restricted to $\tilde{\Gamma}_{e^u}^{\text{Bell}}$.

4.4 BB84 STR Key Rate: a Canonical Approach

In this section, we derive a key rate for the BB84 STR protocol using a single node. By restricting the implementation to a single node, we can use the canonical techniques outlined in Refs. [19, 43] to derive an analytic key rate. This method has two primary drawbacks: 1) it does not easily scale to multiple nodes, and 2) it requires that the basis weighting p_u is uniform. However, we can use this framework to examine a variant of the BB84 STR protocol where the trusted node participates in error correction (see Section 4.4.3).

The proof proceeds as follows: we first reduce the restrictions on the joint state by considering only the basis-dependent error rates between Alice and Bob. Effectively, this changes the maximization over Γ_0 to a maximization over the superset Γ_{e^u}. Signal state symmetries are then exploited to show that the optimal attack lies in the subset $\Gamma_{e^u}^{\text{Bell}} \subset \Gamma_{e^u}$ (Section 4.4.1). Furthermore, we relax our restrictions by considering only the average error rate between Alice and Bob. This allows us to use permutations of the eigenvalues of the joint state to further specify the form of the optimal attack (Section 4.4.2). The proof is visually depicted in Figure 4.3.

4.4.1 Applying Signal State Symmetries

Symmetries may be used to simplify the maximization of the Holevo quantity. Recall in Section 3.5 we outlined criteria that, if met, simplify the form of ρ_{ATB}. Drawing inspiration from Ref. [19], let us examine the action of Pauli matrices on the joint state. For our purposes, we define the Pauli matrices as:

$$U_{r,s} := \sum_{k=0}^{1} (-1)^{ks} |k+r\rangle\langle k| \tag{4.8}$$

where $r, s \in \{0, 1\}$. Note that the BB84 signal states exhibit an invariance with respect to the Pauli matrices. The application of a Pauli matrix permutes the signal states within their basis — but does not switch between bases.

Let us examine the set of states where the same Pauli matrix is applied to both parties in each link:

$$\rho_{ATB}^{U_{r,s}U_{r',s'}} := U_{r,s} \otimes U_{r,s} \otimes U_{r',s'} \otimes U_{r',s'} \rho_{ATB} (U_{r,s} \otimes U_{r,s} \otimes U_{r',s'} \otimes U_{r',s'})^\dagger. \tag{4.9}$$

for $r, s, r', s' \in \{0, 1\}$. Importantly, each state $\rho_{ATB}^{U_{r,s}U_{r',s'}}$ has the same basis-dependent error rates e^{u_1,u_2} as the original state ρ_{ATB} (see Appendix A.3). Therefore, we may utilize symmetries if the following properties hold: 1) the states are invariant with respect to the Holevo quantity and 2) the states are concave with respect to the Holevo quantity. These properties can be shown to hold if we assume that the probability associated with the key bits is uniform as shown in Ref. [19]; however, this is not necessarily true when considering loss. This assumption can be avoided by first rearranging the key rate formula in Eq. 4.5. Using Theorem 2 if follows that

$$\begin{aligned}
r \geq & H(K_A) - \delta_{\text{leak}}^{EC} - \max_{\Gamma_0} \chi(\Psi(\rho_{ATBE}), \mathbf{M}_A^{u_1}) && (4.10)\\
\geq & \sum_{u_1,u_2} p_{u_1} p_{u_2} H(K_A^{u_1,u_2}) - \delta_{\text{leak}}^{EC} && (4.11)\\
& - \max_{\Gamma_0} \sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |b\rangle\langle b|_C, \mathbf{M}_A^{u_1} \right) \\
\geq & \sum_{u_1,u_2} p_{u_1} p_{u_2} H(K_A^{u_1,u_2}) - \delta_{\text{leak}}^{EC} && (4.12)\\
& - \max_{\Gamma_{e^u}} \sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |b\rangle\langle b|_C, \mathbf{M}_A^{u_1} \right).
\end{aligned}$$

Above $H(K_A^{u_1,u_2}) := -\sum_k p_{k|u_1,u_2} \log p_{k|u_1,u_2}$. With regards to local Pauli-operations in each link, the Holevo quantity in Eq. 4.12 can be shown to be invariant (see Appendix A.4). Additionally, the composition of the mapping in Eq. 4.12 and the Holevo quantity can be shown to be concave. This follows directly from the fact that the mapping is linear,[4] and the Holevo quantity is concave [19]. As outlined in Section 3.5, these properties, along with the invariance of the basis-dependent error rates, are enough to show that

$$\max_{\Gamma_{e^u}} \sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |b\rangle\langle b|_C, \mathbf{M}_A^{u_1} \right) \leq \tag{4.13}$$

$$\max_{\Gamma_{e^u}} \sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b} \left(\frac{1}{16} \sum_{r,s,r',s'} \rho_{ATBE}^{U_{r,s}U_{r',s'}} \right) \otimes |b\rangle\langle b|_C, \mathbf{M}_A^{u_1} \right). \tag{4.14}$$

In Appendix A.5 we show that the averaged state adopts a simple form; it is diagonal with respect to tensor products of Bell states

$$\frac{1}{16} \sum_{r,s,r',s'} \rho_{ATB}^{U_{r,s}U_{r',s'}} = \sum_{a,b,a',b'=0}^{1} \alpha_{a,b,a',b'} |\Phi_{a,b}\rangle\langle\Phi_{a,b}|_{A,T_1} \otimes |\Phi_{a',b'}\rangle\langle\Phi_{a',b'}|_{T_2,B} \tag{4.15}$$

for some arbitrary set of coefficients $\alpha_{a,b,a',b'}$. We may now limit our search for the optimal attack to the set $\Gamma_{e^u}^{\text{Bell}}$, which includes all states of the the reduced form

$$\rho_{\text{Bell}} := \sum_{a,b,a',b'=0}^{1} \alpha_{a,b,a',b'} |\Phi_{a,b}\rangle\langle\Phi_{a,b}|_{A,T_1} \otimes |\Phi_{a',b'}\rangle\langle\Phi_{a',b'}|_{T_2,B} \tag{4.16}$$

that are also consistent with the set of observed error rates e^{u_1,u_2}. The process of transforming ρ_{ATB} to ρ_{Bell} is more commonly known as a twirling map. Note for states of the reduced form ρ_{Bell} it holds that

$$\sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |b\rangle\langle b|_C, \mathbf{M}_A^{u_1} \right) = \tag{4.17}$$

$$\sum_{u_1,u_2,b} p_{u_1} p_{u_2} p_{b|u_1,u_2} \chi(\psi^{u_1,u_2,b}(\rho_{ATBE}), \mathbf{M}_A^{u_1}). \tag{4.18}$$

As Thm. 2 suggests, this is not true for general states.

[4] Specifically, $\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |b\rangle\langle b|_C = \sum_b (\mathbb{1}_A \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes \mathbb{1}_{BE}) \rho_{ATBE} (\mathbb{1}_A \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes \mathbb{1}_{BE})^\dagger \otimes |b\rangle\langle b|_C$ is linear.

4.4.2 Applying Permutation Symmetries

We can again take advantage of symmetries to reduce the number of free parameters involved in optimizing the Holevo quantity. Instead of using the Pauli-invariance of the signal states, we use permutations of the eigenvalues of ρ_{ATB}. To simplify notation, let us first use Theorem 3 to eliminate any reference to Eve's system. It follows from Theorem 3 that

$$\chi(\psi^{u_1,u_2,b}(\rho_{ATBE}), \mathbf{M}_A^{u_1}) \leq S(tr_E\{\psi^{u_1,u_2,b}(\rho_{ATBE})\}) - \sum_k p_k S(tr_E\{\psi^{u_1,u_2,b,k}(\rho_{ATBE})\}). \tag{4.19}$$

For each state ρ_{ATB}, a set of states $\{\rho_{ATB}^{P_1}, \ldots, \rho_{ATB}^{P_m}\}$ may be defined by applying the permutations P_i to the eigenvalues $\alpha_{a,b,a',b'}$ of ρ_{ATB}. The Holevo quantity is concave; therefore, if the permutations are chosen so that the error rate is unchanged, and if the permuted states are invariant with respect to the Holevo quantity, the optimal attack is of the form

$$\tilde{\rho}_{\text{Bell}} := \frac{1}{m} \sum_i \rho_{\text{Bell}}^{P_i}. \tag{4.20}$$

Note that error-rate invariance and Holevo invariance do not hold in general for general eigenvalue permutations. However, for specific permutations, the invariance relation can be verified.

In order to examine the effect of a given eigenvalue permutation, it helps to define a matrix consisting of the eigenvalues of ρ_{ATB}:

$$\lambda := \begin{pmatrix} \alpha_{0,0,0,0} & \alpha_{0,0,0,1} & \alpha_{0,0,1,0} & \alpha_{0,0,1,1} \\ \alpha_{0,1,0,0} & \alpha_{0,1,0,1} & \alpha_{0,1,1,0} & \alpha_{0,1,1,1} \\ \alpha_{1,0,0,0} & \alpha_{1,0,0,1} & \alpha_{1,0,1,0} & \alpha_{1,0,1,1} \\ \alpha_{1,1,0,0} & \alpha_{1,1,0,1} & \alpha_{1,1,1,0} & \alpha_{1,1,1,1} \end{pmatrix}. \tag{4.21}$$

The eigenvalue matrix, λ, can be understood as a correlation table between the tensored Bell states in Eq. 4.16. The intersecting eigenvalue is the probability associated with that pair of Bell states. For example, $\alpha_{0,1,1,0}$ is the probability associated with $|U_{0,1}\rangle\langle U_{0,1}| \otimes |U_{1,0}\rangle\langle U_{1,0}|$.

In Appendix A.6, we show that the Holevo quantity in Eq. 4.18 is invariant under several symmetries. For example, it is invariant under the exchange of bit and phase

errors. This is equivalent to exchanging the second and third rows and/or columns of λ (or to swapping the Bell states $|U_{0,1}\rangle$ and $|U_{1,0}\rangle$). The Holevo quantity is also invariant when the links are swapped. This can be visualized as a reflection of λ about the downward diagonal. Furthermore, the Holevo quantity remains invariant when λ is reflected about the upward diagonal. Note that in order for the state to be invariant with respect to these permutations, the basis weighting p_u must be even.

While the basis-dependent error rates e^{u_1,u_2} are not invariant with respect to the above symmetries, the average error rate between Alice and Bob is. We may safely upper-bound the Holevo quantity by only considering the average error rate. With regards to the eigenvalue matrix λ, the average error rate is given by,

$$e = \sum_{u_1,u_2} p_{u_1} p_{u_2} e^{u_1,u_2} = \sum_{a,b,a',b'} \lambda^e_{(ab),(a'b')} \alpha_{a,b,a',b'}, \tag{4.22}$$

$$\lambda^e = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 0 \end{pmatrix}. \tag{4.23}$$

Here $\lambda^e_{(rs),(r's')}$ is the element of λ^e, corresponding to row rs^{th} row and the $r's'^{th}$ column. Given the form of λ^e, it is apparent upon inspection that e is consistent with the symmetries listed above.

