SEMI-QUANTUM KEY DISTRIBUTION: PROTOCOLS, SECURITY ANALYSIS, AND NEW MODELS

by

Walter O. Krawec

A DISSERTATION

Submitted to the Faculty of the Stevens Institute of Technology
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Walter O. Krawec, Candidate

ADVISORY COMMITTEE

Antonio Nicolosi, Chairman Date

Rainer Martini Date

David Naumann Date

Susanne Wetzel Date

STEVENS INSTITUTE OF TECHNOLOGY
Castle Point on Hudson
Hoboken, NJ 07030
2015

SEMI-QUANTUM KEY DISTRIBUTION: PROTOCOLS, SECURITY ANALYSIS, AND NEW MODELS

ABSTRACT

Quantum key distribution (QKD) allows two parties to agree on a secret key, secure against even an all-powerful adversary. In 2007, Boyer et al. [Phys. Rev. Lett. 99] proposed the notion of semi-quantum key distribution (SQKD), which involves the construction and analysis of quantum cryptographic protocols that operate when one of the two users is limited to performing certain "classical" or "semi-quantum" operations. This dissertation advances the state of the art in this field with new protocols, novel analytic tools to assess the security of semi-quantum protocols, and a new communication model.

Specifically, this dissertation develops a series of security results for "single-state" SQKD protocols, i.e., protocols where one of the two parties ("Bob") is classical, whereas the other ("Alice") is restricted to sending a single, publicly known state in each iteration of the protocol. As an important corollary, attacks of the most general form, captured mathematically via two unitary operators, are shown equivalent to restricted attacks specified via a bias parameter b in [-1/2, 1/2] and a single unitary operator. This restricted form in turn enables a complete security analysis of single-state protocols, whereas the only known security results in this setting so far were limited to the more rudimentary notion of "robustness."

A second contribution of this dissertation is the design of a new single-state SQKD protocol. This is the first SQKD protocol where "Hadamard-basis" states contribute to the protocol's key rate (all prior protocols used such states only to probe the security of the channel). The unconditional security of this new protocol is established

leveraging the techniques discussed earlier, and the resulting key rate is compared to that of other (uni-directional) QKD protocols in the literature.

As a final contribution, this dissertation introduces a new type of SQKD protocols, termed "mediated" SQKD protocols. In this setting, both Alice and Bob are limited, classical users who aim at establishing an unconditionally secure secret key with the help of a quantum server. Somewhat surprisingly, mediated SQKD protocols with unconditional security are proven to exist even if the quantum server misbehaves adversarially.

Author: Walter O. Krawec

Advisor: Antonio Nicolosi

Date: April 15, 2015

Department: Computer Science

Degree: Doctor of Philosophy

Dedication

To my family.

Acknowledgments

I would first like to thank my advisor Antonio Nicolosi for all of his guidance and support during my time at Stevens and for encouraging me to pursue this dissertation. He pushed me to stretch myself, and if it weren't for him, I would not have even attempted this work, let alone finish it. I would also like to thank the other members of my dissertation committee, Rainer Martini, David Naumann, and Susanne Wetzel for all of their support, encouragement, and advice.

Of course, I am grateful towards my fellow Ph.D. students at Stevens; in particular my office-mates for our conversations.

Finally, and most importantly, I must thank my family for their never ending support and encouragement, without which this dissertation would not exist.

Thank you all!

Table of Contents

Abstract **iii**

Dedication **v**

Acknowledgements **vi**

List of Figures **ix**

1 Introduction and Overview **1**

2 Preliminaries **7**

2.1 Basic Concepts and Notation 7

2.2 Mixed States 10

2.3 Partial Trace, Entropy, and the Trace Norm 13

2.4 Quantum Key Distribution 14

2.5 Key Rate in the Asymptotic Scenario 17

2.6 Semi-Quantum Cryptography 19

3 Related Work **23**

3.1 Semi-Quantum Cryptography 23

3.2 Mediated Quantum Key Distribution 24

4 Security of Single State Semi-Quantum Protocols **26**

4.1 Definitions and Notation 26

4.2 Core Results 28

4.3 Further Results 38

4.3.1 Robustness of the SQKD Protocol of Zou et al. 38
4.3.2 Regarding Raw Key Bias 42
4.3.3 Key-Rate Comparison with Three-State BB84 44

5 Security Analysis of a New Single State Protocol 55
5.1 The Protocol 55
5.2 Proof of Robustness 57
5.3 Key Bias Attack 60
5.4 Key Rate in the Asymptotic Scenario 63
5.5 Effects of Bias on the Key Rate 68

6 Mediated Semi-Quantum Key Distribution 79
6.1 The Protocol 80
6.2 Collective Attacks 82
6.2.1 An Unentangled Initial State 84
6.2.2 A Unitary Attack Operator 85
6.2.3 Bounding the Key Rate 87
6.2.4 Bounding $I(A:C)$ 89
6.2.5 First Bound: An Honest Center 94
6.2.6 Second Bound: An Adversarial Center 98
6.2.7 General Attacks and Third-Party Eavesdroppers 105

7 Closing Remarks and Future Work 106

Bibliography 109

Vita 117

List of Figures

2.1 Diagram of BB84 [1]. 17

4.1 A graph of the function $b = \sqrt{\lambda(1-\lambda)}$. 44

5.1 Raw key distribution with bias. 62

6.1 A diagram of the situation considered in the mediated setting. 80

6.2 Key rate with an honest or semi-honest server. 99

6.3 Various statistics of the depolarization example with semi-honest server. 99

6.4 Key rate of our mediated protocol in the worst-case scenario. 104

6.5 Improved key rate when the server is adversarial. 104

Chapter 1

Introduction and Overview

Quantum Key Distribution (QKD) protocols allow two parties, referred to as Alice and Bob (which we denote throughout as A and B respectively) to establish, through the use of a quantum communication channel, a shared secret key, secure against even an all powerful adversary, Eve (denoted E). Security in this setting is based not upon computational assumptions, as is the case, for example, with classical public key cryptology, but instead it is based on physical assumptions, Eve being bounded in power only by the laws of physics. The first protocol to achieve this end was BB84 [1] - so named after the protocol's creators: Bennett and Brassard in 1984. Since then several other protocols, for instance B92 [2], three-state BB84 [3], and SARG04 [4] (though there are many more), of varying advantages and disadvantages, have been developed and their security analyzed. The reader is referred to [5, 6] for a general survey.

QKD protocols are in existence today, both experimentally, and commercially. There are currently four different companies which provide commercial QKD systems. They are MagiQ Technologies[1] based in New York, id Quantique[2] based in Geneva, SeQureNet[3] in Paris, and QuintessenceLabs[4] in Australia. These companies produce commercial hardware users can purchase allowing them to operate quantum key distribution protocols.

Besides these commercial companies, quantum key distribution has also been used in various applications. For instance, it was used in the 2007 national elections in

[1] http://www.magiqtech.com
[2] http://www.idquantique.com
[3] http://www.sequrenet.com
[4] http://www.quintessencelabs.com

Geneva to transmit ballot results to the capital [7]. In 2004, quantum key distribution was used for the first time to carry out a bank transfer in Vienna [8].

Beyond commercial implementations, there are also several research and government run implementations of QKD systems. This includes the DARPA Quantum Network [9] which consists of a 10-node QKD network running in Massachusetts since 2004. Los Alamos National Laboratory, since 2011, also runs a QKD network using a "hub and spoke" system consisting of a trusted authority in the middle with several clients connecting to it running a version of BB84 [10]. The EU funded project "Secure Communication Based on Quantum Cryptography" or SECOQC [11] connects six different locations in Vienna using 200km of fiber optic cable. Finally, the Tokyo QKD Network [12], first turned on in 2010, connected several locations in Tokyo.

These QKD protocols, however, assume that both A and B are able to perform various quantum operations. In particular, it is usually assumed that both parties may prepare and measure qubits in at least two alternative bases: typically the computational "Z" basis ($|0\rangle, |1\rangle$) and the Hadamard "X" basis (spanned by $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$). Though there have been many various alterations to the assumptions of A and B, it is still assumed that both may perform these "quantum" operations.

It was recently shown, however, in [13, 14], that QKD protocols may be constructed where A is allowed to perform quantum operations (such as preparing and measuring in the Z or X basis), while B is limited to performing certain operations which are "classical" in nature (exactly what B may do will be defined shortly). Such a protocol, which allows this quantum A and "classical"/limited B to agree on a secret key is called a *semi-quantum key distribution* (SQKD) protocol and they are very interesting from a theoretical standpoint for they attempt to answer the question regarding exactly how "quantum" a protocol needs to be to provide the same benefits as its fully quantum counterpart (such as BB84).

Such semi-quantum protocols also hold great potential from a practical standpoint. With such protocols, we shift the complexity, as far as hardware implementation is concerned, to a single user. One can envision a future key exchange infrastructure where expensive quantum hardware is required only from one user (perhaps a large commercial entity) while multiple, limited "classical" users, which require less hardware, are connected to it. There are many other potential uses for semi-quantum protocols: for instance military applications may be found where the more complicated quantum user is a stationary base, while the classical users connecting to it, thanks to their simpler hardware requirements, are mobile units. Later, when we describe our mediated protocol, the practical advantages become even more clear.

An SQKD protocol typically operates with A starting the communication by sending over to B a qubit, prepared in either the Z or X basis. Bob then, who is the limited "classical"/semi-quantum user, may perform one of two operations: he may either measure the qubit in the Z basis and prepare a new qubit in the same Z basis; alternatively, he may simply "reflect" the incoming qubit, learning nothing about it, back to A. There are other potential operations B may employ which we will discuss in a subsequent chapter - it is these two operations, however, that are our primary concern in this work.

After this quantum communication stage, A and B will, as is typical with QKD protocols, use a public, authenticated classical communication channel (a channel that E may read from, but not write to) to estimate the error rate of the quantum channel; to perform an error correcting protocol; and finally, to perform a privacy amplification protocol which takes their "raw" key, which was distilled from the quantum communication stage and error-corrected, and outputs a new, smaller, secure secret key. See [5] for more information on this process.

Observe that these semi-quantum protocols rely on a two-way quantum commu-

nication channel; that is a channel which permits a qubit to be sent from A to B, and then back again. This makes their security analysis difficult due to E's ability to interact twice with the sent qubit. Up until now, most work concerning the security of SQKD protocols has involved proving they are *robust* - a notion described in [13], whereby any attack by the eavesdropper E, which causes her to learn non-zero information, causes a detectable disturbance. However, a typical operation of any quantum channel induces some noise and it does not make sense for A and B to simply abort if they detect even the slightest error in their communication; thus it becomes important to calculate exactly (or at least determine a bound on) how much noise a protocol can tolerate before E has potentially too much information that a secure key cannot be distilled. Some authors [15, 16] have performed a security analysis when E is restricted to *individual attacks* - those where E performs the same attack each iteration and is forced to perform a measurement of her private ancilla before the key is used for anything. These are not as strong as *collective attacks* however, where, again, E is forced to use the same attack each iteration, however she may wait to perform a measurement. See [5] for more information on the different attack scenarios (we will discuss this, in greater detail, in Chapter 2). Our work, however, is the first to consider security against collective attacks. Furthermore, by utilizing results in [17, 18], security against collective attacks implies, for the protocols discussed here, security against any arbitrary, general attack.

In this dissertation, we are interested in further analyzing SQKD protocols, in particular their security. After introducing the basic concepts of quantum communication (e.g., qubits, measurements, density operators, etc.) and quantum key distribution (Chapter 2) and also after a survey of related work (Chapter 3), we will, in Chapter 4, prove a variety of security lemmas concerning single state SQKD protocols (semi-quantum protocols where A always sends a single, publicly known state each iteration

— typically $|+\rangle$). In particular, we will show that, for such protocols E may actually perform a simpler attack without any loss of power. This result holds for protocols where A sends one of two orthogonal states; however we will also show the result is not necessarily true when A sends one of three states each iteration, or B prepares a qubit different from his measurement result. These results are based on a paper we published in [19].

We will then apply these results to provide an alternative and simpler proof of robustness for the single state SQKD protocol of [20]. This technique we believe could be very useful in proving the robustness of future single state SQKD protocols. Then, turning to collective attacks in the asymptotic scenario, we also apply this result to find an upper-bound on the difference between the key rate [5] of this SQKD protocol and the three-state BB84 protocol [3]. We believe this technique may be useful for analyzing the security of other semi-quantum key distribution protocols.

Next, in Chapter 5, we design a new single state SQKD protocol which, instead of using the measurement results to sift a raw key, as is the case with all other SQKD protocols (not only single state), uses Bob's actual operation to determine the bit string. Namely, if B chooses to reflect, this will constitute a key bit of 0; otherwise if B chooses to measure and resend this will correspond to a 1. Thus this protocol demonstrates, for the first time, the possibility of using reflections and X basis qubits to carry information, even though classical Bob cannot work directly with such qubits. Prior SQKD protocols simply use the X basis to measure the noise of the channel. This protocol is based on our work in [19].

Chapter 5 concludes by considering the key rate of our new protocol in the asymptotic scenario. In particular, we will show an explicit attack on our protocol, found using our search algorithm described in [21], which introduces a quantum bit error rate (QBER) of 5.6% yet causes the key rate [22] to drop below zero. This provides

an upper-bound on the tolerated error rate (the maximal amount of error before an adversary potentially holds too much information for even privacy amplification to distill a secure key) of this SQKD protocol. We will also bound the effects of E's bias attack on the key rate of this protocol.

Finally, in Chapter 6 we will introduce the notion of *mediated semi-quantum key distribution*. In this scenario, both A and B are limited and classical. We design a protocol which allows them to establish a shared secret key using the services of a quantum server. However, this quantum server is not trusted - in fact we will prove the unconditional security of our protocol assuming the worst case: that this server is the adversary. The server is required to prepare certain quantum states, perform a Bell measurement, and report on the results of this measurement. However, since this server is adversarial, A and B do not trust that the state initially prepared is the one specified by the protocol; nor do they necessarily trust that the server's measurement report is correct (if the server actually measured at all). Despite this, we will prove that this protocol allows the two classical users to establish a secure secret key so long as the noise in the quantum channel is less than 10.65%, a bound very close to that of the BB84 [1] protocol which allows up to 11% error [22].

Chapter 2
Preliminaries

2.1 Basic Concepts and Notation

We will now briefly describe the concepts and notation of quantum computing required to understand this work. For more detailed information, the reader is referred to [23] (from which the information in this chapter is derived).