Considering combinations that respect the previously mentioned symmetries, the eigenvalue matrix of $\tilde{\rho}_{\text{Bell}}$ is

$$\tilde{\lambda} = \begin{pmatrix} \beta_0 & \beta_1 & \beta_1 & \beta_2 \\ \beta_1 & \beta_3 & \beta_3 & \beta_1 \\ \beta_1 & \beta_3 & \beta_3 & \beta_1 \\ \beta_2 & \beta_1 & \beta_1 & \beta_0 \end{pmatrix} \tag{4.24}$$

for some arbitrary $\beta_0, \beta_1, \beta_2, \beta_3$, such that $2\beta_0 + 8\beta_1 + 2\beta_2 + 4\beta_3 = 1$. Let us define $\tilde{\Gamma}_{\text{Bell}}$ to be the set of all states $\tilde{\rho}_{\text{Bell}}$, that are consistent with the observed error rate e.

The Holevo quantity may now be analytically maximized. While the convex combination of $\tilde{\rho}_{\text{Bell}}$ depends on four eigenvalues, the maximization only depends on three free parameters. Using the normalization condition and the average error rate between Alice and Bob, two of these parameters can be specified. The Holevo quantity can then be analytically maximized with respect to the last open parameter. The maximum occurs when $\beta_0 + \beta_3 = (1/2)(1-e)^2$, $\beta_1 = (1/4)(1-e)e$ and $\beta_2 + \beta_3 = (1/2)e^2$.

The minimum postselected key rate therefore becomes

$$r \geq \sum_{u_1,u_2} p_{u_1} p_{u_2} H(K_A^{u_1,u_2}) - \delta_{leak}^{EC} - h(e) \tag{4.25}$$

where $H(K_A^{u_1,u_2}) := -\sum_k p_{k|u_1,u_2} \log p_{k|u_1,u_2}$. Note that the final expression for the key rate relies upon only the average error rate between Alice and Bob, e. Thus, the node is not required to participate in parameter estimation.

For realistic error patterns, the qubit key rate in Eq. 4.25 is equal to the qubit key rate arising from a point-to-point BB84 protocol, where Alice and Bob observe an error rate e. However, the key rate is lower than the expected key rate for a conventional trusted relay. In Section 4.6.2, we compare the STR protocol to a conventional trusted relay.

4.4.3 Trusted Nodes and Error Correction

In this section, we posit an alternative version of the BB84 STR protocol. By allowing the trusted node additional complexity, the key rate may be improved. The improvement comes at the cost of increased node complexity.

For realistic parameters, the key rate can be improved by allowing the trusted node to participate in some post-processing. Specifically, we consider the case when the node participates in error correction, but not privacy amplification. For implementations, this would imply that the node generates error correcting information and broadcasts it to Alice and Bob. (The node is not required to partake in the computationally expensive task of correcting its own key.) The key map is defined by the node; therefore, we refer to this alternative protocol as the *node-focused* protocol. This is juxtaposed to our original protocol, which we will refer to as the *user-focused* STN protocol. The key rate formula for this protocol is

$$r_{\text{node-focused}} \geq H(K_T) - \delta_{leak}^{EC} - \max_{\Gamma_0} \chi(K_T : E). \tag{4.26}$$

The postselection formalism from Section 4.3.2 and the symmetry arguments from Sections 4.4.1 and 4.4.2 remain largely unaltered by the new key map. Only two steps are affected: proving that the Holevo quantity is invariant under local Pauli-operations, and proving that the Holevo quantity is invariant under the eigenvalue permutations listed in Section 4.4.2. The proofs outlined in Appendix A.4 and Appendix A.6 can be trivially

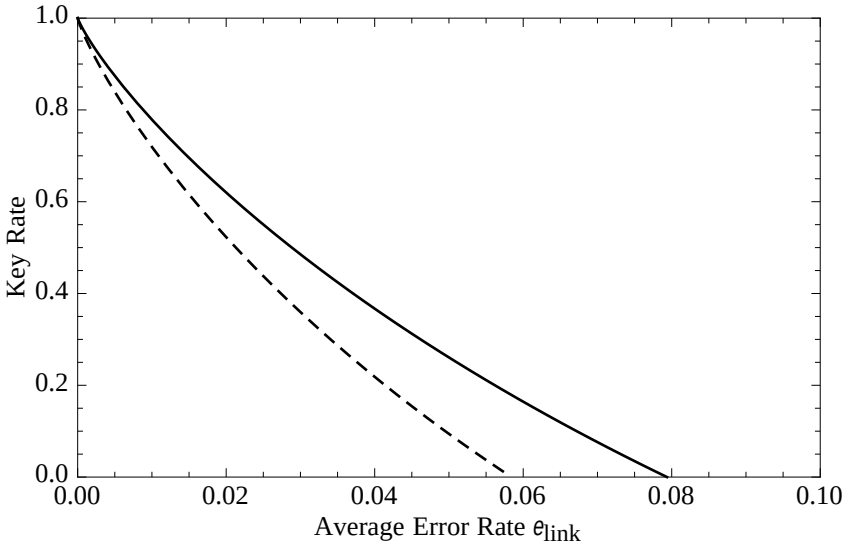

Figure 4.4: The rate at which key bits can be derived from the raw key, in the limit of infinite key length, for a node-focused BB84 STR protocol (solid line), and the user-focused BB84 STR protocol (dashed line), as a function of the error rate in each link, e_{link}. The plot assumes realistic error patterns. Error correction is assumed to be done in the Shannon limit. The difference between the two is strictly due to a difference in the expected value of δ_{leak}^{EC}.

altered to show that these invariance properties hold. The final analytic maximization is then identical to the original proof. The resulting key rate is therefore

$$r_{\text{node-focused}} \geq \sum_{u_1,u_2} p_{u_1} p_{u_2} H(K_T^{u_1,u_2}) - \delta_{leak}^{EC} - h(e). \tag{4.27}$$

While the form of the key rate is identical to that of our original protocol, the amount of information revealed in error correction is expected to be less. This is represented in Fig. 4.4.

4.5 BB84 STR Key Rate: an Alternative Approach

The security proof introduced in the previous section has several limitations. In this section we propose an alternative qubit-level security proof that generalizes to an arbitrary number of nodes. Importantly, this proof does not restrict the basis weighting p_u. To simplify notation, we will first consider the case of a single node, then generalize to multiple nodes in Section 4.5.3.

The proof proceeds as follows. In Section 4.4.1, we demonstrated that when only the basis-dependent error rates are considered, the optimal attack lies in the set $\Gamma^{\text{Bell}}_{e^u}$. Using this insight, the STR protocol is compared to an alternative protocol which is based upon Bell measurements (Section 4.5.1). The alternative protocol has equivalent security, but proves to be easier to work with. Next, in Section 4.5.2, we show that the observed error rates place sufficient restrictions on the joint state. The complexity of the proof is essentially reduced to the typical BB84 security proof.

4.5.1 Utilizing Hypothetical Bell Measurements

To derive an analytical expression for the Holevo quantity in Eq. 4.5, we compare the STR protocol to a hypothetical trusted relay based upon Bell measurements. In the STR protocol, the trusted node measures each link in either the X- or Z-basis. If the intermediate nodes in an STR protocol were instead to perform Bell measurements, this would effectively carry out entanglement swapping, leaving Alice and Bob with entangled states. If the nodes publicly announced the outcome of their measurements, Alice and Bob could establish a secret key without trusting the nodes, or any further involvement from the nodes [28].

A Bell measurement can be deconstructed into a parity measurement and a phase measurement on two qubits. This insight links the entanglement swapping protocol to the STR protocol. The parity component of the Bell measurement is functionally equivalent to the parity announcement in the STR protocol. Unlike the protocol based on entanglement swapping, the phase measurement in the STR protocol is suppressed. Given that the nodes in the STR protocol do not carry out a full Bell measurement, they can obtain the individual measurement outcomes (and do so in practice); therefore, Alice and Bob must trust the node. However, as a proof technique, we can imagine the nodes faithfully performing a phase measurement after performing the parity announcement. In effect, the nodes can be viewed as performing full Bell measurements, even if they only announce the parity bits.

Specifically, let us examine an alternate protocol where the node carries out a measurement in the Bell basis, up to some rotation defined by its basis choices. If we denote the Z-basis with $u_i = 0$ and the X-basis with $u_i = 1$, the rotated Bell basis is given explicitly by

$$\{H^{u_1} \otimes H^{u_2} |\Phi_{a,b}\rangle\}_{a,b=0}^{1} = \begin{cases} \{|\Phi_{0,0}\rangle, |\Phi_{0,1}\rangle, |\Phi_{1,0}\rangle, |\Phi_{1,1}\rangle\} & : u_1 = 0, u_2 = 0 \\ \{|\Phi'_{0,0}\rangle, |\Phi'_{0,1}\rangle, |\Phi'_{1,0}\rangle, |\Phi'_{1,1}\rangle\} & : u_1 = 0, u_2 = 1 \\ \{|\Phi'_{0,0}\rangle, |\Phi'_{1,0}\rangle, |\Phi'_{0,1}\rangle, |\Phi'_{1,1}\rangle\} & : u_1 = 1, u_2 = 0 \\ \{|\Phi_{0,0}\rangle, |\Phi_{1,0}\rangle, |\Phi_{0,1}\rangle, |\Phi_{1,1}\rangle\} & : u_1 = 1, u_2 = 1 \end{cases} \tag{4.28}$$

$$|\Phi'_{a,b}\rangle := (\mathbb{1} \otimes H)|\Phi_{a,b}\rangle \tag{4.29}$$

where H^{u_i} denotes a Hadamard matrix raised to the power u_i and $|\Phi_{a,b}\rangle$ are the four Bell states. When $u_1 = u_2$, the above set is simply a permutation of the Bell states. Similarly, when $u_1 \neq u_2$ the set is a permutation of the Bell states, up to an overall unitary.

If the node announces only the bit value, b, corresponding to the original parity announcement and the node is trusted to faithfully perform a Bell measurement, the security of this alternative protocol can be shown to be equivalent to the original STR protocol. This can be seen by rewriting the conditional state introduced in Eq. 4.3:

$$\psi^{u_1,u_2,b}(\rho_{ATBE}) = \frac{1}{p_{b|u_1,u_2}} \left(\mathbb{1}_A \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes \mathbb{1}_{BE}\right) \rho_{ATBE} \left(\mathbb{1}_A \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes \mathbb{1}_{BE}\right)^{\dagger} \tag{4.30}$$

$$\mathcal{F}_T^{u_1,u_2,b} = \sum_{t=0}^{1} M_{T,t}^{u_1} \otimes M_{T,t\oplus b}^{u_2} = \sum_{a=0}^{1} H^{u_1} \otimes H^{u_2} |\Phi_{a,b}\rangle\langle\Phi_{a,b}| H^{u_1} \otimes H^{u_2}. \tag{4.31}$$

In this case, the node retains an additional bit of information from the measurement. We will refer to this as the *phase bit*, $a \in \{0, 1\}$. If the node were untrusted, the public announcement of the phase bit would be enough for the legitimate parties to verify that the node faithfully performed a Bell measurement. However, if the node *is* trusted to perform a Bell measurement, Bob only needs the parity announcement b to correct his data.

To simplify the security analysis, we may consider announcing the phase bit to Eve (but not to Alice or Bob), effectively putting a lower bound on the key rate of the alternative protocol. Given that the security of alternative protocol is equivalent to the STR protocol, we therefore lowerbound the key rate of the STR protocol. Intuitively, if the phase bit is leaked to Eve, Eve's knowledge of the key cannot decrease. Formally, we can consider the phase information to be stored in another register E' held by Eve. The Holevo quantity can be expressed in terms of the quantum relative entropy. Considering the partial trace over the system E', the monotonicity of the quantum relative entropy [40] ensures that

Eve's knowledge of the key does not decrease. This is expected, as Eve could simply ignore the phase information. This insight, along with Thm. 2, leads to the bound

$$\max_{\Gamma_{e^u}^{\text{Bell}}} \sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_b p_{b|u_1,u_2} \psi^{u_1,u_2,b}(\rho_{ATBE}) \otimes |b\rangle\langle b|_C, \mathbf{M}_A^{u_1} \right) \tag{4.32}$$

$$\leq \max_{\Gamma_{e^u}^{\text{Bell}}} \sum_{u_1,u_2} p_{u_1} p_{u_2} \chi \left(\sum_{a,b} p_{a,b|u_1,u_2} \psi^{u_1,u_2,a,b}(\rho_{ATBE}) \otimes |a,b\rangle\langle a,b|_C, \mathbf{M}_A^{u_1} \right) \tag{4.33}$$

$$= \max_{\Gamma_{e^u}^{\text{Bell}}} \sum_{u_1,u_2,a,b} p_{u_1} p_{u_2} p_{a,b|u_1,u_2} \chi(\psi^{u_1,u_2,a,b}(\rho_{ATBE}), \mathbf{M}_A^{u_1}), \tag{4.34}$$

$$\psi^{u_1,u_2,a,b}(\rho_{ATBE}) := \frac{1}{p_{a,b|u_1,u_2}} \mathbb{I}_A \otimes \mathcal{G}_T^{u_1,u_2,a,b} \otimes \mathbb{I}_{BE} \; \rho_{ATBE} (\mathbb{I}_A \otimes \mathcal{G}_T^{u_1,u_2,a,b} \otimes \mathbb{I}_{BE})^\dagger \tag{4.35}$$

$$\mathcal{G}_T^{u_1,u_2,a,b} := H^{u_1} \otimes H^{u_2} |\Phi_{a,b}\rangle\langle\Phi_{a,b}| H^{u_1} \otimes H^{u_2}. \tag{4.36}$$

Note that this bound makes use of the fact that $\rho_{ATBE} \in \Gamma_{e^u}^{\text{Bell}}$; for states of this form, the mutual information between the phase and parity bits and the key bit (see Thm. 2) is zero.

4.5.2 Maximizing the Holevo Quantity

A conventional method to upper bound Eq. 4.34 is to maximize each term individually. If the set $\Gamma_{e^u}^{\text{Bell}}$ is suitably restrictive, each term can be shown to be a function of the corresponding Z-error rate ($u_1 = 0$) or X-error rate ($u_1 = 1$) arising from the conditioned state $\psi^{u_1,u_2,a,b}(\rho_{ATBE})$. This is done by treating each conditional state as if it had arisen from an independent protocol. Previous security proofs for the point-to-point BB84 protocol have shown that the Z- and X-error rates are enough to detect an eavesdropper (see Ref. [43] for example).

However, it is not immediately apparent that $\Gamma_{e^u}^{\text{Bell}}$ contains suitable restrictions. First, the observed Z- and X-error rates arise from the conditional states $\psi^{u_1,u_2,b}(\rho_{ATBE})$, not $\psi^{u_1,u_2,a,b}(\rho_{ATBE})$. Second, it is not immediately apparent that the Z- and X-error rates can be *simultaneously* determined for each conditioned state. In Eq. 4.37 the Z-error rates arise from the states $\psi^{u_1=0,u_2,b}(\rho_{ATBE})$ and X-error rates arise from the states $\psi^{u_1=1,u_2,b}(\rho_{ATBE})$. It is not clear, for example, how to derive the Z-error rate for the conditioned states $\psi^{u_1=1,u_2,b}(\rho_{ATBE})$. We address the first concern by considering the hypothetical error rates

$e^{u_1,u_2,a,b}$ and later invoking the concavity of the binary entropy to derive a key rate dependent only on the observed error rates e^{u_1,u_2}. The second concern is addressed using a relation among the conditioned states (see Eq. 4.39). In Appendix A.7 we clearly show that the Z- and X-error rates for the BB84 STR protocol are as restrictive as the BB84 protocol.

To address the concerns mentioned above, let us write the set $\Gamma^{\text{Bell}}_{e^u}$ in terms of the hypothetical error rates for each Bell announcement, i.e. $\Gamma^{\text{Bell}}_{e^u}$ is the set of all states ρ_{ATBE} consistent with the error rates $e^{u_1,u_2,a,b}$, such that $\sum_a p_{a,b|u_1,u_2} e^{u_1,u_2,a,b}$ equals the observed error rates e^{u_1,u_2}. The hypothetical error rates $e^{u_1,u_2,a,b}$ are given by

$$e^{u_1,u_2,a,b} = \sum_{x \neq y \oplus b} tr_{ATBE}(M^{u_1}_{A,x} \otimes \mathbb{1}_T \otimes M^{u_2}_{B,y} \otimes \mathbb{1}_E \psi^{u_1,u_2,a,b}(\rho_{ATBE})) \tag{4.37}$$

With these two conditions in mind, we define:

Definition 4. *Let Γ_{hidden} be the set of all states ρ_{ATBE} with the reduced form ρ_{Bell} that are consistent with the error rates $e^{u_1,u_2,a,b}$.*

Definition 5. *Let S_{obs} be the set of all error rates $e^{u_1,u_2,a,b}$ such that $\sum_a p_{a,b|u_1,u_2} e^{u_1,u_2,a,b} = e^{u_1,u_2}$.*

The maximization in Eq. 4.32 can then be treated as two separate maximizations. The equation can therefore be upper bounded by maximizing each term in the summation independently with respect to Γ_{hidden}:

$$\begin{aligned} &\max_{\Gamma^{\text{Bell}}_{e^u}} \sum_{u_1,u_2,a,b} p_{u_1} p_{u_2} p_{a,b|u_1,u_2} \chi(\psi^{u_1,u_2,a,b}(\rho_{ATBE}), M^{u_1}_A) \\ &\quad \leq \max_{S_{\text{obs}}} \sum_{u_1,u_2,a,b} p_{u_1} p_{u_2} p_{a,b|u_1,u_2} \max_{\Gamma_{\text{hidden}}} \chi(\psi^{u_1,u_2,a,b}(\rho_{ATBE}), M^{u_1}_A) \end{aligned} \tag{4.38}$$

For this approach to be useful, we must first show the set Γ_{hidden} contains suitable restrictions on each state $\psi^{u_1,u_2,a,b}(\rho_{ATBE})$. The form of the Bell measurement reveals that certain sets of the conditioned states $\psi^{u_1,u_2,a,b}(\rho_{ATBE})$ are related by trivial relabelings (see Eq. 4.28). Explicitly,

$$\psi^{u_1=i,u_2=j,a=k,b=l}(\rho_{ATBE}) = \psi^{u_1=i\oplus 1,u_2=j\oplus 1,a=l,b=k}(\rho_{ATBE}) \ \forall i,j,k,l. \tag{4.39}$$

The above relations allow us to derive X- and Z-basis error rates for each conditioned state (see Table 4.1).

Restriction	Conditioned States			
	$\rho_{AB}^{u_1=0,u_2=0,a=k,b=l}$	$\rho_{AB}^{u_1=0,u_2=1,a=k,b=l}$	$\rho_{AB}^{u_1=1,u_2=0,a=k,b=l}$	$\rho_{AB}^{u_1=1,u_2=1,a=k,b=l}$
Z-error	$e^{u_1=0,u_2=0,a=k,b=l}$	$e^{u_1=0,u_2=1,a=k,b=l}$	$e^{u_1=0,u_2=1,a=l,b=k}$	$e^{u_1=0,u_2=0,a=l,b=k}$
X-error	$e^{u_1=1,u_2=1,a=l,b=k}$	$e^{u_1=1,u_2=0,a=l,b=k}$	$e^{u_1=1,u_2=0,a=k,b=l}$	$e^{u_1=1,u_2=1,a=k,b=l}$

Table 4.1: Listed here are the hypothetical error rates, $e^{u_1,u_2,a,b}$, that correspond to the Z- and X-error rates restrictions for each conditional state, $\rho_{AB}^{u_1,u_2,a,b} := tr_{TE}\{\psi^{u_1,u_2,a,b}(\rho_{ATBE})\}$. The relations are established using Eq. 4.39.

We can now maximize each term, $\chi(\psi^{u_1,u_2,a,b}(\rho_{ATBE}), \mathbf{M}_A^{u_1})$, as if it had arisen from an independent protocol (after making use of the above relation). Given that we are only interested in an upper bound, we can choose to maximize each term using only the pertinent X- and Z-basis error rates. This maximization can now be handled using techniques outlined in Appendix A of Ref. [43]:

$$\max_{\Gamma_{\text{hidden}}} \chi(\psi^{u_1=i,u_2=j,a=k,b=l}(\rho_{ATBE}), \mathbf{M}_A^{u_1}) \leq h(e^{u_1=i\oplus 1,u_2=j\oplus 1,a=l,b=k}) \quad \forall i,j,k,l.$$

Although the individual error rates, $e^{u_1,u_2,a,b}$, are unknown, we can arrive at a useful key rate by first using the fact that the conditional probability $p_{a,b|u_1,u_2}$ respects similar relations to Eq. 4.39,

$$p_{a=i,b=j|u_1=k,u_2=l} = p_{a=j,b=i|u_1=k\oplus 1,u_2=l\oplus 1}, \ \forall i,j,k,l. \tag{4.40}$$

Then, by using the concavity of the binary entropy, with consideration of Eq. 4.5 and Eq. 4.32, we find the key rate to be

$$\begin{aligned} r &\geq \sum_{u_1,u_2} p_{u_1} p_{u_2} H(K_A^{u_1,u_2}) - \delta_{leak}^{EC} - \max_{S_{\text{obs}}} \sum_{u_1,u_2} p_{u_1\oplus 1} p_{u_2\oplus 1} h(e^{u_1,u_2}) \\ &= \sum_{u_1,u_2} p_{u_1} p_{u_2} \left(H(K_A^{u_1,u_2}) - h(e^{u_1\oplus 1,u_2\oplus 1}) \right) - \delta_{leak}^{EC}. \end{aligned} \tag{4.41}$$

Note that the maximization over S_{obs} is trivial, given each element in S_{obs} results in the same key rate.