A classical bit may be zero or one. It may be copied exactly and read at any time without any loss or disturbance. A *quantum bit* (or qubit) may also be zero or one (denoted $|0\rangle$ and $|1\rangle$ respectively - these $|\cdot\rangle$'s are called *kets* in Dirac's braket notation [24]), however it may also be in what is called a *superposition* of both zero and one which we denote: $\alpha|0\rangle+\beta|1\rangle$. The α and β are called *probability amplitudes*; these are complex numbers such that $|\alpha|^2+|\beta|^2=1$. One cannot, with probability one, copy an arbitrary qubit. Furthermore, "reading" a qubit (called *measuring*) is a probabilistic process whereby the qubit is potentially destroyed. Indeed, if we were to measure the state $\alpha|0\rangle+\beta|1\rangle$, we would not see this superposition - instead we would observe $|0\rangle$ with probability $|\alpha|^2$ (that is, after measuring, the measurement function/device reports not $\alpha|0\rangle+\beta|1\rangle$, but instead simply $|0\rangle$); otherwise, with probability $|\beta|^2$, we would see $|1\rangle$. After this measurement process the original superposition is destroyed and "collapses" to (becomes) the observed state $|0\rangle$ or $|1\rangle$.

More generally, we may consider an n-dimensional quantum system as living in an n-dimensional Hilbert space which for our purposes we may think of as simply the vector space $\mathbb{C}^n$ with the usual dot-product serving as inner product. When considering such a system we will generally define an arbitrary orthonormal basis for

this space denoted: $\{|0\rangle, |1\rangle, \cdots, |n-1\rangle\}$. Orthonormal implies that each basis ket $|i\rangle$ is normalized and, for each $i \neq j$, the inner product of $|i\rangle$ with $|j\rangle$ is zero. Each of these kets (the $|i\rangle$'s) are simply n column vectors with complex entries. Unless otherwise stated, in this work we will assume that this basis is the standard "computational" basis; that is: $|i\rangle = (0, \cdots, 0, 1, 0, \cdots, 0)^T$, with the i'th entry a one and $(\cdot)^T$ representing the transpose operation (since kets are column vectors).

An arbitrary state in this n-dimensional system can then be written as a superposition of these basis states. That is: $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle$ where $\alpha_i \in \mathbb{C}$ and $\sum_i |\alpha_i|^2 = 1$. We may manipulate these states as we would ordinary vectors; thus the state $|\psi\rangle$ is simply a $\mathbb{C}$-linear combination of the basis states $|i\rangle$ and we may write it as a vector (often called a *state vector*): $|\psi\rangle = (\alpha_1, \alpha_2, \cdots, \alpha_n)^T$. A measurement of this state produces one of the n basis states $|i\rangle$ with probability exactly $|\alpha_i|^2$ (note that some of the α_i's may be zero, in which case $|i\rangle$ is never measured). As with the qubit case (which is a two-dimension system), the original superposition is destroyed and collapses to the observed basis state.

For every ket $|\psi\rangle$ there is a corresponding *bra* (thus the name "braket" notation - a play on the word bracket), denoted $\langle\psi|$ which is simply the conjugate transpose of the ket. Thus a bra is a row vector. Observe that, for any two arbitrary n-dimensional quantum states $|\psi\rangle$ and $|\phi\rangle$, the product $(\langle\phi|)(|\psi\rangle)$, computed using ordinary matrix multiplication, is a 1×1 matrix which we may view as simply a scalar in $\mathbb{C}$. This value is exactly the dot-product (inner-norm) of these two vectors. This, being a common operation, is denoted simply as: $\langle\phi|\psi\rangle$, the result of which is considered a scalar in $\mathbb{C}$ (not a 1×1 matrix). Observe that we may now write the requirements for an orthonormal basis simply as: $\langle i|j\rangle = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta function.

Another important computation occurs when we multiply $|\phi\rangle$ with $\langle\psi|$ denoted

simply: $|\phi\rangle \langle\psi|$. This produces an $n \times n$ matrix with complex entries. We will return to this shortly.

Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ of dimension n and m respectively, we may combine these two spaces into a new $n \cdot m$ dimensional space denoted $\mathcal{H}_1 \otimes \mathcal{H}_2$. If $\{|1\rangle_1, |2\rangle_1, \cdots, |n\rangle_1\}$ is an orthonormal basis of $\mathcal{H}_1$ and $\{|1\rangle_2, |2\rangle_2, \cdots, |m\rangle_2\}$ is an orthonormal basis of $\mathcal{H}_2$, then we define an orthonormal basis of $\mathcal{H}_1 \otimes \mathcal{H}_2$ by $\{|i\rangle_1 \otimes |j\rangle_2 \mid i = 1, 2, \cdots, n; j = 1, 2, \cdots, m\}$. Given two column vectors $|\psi\rangle$ and $|\phi\rangle$ (of size n and m respectively), the tensor product, denoted $|\psi\rangle \otimes |\phi\rangle$, results in a $n \cdot m$ column vector. This is easily computed. If $|\psi\rangle = (\alpha_1, \alpha_2, \cdots, \alpha_n)^T$, then:

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_1 |\phi\rangle_2 \\ \alpha_2 |\phi\rangle_2 \\ \vdots \\ \alpha_n |\phi\rangle_2 \end{pmatrix},$$

where each $\alpha_i |\phi\rangle$ is an m column vector constructed by the scalar multiplication of α_i with $|\phi\rangle$. The corresponding bra: $\langle\psi| \otimes \langle\phi|$ is constructed similarly. To simplify notation, we often write $|\psi\rangle |\phi\rangle$; if the context is clear, we will often drop the subscripts or even simply write $|\psi, \phi\rangle$.

This process may be repeated to combine three or more Hilbert spaces.

Besides measurements, another important operation is the application of a unitary operator. An $n \times n$ matrix U is said to be *unitary* if $UU^* = I$. Here U^* is the conjugate transpose of U and I is the $n \times n$ identity matrix. Given an n-dimensional quantum state $|\psi\rangle$, one may apply any unitary operator to it. The resulting state is simply $U |\psi\rangle$, which may be computed using basic matrix multiplication; note that the result is a new column vector.

If given a joint system $\mathcal{H}_1 \otimes \mathcal{H}_2$, where $\dim \mathcal{H}_i = d_i$ (thus the dimension of the

joint system is $d_1 d_2$), one may construct a unitary operator U, acting on the entire space, as a $d_1 d_2 \times d_1 d_2$ unitary matrix as described above. However, if given a unitary matrix U_1 which acts only on $\mathcal{H}_1$ (thus it is a $d_1 \times d_1$ matrix) and a unitary matrix U_2 acting only on $\mathcal{H}_2$, one may construct the operator $U := U_1 \otimes U_2$ which acts on the entire joint system. The action is simply: $U(|\psi\rangle_1 \otimes |\phi\rangle_2) = (U_1 |\psi\rangle_1) \otimes (U_2 |\phi\rangle_2)$. If $U_1 = (u_{i,j})_{i,j=1}^{d_1}$, then:

$$U = \begin{pmatrix} u_{1,1}U_2 & u_{1,2}U_2 & \cdots & u_{1,d_1}U_2 \\ u_{2,1}U_2 & u_{2,2}U_2 & \cdots & u_{2,d_1}U_2 \\ \vdots & & & \vdots \\ u_{d_1,1}U_2 & u_{d_1,2}U_2 & \cdots & u_{d_1,d_1}U_2 \end{pmatrix}, \tag{2.1}$$

where, $u_{i,j}U_2$ is a $d_2 \times d_2$ matrix resulting from the scalar multiplication of $u_{i,j}$ with U_2. It can be shown that U is a unitary $d_1 d_2 \times d_1 d_2$ matrix and thus a permissible quantum operator on the joint system. This process may also be repeated multiple times in case there are three or more subspaces.

2.2 Mixed States

Let $\mathcal{H}$ be an n-dimensional Hilbert space spanned by orthonormal basis $\{|1\rangle, \cdots, |n\rangle\}$. The state $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle = (\alpha_1, \cdots, \alpha_n)^T$ is called a *pure state* (even though it is a superposition, it can be represented as a state vector). Very often in quantum computing, it is useful to consider a more general *mixed state* which may be represented, not by an $n \times 1$ vector, but instead an $n \times n$ matrix, with complex entries, called a *density matrix*. Any pure state $|\psi\rangle$ may be represented by the density matrix: $|\psi\rangle \langle\psi|$ (recall that we are multiplying the column vector $|\psi\rangle$ with its conjugate transpose (a row vector) thus resulting in an $n \times n$ matrix). Mixed states, which describe a probability distribution over pure states, cannot be represented as a state vector. Given a

collection of pure states $\{|\phi_i\rangle\}_{i=1}^k$, an example of a mixed state is: $\rho = \sum_{i=1}^k p_i |\phi_i\rangle \langle\phi_i|$ where $k > 1$, $p_i \in \mathbb{R}_+$, $\sum_i p_i = 1$. This state ρ, models a system which is in (pure) state $|\phi_i\rangle$ with probability p_i.

It should be observed that density matrices are Hermitian, positive semi-definite matrices with trace 1.

There are various circumstances where mixed states arise. For instance, suppose we are given a quantum system prepared in some initial state by another individual. We know that the state which was prepared was one of $|\phi_i\rangle$ and that the probability that the preparer sent us the state $|\phi_i\rangle$ is exactly p_i; however we do not actually know which state was prepared. This situation may be described with the density matrix ρ described above. Alternatively, suppose we started with a system $|\phi\rangle$ (a pure state), and performed a measurement on it but did not observe the result (or maybe someone else measured the system and gave it back to us without telling us the measurement result). This measurement probabilistically collapsed the state to one of the basis states. Such a state may now be represented as a mixed state.

Mixed states also arise when dealing with "imperfect" state preparations, errors, and when modeling environment "noise".

Let us now describe how measurements are performed on density matrices. Following that, we will discuss the application of unitary operators.

Given a joint system $\mathcal{H} := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k$, with each $\mathcal{H}_i$ spanned by the orthonormal basis $\{|0\rangle_i, |1\rangle_i, \cdots, |d_i - 1\rangle\}$, we may perform a measurement on any one of the k subspaces (leaving the others unmeasured). To do so, we first define, for all appropriate i, j, measurement operators:

$$M(i,j) = I_1 \otimes I_2 \otimes \cdots \otimes I_{i-1} \otimes |j\rangle \langle j|_i \otimes I_{i+1} \otimes \cdots \otimes I_k, \tag{2.2}$$

where I_m is the identity operator acting on $\mathcal{H}_m$ (i.e., it is the identity matrix of size $d_m \times d_m$, where $d_m = \dim \mathcal{H}_m$). Let ρ be a $D \times D$ density matrix where $D = \dim \mathcal{H}$. Then, if we perform a measurement of the i'th subspace of $\mathcal{H}$, $\mathcal{H}_i$ (that is, we measure only the i'th component of ρ), the probability of observing outcome $|j\rangle_i$ is: $p_{i,j} := tr(M(i,j)\rho)$. Here $M(i,j)\rho$ is computed via matrix multiplication and $tr(\cdot)$ is the trace operation. Furthermore, on observing outcome $|j\rangle_i$, the state collapses to:

$$\rho' = \frac{M(i,j)\rho M(i,j)}{p_{i,j}} = \frac{M(i,j)\rho M(i,j)}{tr(M(i,j)\rho)},$$

To measure multiple subspaces, one may repeat this process measuring first one subspace, followed by another, and so on. Also, our choice of basis was arbitrary: one may define an alternative basis for $\mathcal{H}_i$, define the operator $M(i,j)$ with respect to that basis (replacing the $|j\rangle \langle j|_i$ portion with the new j'th basis vector) and repeating the above.

Two important bases we will consider in the two-dimensional (qubit) case are the computational Z basis, already defined as $\{|0\rangle, |1\rangle\}$, and the Hadamard X basis, denoted $\{|+\rangle, |-\rangle\}$, where:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle).$$

Unitary operators work similarly as with pure states, however now we require two multiplications. Indeed, given density matrix ρ and a unitary operator U, then, after applying U to the quantum system, the new state is described by the density matrix:

$$\rho' = U\rho U^*. \tag{2.3}$$

2.3 Partial Trace, Entropy, and the Trace Norm

If ρ_{AB} is a density operator acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, we can compute its *partial trace*; that is, we may *trace out* one of the subspaces $\mathcal{H}_A$ or $\mathcal{H}_B$, an operation denoted $tr_A(\rho_{AB})$ leaving a density matrix ρ_B (alternatively ρ_A, with the trace operation denoted $tr_B(\rho_{AB})$) which describes only the $\mathcal{H}_B$ portion (respectively $\mathcal{H}_A$) of the original state. Let $\{|i\rangle_A\}$ be an orthonormal basis for $\mathcal{H}_A$ and write $\rho = \sum_{i,j} |i\rangle \langle j|_A \otimes \rho_B^{i,j}$. To trace over $\mathcal{H}_A$, we simply compute:

$$\rho_B = tr_A(\rho_{AB}) = tr_A \left(\sum_{i,j} |i\rangle \langle j|_A \otimes \rho_B^{i,j} \right) = \sum_i \rho_B^{i,i}. \tag{2.4}$$

The computation of $tr_B(\rho_{AB})$ is similar (leaving a density matrix ρ_A acting only on $\mathcal{H}_A$). If $\rho_{ABC\ldots}$ is a density matrix acting on the joint system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \cdots$ (finitely many times), we will often take the notational shortcut of writing $\rho_{AC\ldots}$ to mean $tr_B(\rho_{ABC\ldots})$; similarly for the removal of any combination of subscript letters.

Given a density matrix ρ, it is often useful to compute its *von Neumann Entropy* - the extension of Shannon entropy to the quantum domain - denoted $S(\rho)$. It is defined as $S(\rho) = -tr(\rho \ln \rho)$. If $\{\lambda_i\}_{i=1}^D$ are the eigenvalues of ρ (note that since ρ is Hermitian, all eigenvalues are real; furthermore they are non-negative due to ρ being positive semi-definite), this may be computed as: $S(\rho) = -\sum_i \lambda_i \ln \lambda_i$.

A second important computation is the *trace distance* of two density matrices ρ and σ (both acting on the same Hilbert space). This we denote $\Delta(\rho, \sigma) := \frac{1}{2}||\rho - \sigma||$ where $||A||$ represents the *trace norm* of matrix M defined as $||M|| := tr(\sqrt{M^* M})$ (here $N = \sqrt{M^* M}$ is a matrix such that $N^2 = M^* M$). For our purposes (working only with density matrices which are Hermitian), if $\{\lambda_i\}_{i=1}^D$ are the eigenvalues of the (Hermitian) matrix $\rho - \sigma$, then:

$$\Delta(\rho, \sigma) = \frac{1}{2} \sum_{i=1}^{D} |\lambda_i|. \tag{2.5}$$

2.4 Quantum Key Distribution

The first quantum key distribution (QKD) protocol was developed by Bennett and Brassard in 1984 [1]. Since then several protocols have been proposed and analyzed (e.g., SARG04 [4], the six-state BB84 protocol [1, 25], the three-state BB84 protocol [3], higher-dimensional protocols [26, 27], and the B92 protocol [2] just to list a few; also see [5] for more information). These protocols permit two participants, Alice (A) and Bob (B), to agree on a secure secret key even when faced with an all powerful adversary Eve (E). In general no restrictions, beyond those forced upon her by the laws of physics, are placed on E.

These protocols assume the existence of a quantum communication channel, permitting A and B to swap quantum resources (typically qubits). After communicating with qubits, generally with A preparing a qubit, then B measuring it, A and B share some random information called a *raw key* (we will also denote this raw key, often called an *info string* in the semi-quantum literature, by $\texttt{info}_A$ and $\texttt{info}_B$). It is to be desired that their respective raw keys almost match (noise in the channel or, as we will see, noise induced by E's attack will make an exact match unlikely).

QKD protocols also require a classical public authenticated channel which allows A and B to send classical messages to one another. This channel is authenticated, however, so while the attacker E may listen in on any message sent over this channel, she cannot send messages of her own. This authenticated channel is used, at least, to perform an error correcting protocol, and privacy amplification protocol to first remove any errors from their raw key and then distill a smaller, secure secret key.

More information on these processes will be provided later.

E meanwhile captured and probed each qubit, via the application of a unitary operator entangling the sent qubit with her own private ancilla $\mathcal{H}_E$, before forwarding it to the recipient (either A or B depending on the protocol). Exactly how E performs this attacks depends on the attack model under consideration. There are typically three [5]:

1. **Individual Attacks**: On each iteration, E will apply a unitary U, acting on the qubit and her private ancilla $\mathcal{H}_E$. The same attack U is used on each iteration. When the quantum communication stage is complete, E will measure her ancilla. This measurement may be any POVM, however it is performed before error correction (EC) and privacy amplification (PA).

2. **Collective Attacks**: Like individual attacks, E will again use the same operation U on each iteration. However she may now wait to measure her ancilla until some point in the future. For instance, she may wait to perform an optimal measurement until after she has seen a cipher text sent using the distilled secret key (after EC and PA).

3. **General Attacks**: E may perform any arbitrary attack on each iteration. For instance, she may apply different unitary operators on each iteration; or different attacks based on measurements in past iterations.

This paper concerns itself mostly with collective attacks. We have been claiming up until now that we consider an all powerful adversary; however as it turns out, for the protocols we will be considering, we may, using the results of [28, 22], show that security in this case implies security under general attacks. Showing security against collective attacks is simpler than the general case due to various simplifications one

may consider. It is important to note that the same is not true if one only considers individual attacks.

To illustrate, we will consider the BB84 protocol [1], the quantum communication stage of which works by repeating the following:

1. A sends a qubit prepared randomly from one of the forms: $|0\rangle, |1\rangle, |+\rangle$, or $|-\rangle$, each chosen with equal probability 1/4.

2. B will choose randomly, and independently of A, to measure the incoming qubit in either the Z or X basis. If he chooses Z and if A sent $|0\rangle$ or $|1\rangle$ they now have a shared bit of information; likewise if A sent $|+\rangle$ or $|-\rangle$ and B choose to measure in the X basis (they agree publicly that, as far as their raw keys are concerned, a $|+\rangle$ represents a classical 0 while $|-\rangle$ represents a 1). All other cases are disregarded (next step).

3. B informs A of his measurement choice (but not the measurement result). A tells B whether to keep or reject the iteration (rejection taking place if A sent $|0\rangle$ or $|1\rangle$ while B measured in X; likewise for the other case).

Repeating this N times, for N sufficiently large, B will divulge a small, randomly chosen subset of his measurement results to A (using the authenticated public channel). Doing so allows A and B to estimate the amount of noise in the quantum channel thus permitting them to compute an upper bound on the amount of information E can possibly hold on their key. If the noise is low enough (that is, if E's "probe" was weak enough), A and B will finish with EC and PA to distill a secure secret key.

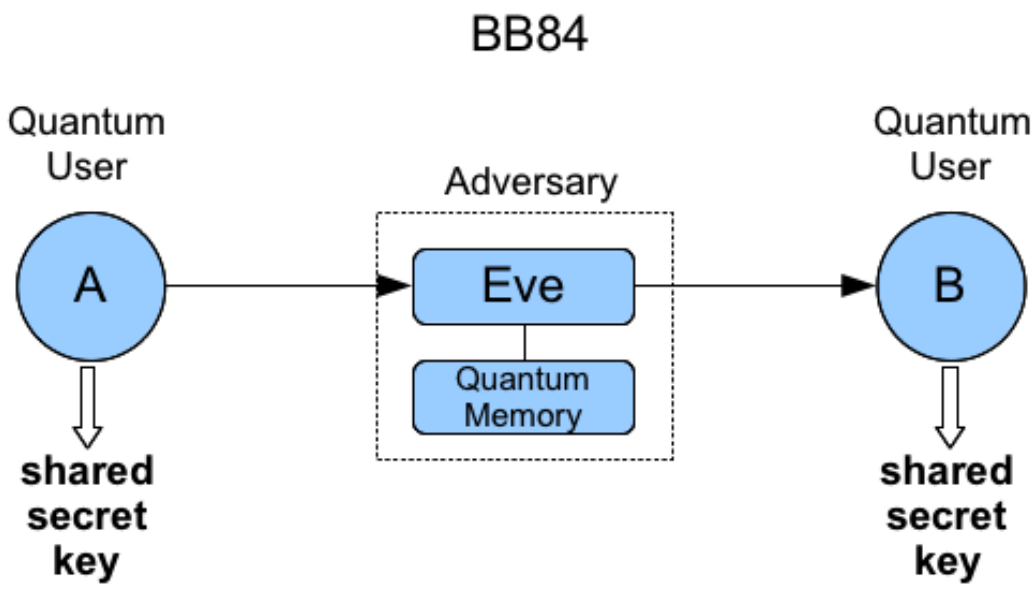

Figure 2.1: Diagram of BB84 [1].

2.5 Key Rate in the Asymptotic Scenario

If we assume that all noise in the quantum communication channel is caused by Eve, as is the common approach [5], a question of great interest then is to calculate exactly how much error these protocols can withstand before Alice and Bob are unable to distill a secure secret key even after privacy amplification. Essentially, the question is, to what value should we set the security threshold parameters to so that, if Alice detects more than that many errors, the protocol aborts.

We will now be adopting the notation and definitions described in [22, 28]. It is assumed that Alice and Bob repeat the quantum communication stage of a protocol until they are able to compute an n-bit raw key denoted $\texttt{info}_A$ and $\texttt{info}_B$. At this point, A, B, and E share a tripartite system ρ_{ABE}. Following this, they will perform an error correcting protocol so that, with high probability, $\texttt{info}_A = \texttt{info}_B$. They will then perform privacy amplification - a process that will distill an $l(n) \leq n$ bit key that is ϵ secure. That is to say, if, after performing the quantum communication (resulting

in state ρ_{ABE}), error correcting, and privacy amplification, the joint system, shared by A, B, and E is in the state σ_{ABE} (where now the systems A and B hold the $l(n)$ bit distilled key and E now consists of additional information gained by Eve during the public discussion), it holds that:

$$\Delta(\sigma_{ABE}, \tau_K \otimes \sigma_E) = \frac{1}{2} ||\sigma_{ABE} - \tau_K \otimes \sigma_E|| \leq \epsilon,$$

where $\sigma_E = tr_{AB}(\sigma_{ABE})$, τ_K is the completely mixed state of all possible key values chosen with equal probability [5], and $|| \cdot ||$ is the trace norm. Such a requirement on the protocol leads to the notion of *composable* security which allows Alice and Bob to safely use their resulting key for any other cryptographic tasks. Intuitively, the above definition implies that the resulting distilled key is "almost" the same as one drawn from uniform independently of E's system.

A useful measure of a protocol's effectiveness is the key rate. That is, how many ϵ secure bits may be distilled from n `info` bits (denoted $l(n) \leq n$). In the asymptotic scenario, this is defined as:

$$r := \lim_{n \to \infty} \frac{l(n)}{n}$$

Let us assume, for the time being, that Eve is restricted to collective attacks; these are attacks where Eve performs the same attack operation on each quantum communication iteration (however she is not required to perform any measurements until such time that is most advantageous to her). If $\tilde{\rho}_{ABE}$ is the tripartite density operator describing the system immediately after the protocol's quantum communication (and before error correction and privacy amplification), then it is of the form $\tilde{\rho}_{ABE} = \rho_{ABE}^{\otimes n}$, where ρ_{ABE} describes the system after a single iteration of the quantum communication stage. For such a state, it was then shown in [29] that, assuming

collective attacks and no preprocessing, the key rate is:

$$r = S(A|E) - H(A|B) \tag{2.6}$$

(note we use the equivalent version presented in [30] which we find easier to work with). Where $S(A|E) = S(\rho_{AE}) - S(\rho_E)$; S denotes the von Neumann entropy; and H denotes the classical conditional entropy.

Thus, so long as $r > 0$ it is possible for Alice and Bob to distill an ϵ secure key (in the asymptotic scenario, and with the equation described above, it is assumed ϵ is a function of n which approaches 0 as n approaches infinity). Clearly the value of r depends not only on the protocol in question but on the attack operator used by Eve. This attack must induce some amount of noise that the protocol can detect. The question then is, how much error can a protocol withstand before $r \leq 0$ (before Eve has too much information, and/or before there is too much error in the `info` strings that error correction leaks too much information). For example, the BB84 protocol, assuming no post-processing, can withstand a quantum bit error rate (QBER) of 11% [31] - that is to say, if, after Alice and Bob verify that the amount of error induced in the Z and X bases is no higher than 11%, it is guaranteed that $r > 0$ and thus, they may generate a secure key. Anything higher than 11% and this is no longer guaranteed (so they should abort).

2.6 Semi-Quantum Cryptography

Prior QKD protocols all assumed that the two users A and B were allowed to work directly with quantum resources. In particular, they were both capable of preparing and measuring qubits in a variety of bases (e.g., the Z and X bases). However, in 2007, Boyer, Kenigsberg, and Mor introduced a new field of study which they called

Semi-Quantum Key Distribution (SQKD) [13]. Now, instead of assuming both A and B are capable of working with quantum resources, we assume only A is allowed to do so, while B is limited to performing certain "classical" operations. Such an A is called a *fully-quantum user*; the limited B is called a *classical user* or a *semi-quantum user*. Protocols which allow for the establishment of a secure secret key when there is at least one classical user, are called semi-quantum protocols. Of course we make no assumptions on the attacker who is fully quantum and bounded only by the laws of physics.

In more detail, an SQKD protocol relies on a two-way quantum communication channel - one where a qubit is allowed to travel from A to B, then back to A. This greatly complicates the security analysis of the protocol as the attacker is now able to interact twice with the qubit. For this reason, most semi-quantum protocols have been proven secure with respect to the following definition of robustness:

Definition 2.6.1. From [13]: An SQKD protocol is called *robust* if, for any attack employed by E which allows her to potentially gain information on either A or B's raw key (before error correction), necessarily induces a disturbance which may be detected by either A or B with non-zero probability.

Note that this is a much weaker definition of security when compared to the key rate computation described last section. Robustness only tells us an attack can be detected - but it says nothing about the size of the final key based on the amount of induced noise. Robustness also does not say anything about how much noise a protocol can withstand before A and B should abort.

We will now describe B's limitations in greater detail. The classical user, when given a qubit from a fully-quantum user, is allowed to perform one of the following operations:

1. **Measure and Resend**: The classical user may measure any incoming qubit in the computational Z basis and resend the result. That is, if the measurement resulted in outcome $|r\rangle$, for $r \in \{0, 1\}$, then the classical user will prepare a new qubit of the form $|r\rangle$ and send it.

2. **Reflect**: The classical user may simply ignore the incoming qubit and "reflect" it back to the fully-quantum user. When performing this operation, the classical user learns nothing about its state and does not disturb the qubit in any way.

There have been some variations to these restrictions. For instance, in [32, 16], B was allowed to *Measure and Prepare*: that is, measure in the Z basis, and prepare a new qubit in either state $|0\rangle$ or $|1\rangle$ (not necessarily the same state that was measured). However, it is the reflect and the measure and resend operations that we are interested in here. Note that B is limited to only working directly with the Z basis.

To illustrate how such protocols typically operate, we recall the first SQKD protocol of [13]. Each iteration of this protocol operates as follows:

1. A will send a qubit of the form $|0\rangle, |1\rangle, |+\rangle$, or $|-\rangle$, choosing one at random (as with BB84 [1]

2. B will choose randomly to reflect the qubit or measure and resend. If he measures and resends, he saves his measurement result as his raw key bit for this iteration.

3. A will choose to measure in the same basis (Z or X) that she originally used to prepare the qubit in.

4. B will now inform A of his choice to measure and resend or reflect.

    - If B measured and resent and if A prepared (and thus later measured) in the Z basis, they now share a random bit.

- If B reflected and A prepared and measured in the X basis, this iteration can be used to verify the security of the quantum channel in the X basis (verifying the security in the Z basis may be done by disclosing a certain amount of randomly chosen iterations where B measured, and A chose the Z basis).

As usual, after they perform the above operation, they will, assuming the error rate is "low enough," run an error correcting protocol and a privacy amplification protocol. However, up until our work, to be presented in this dissertation, no one knew how low was "low enough" as most protocols were only proven robust (which only states that noise implies an attack), or secure against individual attacks - which is too weak a notion for general security.

Chapter 3
Related Work

3.1 Semi-Quantum Cryptography

Semi-quantum key distribution was introduced in [13]. In that source, the authors introduced the concept of a *classical user*. They also introduced the security notion of *robustness* and described a protocol which allowed a fully quantum A and a classical B to agree on a secret key; they also proved the protocol was robust. A second semi-quantum protocol was introduced, by the same authors, in [14] along with a proof of its robustness.

In [20], Zou et al., designed semi-quantum protocols where the fully quantum user is limited to preparing three, two, or even one state each iteration (as opposed to the original SQKD protocol which allowed A to choose from all four BB84 states). We call a semi-quantum protocol where A is limited to sending a single, publicly known state, each iteration of the quantum communication stage a *single state protocol* and they are of great interest to us in this dissertation. With such protocols, A is limited to preparing and sending only one type of state $|a\rangle$ (typically $|a\rangle = |+\rangle$). She cannot prepare a different state on any of the iterations. Furthermore, E is fully aware that the qubit leaving A's lab is $|a\rangle$. Despite this limitation, it was shown in [20] that robust protocols exist.