4.5.3 Multiple Trusted Nodes

The same analysis may easily be extended to the case where n trusted nodes are used. In this case, the parity announcements made by the nodes may be described as a vector,

$\mathbf{b} := \{b_1, \ldots, b_n\}$. Similarly, the basis choices for the $n+1$ links are described as $\mathbf{u} := \{u_1, \ldots, u_{n+1}\}$. For n-nodes, the legitimate parties share the postselected state

$$\Psi(\rho_{AT_nBE}) := \sum_{\mathbf{u},\mathbf{b}} p_{\mathbf{u}} p_{\mathbf{u}|\mathbf{b}} \psi^{\mathbf{u},\mathbf{b}}(\rho_{AT_nBE}) \otimes |\mathbf{u},\mathbf{b}\rangle\langle\mathbf{u},\mathbf{b}|_C. \tag{4.42}$$

$$\psi^{\mathbf{u},\mathbf{b}}(\rho_{AT_nBE}) := \frac{1}{p_{\mathbf{b}|\mathbf{u}}} (\mathbb{1}_A \otimes \mathcal{F}_{T_n}^{\mathbf{u},\mathbf{b}} \otimes \mathbb{1}_{BE}) \rho_{AT_nBE} (\mathbb{1}_A \otimes \mathcal{F}_{T_n}^{\mathbf{u},\mathbf{b}} \otimes \mathbb{1}_{BE})^\dagger \tag{4.43}$$

$$\mathcal{F}_{T_n}^{\mathbf{u},\mathbf{b}} := \bigotimes_{i=1}^{n} \mathcal{F}_{T_i}^{u_i,u_i+1,b_i} \tag{4.44}$$

where $\mathcal{F}_{T_i}^{u_i,u_i+1,b_i}$ is defined in Eq. 4.4. Above, $p_{\mathbf{u}}$ is the probability of the announcement combination $\mathbf{u}$, and $p_{\mathbf{b}|\mathbf{u}}$ is the probability of parity announcements $\mathbf{b}$ conditioned $\mathbf{u}$.

For multiple nodes, Alice and Bob monitor the error rate for each combination of announcements. We define the set $\Gamma^n_{e^u}$ similarly to Def. 3,

Definition 6. *Let $\Gamma^n_{e^u}$ be the set of all states ρ_{AT_nBE} consistent with the set of basis-dependent error rates $e^{\mathbf{u}}$.*

Similar to the single-node case, we show that the joint state ρ_{AT_nBE} has eigenstates composed of tensored Bell states. Following the same arguments outlined in Section 4.4.1, we examine the set of states where the same local Pauli-operation is applied in each link:

$$\rho_{AT_nB}^{U_{\mathbf{r},\mathbf{s}}} := \left(\bigotimes_{i=1}^{n+1} U_{r_i,s_i} \otimes U_{r_i,s_i} \right) \rho_{AT_nB} \left(\bigotimes_{i=1}^{n+1} U_{r_i,s_i} \otimes U_{r_i,s_i} \right)^\dagger \tag{4.45}$$

for some $\mathbf{r} = \{r_i\}$ and $\mathbf{s} = \{s_i\}$. Through straightforward extensions of Appendix A.3 and Appendix A.4, the basis-dependent error rates and Holevo quantity may be shown to be invariant with respect to these states. Given the concavity of the Holevo quantity, it follows that the extremum for the key rate formula is obtained by a state of the form

$$\rho^n_{\text{Bell}} := \frac{1}{4^{n+1}} \sum_{i=1}^{n+1} \sum_{r_i,s_i} \rho_{AT_nB}^{U_{r,s}}. \tag{4.46}$$

Using techniques from Appendix A.5, all states of this form can be shown to have eigenstates composed of tensor products of Bell states. Importantly, for these states it holds that

$$\chi\left(\sum_{\mathbf{u},\mathbf{b}} p_{\mathbf{u}} p_{\mathbf{u}|\mathbf{b}} \psi^{\mathbf{u},\mathbf{b}}(\rho_{AT_nBE}) \otimes |\mathbf{u},\mathbf{b}\rangle\langle\mathbf{u},\mathbf{b}|_C, \mathbf{M}_A^{u_1} \right) = \sum_{\mathbf{u},\mathbf{b}} p_{\mathbf{u}} p_{\mathbf{u}|\mathbf{b}} \chi(\psi^{\mathbf{u},\mathbf{b}}(\rho_{AT_nBE}), \mathbf{M}_A^{u_1}). \tag{4.47}$$

Again, we simplify the calculation by considering a hypothetical protocol based upon Bell measurements. Each node performs the measurement outlined in Eq. 4.28 and leaks the phase bit to Eve. Analogous to Eq. 4.39, we use the same intuition to derive a relation among the conditional states. Let $\mathbf{a} := \{a_1, \ldots, a_n\}$ be a vector describing the phase bit announcements, and let $\tilde{\mathbf{u}} := \{u_1 \oplus 1, \ldots, u_{n+1} \oplus 1\}$. Furthermore, let $\mathbf{k}$, and $\mathbf{l}$ be arbitrary binary vectors of length n. It holds that

$$\psi^{\mathbf{u},\mathbf{a}=\mathbf{k},\mathbf{b}=\mathbf{l}}(\rho_{AT_nBE}) = \psi^{\tilde{\mathbf{u}},\mathbf{a}=\mathbf{l},\mathbf{b}=\mathbf{k}}(\rho_{AT_nBE}). \tag{4.48}$$

The subsequent steps presented in Section 4.5.2 may now be replicated to find the key rate

$$r \geq \sum_{u_1,\ldots,u_{n+1}} p_{\mathbf{u}} \left(H(K_A^{\mathbf{u}}) - h(e^{\tilde{\mathbf{u}}}) \right) - \delta_{leak}^{EC}. \tag{4.49}$$

4.6 Realistic Considerations

The key rates found in the previous sections are constructed for the ideal case where the legitimate parties exchange qubits over a lossless channel, and Eve performs collective attacks. Most QKD implementations use optical modes to transmit signal states over a lossy channel. This is problematic, as Eve can actively select for pulses that contain additional information. Additionally, Eve is not limited to collective attacks. In this section, we will address these concerns.

4.6.1 From Collective Attacks to General Attacks

First, let us justify our examination of collective attacks in the previous sections. The techniques developed in Ref. [14] provide a method for extending the security of collective attacks to general attacks, provided the protocol is invariant with respect to permutations of the input states. Even when exchanging qubit signal states in a lossless setting, the STR protocol is *not* permutation invariant, due to the fact that basis sifting occurs before the parity announcement.

We may still extend the security of the STR protocol to general attacks by noting that key elements of the STR protocol are permutation invariant. Note that the process of basis sifting commutes with measurements on the signal states. This allows us to view basis sifting as an initial step preceding measurements. In a general attack, Eve may store

all the signal states in a large quantum memory before distributing them to the legitimate parties. Let us denote this state with ρ^N. The prestep of basis sifting maps the state ρ^N to a smaller state ρ^n_{data}:

$$\psi_{\text{sifting}} : \rho^N \to \rho^n_{\text{data}}. \tag{4.50}$$

Importantly, the remainder of the STR protocol acting on ρ^n_{data} (measurements and post-processing) is permutation invariant.[5]

In order to separate the initial sifting step from the remainder of the STR protocol, a common proof technique is to assume Eve performs the sifting step. However, Eve is unable to perform the process of basis sifting as she does not have access to the basis information. We therefore posit a hypothetical protocol that proceeds identically to the STR protocol; however, before the protocol begins, whether signals will be kept or discarded during sifting is announced to Eve for each time slot. Without loss of generality, we may now assume Eve removes any signals that would be lost in basis sifting. More rigorously, for any attack that Eve performs, there exists another attack that 1) does not change Eve's knowledge of the state, 2) does not change the observed error rates, and 3) removes states that will be lost in basis sifting. The steps following sifting are now permutation invariant with respect to the signals grouped by the parity announcements. Without loss of generality, we may now assume that Eve performs collective attacks on these signals, when considering the infinite key limit [14]. This is precisely the situation we have analyzed in previous sections.

Importantly, the key rate for this hypothetical protocol is a lower bound on the BB84 STR protocol. (Similar to the phase bit announcement in Section 4.5, Eve can always choose to ignore the additional sifting information.) Therefore the analysis given in the previous sections provides a lower bound on the key rate of the BB84 STR protocol, when considering general attacks on qubit signal states sent over lossless channels.

We may extend our above analysis to include qubit signals exchanged over lossy channels. In the case of a lossy channel, the legitimate parties discard any data in which a detector did not click. Similar to basis sifting, the removal of these events commutes with the measurement process. We may therefore simply treat vacuum sifting as part of the sifting map ψ_{sifting}. The remainder of the argument follows similarly.

[5] This follows from the fact that the measurements have a tensor product structure. As well, note that there exist permutation invariant methods for carrying out privacy amplification; however, not all methods of privacy amplification are permutation invariant.

4.6.2 STR Protocol with Decoy States

Recall that when considering qubit-level security, our analysis directly applied to a number of protocols with different variations of state creation and measurement (see the discussion beginning Section 4.3). In order to move beyond qubit-level security, we restrict our focus to the BB84 STR protocol as detailed in Section 4.2. While the following analysis still applies to the case where the roles of state preparation and measurement are interchanged, it does not directly apply to entanglement-based or measurement-device independent STR protocols.

Current QKD implementations do not have access to ideal single photon sources. Typically, highly attenuated lasers are used to generate the signal states. These sources are described by coherent states, where the photon number adheres to a Poisson distribution. The probability of sending multi-photon pulses is therefore non-zero. An eavesdropper can exploit multi-photon pulses through a Photon Number Splitting attack [30, 31]. In order to improve the key rate for realistic sources, the legitimate parties may employ *decoy state* analysis [24, 29, 55], supported by tagging [21, 25]. In addition to the original pulses, the legitimate parties send decoy states which have a variable mean photon number, μ_n. By introducing these additional observables, a lower bound may be estimated on the number of single photon pulses in each link. On the detection side, squashing methods can deal with the possibility of multiple photons entering a detector [6, 54, 35]. Given the existence of a squashing map, the detection pattern can be interpreted as if it resulted from a vacuum or single-photon pulse.

Decoy state analysis has been thoroughly explored in the literature. Most techniques assume that the detected signal states are independent and identically distributing (i.i.d.). In general, this assumption is not valid. For this reason, we rely on the analysis found in Ref. [16], which does not assume i.i.d. signal states. The analysis in Ref. [16] uses observables arising from ρ^N (the overall state shared between the legitimate parties, including vacuum and multi-photon signals) to bound the fraction of tagged signals and the single-photon error rate by use of decoy states. While the analysis directly applies for a single node, it may be extended to an STR protocol with an arbitrary number of nodes. Intuitively, it may be helpful to view this information as a promise about the fraction of detected signals that are tagged. The same analysis from Section 4.6.1 may be applied to extend the security analysis from collective attacks to general attacks; the final key rate simply needs to be updated with respect to this promise.

Due to the structure of the parity announcement, if *any* of the legitimate parties emits a multi-photon pulse, Eve may perform a Photon Number Splitting attack. For simplicity, we assume Eve obtains full information of the corresponding raw key bit whenever this

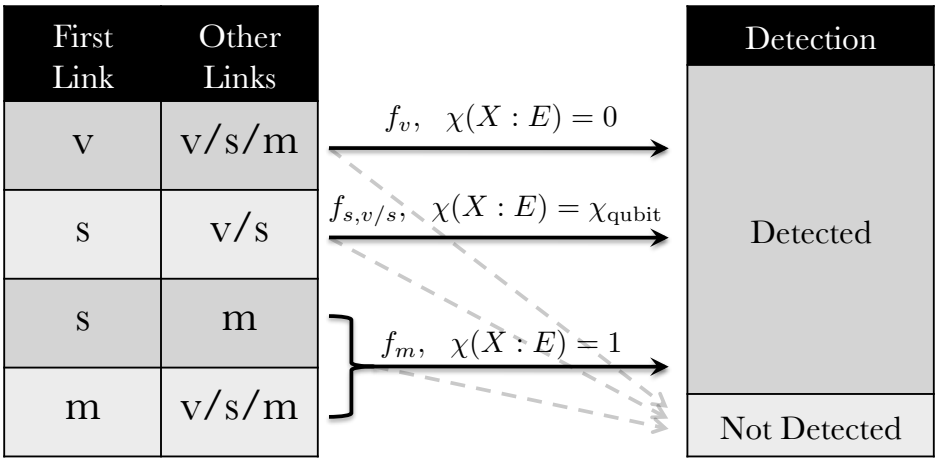

Figure 4.5: When the first link contains a vacuum signal (v), no information about the key bit is revealed. Only when the source in the first link emits a single photon (s), and all other links similarly emit single-photon or vacuum signals, does the qubit security analysis apply. Whenever a multiphoton signal (m) is emitted (and the first link contains a non-vacuum signal) Eve is assumed to obtain full knowledge of the state. Note that all emitted signals that are not detected are discarded during sifting.

happens — except when a vacuum signal is sent in the first link (assuming Alice defines the key map). Additionally, we need to rescale privacy amplification to account for Eve's interaction with the single photon pulses (see Figure 4.5). Let us denote the fraction of detected events used for the raw key in which a single photon was sent in the first link and all other links sent a single photon (vacuum or single photon) pulse to be $f_{s,s}$ ($f_{s,v/s}$). Similarly, f_v is the fraction of events where a vacuum pulse was sent in the first link, and $e^{\mathbf{u},\mathbf{b}}_{s,s/v}$ is the error rate arising from events where a single photon was sent in the first link and all other links sent vacuum or single photon pulses. The fraction of multi-photon events is then given by $f_m = 1 - f_v - f_{s,v/s}$. This is directly subtracted from the key rate. For n nodes, the corresponding decoy state key rate is

$$r \geq \sum_{u_1,\ldots,u_{n+1}} p_{\mathbf{u}} H(K_A^{\mathbf{u}}) - \delta^{EC}_{obs} - f_{s,s/v}\left(\sum_{u_1,\ldots,u_{n+1}} p_{\mathbf{u}} \;\; h(e^{\tilde{\mathbf{u}}}_{s,s/v})\right) - (1 - f_v - f_{s,v/s}) \quad (4.51)$$

for the asymptotic limit. Note that in practice, $f_{s,v}$ will be small. The approximations $f_{s,s/v} \approx f_{s,s}$ and $e_{s,s/v} \approx e_{s,s}$ will safely lower bound the key rate.

In Section 4.4.3, we outlined an alternative node-focused protocol where the trusted node generated the error correcting information. Importantly, our analysis of this protocol was limited to the case of a single node. Let us divide the node into two parties, a pseudo-Bob (T) and a pseudo-Alice (T'). Let us imagine that pseudo-Bob generates the error-correcting information based upon the raw key it holds with Alice. The decoy state key rate is similarly

$$r_{\text{node-focused}} \geq \sum_{u_1,u_2} p_{u_1} p_{u_2} H(K_T^{u_1,u_2}) - \delta_{leak}^{EC} - f_{s,s/v} h(e_{s,s/v}) - (1 - f_v - f_{s,v/s}). \tag{4.52}$$

Recall that the node-focused protocol required that the basis choices be evenly weighted, i.e. $p_{u_1} = p_{u_2} = 1/2$.

4.7 Discussion

In this section, we compare the BB84 STR protocol to a conventional trusted relay, which implements the BB84 protocol in each link. As we show below, the benefits of the BB84 STR protocol come at the cost of a lower key rate.

Let us reexamine the lossless case where the legitimate parties exchange qubit signals. In Section 4.5.3 we determined the key rate for an arbitrary number of nodes to be

$$r \geq \sum_{u_1,\ldots,u_{n+1}} p_{\mathbf{u}} \left(H(K_A^{\mathbf{u}}) - h(e^{\tilde{\mathbf{u}}}) \right) - \delta_{leak}^{EC}. \tag{4.53}$$

For realistic error patterns $\sum_{\mathbf{u}} p_{\mathbf{u}} (H(K_A^{\mathbf{u}}) - h(e^{\tilde{\mathbf{u}}})) \approx H(K_A) - h(e)$, where e is the average error rate between Alice and Bob for the entire raw key. This is reminiscent of the key rate for the point-to-point BB84 protocol.

The qubit security of an STR differs from conventional trusted relays in two major ways. First, the key rate is only a function of the error rate between Alice and Bob. Second, the addition of new nodes in an STR protocol degrades the key rate due to compounding errors. (In a conventional relay, errors are corrected in each link.) The qubit key rates for one and two nodes are plotted in Figure 4.6, along with the key rate for a conventional trusted relay implementing the BB84 protocol. As shown, the simplicity of the STR protocol comes at the cost of a reduced key rate.

In Figure 4.7, we examine the effects of loss on the the STR protocol, when decoy state techniques are used. We plot the key generation rate per clock cycle as a function of channel

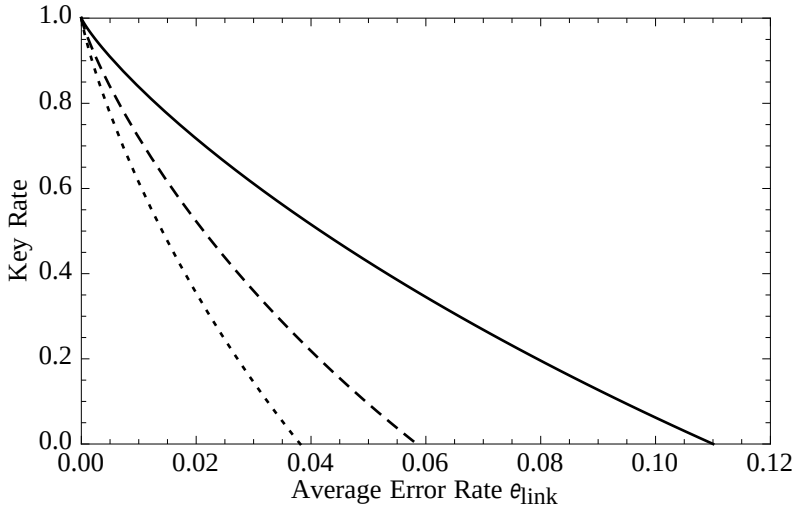

Figure 4.6: The rate at which key bits can be derived from the raw key, in the limit of an infinite key length, for a conventional trusted node (solid line), an STR with one node (dashed line), and an STR with two nodes (dotted line), as a function of the error rate in a single link, e_{link}. The plot assumes realistic error patterns. Error correction is assumed to be done in the Shannon limit.

loss in one arm of the relay, optimizing the mean photon intensity, μ, at each distance. While the key generation rate per clock cycle is lower for an STR, the computational load on each node is also reduced. If the nodes are computationally limited, the key generation rate *per unit time* may in fact be greater for an STR than a conventional trusted relay.

While STRs are not a substitute for conventional trusted relays, they may prove to be a valuable tool in quantum networks. For example, in *hub-and-spoke* quantum networks, in which the majority of traffic is routed through a small number of trusted nodes, the network hubs may function as an STR. This would serve to reduce *bottleneck* effects by shifting the majority of post-processing from the hubs to the end users. Additionally, STRs may be useful for small satellites which are limited in both computational resources and communication bandwidth.

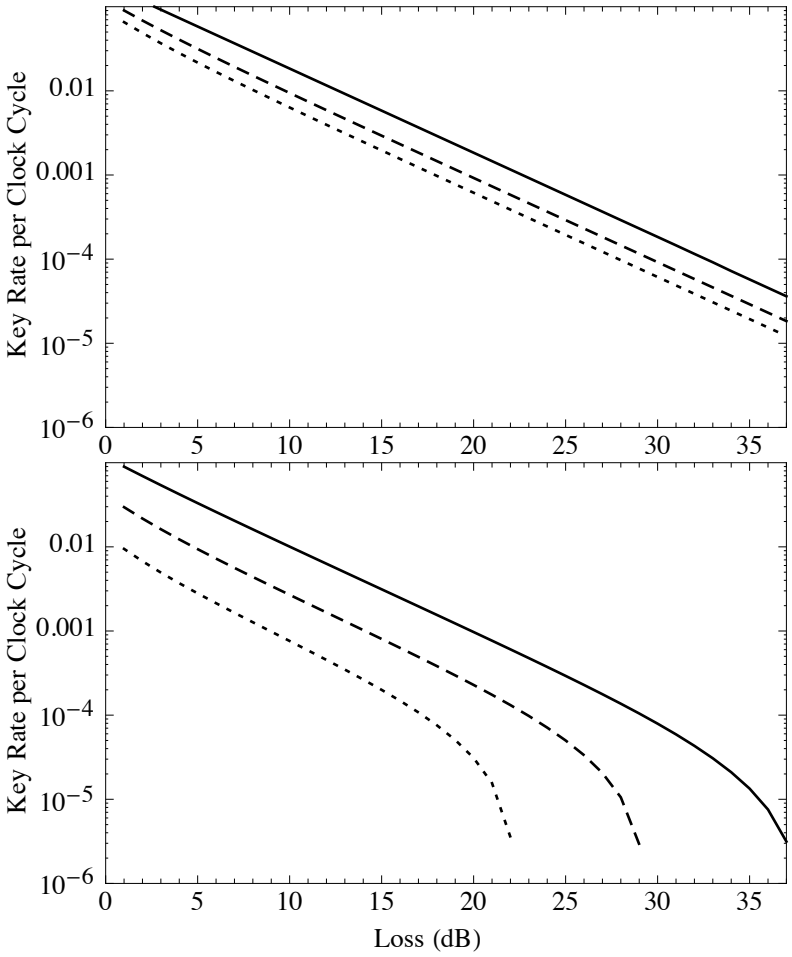

Figure 4.7: The number of secret key bits generated per clock cycle, for a conventional trusted node (solid line), an STR with one node (dashed line), and an STR with two nodes (dotted line), as a function of the loss in a single link. *Above:* The scaling is examined in the error-free limit. *Below:* In each link, we use an intrinsic error rate of 1.85% and a dark count rate of 6×10^{-6} per clock cycle. Furthermore, we assume the information lost during error correction is 1.2 times greater than the Shannon limit. For both cases, we assume a detector efficiency of 50%. For each value of loss, the signal intensity is optimized. Finite size effects are not considered, and Alice and Bob are assumed to perfectly determine f_v and $f_{s,v/s}$.