Extending their work, [15] described an equation which relates the information gain of E as a function of the disturbance caused by her individual attack. This is a good step forward from robustness; however the ultimate goal is to show security against collective attacks (which are sufficient to prove security against general

attacks).

Many other protocols were developed since these first [32, 33, 34]. All of these protocols utilized measurement results directly to distill a raw key (e.g., a measurement of $|1\rangle$ implied a key bit of 1 for that iteration). In [32], the idea of allowing B to send a qubit in a different state than what he measured (though still in the Z basis) was introduced. A similar idea was used in [16]. Though this ability, in the single-state case, seems to add some extra complexity to the security analysis.

Other protocols, such as [35, 16], were designed to allow a fully quantum A, to distill a secure secret key with multiple classical users $B, C, \ldots$. The protocol of [35] required the quantum user A to be fully trusted (and this user is also a key holder). The protocol described in [16] operated over a cycle topology, allowing a qubit to travel from A to B, then to C, and finally back to A. An important consideration in their security proof was that A could not access the channel between B and C. Such a protocol allowed B and C to establish a secure key which A could not gain information on. We will return to this idea shortly. We observe, however, that besides proving robustness, this protocol was also shown secure against individual attacks.

Beyond key distribution, there have been several secret sharing protocols designed allowing a quantum A to share a secret with two semi-quantum users B and C [36, 37, 38, 39]. Security in all these protocols was based on a notion of robustness.

3.2 Mediated Quantum Key Distribution

We define a *mediated QKD protocol* (also referred to as a *multi-user QKD protocol* in some literature) as a protocol which allows two or more users to establish a secure key with the help of an untrusted quantum server. This server should be unable to gain information on the key (without causing a disturbance at least) and, in fact, is

often considered to be the adversary.

While there have been several mediated QKD protocols developed, none, with the exception of [16], were for the semi-quantum setting. However, we observe that the protocol in [16] required the existence of a private quantum channel connecting the two semi-quantum users A and B: while E was allowed access to this channel, the quantum server C was not. In fact, it is not difficult to show that their protocol is insecure in the event the quantum server is given access to this channel.

The first multi-user QKD protocol (not semi-quantum) was designed by Phoenix et al., in [40]. Their protocol required the server to prepare and send Bell states (one particle to each quantum user). A and B then performed certain unitary operations on their respective qubits, returning the result to the server.

The mediated QKD protocol described in [41] required the two users A and B to prepare and send qubits to the server C in one of the four states $|0\rangle, |1\rangle, |+\rangle$, or $|-\rangle$. The server then stored them in a quantum memory until some future time when A and B wish to distill a secret key (this can be a long time delay). The protocols described in [42, 43, 44, 45] all required the two users to perform both Z and X basis measurements. The protocol of [43, 46] required the users A and B to apply various unitary operators on qubits sent to them from the server.

In [47], a protocol was designed which required the two users to prepare Bell states (the server performed Bell measurements). The security of this protocol was later improved in [48, 49] by requiring the users to measure in both Z and X bases. In [46], the server prepared states involving the entanglement of four qubits. This was later improved in [44]. Furthermore, this protocol required that one of the two users perform a Bell basis measurement.

Chapter 4

Security of Single State Semi-Quantum Protocols

In this chapter, we discuss a set of security theorems that we have proven which apply to any single state SQKD protocol. These results provide a general "tool-set" which allow for the simplified mathematical analysis of such protocols. We will define a new form of collective attack: the *restricted collective attack* which consists only of a single real parameter in the range $[-1/2, 1/2]$ and a single unitary operator. We will then show that to prove security against the most general form of collective attacks, which consist of two unitary operators, it suffices to consider and prove security against only restricted collective attacks. This makes the security analysis of single state SQKD protocols far simpler mathematically. These results are derived from a paper we published in [19].

4.1 Definitions and Notation

To analyze an SQKD protocol, we will work with the following Hilbert space:

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_T \otimes \mathcal{H}_E \otimes \mathcal{H}_B.$$

In this system, $\mathcal{H}_A$ and $\mathcal{H}_B$ are quantum registers used to model A and B's private (classical) memory. They may be spanned by such states as $|0\rangle$ and $|1\rangle$. Additionally, B's register may have states $|\texttt{measure}\rangle$ and $|\texttt{reflect}\rangle$. These registers are simply used to model any "bookkeeping" required of A and B (for example, B must remember if he reflected a particle on a certain iteration). While B is classical, and A does not wish to use a quantum memory, our use of these registers will be exactly equivalent

to these two parties simply saving their information in classical memory. We adopt this use, however, as it provides a very convenient system of notation.

$\mathcal{H}_T$ is used to model the two-dimensional qubit: it is the *transit* or *travel* space. At the beginning of each iteration, A holds access to this space and prepares a new qubit. Next it is "passed" to E who performs some attack operation on it. Following this, B is allowed access to the transit space and he will measure and resend or reflect (ignore) it. It is passed back to E who attacks a second time. Finally it is passed back to A.

Lastly, $\mathcal{H}_E$ is used to model E's personal private ancilla space. It is, without loss of generality, finite dimensional.

As mentioned, an SQKD protocol relies on a two-way quantum communication channel - one that allows a qubit to travel from A to B, then back to A. In this section we will consider two forms of collective attack (recall a collective attack is one where E performs the same operation each iteration, however is allowed to postpone her measurement to a time of her choosing). The first form is the most general collective attack available to E:

Definition 4.1.1. A *general collective attack* consists of two unitary operators (U_E, U_F), both acting on $\mathcal{H}_T \otimes \mathcal{H}_E$. The attack consists of E applying U_E on the forward channel (when the qubit initially travels from A to B) and then applying U_F on the return (when the qubit is traveling from B to A).

We next consider a more restricted form of collective attack:

Definition 4.1.2. A *restricted collective attack* consists of a real number b and a single unitary U acting on $\mathcal{H}_T \otimes \mathcal{H}_E$. This attack consists of E preparing the qubit:

$$|e\rangle = \sqrt{\frac{1}{2} + b}\,|0\rangle + \sqrt{\frac{1}{2} - b}\,|1\rangle\,,$$

and sending it to B (regardless of the state A originally sent). On the qubit's return from B, E will apply the unitary operator U.

4.2 Core Results

Theorem 4.2.1. If B is a limited classical user, and if A is restricted to sending a single qubit state $|a\rangle$ each iteration (the state of which is publicly known), and assuming that E's ancilla state is known to her (i.e., it is in some "zero" state $|0\rangle_E \in \mathcal{H}_E$), then for every general collective attack (U_E, U_F), there exists an equivalent restricted attack (b, U).

Proof. Fix a general collective attack (U_E, U_F) and let us first consider the result of E applying this attack. After E applies U_E to $|a\rangle$ in the forward direction, the state evolves to $|a'\rangle = |0, e_0\rangle + |1, e_1\rangle$ where the $|e_i\rangle$ are arbitrary states, not necessarily orthogonal or normalized, in $\mathcal{H}_E$. Unitarity of U imposes the condition that $\langle e_0|e_0\rangle + \langle e_1|e_1\rangle = 1$. E then forwards the qubit to B.

Next, B will, with probability p_R reflect the qubit; otherwise he will measure and resend (with probability $p_M = 1 - p_R$). If he reflects, he will set his private quantum register to some state σ_R (this may also store randomly chosen data for example). Otherwise, if he measures $|i\rangle$, he will set his register $\mathcal{H}_B$ to the state $\sigma_{M,i}$ (this may save his measurement result and some other data for example). These σ states are density operators acting only on $\mathcal{H}_B$. We make no assumptions on these states other then that they are density operators of unit trace.

Thus, after B's operation, and when E receives a qubit from B, the state of the quantum system is (ignoring A's system which, in a single state protocol, is necessarily

separate from $\mathcal{H}_T$ at this point):

$$\rho = p_R(|0,e_0\rangle\langle 0,e_0| + |1,e_1\rangle\langle 1,e_1| + |0,e_0\rangle\langle 1,e_1| + |1,e_1\rangle\langle 0,e_0|) \otimes \sigma_R$$
$$+ p_M(|0,e_0\rangle\langle 0,e_0| \otimes \sigma_{M,0} + |1,e_0\rangle\langle 1,e_1| \otimes \sigma_{M,1}).$$

Now, let us consider the result of the following restricted collective attack. Let $\alpha = \sqrt{\langle e_0|e_0\rangle}$ and $\beta = \sqrt{\langle e_1|e_1\rangle}$. Since E has full information on her attack operator U_E, she may compute these two values. Since, for any vector x, $\langle x|x\rangle$ is real and non-negative, α and β are both real and non-negative. It is clear, then, that there exists a value $b \in [-1/2, 1/2]$ such that $\alpha = \sqrt{1/2+b}$. Since $\alpha^2 + \beta^2 = 1$, it then holds that $\beta = \sqrt{1/2-b}$.

Assume, then, that E prepares the state $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ and sends this qubit to B (unentangled with her ancilla). This is the first step of a restricted attack with parameter b. B applies the same operations as before yielding the system:

$$\rho^{\text{restricted}} = p_R(\alpha^2|0\rangle\langle 0| + \beta^2|1\rangle\langle 1| + \alpha\beta|0\rangle\langle 1| + \beta\alpha|1\rangle\langle 0|) \otimes \sigma_R$$
$$+ p_M(\alpha^2|0\rangle\langle 0| \otimes \sigma_{M,0} + \beta^2|1\rangle\langle 1| \otimes \sigma_{M,1})) \otimes |0\rangle\langle 0|_E,$$

note that, above, we assumed E's system is cleared to some zero state $|0\rangle_E \in \mathcal{H}_E$ known to her. (With collective attacks such an assumption may be made without loss of generality.) We will now construct a unitary operator V such that $V\rho^{\text{restricted}}V^* = \rho$.

Case 1: First assume that both α and β are non-zero. We define V's action on states $|i,0\rangle$ to be:

$$V|i,0\rangle = \frac{|i,e_i\rangle}{\sqrt{\langle e_i|e_i\rangle}}.$$

Since E knows exactly how her probe U_E operates, she has full information on the states $|e_i\rangle$ and so may construct such an operator. Note that it is not relevant how V operates on states of the form $|i,j\rangle$ for $j \neq 0$ - its action may be arbitrary in such instances. It is not difficult to see that this operator V is unitary.

Applying this operator, yields:

$$\begin{aligned} V\rho^{\text{restricted}}V^* &= p_R \left(\frac{\alpha^2}{\alpha^2} |0,e_0\rangle \langle 0,e_0| + \frac{\beta^2}{\beta^2} |1,e_1\rangle \langle 1,e_1| \right. \\ &\quad \left. + \frac{\alpha\beta}{\alpha\beta} |0,e_0\rangle \langle 1,e_1| + \frac{\beta\alpha}{\beta\alpha} |1,e_1\rangle \langle 0,e_0| \right) \otimes \sigma_R \\ &\quad + p_M \left(\frac{\alpha^2}{\alpha^2} |0,e_0\rangle \langle 0,e_0| \otimes \sigma_{M,0} + \frac{\beta^2}{\beta^2} |1,e_1\rangle \langle 1,e_1| \otimes \sigma_{M,1} \right) \\ &= \rho. \end{aligned}$$

Case 2: One of α or β is zero. This is similar, however, to the first case. We may follow the above arguments, however we need not worry about V's action on $|0,0\rangle$ if $\alpha = 0$, or $|1,0\rangle$ if $\beta = 0$.

Since both α and β cannot both be zero ($\alpha^2 + \beta^2 = 1$), we are finished. Indeed, let $U = U_F V$, then it is clear that the restricted collective attack (b, U) (where b was defined above) yields the same density operator as if the general collective attack (U_E, U_F) had been applied. The quantum systems are indistinguishable. In particular, the key rate equation, described in Chapter 2, are equal in both cases.

Since (U_E, U_F) was arbitrary, the proof is complete. □

This result shows that, at least for single-state protocols, the most general collective attack is equivalent to a simplified attack where E simply "biases" the qubit superposition (and thus B's measurement results) and then attacks with a single unitary operator. This b parameter makes sense when A is restricted to sending the state

$|+\rangle$ each iteration. However, for other initial states, the same result holds.

We now consider how "tight" this result is. It is not difficult to see a similar statement may be made if A prepares and sends one of $|a\rangle$ or $|b\rangle$ each iteration, chosen randomly, if $\langle a|b\rangle = 0$. Indeed, in this case, E may simply make a measurement of the incoming qubit, and apply the same analysis as above. Of course, in this case there may be two different bias values and two different unitary operators (one if A sends $|a\rangle$ and the other if A sends $|b\rangle$).

For other scenarios, when A chooses to send a state $|a\rangle$ from a collection of non-orthogonal states (e.g., if A chooses to send one of $|0\rangle, |1\rangle,$ or $|+\rangle$), the question is more difficult. In this case, the difficulty is in actually defining the restricted collective attack. In the single-state case (or even in the two-orthogonal-state case), it made sense that E would prepare a fresh qubit each iteration as she had full knowledge of what state was leaving A's device. This is not the case when A sends non-orthogonal states.

Our first attempt at this is to consider a very general notion of restricted attack. We define this as an attack whereby, on each iteration of the protocol, E sends a qubit to B that is unentangled with her own ancilla $\mathcal{H}_E$. How she prepares such a qubit is not relevant. She may prepare a fresh qubit of any form; or perhaps she applies a unitary operator to the incoming qubit (from A) - though this operator must act only on $\mathcal{H}_T$. This is a very broad definition and it includes the restricted attack in the single-state case, however it is not entirely satisfactory as it does not include the two-orthogonal-state case (where E performs a measurement and remembers the result thus entangling the qubit with her private two-dimensional memory). There may be other definitions that are worth considering in the future.

We will now show the existence of a general collective attack for which no restricted attack, even using a definition as broad as ours, exists.

Let $|a_t\rangle = \alpha_t |0\rangle + \beta_t |1\rangle$ be the state A sends on iteration t, where α_t and β_t are unknown to E (i.e., she chose to prepare this state probabilistically from a set of states $\mathcal{S}$ which contains at least one pair that is non-orthogonal). Consider now the result of E's general collective attack (U_E, U_F). We will define U_E's action on basis states as follows (recall that E's private ancilla is cleared to some zero state $|0\rangle \in \mathcal{H}_E$):

$$U_E |0,0\rangle = |0,e_0\rangle + |1,e_1\rangle$$
$$U_E |1,0\rangle = |0,e_2\rangle + |1,e_3\rangle .$$

Unitarity imposes the usual restrictions on the states $|e_i\rangle$.