4.8 Conclusion and Outlook

We have examined the security of an STR which implements the quantum phase of the BB84 protocol. In addition to providing an analytic key rate for an ideal case (lossless and i.i.d. qubit signals), we have provided a clear path for extending the proof to realistic circumstances (loss, general attacks, and weak coherent signal states). Our results show that a trusted relay can function securely without the nodes participating in parameter estimation, error correction or privacy amplification.

In comparison to conventional trusted relays, the STR protocol benefits from its simplicity; however, this comes at the cost of a lower key rate. Compounding errors prevent a naive implementation of the STR protocol from achieving long distances; however, several STRs may be chained together (similar to a conventional trusted relay) to form a pattern of simplified and conventional trusted relay nodes. For many scenarios, the optimal network likely incorporates STRs and conventional trusted relays. In addition, for situations where the intermediate nodes have limited computational power (such as lightweight satellites), STRs may prove to have a higher key generation rate per second, as they reduce the computational load on the intermediate nodes.

This work provides the foundation for several future research directions. While we have demonstrated the basic security of STRs, it is unclear whether more refined classical post-processing can significantly increase the key generation rate. For particular implementations, STRs are likely to benefit from tricks such as noisy preprocessing [39] or two-way communication during error correction [22]. However, as we have demonstrated in Section 4.4.3, there exist additional improvements that are unique to the STR protocol (such as allowing a node limited participation in error correction and privacy amplification). At the moment we do not have a rigorous understanding of the limitations of STR protocols. A thorough analysis may yield additional low-cost measures for increasing the key generation rate in STR protocols — especially in network settings.

Furthermore, it remains an open question whether allowing a node limited participation in error correction truly affects the security of the BB84 STR relay — or whether the difference in key rates (see Section 4.4.3 and Section 4.5.2) is merely an artifact of an overly pessimistic security proof. If the difference is simply due to proof technique, a refined analysis that accounts for any party generating and broadcasting the error correcting information would provide a better understanding of how STRs best fit into network settings.

Finally, it is of practical interest whether STR protocols may be implemented on the first generation of QKD satellites. Technical analysis shows that QKD satellites are near

the limits of current technology [34]. This may cause difficulties given the lowered error tolerance of STRs. A rigorous analysis of an STR implementation (including finite-size effects) is critical if STRs are to be implemented.

APPENDICES

Appendix A

Proofs from Chapter 3 and Chapter 4

A.1 Simplification of the Postselected Holevo Quantity

In this appendix we prove Theorem 2 from Section 3.4.2.

Proof. Given the form of the key map implicit in the notation (see the discussion in Section 3.4.2) the Holevo quantity can be written as

$$\chi\left(\sum_u p_u \rho_{AE}^u \otimes |u\rangle\langle u|, \mathbf{M}_A^u\right) = S\left(\sum_u p_u \rho_E^u \otimes |u\rangle\langle u|\right) - \sum_k p_k S\left(\sum_u p_{u|k} \rho_E^{u,k} \otimes |u\rangle\langle u|\right) \tag{A.1}$$

where $\rho^{u,k}$ denotes the state ρ^u conditioned on the key bit k and $p_{u|k} := p_{u,k}/p_k$ is a conditional probability. Using basic properties of the von Neumann entropy, it follows that

$$\begin{aligned} &\chi\left(\sum_u p_u \rho_{AE}^u \otimes |u\rangle\langle u|, \mathbf{M}_A^u\right) = \\ &\sum_u p_u S\left(\rho_E^u\right) - \sum_u p_u \log p_u - \sum_u p_u \sum_k p_{k|u} S(\rho_E^{u,k}) + \sum_k p_k \sum_u p_{u|k} \log p_{u|k} = \\ &H(\mathbf{p}_u) - \sum_k p_k H(\mathbf{p}_{u|k}) + \sum_u p_u \chi(\rho_{AE}^u, \mathbf{M}_A^u) = \sum_u p_u \chi(\rho_{AE}^u, \mathbf{M}_A^u) + I(\mathbf{p}_{u,k}). \end{aligned} \tag{A.2}$$

□

A.2 Eve's Attack is Bounded by Pure Conditional States

In this appendix we prove Theorem 3 from Section 3.4.2.

Proof. Using the monotonicity of the quantum relative entropy [40], we can write

$$\begin{aligned}
\chi(X:E) &= S(\rho_E) - \sum_k p_k S(\rho_E^k) && \text{(A.3)}\\
&= \sum_k p_k S(\rho_E^k || \rho_E) && \text{(A.4)}\\
&\leq \sum_k p_k S(\rho_{EE'}^k || \rho_{EE'}) && \text{(A.5)}\\
&= S(\rho_{EE'}) - \sum_k p_k S(\rho_{EE'}^k). && \text{(A.6)}
\end{aligned}$$

Given that the states $\rho_{AEE'}$ and $\rho_{AEE'}^k$ are pure, we may use the Schmidt decomposition to show that $S(\rho_{EE'}) = S(\rho_A)$ and $S(\rho_{EE'}^k) = S(\rho_A^k)$. Therefore

$$\chi(X:E) \leq S(\rho_A) - \sum_k p_k S(\rho_A^k). \quad \text{(A.7)}$$

□

Note that equality is reached when the conditional states ρ_{AE}^k are pure.

A.3 Error Rate Invariance Under Local Pauli-operations

The basis-dependent error rates arising from the states $\rho_{ATB}^{U_{r,s}U_{r',s'}}$ can be shown to be the same as the observed error rates. We can consider the observed error rates to arise from the function

$$\begin{aligned}
e^{u_1,u_2} &= f_{\text{err.}}^{u_1,u_2}(\rho_{ATB}) && \text{(A.8)}\\
f_{\text{err.}}^{u_1,u_2}(\sigma_{ATB}) &:= \sum_b \sum_{x \neq y \oplus b} tr_{AB}(M_{A,x}^{u_1} \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes M_{B,y}^{u_2} \sigma_{ATB}) && \text{(A.9)}
\end{aligned}$$

where $\mathcal{F}_T^{u_1,u_2,b}$ is defined in Eq. 4.4.

We will make use of the fact that Pauli matrices only permute the BB84 signal states within each basis. Let us define the action of the Pauli operator $U_{r,s}$ on the signal state $|\phi_x^u\rangle$ to be $U_{r,s}|\phi_x^u\rangle = |\phi^u_{x\oplus h(u,r,s)}\rangle$ for some function $h(u,r,s)$ with binary output. It follows that this relation similarly applies to the BB84 POVM elements. The averaged error rate arising from the state $\rho_{ATB}^{U_{r,s}U_{r',s'}}$ can then be rewritten

$$
\begin{aligned}
f_{\text{err.}}^{u_1,u_2}(\rho_{ATB}^{U_{r,s}U_{r',s'}}) &= \sum_b \sum_{x\neq y\oplus b} tr_{AB}(M_{A,x}^{u_1} \otimes \mathcal{F}_T^{u_1,u_2,b} \otimes M_{B,y}^{u_2} \rho_{ATB}^{U_{r,s}U_{r',s'}}) && \text{(A.10)}\\
&= \sum_b \sum_{x,t} tr_{AB}(M_{A,x}^{u_1} \otimes M_{T,t}^{u_1} \otimes M_{T,t\oplus b}^{u_2} \otimes M_{B,x\oplus b\oplus 1}^{u_2} \rho_{ATB}^{U_{r,s}U_{r',s'}}) && \text{(A.11)}\\
&= \sum_b \sum_{x,t} tr_{AB}(M_{A,x\oplus h(u_1,r,s)}^{u_1} \otimes M_{T,t\oplus h(u_1,r,s)}^{u_1} && \text{(A.12)}\\
&\quad \otimes M_{T,t\oplus b\oplus h(u_2,r',s')}^{u_2} \otimes M_{B,x\oplus b\oplus h(u_2,r',s')\oplus 1}^{u_2} \rho_{ATB}).
\end{aligned}
$$

Let us define $x' := x \oplus h(u_1,r,s), t' := t \oplus h(u_1,r,s)$, and $b' := b \oplus h(u_1,r,s) \oplus h(u_2,r',s')$:

$$
\begin{aligned}
&= \sum_b \sum_{x',t} tr_{AB}(M_{A,x'}^{u_1} \otimes M_{T,t\oplus h(u_1,r,s)}^{u_1} && \text{(A.13)}\\
&\quad \otimes M_{T,t\oplus b\oplus h(u_2,r',s')}^{u_2} \otimes M_{B,x'\oplus h(u_1,r,s)\oplus h(u_2,r',s')\oplus b\oplus 1}^{u_2} \rho_{ATB})\\
&= \sum_b \sum_{x',t'} tr_{AB}(M_{A,x'}^{u_1} \otimes M_{T,t'}^{u_1} \otimes M_{T,t'\oplus b\oplus h(u_1,r,s)\oplus h(u_2,r',s')}^{u_2} && \text{(A.14)}\\
&\quad \otimes M_{B,x'\oplus h(u_1,r,s)\oplus h(u_2,r',s')\oplus b\oplus 1}^{u_2} \rho_{ATB})\\
&= \sum_{b'} \sum_{x',t'} tr_{AB}(M_{A,x'}^{u_1} \otimes M_{T,t'}^{u_1} \otimes M_{T,t'\oplus b'}^{u_2} \otimes M_{B,x'\oplus b'\oplus 1}^{u_2} \rho_{ATB}) && \text{(A.15)}\\
&= e^{u_1,u_2} && \text{(A.16)}
\end{aligned}
$$

Therefore the basis-dependent error rates are invariant when the same Pauli-operation is applied in each link.

A.4 Holevo Invariance Under Local Pauli Operations

In this appendix we demonstrate that the state ρ_{ATBE} is invariant with respect to the postselected Holevo quantity in Eq. 4.12 when local Pauli operations are applied, i.e.

$$\chi\left(\sum_b p_{b|u_1,u_2}\psi^{u_1,u_2,b}(\rho_{ATBE}^{U_{r,s}U_{r',s'}})\otimes|b\rangle\langle b|_C,\mathbf{M}_A^{u_1}\right)= \tag{A.17}$$

$$\chi\left(\sum_b p_{b|u_1,u_2}\psi^{u_1,u_2,b}(\rho_{ATBE})\otimes|b\rangle\langle b|_C,\mathbf{M}_A^{u_1}\right). \tag{A.18}$$

Similar to Appendix A.3, we can make use to the fact that Pauli operators simply permute the BB84 signal states. Again we define $U_{r,s}|\phi_x^u\rangle=|\phi^u_{x\oplus h(u,r,s)}\rangle$, $k':=k\oplus h(u_1,r,s)$, and $b':=b\oplus h(u_1,r,s)\oplus h(u_2,r',s')$ for some function $h(u,r,s)$ with binary output. The invariance of the Holevo quantity stems from the fact that the following operators are equivalent up to a global unitary

$$\begin{aligned}M_{A,k}^{u_1}\otimes\mathcal{F}_T^{u_1,u_2,b}\otimes\mathbb{1}_B\rho_{ATB}^{U_{r,s}U_{r',s'}}(M_{A,k}^{u_1}\otimes\mathcal{F}_T^{u_1,u_2,b}\otimes\mathbb{1}_B)^\dagger\overset{U}{=}\\ M_{A,k'}^{u_1}\otimes\mathcal{F}_T^{u_1,u_2,b'}\otimes\mathbb{1}_B\rho_{ATB}(M_{A,k'}^{u_1}\otimes\mathcal{F}_T^{u_1,u_2,b'}\otimes\mathbb{1}_B)^\dagger.\end{aligned} \tag{A.19}$$

Note that $\overset{U}{=}$ represents equality up to a global unitary.

In order to show that the Holevo quantity is invariant, we need examine the probability of obtaining a key bit (p_k) and Eve's conditional states (ρ_E^k). Given that the trace is invariant under a global unitary, the probability distribution p_k is simply permuted:

$$p_k^{U_{r,s}U_{r',s'}}:=tr_{ATBE}\{M_{A,k}^{u_1}\otimes\mathbb{1}_{TBE}\rho_{ATBE}^{U_{r,s}U_{r',s'}}\}=p_{k'}. \tag{A.20}$$

It follows similarly that the action of the local Pauli operations simply permutes Eve's conditional state up to a relabelling of the classical register,

$$\rho_E^{k,U_{r,s}U_{r',s'}}:=\frac{1}{p_k^{U_{r,s}U_{r',s'}}}\sum_b tr_{ATB}\{M_{A,k}^{u_1}\otimes\mathcal{F}_T^{u_1,u_2,b}\otimes\mathbb{1}_{BE}\rho_{ATBE}^{U_{r,s}U_{r',s'}}\}\otimes|b\rangle\langle b|_C \tag{A.21}$$

$$=\frac{1}{p_{k'}}\sum_b tr_{ATB}\{M_{A,k'}^{u_1}\otimes\mathcal{F}_T^{u_1,u_2,b'}\otimes\mathbb{1}_{BE}\rho_{ATBE}\}\otimes|b\rangle\langle b|_C \tag{A.22}$$

$$=\rho_E^{k'}. \tag{A.23}$$

Therefore

$$\chi\left(\sum_b p_{b|u_1,u_2}\psi^{u_1,u_2,b}(\rho_{ATBE}^{U_{r,s}U_{r',s'}})\otimes|b\rangle\langle b|_C,\mathbf{M}_A^{u_1}\right)= \tag{A.24}$$

$$S\left(\sum_k p_k^{U_{r,s}U_{r',s'}}\rho_E^{k,U_{r,s}U_{r',s'}}\right)-\sum_k p_k^{U_{r,s}U_{r',s'}}S(\rho_E^{k,U_{r,s}U_{r',s'}})= \tag{A.25}$$

$$S\left(\sum_{k'} p'_k\rho_E^{k'}\right)-\sum_{k'} p_{k'}S(\rho_E^{k'})= \tag{A.26}$$

$$\chi\left(\sum_b p_{b|u_1,u_2}\psi^{u_1,u_2,b}(\rho_{ATBE})\otimes|b\rangle\langle b|_C,\mathbf{M}_A^{u_1}\right). \tag{A.27}$$

A.5 Calculation of Symmetric State for BB84 STN Protocol

The form of ρ_{Bell} is calculated using an extension of the work presented in Ref. [19]. We can express the averaged state in Eqn. 4.15 in terms of the Pauli matrices:

$$\frac{1}{16}\sum_{r,s,r',s'}\rho_{ATB}^{U_{r,s}U_{r',s'}}=\frac{1}{16}\sum_{r,s,r',s'}U_{r,s}\otimes U_{r,s}\otimes U_{r',s'}\otimes U_{r',s'}\rho_{ATB}(U_{r,s}\otimes U_{r,s}\otimes U_{r',s'}\otimes U_{r',s'})^\dagger. \tag{A.28}$$

Any state ρ_{ATB} can be expressed in the tensored Bell basis $\mathcal{B}=\{|U_{r,s}\rangle\otimes|U_{r',s'}\rangle : r,s,r',s'=0,1\}$. Note that the action of the Pauli matrices on a basis element is

$$\begin{aligned}&U_{r,s}\otimes U_{r,s}\otimes U_{r',s'}\otimes U_{r',s'}|U_{m,n}\rangle\otimes|U_{p,q}\rangle \\ &\quad=(-1)^{-sm+rn-s'p+r'q}|U_{m,n}\rangle\otimes|U_{p,q}\rangle.\end{aligned} \tag{A.29}$$

By averaging over the Pauli matrices, we find

$$\begin{aligned}&\sum_{r,s,r',s'}U_{r,s}\otimes U_{r,s}\otimes U_{r',s'}\otimes U_{r',s'}|U_{m,n}\rangle\langle U_{m',n'}|\otimes|U_{p,q}\rangle\langle U_{p',q'}|(U_{r,s}^*\otimes U_{r,s}\otimes U_{r',s'}\otimes U_{r',s'}^*)^\dagger \\ &=\sum_{r,s,r',s'}(-1)^{-s(m+m')+r(n+n')-s'(p+p')+r'(q+q')}|U_{m,n}\rangle\langle U_{m',n'}|\otimes|U_{p,q}\rangle\langle U_{p',q'}|.\end{aligned} \tag{A.30}$$

The off diagonal elements can be shown to vanish by observing that the coefficient in Eqn. A.30 is equivalent to $16\delta_{m,m'}\delta_{n,n'}\delta_{p,p'}\delta_{q,q'}$. Therefore the averaged state can be expressed simply as

$$\frac{1}{16}\sum_{r,s,r',s'}\rho_{ATB}^{U_{r,s}U_{r',s'}} = \sum_{m,n,p,q}\alpha_{m,n,p,q}|U_{m,n}\rangle\langle U_{m,n}|\otimes|U_{p,q}\rangle\langle U_{p,q}|. \tag{A.31}$$

A.6 Holevo Invariance Under Eigenvalue Permutations

In this appendix we demonstrate that the state ρ_{Bell} is invariant with respect to the Holevo quantity under four permutations of the eigenvalues of ρ_{Bell}. With regards to the eigenvalue matrix λ, these permutations are: exchanging the second and third columns, exchanging the second and third rows, reflecting the matrix about the upward diagonal, and reflecting the matrix about the downward diagonal. Each permutation can be described by a unitary transformation acting on ρ_{Bell}. We denote the permutations respectively as U_{col}, U_{row}, U_{errors}, and U_{links}.

For clarity, let us denote the system T with two qubit spaces T_1 and T_2. Consider the action of the postselection operator $\mathbb{1}_A\otimes\mathcal{F}_T^{u_1,u_2,b}\otimes\mathbb{1}_B$ on the eigenstates of ρ_{Bell}. It can be shown that

$$\mathbb{1}_A\otimes\mathcal{F}_T^{u_1,u_2,b}\otimes\mathbb{1}_B|\Phi_{i,j}\rangle_{AT_1}|\Phi_{i',j'}\rangle_{T_2B} = \begin{cases} \sum_a|\Phi_{a\oplus i\oplus i',b\oplus j\oplus j'}\rangle_{AB}|\Phi_{a,b}\rangle_{T_1T_2} & : \ u_1=0,\ u_2=0 \\ \sum_a(\mathbb{1}_A\otimes H\otimes\mathbb{1}_{T_1}\otimes H)|\Phi_{a\oplus i\oplus j',b\oplus j\oplus i'}\rangle_{AB}|\Phi_{a,b}\rangle_{T_1T_2} & : \ u_1=0,\ u_2=1 \\ \sum_a(H\otimes\mathbb{1}_B\otimes H\otimes\mathbb{1}_{T_2})|\Phi_{a\oplus j\oplus i',b\oplus i\oplus j'}\rangle_{AB}|\Phi_{a,b}\rangle_{T_1T_2} & : \ u_1=1,\ u_2=0 \\ \sum_a(H\otimes H\otimes H\otimes H)|\Phi_{a\oplus j\oplus j',b\oplus i\oplus i'}\rangle_{AB}|\Phi_{a,b}\rangle_{T_1T_2} & : \ u_1=1,\ u_2=1 \end{cases} \tag{A.32}$$

Futhermore, we can show the action of the permutations on the Bell-states:

$$U_{\text{col}}|\Phi_{i,j}\rangle_{AT_1}|\Phi_{i',j'}\rangle_{T_2B} = |\Phi_{j,i}\rangle_{AT_1}|\Phi_{i',j'}\rangle_{T_2B} \tag{A.33}$$

$$U_{\text{row}}|\Phi_{i,j}\rangle_{AT_1}|\Phi_{i',j'}\rangle_{T_2B} = |\Phi_{i,j}\rangle_{AT_1}|\Phi_{j',i'}\rangle_{T_2B} \tag{A.34}$$

$$U_{\text{errors}}|\Phi_{i,j}\rangle_{AT_1}|\Phi_{i',j'}\rangle_{T_2B} = |\Phi_{i'\oplus1,j'\oplus1}\rangle_{AT_1}|\Phi_{i\oplus1,j\oplus1}\rangle_{T_2B} \tag{A.35}$$

$$U_{\text{links}}|\Phi_{i,j}\rangle_{AT_1}|\Phi_{i',j'}\rangle_{T_2B} = |\Phi_{i',j'}\rangle_{AT_1}|\Phi_{i,j}\rangle_{T_2B}. \tag{A.36}$$

Note that for all elements in Γ_{Bell} it holds that

$$\chi(\Psi(\rho_{\text{Bell}}), \mathbf{M}_A^{u_1}) = \sum_{u_1,u_2,b} p_{u_1} p_{u_2} p_{b|u_1,u_2} \chi(\psi^{u_1,u_2,b}(\rho_{\text{Bell}}), \mathbf{M}_A^{u_1}). \tag{A.37}$$

Furthermore, the symmetric form of ρ_{Bell} ensures that $p_{k|u_1,u_2,b} = p_{b|u_1,u_2} = 1/2$. Given that the Hadamard matrix permutes the basis of Alice's POVM elements ($HM_{A,x}^{u_1=i}H = M_{A,x}^{u_1=i\oplus 1}$) the above relations can be used to show that for all i, j, k:

$$\chi(\psi^{u_1=i,u_2=j,b=k}(U_{\text{col}}\rho_{\text{Bell}}U_{\text{col}}^\dagger), \mathbf{M}_A^{u_1=i}) = \chi(\psi^{u_1=i\oplus 1,u_2=j,b=k}(\rho_{\text{Bell}}), \mathbf{M}_A^{u_1=i\oplus 1}) \tag{A.38}$$

$$\chi(\psi^{u_1=i,u_2=j,b=k}(U_{\text{row}}\rho_{\text{Bell}}U_{\text{row}}^\dagger), \mathbf{M}_A^{u_1=i}) = \chi(\psi^{u_1=i,u_2=j\oplus 1,b=k}(\rho_{\text{Bell}}), \mathbf{M}_A^{u_1=i}) \tag{A.39}$$

$$\chi(\psi^{u_1=i,u_2=j,b=k}(U_{\text{errors}}\rho_{\text{Bell}}U_{\text{errors}}^\dagger), \mathbf{M}_A^{u_1=i}) = \chi(\psi^{u_1=j,u_2=i,b=k}(\rho_{\text{Bell}}), \mathbf{M}_A^{u_1=j}) \tag{A.40}$$

$$\chi(\psi^{u_1=i,u_2=j,b=k}(U_{\text{links}}\rho_{\text{Bell}}U_{\text{links}}^\dagger), \mathbf{M}_A^{u_1=i}) = \chi(\psi^{u_1=j,u_2=i,b=k}(\rho_{\text{Bell}}), \mathbf{M}_A^{u_1=j}). \tag{A.41}$$

In consideration of the above, the Holevo invariance follows directly, so long as $p_{u_1} = p_{u_2} = 1/2$.