Consider now the specific attack where $\langle e_j|e_j\rangle > 0$ for all $j = 1, \cdots, 4$ and $\langle e_j|e_k\rangle = 0$ for all $j \neq k$. This can be done unitarily. By linearity, we have: $U_E |a_t\rangle = |0,\tilde{e}_0^t\rangle + |1,\tilde{e}_1^t\rangle$ where:

$$|\tilde{e}_0^t\rangle = \alpha_t |e_0\rangle + \beta_t |e_2\rangle$$
$$|\tilde{e}_1^t\rangle = \alpha_t |e_1\rangle + \beta_t |e_3\rangle .$$

After B's operation, the state becomes:

$$\rho = p_R U_E |a_t,0\rangle \langle a_t,0| U_E^* \otimes \sigma_R$$
$$+ p_M \left(|0,\tilde{e}_0^t\rangle \langle 0,\tilde{e}_0^t| \otimes \sigma_{M,0} + |1,\tilde{e}_1^t\rangle \langle 1,\tilde{e}_1^t| \otimes_{M,1} \right) .$$

Now consider the result of a restricted collective attack, according to our definition described above. In this case, E will send the state $|E_t\rangle = x_t |0\rangle + y_t |1\rangle$, for some

$x_t, y_t \in \mathbb{C}$. This may have been the result of a unitary operator action on the qubit $|a_t\rangle$ only (and so it could be that $|E_t\rangle = |a_t\rangle$); or it may be something E prepared fresh this iteration (though in this case, it must be the same state each iteration since we are assuming collective attacks). After B's operation, the system becomes:

$$\begin{aligned}\rho^{\text{restricted}} &= p_R \left|E_t\right\rangle \left\langle E_t\right| \otimes \sigma_R \\ &\quad + p_M \left(|x_t|^2 \left|0\right\rangle \left\langle 0\right| \otimes \sigma_{M,0} + |y_t|^2 \left|1\right\rangle \left\langle 1\right| \otimes \sigma_{M,1}\right).\end{aligned}$$

(Note we did not bother writing E's system down above, as it is cleared to $|0\rangle_E$.)

From this, it is clear that the state initial sent by E must satisfy $\langle \tilde{e}_0^t | \tilde{e}_0^t \rangle = |x_t|^2$ and also $\langle \tilde{e}_1^t | \tilde{e}_1^t \rangle = |y_t|^2$. If this does not hold, the restricted attack is not equivalent to the general one as B's measurement operation produces outcomes with different probabilities in each case (this may or may not be advantageous to E).

Now, E needs to apply a unitary operator V, acting on $\mathcal{H}_T \otimes \mathcal{H}_E$ such that $V\rho^{\text{restricted}}V^* = \rho$. This cannot be done.

Indeed, consider iteration $t = 0$. From the above discussion, it must be that $V\left|0,0\right\rangle = e^{i\theta_0^0}\left|0,\tilde{e}_0^0\right\rangle / |x_0|$. On the next iteration, it is again required that $V\left|0,0\right\rangle = e^{i\theta_0^1}\left|0,\tilde{e}_0^1\right\rangle / |x_1|$. By our assumptions on the original attack (our assumptions on the states $|e_i\rangle$), x_0 and x_1 are both non-zero. By this, we have:

$$\begin{aligned}& V\left|0,\chi\right\rangle = V\left|0,\chi\right\rangle \\ \iff & \frac{e^{i\theta_0^0}}{|x_0|}(\alpha_0\left|e_0\right\rangle + \beta_0\left|e_2\right\rangle) = \frac{e^{i\theta_0^1}}{|x_1|}(\alpha_1\left|e_0\right\rangle + \beta_1\left|e_2\right\rangle) \\ \iff & \left(\alpha_0 - \frac{|x_0|}{|x_1|}e^{i(\theta_0^1-\theta_0^1)}\alpha_1\right)\left|e_0\right\rangle = \left(\frac{|x_0|}{|x_1|}\beta_1 e^{i(\theta_0^1-\theta_0^0)} - \beta_0\right)\left|e_2\right\rangle\end{aligned}$$

But, since $\langle e_0 | e_2 \rangle = 0$ and $\langle e_i | e_i \rangle > 0$ (by our initial assumptions on the general

collective attack), it must be that $\alpha_0 = xe^{i\theta}\alpha_1$ and $\beta_0 = xe^{i\theta}\beta_1$, where $x = |x_0|/|x_1|$ and $\theta = \theta_0^1 - \theta_0^0$. This implies that $|a_0\rangle = xe^{i\theta}|a_1\rangle$; that is, these two states which A prepared, are equivalent (up to an irrelevant global phase change). In other words, the state A sent on iteration 1 must be the same as on iteration 0 for the restricted attack to be equivalent to the general one. Otherwise this cannot be guaranteed. Of course this argument may be repeated for subsequent iterations.

Thus, Theorem 4.2.1 cannot be extended immediately to multi-state protocols. However, there may be a better definition of restricted attack for this scenario which does apply. In particular, perhaps a restricted attack could be defined as one where E's ancilla in the first attack is of dimension less that 4. This would make for interesting future work.

Returning, however, to the single state case, the SQKD protocols of [32, 16] allow B to measure in the Z basis but then prepare and send a new Z basis qubit in a different state. That is, if he measures $|r\rangle$, he may choose to send $|1-r\rangle$. In this case, there exist general collective attacks for which no equivalent restricted attack exists.

Indeed, let $|a\rangle$ be the state A sends each iteration (this is a single state protocol). Also assume that there is a non-zero probability that B, after measuring $|r\rangle$, may send $|1-r\rangle$ ($r \in \{0,1\}$). After E's initial probe, in the general collective attack case, the qubit evolves to the state $|0,e_0\rangle + |1,e_1\rangle$. Since we only need to show the existence of a general collective attack for which no equivalent restricted attack exists, let us assume $\langle e_i|e_i\rangle > 0$ and $\langle e_0|e_1\rangle = 0$.

Consider now the restricted attack, where E simply sends the state $|E\rangle = \alpha|0\rangle + \beta|1\rangle$. After B's operation, E must construct an operator capable of mapping $|0\rangle$ to $e^{i\theta_0}|0,e_0\rangle / \sqrt{\langle e_0|e_0\rangle}$ in case B reflected (or measured $|0\rangle$ and resent $|0\rangle$); it must also map $|0\rangle$ to $e^{i\theta_1}|0,e_1\rangle / \sqrt{\langle e_1|e_1\rangle}$ in case B measured $|1\rangle$ but sent $|0\rangle$. But this, of

course, implies:

$$|e_0\rangle = \left(\frac{\sqrt{\langle e_0|e_0\rangle}}{\sqrt{\langle e_1|e_1\rangle}}\right) e^{i(\theta_1-\theta_0)}\,|e_1\rangle\,,$$

which is not true in our example (where $\langle e_0|e_1\rangle = 0$).

We conclude this section with one further theorem which turns out to be very useful for proving the robustness of an SQKD protocol. This result states that, in a single state protocol, in order to avoid detection, E cannot "bias" the state A initially sent. Further, there is no advantage to her sending a different state. Thus, when proving robustness of a single state protocol, it suffices to consider only the result of E's attack on the return channel.

Theorem 4.2.2. Let $|a\rangle$ be the state A initially sends each iteration of a single state SQKD protocol and let $|b\rangle$ be a two-dimensional qubit state, orthogonal to $|a\rangle$. Assume that, on any iteration, there is a non-zero probability that B will reflect and A will measure in the $\{|a\rangle\,, |b\rangle\}$ basis to verify the security of the channel. Also assume that there is a non-zero probability that B will measure and resend and A chooses to measure in the Z basis, again for the purpose of verifying the security of the channel. Then, assuming E is limited to restricted collective attacks (which are sufficient in the single state case):

1. To avoid detection, E must send to B a state of the form $|E\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ where $|\alpha|^2 = |\,\langle 0|a\rangle\,|^2$ and $|\beta|^2 = |\,\langle 1|a\rangle\,|^2$.

2. If E wishes to avoid detection, there is no advantage to E in sending to B a state other than $|a\rangle$.

Proof. Write $|a\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$ for $\gamma, \delta \in \mathbb{C}$. Since this is a single state protocol, these parameters are known to E. With a restricted attack, E will send to B the state $|E\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha, \beta \in \mathbb{C}$ (we are providing her with extra power now, allowing

E to prepare a state with complex probability amplitudes, even though our previous result showed they might as well be real).

After B's operation, E will attack with a unitary operator U which acts on $\mathcal{H}_T \otimes \mathcal{H}_E$. We may assume that E's ancilla is cleared to some zero state, and so we may describe U's action as follows:

$$U\left|0,0\right\rangle_{TE} = \left|U_0\right\rangle = \left|0,e_0\right\rangle + \left|1,e_1\right\rangle$$
$$U\left|1,0\right\rangle_{TE} = \left|U_1\right\rangle = \left|0,e_2\right\rangle + \left|1,e_3\right\rangle,$$

where $\left|e_i\right\rangle$ are arbitrary states in $\mathcal{H}_E$ satisfying the usual unitary conditions.

If B reflected, and after E's attack U, the state of the quantum system is:

$$\begin{aligned}\rho^{\text{reflect}} =& U\left|E\right\rangle\left\langle E\right|U^* = \left|\alpha\right|^2\left|U_0\right\rangle\left\langle U_0\right| + \left|\beta\right|^2\left|U_1\right\rangle\left\langle U_1\right| \\ &+ \alpha\beta^*\left|U_0\right\rangle\left\langle U_1\right| + \alpha^*\beta\left|U_1\right\rangle\left\langle U_0\right|,\end{aligned}$$

where α^*, β^* denote the complex conjugate and U^* is the conjugate transpose of U.

Alternatively, if B measured and resent, the system is in the state:

$$\rho^{\text{measure}} = \left|\alpha\right|^2\left|U_0\right\rangle\left\langle U_0\right| + \left|\beta\right|^2\left|U_1\right\rangle\left\langle U_1\right|,$$

in which case, in order to avoid detection, it must hold that $\left|e_1\right\rangle = \left|e_2\right\rangle = 0$. If this is not the true, then A, measuring in the Z basis, would detect E's attack. Thus we may simplify the description of U to: $\left|U_0\right\rangle = \left|0,e_0\right\rangle$ and $\left|U_1\right\rangle = \left|1,e_3\right\rangle$ with $\left\langle e_0|e_0\right\rangle = 1$ and $\left\langle e_3|e_3\right\rangle = 1$.

Next, assume that B reflects and A measures in the $\{\left|a\right\rangle, \left|b\right\rangle\}$ basis. Let p_a denote the probability that A receives outcome $\left|a\right\rangle = \gamma\left|0\right\rangle + \delta\left|1\right\rangle$ in this event. To avoid

detection, it must be that $p_a = 1$. From the above description of the state ρ^{reflect}, this value is:

$$p_a = |\alpha\gamma|^2 \langle e_0|e_0\rangle + |\beta\delta|^2 \langle e_3|e_3\rangle + \alpha\beta^*\gamma\delta^* \langle e_0|e_3\rangle + \alpha^*\beta\gamma^*\delta \langle e_3|e_0\rangle .$$

Write $\gamma = \sqrt{p}e^{i\theta_a}$, $\delta = \sqrt{1-p}e^{i\theta_b}$, and $\langle e_0|e_3\rangle = re^{i\theta_e}$ (for $r \in [0,1]$). Also, write $\alpha = \sqrt{q}e^{i\theta_n}$ and $\beta = \sqrt{1-q}e^{i\theta_m}$. We show that $p_a = 1$ implies $p = q$ thus proving the first claim.

$$\begin{aligned} p_a &= |\alpha\gamma|^2 \langle e_0|e_0\rangle + |\beta\delta|^2 \langle e_3|e_3\rangle + \alpha\beta^*\gamma\delta^* \langle e_0|e_3\rangle + \alpha^*\beta\gamma^*\delta \langle e_3|e_0\rangle , \\ &= qp + (1-q)(1-p) \\ &+ r\sqrt{q(1-q)p(1-p)}\left(e^{i(\theta_n-\theta_m+\theta_a-\theta_b+\theta_e)} + e^{i(\theta_m-\theta_n+\theta_b-\theta_a-\theta_e)}\right) \\ &\leq qp + (1-q)(1-p) + 2\sqrt{q(1-q)p(1-p)}. \end{aligned} \tag{4.1}$$

Equality above, holds only if $r = 1$ and $\theta_e = \theta_m - \theta_n + \theta_b - \theta_a + 2\pi k$ (for $k \in \mathbb{Z}$). Observe that r and θ_e are both in E's control and that θ_a and θ_b are public. Equation 4.1 is bounded by one and, since E wishes to avoid detection by setting $p_a = 1$, it must hold that she set the values r and θ_e as described. Thus $p_a = 1$ yielding:

$$\begin{aligned} p_a = \quad & qp + (1-q)(1-p) + 2\sqrt{q(1-q)p(1-p)} && = && 1 \\ \Rightarrow \quad & p^2 - 2pq + q^2 && = && 0 \\ \Rightarrow \quad & p = q \end{aligned}$$

This shows that $q = |\alpha|^2 = p = |\gamma|^2 = |\langle 0|a\rangle|^2$ and $|\beta|^2 = |\delta|^2 = |\langle 1|a\rangle|^2$, thus proving the first claim of this theorem.

The second claim is obvious as E may always apply a unitary operator, arbitrarily rotating the phase of $|0\rangle$ and $|1\rangle$ after B returns a qubit. □

Note that, the results in this section apply only to collective attacks. As we will soon show, when proving the robustness of a protocol, this is sufficient. When moving away from robustness to more rigorous definitions of security (for instance, computing the key rate of a protocol in the asymptotic scenario), the results of [17, 18] may be applied which state that to prove security against the most general form of attack possible, it is sufficient to prove security against collective attacks. Thus, our results above provide a powerful framework from which to prove the security of single state SQKD protocols.

4.3 Further Results

We now show how Theorems 4.2.1 and 4.2.2 can be used to show the robustness of the single-state SQKD protocol introduced in [20]. While these results apply only to collective attacks, this is sufficient in the case of robustness if we assume A sends a qubit only after receiving a response from B (the usual assumption in SQKD protocol robustness proofs [20]).

Later we will consider how the bias term affects the key rate of this same protocol in the asymptotic scenario. In particular, we will derive an expression bounding the key rate of the SQKD protocol, in terms of the key rate of a known uni-directional QKD protocol and a function of the bias term.

4.3.1 Robustness of the SQKD Protocol of Zou et al.

Let us first recall the single-state protocol of [20]. As we will be referring to this protocol multiple times throughout this work, we will refer to it as SQKD-1. This protocol operates as follows:

1. On each iteration, A sends the state $|+\rangle$ to B

2. B chooses to measure and resend or to reflect the qubit. If he measures and resends, he will save his measurement result to use as his raw key bit.

3. A will choose, randomly, to measure in the Z or X basis.

4. B informs A of his choice (but not his measurement result if he made one)

    - If B measured and resent, and if A chose to measure in the Z basis, they will share a bit of information
    - If B reflected and A measured in the X basis, A can use this iteration to verify the X basis security.
    - All other cases are discarded

The above procedure will repeat N times. A and B will then run an error correcting protocol, and a privacy amplification protocol as is usual in QKD protocols. However, as with other proofs of robustness [13, 14, 20], we do not consider these procedures when proving robustness (error correction necessarily leaks information without detection).

Note that we may improve the efficiency of this protocol by employing a technique used in [50]. Namely, we alter the protocol so that A measures in the Z basis more often than the X basis. Similarly, B will measure and resend more often than reflecting. Thus, in the asymptotic scenario at least (which is all we consider in this dissertation), the fraction of iterations which actually contribute to the raw key can be made arbitrarily close to one.

Robustness of SQKD-1 was already proven in [20]. However, we now provide an alternative proof based on our security results proven last section. This method of proof extends easily to other single-state protocols, as we will demonstrate later.

Theorem 4.3.1. SQKD-1 is completely robust

Proof. Let us consider the very first iteration of this protocol. Observe that there is a non-zero probability that this iteration may be used to verify the security of the channel, either in the Z basis or the X basis. Also, since this is the first iteration, E's private ancilla is cleared to some zero state (known to her). Thus, when the first qubit is intercepted by E, Theorem 4.2.1 applies and, so, the most general attack E may chose to employ at this point, is equivalent to a restricted attack (b, U). Thus, E sends to B the qubit state $|E\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\alpha = \sqrt{1/2 + b}$ and $\beta = \sqrt{1/2 - b}$. To avoid detection, however, Theorem 4.2.2 states that $b = 0$. Thus, E sends $|+\rangle$ to B.

Next, B will either reflect (with probability p_R), or measure and resend (with probability $p_M = 1 - p_R$). As usual, B will store his decision and measurement results (if any) in his own private register. Thus, the state of the quantum system, when E receives a qubit back from B is:

$$\begin{aligned} \rho &= p_R |+\rangle\langle+|_T \otimes |0\rangle\langle 0|_E \otimes |\texttt{reflect}\rangle\langle\texttt{reflect}|_B \\ &+ \tfrac{p_M}{2} |0\rangle\langle 0|_T \otimes |0\rangle\langle 0|_E \otimes |\texttt{measure}, 0\rangle\langle\texttt{measure}, 0|_B \\ &+ \tfrac{p_M}{2} |1\rangle\langle 1|_T \otimes |0\rangle\langle 0|_E \otimes |\texttt{measure}, 1\rangle\langle\texttt{measure}, 1|_B \end{aligned} \tag{4.2}$$

E now applies her attack operator U which acts on basis states as follows:

$$U|0,0\rangle = |U_0\rangle := |0, e_0\rangle + |1, e_1\rangle$$
$$U|1,0\rangle = |U_1\rangle := |0, e_2\rangle + |1, e_3\rangle$$

Where the $|e_i\rangle$ are arbitrary states in $\mathcal{H}_E$ which satisfy:

$$\langle e_0|e_0\rangle + \langle e_1|e_1\rangle = \langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1$$
$$\langle e_2|e_0\rangle + \langle e_3|e_1\rangle = \langle e_0|e_2\rangle + \langle e_1|e_3\rangle = 0$$

Let $\sigma = U\rho U^*$ be the state of the system after E's attack. This state is:

$$\begin{aligned}\sigma &= \tfrac{p_R}{2}(|U_0\rangle\langle U_0| + |U_1\rangle\langle U_1| + |U_0\rangle\langle U_1| + |U_1\rangle\langle U_0|) \otimes |\texttt{reflect}\rangle\langle\texttt{reflect}|_B \\ &+ \tfrac{p_M}{2}|U_0\rangle\langle U_0| \otimes |\texttt{measure}, 0\rangle\langle\texttt{measure}, 0|_B \\ &+ \tfrac{p_M}{2}|U_1\rangle\langle U_1| \otimes |\texttt{measure}, 1\rangle\langle\texttt{measure}, 1|_B\end{aligned} \tag{4.3}$$

The qubit is then returned to A who performs a Z or X basis measurement. Assume first that B chose to measure and resend and that A choose to measure in the Z basis. Let us also assume that A and B both agree to use this iteration to check the security (thus B will divulge his measurement result). The probability that these events occur is non-zero and it is clear, in this case, that if E wants to avoid detection, she must set $|e_1\rangle = |e_2\rangle = 0$.

Now, assume that B reflected and A measures in the X basis. Let $\sigma^{\text{reflect}} = \frac{1}{2}(|U_0\rangle\langle U_0| + |U_1\rangle\langle U_1| + |U_0\rangle\langle U_1| + |U_1\rangle\langle U_0|)$ be the state of the system in this event. Then, the probability that A measures $|+\rangle$ is:

$$\begin{aligned}p_+ &:= tr(|+\rangle\langle+|\,\sigma^{\text{reflect}}\,|+\rangle\langle+|) \\ &= \tfrac{1}{2}tr\left(\tfrac{1}{2}(|+\rangle(|e_0\rangle\langle e_0| + |e_3\rangle\langle e_3| + |e_0\rangle\langle e_3| + |e_3\rangle\langle e_0|)\langle+|)\right) \\ &= \tfrac{1}{4}(\langle e_0|e_0\rangle + \langle e_3|e_3\rangle + \langle e_0|e_3\rangle + \langle e_3|e_0\rangle)\end{aligned} \tag{4.4}$$

Of course, E avoids detection only if $p_+ = 1$. Since $\langle e_0|e_0\rangle = \langle e_3|e_3\rangle = 1$, this is the case only if $\langle e_0|e_3\rangle = \langle e_3|e_0\rangle = 1$. This, however, forces $|e_0\rangle = |e_3\rangle$, a fact not difficult to show: indeed, assume for contradiction, that we may write $|e_3\rangle = |e_0\rangle + |x\rangle$ for some non-zero $|x\rangle$. Then, $1 = \langle e_0|e_3\rangle = \langle e_0|e_0\rangle + \langle e_0|x\rangle \Rightarrow \langle e_0|x\rangle = 0$. But, $1 = \langle e_3|e_3\rangle = \langle e_3|e_0\rangle + \langle e_3|x\rangle \Rightarrow \langle e_3|x\rangle = 0$. So, $0 = \langle e_3|x\rangle = \langle e_0|x\rangle + \langle x|x\rangle \Rightarrow \langle x|x\rangle = 0 \iff |x\rangle = 0 \iff |e_0\rangle = |e_3\rangle$.

Thus, at the conclusion of the first iteration of SQKD-1, in order to avoid detection, E's ancilla is in some state $|e_0\rangle\langle e_0|$ regardless of A and B's raw key bit. Therefore, she learns nothing on the first iteration. However, since her ancilla is in this known state, the same arguments may be applied on the second iteration. Thus, by induction, the claim follows and the protocol is robust. □

4.3.2 Regarding Raw Key Bias

Theorem 4.2.1 makes obvious a particular form of attack Eve may perform: namely she can attempt to easily bias the raw key causing Alice and Bob to agree on a key that is not uniform. While Eve may not learn anything about specific key bits in Alice and Bob's respective bit strings, it is still, in some manner, an information gain. Of course, since the SQKD protocols we've analyzed in this paper are robust, the attack described in this section is detectable by Alice and Bob (as a consequence of Theorem 4.2.2, Eve cannot attempt this attack as described in this section without running the risk of being detected). Nonetheless, since A and B must accept some amount of noise, it is interesting to consider exactly by how much Eve may bias the raw key.

Let us analyze the SQKD-1 protocol in [20], described in the previous section, to determine exactly how much bias Eve may introduce into the `info` string based on the total permitted error allowed by the honest parties A and B. Recall that Theorem 4.2.1 applies to this protocol. Now, consider the attack whereby Eve sends the state $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha = \sqrt{1/2 + b}$ and $\beta = \sqrt{1/2 - b}$ for some $b \in [0, 1/2]$ (the following results are symmetric if $b \in [-1/2, 0]$). Eve does not attack the return line which, in her absence, we assume is noiseless (it is usually the case, with quantum key distribution, to assume any noise is caused by Eve [5]). Such an attack causes both Alice and Bob to agree on a raw key that is drawn from the distribution whereby $\Pr(0) = 1/2 + b$. If Bob reflects this qubit, Alice will detect an error in the line (that

is, she will measure $|-\rangle$) with probability: $p(b) := 1/2 - \sqrt{1/4 - b^2} \leq 1/2$.

Recall that Alice permits a certain number of errors to register when reading the reflected qubits. After Alice and Bob transmit N qubits as described in the protocol, denote by R the number of qubits that were reflected (one would expect this to be $p_R N$, where p_R is the probability Bob reflects). If P is the threshold value used by Alice when determining whether to abort the protocol (that is, if Alice measures $|-\rangle$ P or more times, they abort), then Eve's optimal attack in this case is to set b so that $p(b)R < P$ (since p_R is public she can estimate R). Since N, p_R, and P are public knowledge, Eve can compute an optimal value for b. In particular: $b < \sqrt{\frac{P}{R}\left(1 - \frac{P}{R}\right)}$ (if $\frac{P}{R} \leq \frac{1}{2}$; otherwise, $b \leq \frac{1}{2}$).

If we let $P = \lambda R$ for some $\lambda \leq 1/2$ (now P represents the fraction of reflected qubits that are acceptable as errors), then we have: $b < \sqrt{\lambda(1-\lambda)}$, The graph of which is shown in Fig. 4.1.

Note that we may reword this statement. If Alice allows for a $\lambda \leq 1/2$ proportion of errors in the reflected qubits, Alice and Bob may expect to agree on a key not drawn from uniform, but from the distribution whereby:

$$Pr(k = 0) = \frac{1}{2} + \sqrt{\lambda(1-\lambda)} - \epsilon,$$

for some small $\epsilon > 0$. For instance, if $\lambda = 11\%$ (roughly the acceptable error rate of BB84 [31]), then, Alice and Bob can expect their `info` strings to be drawn from a distribution whereby $\Pr(k = 0) = .812$. Thus, by introducing only eleven percent error, there is an attack Eve may employ which causes eighty percent of Alice and Bob's raw key to be zero.

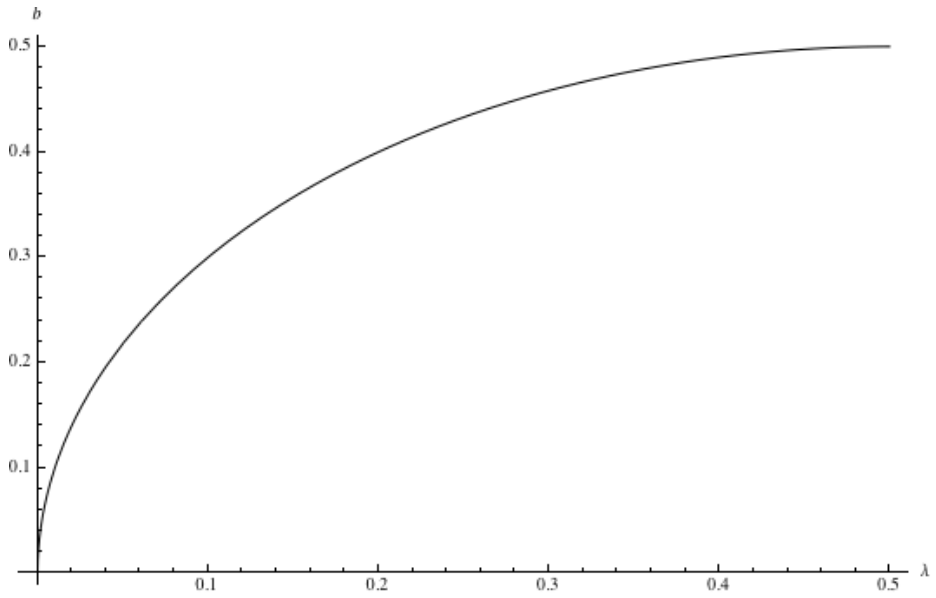

Figure 4.1: A graph of the function $b = \sqrt{\lambda(1-\lambda)}$. This is the maximal value of bias b which avoids the abortion of the protocol, provided A accepts a λ proportion of errors in the reflected qubits in the SQKD-1 protocol.

4.3.3 Key-Rate Comparison with Three-State BB84

Theorem 4.2.1 leads us to an interesting observation: if Eve sends the state $|+\rangle$ to Bob (that is, if she does not attack the first channel), then this is exactly equivalent to the three state BB84 protocol described in [3]. This three-state BB84 has Bob sending to Alice the states $|0\rangle$, $|1\rangle$, or $|+\rangle$ (we swap the roles of Alice and Bob in this paper so as to be analogous with SQKD-1; ordinarily Alice transmits to Bob). The Z basis states are used to distill their keys (along with some being used to estimate the error of the channel in the Z basis) while the $|+\rangle$ state is used to estimate the error of the channel in the X basis. If there is no noise in the first channel, this is exactly how the SQKD-1 protocol [20] works: if Bob reflects, he is sending a $|+\rangle$, otherwise he is sending a $|0\rangle$ or $|1\rangle$ randomly (based on his measurement result of $|+\rangle$ in the Z basis). The critical difference between the two is that Eve may attack on the first communication line from Alice to Bob. If we assume that Eve is honest in

the first attack stage (but not the second when the qubit is returning to Alice from Bob), the key rate of this SQKD protocol is exactly that achieved by the three-state BB84. However, we cannot assume Eve is honest.

Considering collective attacks, Theorem 4.2.1 implies that any attack by Eve on the first quantum channel, connecting Alice to Bob, is equivalent to Eve simply sending the biased state $|e\rangle = \sqrt{1/2+b}\,|0\rangle + \sqrt{1/2-b}\,|1\rangle$ for $b \in [-1/2, 1/2]$. Thus, in this case, the SQKD-1 protocol becomes a "biased" three-state BB84 protocol. The question we then ask is how does this bias affect the key rate (Equation 2.6). In the following we determine, for any quantum operator that Eve may employ, a bound on the difference between the effective key rates of these two protocols as a function of the bias induced in the first channel. This is sufficient to get a bound on the key rate of SQKD-1, thus proving its unconditional security for the first time.