A.7 Z- and X-errors in the BB84 STR Protocol

In deriving an alternative security proof of the BB84 STR Protocol (Section 4.5) we first compare the protocol to a hypothetical Bell measurement-based protocol. Furthermore, we reduce the complexity of security proof for the BB84 STR protocol to the point-to-point BB84 protocol. Implicit in this proof is the notion that the Z- and X-error rates in the STR protocol place the same restrictions on the joint state, as they do in the BB84 protocol. In this Appendix, we justify this assumption.

For the Bell measurement-based protocol, the hypothetical error rates conditioned on all four announcements can be viewed as a function of Alice and Bob's conditioned states,

$$e^{u_1,u_2,a,b} = f_{\text{err.}}^{u_1,u_2,b}(tr_{TE}\{\psi^{u_1,u_2,a,b}(\rho_{ATBE})\}) \tag{A.42}$$

$$f_{\text{err.}}^{u_1,u_2,b}(\rho_{AB}) := \sum_{x\neq y\oplus b} tr_{AB}(M_{A,x}^{u_1} \otimes M_{B,y}^{u_2}\rho_{AB}) \tag{A.43}$$

In the point-to-point BB84 protocol, the Z- and X-error rates for the state ρ_{AB} are given by a different function

$$e^u = f_{\text{err.}}^u(\rho_{AB}) \tag{A.44}$$

$$f_{\text{err.}}^u(\rho_{AB}) := \sum_{x\neq y} tr_{AB}(M_{A,x}^u \otimes M_{B,y}^u\rho_{AB}). \tag{A.45}$$

From conventional point-to-point BB84 security proofs, we know that by specifying the value of $f_{\text{err.}}^{u=Z}(\rho_{AB})$ and $f_{\text{err.}}^{u=X}(\rho_{AB})$ (i.e. measuring the Z- and X-error rates) the function $\chi(\rho_{ABE}, \mathbf{M}_A^u)$ can be upper bounded. In order to make use of this fact, we need to clearly show that specifying the value of $f_{\text{err.}}^{u_1,u_2,b}(\rho_{AB})$ places the same restrictions on ρ_{AB} as does specifying the value of $f_{\text{err.}}^{u}(\rho_{AB})$. Note the functions differ by the parity announcement b and the addition of a second basis, u_2.

First, we can make use of the fact that $\chi(\rho_{ABE}, \mathbf{M}_A^u)$ is invariant if Bob applies a local unitary transformation. This follows directly from the unitary invariance of the von Neumann entropy. This allows us to write $\chi(\rho_{ABE}, \mathbf{M}_A^u) = \chi(\rho'_{ABE}, \mathbf{M}_A^u)$, where $\rho'_{ABE} := (\mathbb{1}_A \otimes H^{u_1 \oplus u_2} \otimes \mathbb{1}_E)\rho_{ABE}(\mathbb{1}_A \otimes H^{u_1 \oplus u_2} \otimes \mathbb{1}_E)^\dagger$. The restriction may now be rewritten $f_{\text{err.}}^{u_1,u_2,b}(\rho_{AB}) = \sum_{x \neq y \oplus b} tr_{AB}(M_{A,x}^{u_1} \otimes M_{B,y}^{u_1} \rho'_{AB})$. Formally, the error rates can be viewed as restrictions on ρ'_{AB}, and we instead optimize $\chi(\rho'_{ABE}, \mathbf{M}_A^u)$.

In addition, we can make use of the fact that the POVM elements satisfy the relation $\sum_x M_x^u = \mathbb{1}$. Using this it easily follows that

$$f_{\text{err.}}^{u_1,u_2,b}(\rho_{AB}) = \begin{cases} f_{\text{err.}}^{u_1}(\rho'_{AB}) & : \quad b = 0 \\ 1 - f_{\text{err.}}^{u_1}(\rho'_{AB}) & : \quad b = 1. \end{cases} \tag{A.46}$$

By specifying $f_{\text{err.}}^{u_1,u_2,b}(\rho_{AB})$, we can uniquely specify $f_{\text{err.}}^{u_1}(\rho'_{AB})$. Therefore the Z- and X-error rates in the BB84 STR protocol are as restrictive as the point-to-point BB84 protocol. Note that $u_1 = 0$ defines the Z-error and $u_1 = 1$ defines the X-error. In the main text, we show that it is possible to derive Z- and X-error rates for each conditioned state $\psi^{u_1,u_2,b}(\rho_{ATBE})$.

References

[1] Silvestre Abruzzo, Sylvia Bratzik, Nadja K Bernardes, Hermann Kampermann, Peter van Loock, and Dagmar Bruß. Quantum repeaters and quantum key distribution: Analysis of secret-key rates. *Physical Review A*, 87(5):052315, 2013.

[2] Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[3] Y. Aumann, Yan Zong Ding, and M.O. Rabin. Everlasting security in the bounded storage model. *Information Theory, IEEE Transactions on*, 48(6):1668–1680, Jun 2002.

[4] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, 2005.

[5] Travis R Beals and Barry C Sanders. Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network. In *Information Theoretic Security*, pages 29–39. Springer, 2008.

[6] Normand J Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Physical Review Letters*, 101(9):093601, 2008.

[7] H Bechmann-Pasquinucci and Nicolas Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238, 1999.

[8] Charles H Bennett, Gilles Brassard, et al. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[9] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557, 1992.

[10] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[11] H-J Briegel, W Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[12] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018–3021, 1998.

[13] Carlton M Caves, Christopher A Fuchs, and Rüdiger Schack. Unknown quantum states: the quantum de Finetti representation. *Journal of Mathematical Physics*, 43(9):4537–4559, 2002.

[14] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102:020504, Jan 2009.

[15] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[16] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications*, 5, 2014.

[17] Chip Elliott. Building the quantum network. *New Journal of Physics*, 4(1):46, 2002.

[18] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. Current status of the DARPA quantum network. In *Defense and Security*, pages 138–149. International Society for Optics and Photonics, 2005.

[19] Agnes Ferenczi and Norbert Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Physical Review A*, 85(5):052310, 2012.

[20] Chi-Hang Fred Fung, Xiongfeng Ma, HF Chau, and Qing-yu Cai. Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol. *Physical Review A*, 85(3):032308, 2012.

[21] D. Gottesman, Hoi-Kwong Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, pages 136–, 2004.

[22] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *Information Theory, IEEE Transactions on*, 49(2):457–475, 2003.

[23] Richard J Hughes, Jane E Nordholt, Kevin P McCabe, Raymond T Newell, Charles G Peterson, and Rolando D Somma. Network-centric quantum communications with application to critical infrastructure protection. *arXiv preprint arXiv:1305.0305*, 2013.

[24] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[25] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal D*, 41(3):599–627, 2007.

[26] Barbara Kraus, Nicolas Gisin, and Renato Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical Review Letters*, 95(8):080501, 2005.

[27] Antía Lamas-Linares and Christian Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Optics express*, 15(15):9388–9393, 2007.

[28] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503, 2012.

[29] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94:230504, Jun 2005.

[30] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000.

[31] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44, 2002.

[32] Norbert Lütkenhaus and Xiongfeng Ma. System and method for quantum key distribution, WO 2013037062 A1, 2013.

[33] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[34] Evan Meyer-Scott, Zhizhong Yan, Allison MacDonald, Jean-Philippe Bourgoin, Hannes Hübel, and Thomas Jennewein. How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss. *Physical Review A*, 84(6):062326, 2011.

[35] Tobias Moroder, Otfried Gühne, Normand Beaudry, Marco Piani, and Norbert Lütkenhaus. Entanglement verification with realistic measurement devices via squashing operations. *Physical Review A*, 81(5):052342, 2010.

[36] Jörn Müller-Quade and Renato Renner. Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006, 2009.

[37] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, JF Dynes, et al. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11(7):075001, 2009.

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

[39] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1):012332, 2005.

[40] Mary Beth Ruskai. Inequalities for quantum entropy: A review with conditions for equality. 43(9), 2002.

[41] Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18(1):61–87, 2010.

[42] M Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express*, 19(11):10387–10409, 2011.

[43] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[44] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20):200501, 2008.

[45] Claude Elwood Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27(379–423):623–655, 1948.

[46] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509, 1997.

[47] Peter W Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[48] William S Stacey, Razieh Annabestani, Xiongeng Ma, and Norbert Lütkenhaus. The security of quantum key distribution using a simple trusted relay, in prep.

[49] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. The case for quantum key distribution. In *Quantum Communication and Quantum Networking*, pages 283–296. Springer, 2010.

[50] Damien Stucki, Matthieu Legré, Laurent Monat, Samuel Robyr, Patrick Trinkler, Grégoire Ribordy, Rob Thew, Nino Walenta, Nicolas Gisin, François Buntschu, et al. Performance of the SwissQuantum network over 21 months. In *SPIE Security+ Defence*, pages 81891D–81891D. International Society for Optics and Photonics, 2011.

[51] M. Takeoka, S. Guha, and M. Wilde. The squashed entanglement of a quantum channel. *Information Theory, IEEE Transactions on*, PP(99):1–1, 2014.

[52] Marco Tomamichel, Jesus Martinez-Mateo, Christoph Pacher, and David Elkouss. Fundamental finite key limits for information reconciliation in quantum key distribution. *arXiv preprint arXiv:1401.5194*, 2014.

[53] Morio Toyoshima, Takashi Sasaki, Hideki Takenaka, Yozo Shoji, Yoshihisa Takayama, Yoshisada Koyama, Hiroo Kunimori, Maki Akioka, Mikio Fujiwara, and Masahide Sasaki. Research and development of free-space laser communications and quantum key distribution technologies at NICT. In *Space Optical Systems and Applications (ICSOS), 2011 International Conference on*, pages 1–7. IEEE, 2011.

[54] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Physical Review A*, 78(3):032302, 2008.

[55] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94(23):230503, 2005.

[56] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[57] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[58] Juan Yin, Yuan Cao, Shu-Bin Liu, Ge-Sheng Pan, Jin-Hong Wang, Tao Yang, Zhong-Ping Zhang, Fu-Min Yang, Yu-Ao Chen, Cheng-Zhi Peng, et al. Experimental quasi-single-photon transmission from satellite to earth. *Optics express*, 21(17):20032–20040, 2013.