Since we are considering collective attacks, it is clear that, at the conclusion of a single iteration of the protocol (an iteration used to contribute to the raw key), B and E's system may be represented by the mixed state:

$$\rho_{BE}(b) = \left(\frac{1}{2}+b\right)|0\rangle\langle 0|_B \otimes \rho_{E,0} + \left(\frac{1}{2}-b\right)|1\rangle\langle 1|_B \otimes \rho_{E,1}, \tag{4.5}$$

where b is the bias term introduced by E's initial attack and $\rho_{E,i}$ describes the state of E's ancilla in the event B's measurement is $|i\rangle$. In particular, let U be the attack operator used by E. We describe its action as follows:

$$\begin{aligned} U|0\rangle &\rightarrow |0,e_0\rangle_{TE} + |1,e_1\rangle_{TE} \\ U|1\rangle &\rightarrow |0,e_2\rangle_{TE} + |1,e_3\rangle_{TE}\,. \end{aligned} \tag{4.6}$$

Then it is clear that:

$$\rho_{E,0} = tr_T U \left|0\right\rangle \left\langle 0\right| U^* = \left|e_0\right\rangle \left\langle e_0\right| + \left|e_1\right\rangle \left\langle e_1\right|$$
$$\rho_{E,1} = tr_T U \left|1\right\rangle \left\langle 1\right| U^* = \left|e_2\right\rangle \left\langle e_2\right| + \left|e_3\right\rangle \left\langle e_3\right|.$$

Note that, without loss of generality, we may assume $\dim \mathcal{H}_E = 4$ where $\mathcal{H}_E$ is E's private ancilla.

In the asymptotic scenario, this parameter b may be estimated by A and B. As mentioned, if $b = 0$, this protocol is identical to the three state BB84 protocol [3], and in this case, the security of the SQKD-1 is identical to that of the fully quantum three state BB84. We now analyze the effect this bias term has on the key rate.

In the following, we will denote by $r(b, U)$, the key rate of SQKD-1, assuming E uses the attack with bias term b and unitary U. Furthermore, we will assume the Z basis noise induced by U is symmetric: that is $\langle e_0|e_0\rangle = \langle e_3|e_3\rangle = 1 - Q$ and $\langle e_1|e_1\rangle = \langle e_2|e_2\rangle = Q$. This is a common assumption and since we will later utilize previous key rate bounds for the three-state BB84 protocol, we make the same assumption here. From this, $r(b, U) = S(B|E) - H(B|A)$ where the quantum system is described by Equation 4.5 substituting in the appropriate values of $|e_i\rangle$ based on the operator U's action on basis states.

We first prove some basic Lemmas:

Lemma 4.3.1. Let b be the bias term and $\rho_{BE}(b)$ be as described in Equation 4.5. Then:

$$S(\rho_{BE}(0)) - S(\rho_{BE}(b)) = 1 - h\left(\frac{1}{2} + b\right) - b\Delta, \tag{4.7}$$

where $\Delta = S(\rho_{E,0}) - S(\rho_{E,1})$, and h is the binary entropy function. Note that $\Delta \in [-\log_2 \dim \mathcal{H}_E, \log_2 \dim \mathcal{H}_E] = [-2, 2]$.

Proof. Let $\{\lambda_i^j\}_{i=1}^4$ be the eigenvalues of $\rho_{E,j}$ (for $j = 0, 1$). Since $\rho_{E,i}$ is positive Hermitian they are real and non negative. Choosing a suitable basis (recall von Neumann entropy is invariant to unitary changes in basis), we may write $\rho_{BE}(b)$ as a block diagonal matrix:

$$\rho_{BE}(b) = \begin{pmatrix} \left(\frac{1}{2}+b\right)\rho_{E,0} & 0 \\ 0 & \left(\frac{1}{2}-b\right)\rho_{E,1} \end{pmatrix},$$

and so the eigenvalues of $\rho_{BE}(b)$ are: $\left\{\left(\frac{1}{2}+b\right)\lambda_i^0\right\}_{i=1}^4 \cup \left\{\left(\frac{1}{2}-b\right)\lambda_i^1\right\}_{i=1}^4$. Then:

$$\begin{aligned} -S(\rho_{BE}(b)) &= \sum_{i=1}^4 \left(\frac{1}{2}+b\right)\lambda_i^0 \log\left(\frac{1}{2}+b\right)\lambda_i^0 + \sum_{i=1}^4 \left(\frac{1}{2}-b\right)\lambda_i^1 \log\left(\frac{1}{2}-b\right)\lambda_i^1 \\ &= \left(\frac{1}{2}+b\right)\left[\sum_{i=1}^4 \lambda_i^0 \log\lambda_i^0 + \log\left(\frac{1}{2}+b\right)\sum_{i=1}^4 \lambda_i^0\right] \\ &+ \left(\frac{1}{2}-b\right)\left[\sum_{i=1}^4 \lambda_i^1 \log\lambda_i^1 + \log\left(\frac{1}{2}-b\right)\sum_{i=1}^4 \lambda_i^1\right] \\ &= \frac{1}{2}\left[\sum_{i=1}^4 \lambda_i^0 \log\lambda_i^0 + \sum_{i=1}^4 \lambda_i^1 \log\lambda_i^1\right] - h\left(\frac{1}{2}+b\right) \\ &- b\left[\sum_{i=1}^4 \lambda_i^0 \log\lambda_i^0 + \sum_{i=1}^4 \lambda_i^1 \log\lambda_i^1\right] \\ &= \frac{1}{2}\sum_{i,j} \lambda_i^j \log\lambda_i^j - h\left(\frac{1}{2}+b\right) - b\left(S\left(\rho_{E,0}\right) - S\left(\rho_{E,1}\right)\right). \end{aligned}$$

From this, it is clear that:

$$S(\rho_{BE}(0)) - S(\rho_{BE}(b)) = 1 - h\left(\frac{1}{2} + b\right) - b\left(S(\rho_{E,0}) - S(\rho_{E,1})\right)$$

□

We now show a similar bound for the classical joint entropy $H(A, B)$:

Lemma 4.3.2. Let $H(A, B_b)$ be the joint entropy of A and B's system in the event E uses bias b when attacking SQKD-1. Then:

$$H(A, B_0) - H(A, B_b) = 1 - h\left(\frac{1}{2} + b\right). \tag{4.8}$$

Proof. Denote by $p_b(x, y)$ the probability that B's raw key bit is x and A's key bit is y given that E used a bias term of b. Since we are assuming a symmetric attack, these values are:

$$\begin{aligned} p_b(0,0) &= \left(\frac{1}{2} + b\right)(1 - Q) \\ p_b(1,1) &= \left(\frac{1}{2} - b\right)(1 - Q) \\ p_b(0,1) &= \left(\frac{1}{2} + b\right) Q \\ p_b(1,0) &= \left(\frac{1}{2} - b\right) Q. \end{aligned} \tag{4.9}$$

Then:

$$
\begin{aligned}
-H(A,B_b) &= \left(\frac{1}{2}+b\right)(1-Q)\log\left(\frac{1}{2}+b\right)(1-Q) \\
&+ \left(\frac{1}{2}-b\right)(1-Q)\log\left(\frac{1}{2}-b\right)(1-Q) \\
&+ \left(\frac{1}{2}+b\right)Q\log\left(\frac{1}{2}+b\right)Q \\
&+ \left(\frac{1}{2}-b\right)Q\log\left(\frac{1}{2}-b\right)Q \\
\\
&= (1-Q)\log(1-Q) + Q\log Q \\
&+ \left(\frac{1}{2}+b\right)\log\left(\frac{1}{2}+b\right) + \left(\frac{1}{2}-b\right)\log\left(\frac{1}{2}-b\right) \\
\\
&= -h(Q) - h\left(\frac{1}{2}+b\right).
\end{aligned}
$$

From this, the claim follows immediately. □

We may now prove our bound on the key rate:

Theorem 4.3.2. Let (b,U) be an attack against protocol SQKD-1 and denote by $r(b,U)$ the resulting key rate. Then:

$$|r(0,U) - r(b,U)| \leq 2h(|b|) + |b|\log 3 + |b\Delta| \tag{4.10}$$

$$\leq 2h(|b|) + (2+\log 3)|b|. \tag{4.11}$$

Proof. By definition, $r(b,U) = S(\rho_{BE}(b)) - S(\rho_E(b)) - H(A,B_b) + H(A_b)$, where $H(A_b)$ is the classical entropy of A's system in the event E uses bias b in her initial

attack. From Lemmas 4.3.1, 4.3.2, it follows that:

$$\begin{aligned}|r(0,U) - r(b,U)| &= |S(\rho_{BE}(0)) - S(\rho_{BE}(b)) + S(\rho_E(b)) - S(\rho_E(0)) \\ &\quad - (H(A,B_0) - H(A,B_b)) + H(A_0) - H(A_b)| \\ &\leq |b\Delta| + |S(\rho_E(0)) - S(\rho_E(b))| + |H(A_0) - H(A_b)|.\end{aligned}$$

We must now bound $|S(\rho_E(0)) - S(\rho_E(b))|$. To do so, we will employ the Fannes-Audenaert inequality [51] which states that, for any two density matrices σ_1 and σ_2 both of dimension D, it holds that:

$$|S(\sigma_1) - S(\sigma_2)| \leq T \log(D-1) + h(T),$$

where $T := \frac{1}{2}||\sigma_1 - \sigma_2||$. Observe that $\rho_E(b) = tr_B \rho_{BE}(b) = \frac{1}{2}\rho_{E,0} + \frac{1}{2}\rho_{E,1} + b(\rho_{E,0} - \rho_{E,1})$. So:

$$\begin{aligned}T &= \frac{1}{2}||\rho_E(0) - \rho_E(b)|| = \frac{1}{2}||b(\rho_{E,1} - \rho_{E,0})|| \\ &\leq \frac{|b|}{2}(||\rho_{E,1}|| + ||\rho_{E,0}||) = |b|.\end{aligned}$$

The above inequality follows from the triangle inequality; the final equality follows from the fact that, for any positive-semidefinite matrix A, it holds that $||A|| = trA$.

A similar technique may be used to show that $|H(A_0) - H(A_b)| \leq h(|b|)$ (even though these are classical, the Fannes-Audenaert inequality may be used by representing the classical system as a quantum one via a diagonal matrix). Indeed, let $p_b(y)$ be the probability that A's raw key bit is y given a bias term of b was used.

From Equation 4.9, it follows that these values are:

$$p_b(0) = \left(\frac{1}{2} + b\right)(1 - Q) + \left(\frac{1}{2} - b\right)Q = \frac{1}{2} + b(1 - 2Q)$$
$$p_b(1) = \left(\frac{1}{2} + b\right)Q + \left(\frac{1}{2} - b\right)(1 - Q) = \frac{1}{2} - b(1 - 2Q).$$

Then, $\rho_A(b) = p_b(0)\,|0\rangle\langle 0| + p_b(1)\,|1\rangle\langle 1|$ and $S(\rho_A(b)) = H(A_b)$. Thus we may use the Fannes-Audenaert inequality again to bound $|H(A_0) - H(A_b)| \leq T_2 \log 1 + h(T_2) = h(T_2)$, where:

$$T_2 = \frac{1}{2}||\rho_A(0) - \rho_A(b)|| = \frac{1}{2}(|p_0(0) - p_b(0)| + |p_0(1) - p_b(1)|)$$
$$= |b| \cdot |1 - 2Q| \leq |b|.$$

The theorem's statement now follows. □

We have thus computed a function $f(b) = 2h(|b|) + (2 + \log 3)|b|$ such that $f(0) = 0$ and:

$$|r(0, U) - r(b, U)| \leq f(b) \Rightarrow r(b, U) \geq r(0, U) - f(b).$$

As mentioned, $r(0, U)$ is the key rate of the three state BB84 protocol. What we really want, however, is to know the key rate of the protocol, given only the bias, and the Z and X basis error rates (parameters that can be estimated). That is, we want to compute the following:

$$r_b = \inf_{U \in \Gamma_b(Q, Q_X)} r(b, U),$$

where Q is the observed Z basis error, Q_X is the observed X basis error (the probability that A measures $|-\rangle$ if B reflected - this depends on the bias term b and the attack operator U), and $\Gamma_b(Q, Q_X)$ is the set of all unitary operators which induce the specified error rate. We may use the results in this section to compute a lower

bound on this value.

In more detail, let $\Gamma_b(Q, Q_X)$ be the set of all unitary operators U such that $|\langle i|U|1-i\rangle|^2 = Q$ and $|\langle -|U|e\rangle|^2 = Q_X$. From our work above, we have:

$$r_b = \inf_{U \in \Gamma_b(Q,Q_X)} r(b,U) \geq \inf_{U \in \Gamma_b(Q,Q_X)} r(0,U) - f(b).$$

As mentioned earlier, $r(0,U)$ is the key rate of the three-state BB84 protocol if attack operator U is used. It was shown in [3] that:

$$\inf_{U \in \Gamma_0(Q,\widetilde{Q}_X)} r(0,U) \geq g(Q,\widetilde{Q}_X) = 1 - h(Q) - h(e_p), \tag{4.12}$$

where Q denotes the observed Z basis error (as described above), $\widetilde{Q}_X = |\langle -|U|+\rangle|^2$ is the error in the X basis (without bias - three state BB84 is a uni-directional protocol), and:

$$e_p = \min\left(\frac{1}{2}, \widetilde{Q}_X + 2Q + \sqrt{Q\widetilde{Q}_X}\right).$$

However, when a user is working with SQKD-1, they cannot directly observe $\widetilde{Q}_X$ - they can only observe Q_X which is the error induced by E's unitary attack operator and her initial bias. Thus, to use the above equation to bound the key rate of this SQKD protocol, we must find a bound on $\widetilde{Q}_X$ given only Q, Q_X, and b.

Pick an arbitrary unitary operator U. Let $\alpha = \sqrt{1/2+b}$, $\beta = \sqrt{1/2-b}$, and $|e\rangle = \alpha|0\rangle + \beta|1\rangle$. From Equation 4.6, we may compute the values Q_X and $\widetilde{Q}_X$:

$$Q_X = |\langle -|U|e\rangle|^2 = \frac{1}{2} - Re\left(\alpha^2\langle e_0|e_1\rangle + \alpha\beta\langle e_0|e_3\rangle + \alpha\beta\langle e_1|e_2\rangle + \beta^2\langle e_2|e_3\rangle\right)$$
$$\widetilde{Q}_X = |\langle -|U|+\rangle|^2 = \frac{1}{2} - Re\left(\frac{1}{2}\langle e_0|e_1\rangle + \frac{1}{2}\langle e_0|e_3\rangle + \frac{1}{2}\langle e_1|e_2\rangle + \frac{1}{2}\langle e_2|e_3\rangle\right).$$

Note that we have used the fact that $\langle e_0|e_2\rangle + \langle e_1|e_3\rangle = 0$ which is a consequence of

U being unitary.

From this, we have:

$$\begin{aligned}
|\widetilde{Q}_X - Q_X| &= \left| \left(\alpha^2 - \frac{1}{2}\right) \langle e_0|e_1\rangle + \left(\beta^2 - \frac{1}{2}\right) \langle e_2|e_3\rangle \right. \\
&\quad \left. + \left(\alpha\beta - \frac{1}{2}\right) (\langle e_0|e_3\rangle + \langle e_1|e_2\rangle) \right| \\
&\leq |b| \cdot |\langle e_0|e_1\rangle| + |b| \cdot |\langle e_2|e_3\rangle| \\
&\quad + \left| \sqrt{\frac{1}{4} - b^2} - \frac{1}{2} \right| (|\langle e_0|e_3\rangle| + |\langle e_1|e_2\rangle|) \\
&\leq |b|\sqrt{Q(1-Q)} + |b|\sqrt{Q(1-Q)} + \left| \sqrt{\frac{1}{4} - b^2} - \frac{1}{2} \right| (1 - Q + Q),
\end{aligned}$$

where the last inequality follows from the Cauchy-Schwarz inequality. Observe that, since $Q \in [0,1]$, it holds that $\sqrt{Q(1-Q)} \leq 1/2$. Also observe that $|\sqrt{1/4 - b^2} - 1/2| \leq |b|$. Thus:

$$|\widetilde{Q}_X - Q_X| \leq 2|b|$$

and so:

$$\widetilde{Q}_X \in [Q_X - 2|b|, Q_X + 2|b|].$$

Let $\widetilde{\Gamma}_b(Q, Q_X) = \bigcup_{\delta \in [-2|b|, 2|b|]} \Gamma_0(Q, Q_X + \delta)$. It is clear, from the above discussion,

that $\Gamma_b(Q, Q_X) \subset \widetilde{\Gamma}_b(Q, Q_X)$. Thus we conclude:

$$\begin{aligned} r_b = \inf_{U \in \Gamma_b(Q,Q_X)} r(b,U) &\geq \inf_{U \in \Gamma_b(Q,Q_X)} r(0,U) - f(b) \\ &\geq \inf_{U \in \widetilde{\Gamma}_b(Q,Q_X)} r(0,U) - f(b) \\ &\geq \inf_{\delta \in [-2|b|, 2|b|]} g(Q, Q_X + \delta) - f(b), \end{aligned} \tag{4.13}$$

where $g(Q, Q_X)$ is defined in Equation 4.12. This provides us with a lower bound on the key rate of SQKD-1 given only the observed parameters: Q, Q_X, and b.

Note that, while we only considered a collective attack, since Alice and Bob may permute their key bits in both protocols, without otherwise affecting the protocols, this implies the same result holds in the general attack scenario as shown in [17, 28].

Chapter 5
Security Analysis of a New Single State Protocol

In this chapter, we present a new single-state SQKD protocol along with its security analysis. This protocol is interesting in that it is the first which allows reflections (and, thus, X basis states) to contribute to the raw key, despite the fact that B is unable to directly work with such states (that is, he cannot prepare or measure in the X basis). Our protocol generates a raw key, not by using actual measurement results, but by using B's choice to reflect or measure and resend. In particular, if he chooses to reflect A's qubit, this will count as a raw key bit of zero; otherwise, if he measures and resends, this will be a key bit of one. While the SQKD protocols described in [13, 14] may be considered semi-quantum versions of the BB84 protocol, the protocol we discuss here may be considered the semi-quantum version of SARG04 [4] and, in fact, we took some inspiration from this QKD protocol (though, interestingly, even though SARG04 was our inspiration, we will later show a similarity to the B92 [2] QKD protocol). The work in this chapter is derived from a paper we published in [19].

5.1 The Protocol

Each iteration of our protocol runs as follows:

1. A sends to B the state $|+\rangle$.

2. B chooses a random bit k_B which will be his candidate raw key bit for this iteration. If $k_B = 0$, then B will reflect the incoming qubit; otherwise he will measure and resend. Finally, he will set an internal register called $\texttt{accept}_B$ in

the following manner:

- If $k_B = 0$ (that is, he reflected), then with probability 1/2 he will set $\texttt{accept}_B = \texttt{TRUE}$; otherwise $\texttt{accept}_B = \texttt{FALSE}$.
- If $k_B = 1$ (B measured and resent), then he sets $\texttt{accept}_B = \texttt{TRUE}$ only if his measurement produced outcome $|0\rangle$

The value of $\texttt{accept}_B$ is kept private for now.

3. When a qubit returns to A, she will choose randomly to measure in the Z or X basis. She will then set two internal registers, $\texttt{accept}_A$ and k_A (her raw key bit), in the following manner:
   - If she choose to measure in the Z basis and the result was $|1\rangle$, she sets $\texttt{accept}_A = \texttt{TRUE}$ and $k_A = 0$
   - If, instead, she choose the X basis and the measurement result was $|-\rangle$, she sets $\texttt{accept}_A = \texttt{TRUE}$ and $k_A = 1$.
   - For all other cases, she simply sets $\texttt{accept}_A = \texttt{FALSE}$; the value of k_A is not important in this case.
4. Next, A and B will broadcast their values of $\texttt{accept}_A$ and $\texttt{accept}_B$ using the classical authenticated channel. If both values are TRUE, then they will use k_A and k_B as their raw key bit for this iteration.
5. If either A or B's value is FALSE, this iteration can be used to verify the security of the channel. This requires further communication from B concerning his measurement result (if any) and his choice of k_B. Note that A and B will also perform this security verification on randomly chose iterations when $\texttt{accept}_A = \texttt{accept}_B = \texttt{TRUE}$.

The above procedure repeats N times and, as is usual, A and B will then run an error correcting and a privacy amplification protocol.

One of the disadvantages to this protocol is the loss of efficiency. Unlike SQKD-1 considered last chapter (the protocol of Zou et al. [20]), where the probability of B measuring and resending, and the probability of A choosing to measure in the Z basis, may be set close to one, here these probabilities must remain at $1/2$. In the absence of noise, one can expect only $1/8$ of the sent qubits to contribute to the raw key (unlike in SQKD-1, where in the absence of noise, one can expect, asymptotically, all qubits to contribute to the raw key). Interestingly, this is the same disadvantage SARG04 has when compared with BB84 [5]. We suspect our protocol can be made immune to multi-photon attacks (which was also the primary advantage to SARG04) and are currently investigating this possibility - thus providing a possible advantage to this protocol offsetting the obvious efficiency issue.

5.2 Proof of Robustness

Theorem 5.2.1. The SQKD protocol, as described above, is correct. That is to say, in the absence of noise, both parties will agree on the same raw key.

Proof. Let us consider a single iteration of our protocol. After B's operation, the system, assuming no noise, may be described by the mixed state:

$$\begin{aligned} \rho &= \tfrac{1}{4} |+\rangle \langle +| \otimes |a,0\rangle \langle a,0|_B + \tfrac{1}{4} |+\rangle \langle +| \otimes |r\rangle \langle r|_B \\ &+ \tfrac{1}{2} \left(\tfrac{1}{2} |0\rangle \langle 0| \otimes |a,1\rangle \langle a,1|_B + \tfrac{1}{2} |1\rangle \langle 1| \otimes |r\rangle \langle r|_B \right). \end{aligned} \tag{5.1}$$

Note that here, we have provided B with a quantum register (used to model his classical memory) spanned by states $\{|a,0\rangle, |a,1\rangle, |r\rangle\}$ which denotes his choice to "accept" with a raw key bit of zero, accept with a raw key bit of one, or reject.

When the qubit returns to A, she will choose to measure either in the Z or the X basis (each chosen with probability 1/2). Providing her with a register similar to that of B's, the system, after A's operation, is in the state:

$$\sigma = \frac{1}{2}M_X(\rho) + \frac{1}{2}M_Z(\rho), \tag{5.2}$$

where:

$$\begin{aligned} M_X(\rho) &= \tfrac{1}{4}\left|+\right\rangle\left\langle+\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|a,0\right\rangle\left\langle a,0\right|_B + \tfrac{1}{4}\left|+\right\rangle\left\langle+\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|r\right\rangle\left\langle r\right|_B \\ &+ \tfrac{1}{8}\left|+\right\rangle\left\langle+\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|a,1\right\rangle\left\langle a,1\right|_B \\ &+ \tfrac{1}{8}\left|-\right\rangle\left\langle-\right| \otimes \left|a,1\right\rangle\left\langle a,1\right|_A \otimes \left|a,1\right\rangle\left\langle a,1\right|_B \\ &+ \tfrac{1}{8}\left|+\right\rangle\left\langle+\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|r\right\rangle\left\langle r\right|_B \\ &+ \tfrac{1}{8}\left|-\right\rangle\left\langle-\right| \otimes \left|a,1\right\rangle\left\langle a,1\right|_A \otimes \left|r\right\rangle\left\langle r\right|_B \end{aligned} \tag{5.3}$$

and:

$$\begin{aligned} M_Z(\rho) &= \tfrac{1}{8}(\left|0\right\rangle\left\langle 0\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|a,0\right\rangle\left\langle a,0\right|_B + \left|1\right\rangle\left\langle 1\right| \otimes \left|a,0\right\rangle\left\langle a,0\right|_A \otimes \left|a,0\right\rangle\left\langle a,0\right|_B) \\ &+ \tfrac{1}{8}(\left|0\right\rangle\left\langle 0\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|r\right\rangle\left\langle r\right|_B + \left|1\right\rangle\left\langle 1\right| \otimes \left|a,0\right\rangle\left\langle a,0\right|_A \otimes \left|r\right\rangle\left\langle r\right|_B) \\ &+ \tfrac{1}{4}(\left|0\right\rangle\left\langle 0\right| \otimes \left|r\right\rangle\left\langle r\right|_A \otimes \left|a,1\right\rangle\left\langle a,1\right|_B + \left|1\right\rangle\left\langle 1\right| \otimes \left|a,0\right\rangle\left\langle a,0\right|_A \otimes \left|r\right\rangle\left\langle r\right|_B). \end{aligned} \tag{5.4}$$

It is not difficult to see that, if both A and B "accept" (they set their `accept` flags to `TRUE`), they will agree on the same raw key bit. □

We will use a similar technique as used in the proof of Theorem 4.3.1 to prove the robustness of our protocol:

Theorem 5.2.2. Our protocol, as described above, is completely robust.

Proof. Let us consider the first iteration of the protocol. As with SQKD-1, the

probability of performing a security check of the quantum channel, in either the Z or X basis, on this first iteration is non-zero. Using the same arguments as in the proof of Theorem 4.3.1, we can show that, after this first iteration, E's private ancilla is in some state $|e_0\rangle_E$, which is known to her, and which is independent of A and B's raw key bit.

The only additional element that must be shown is that the public discussion performed by A and B over the authenticated classical channel, does not leak information to E. However, this is not difficult to see. Only a single bit of information is sent by each party: namely whether A and B accept the iteration. If one of A or B reject, that particular iteration is not used to contribute to the raw key and thus no information leaks. We must, therefore, only consider the case when both accept. But this happens only in the case of two events:

- If B chose to reflect and accept, and if A chose to measure in the Z basis resulting in measurement outcome $|1\rangle$. In this case, A and B agree on a raw key bit of zero.

- If B chose to measure and resend and if his measurement result was $|0\rangle$; also if A chose to perform an X basis measurement resulting in outcome $|-\rangle$. In this case they both agree on a raw key bit of one.

It is not difficult to show that the probability of either event occurring is $1/16$. Therefore, when E learns that both parties accepted the iteration, the raw key bit is equally likely to have been a zero or one. Furthermore, E may incorporate the information of A and B's acceptance into her private ancilla; but even then, she is still fully aware of its state and so Theorems 4.2.1 and Theorems 4.2.2 apply again on the second iteration. Thus, by induction, the protocol is robust. □

5.3 Key Bias Attack

Since this is a single state protocol, Theorem 4.2.1 applies. Thus, any general collective attack, consisting of two unitary operators, is equivalent to an attack (b, U) where b is a bias parameter and U is a unitary operator. In prior SQKD protocols, where any measurement result was used directly as the raw key bit for a particular iteration, it was obvious how this b value biases the raw key. One might think that our new protocol would be immune to a bias attack due to the fact that Bob chooses himself how to set his raw key bit (reflecting causes a zero, measuring and resending a one), unlike in prior SQKD protocols where the measurement result itself is used for this bit string. However, Eve may still bias the key by causing Alice and Bob to accept more often on those iterations whereby Bob reflected (or measured) and to reject more often any other iteration, as we now show.

Note that we are only interested in the case when both Alice and Bob accept. Assume that Eve sends the state $|e\rangle = \alpha |0\rangle + \beta |1\rangle$ with $\alpha = \sqrt{1/2 + b}$ and $\beta = \sqrt{1/2 - b}$. Furthermore, assume she does not attack the qubit on its return from Bob to Alice (as we did in Chapter 4.3.2). Then, the system's state, adopting similar notation for Bob's register to that used in the proof of Theorem 5.2.1, when Alice receives a qubit from Bob is (assuming Bob has accepted):

$$\rho^{\text{accept}} = \frac{1}{2b+2} |e\rangle \langle e| \otimes |a,0\rangle \langle a,0|_B + \frac{2b+1}{2b+2} |0\rangle \langle 0| \otimes |a,1\rangle \langle a,1|_B . \tag{5.5}$$

This state was computed by first modifying Equation 5.1 (replacing $|+\rangle$ with $|e\rangle$), projecting to a state whereby Bob accepts, then dividing by the trace of the resulting density matrix.

Recall that Alice accepts a raw key bit of 0 only if she chooses to measure in the Z basis and her measurement outcome is $|1\rangle$; and that she accepts a raw key bit of 1 only if she chooses to measure in the X basis and the result is $|-\rangle$. The state of the system then is, again assuming Alice accepts:

$$\begin{aligned}\sigma &= \tfrac{1}{4p(b+1)}(\beta^2 |1\rangle\langle 1|_T \otimes |0,0\rangle\langle 0,0|_{AB} + \tfrac{1}{2}(\alpha-\beta)^2 |-\rangle\langle -|_T \otimes |1,0\rangle\langle 1,0|_{AB} \\ &+ \alpha^2 |-\rangle\langle -|_T \otimes |1,1\rangle\langle 1,1|_{AB}),\end{aligned} \tag{5.6}$$

where:

$$p = \frac{1}{4b+4}\left(\beta^2 + \frac{1}{2}(\alpha-\beta)^2 + \alpha^2\right) = \frac{1}{4b+4}\left(\frac{3}{2} - \alpha\beta\right).$$

Denote by $p(x,y)$ the probability Alice's bit is x while Bob's bit is y given that both A and B accepted. These values, are now easy to calculate as:

$$\begin{aligned} p(0,0) &= \beta^2/(3/2-\alpha\beta) \\ p(1,1) &= \alpha^2/(3/2-\alpha\beta) \\ p(0,1) &= 0 \\ p(1,0) &= (\alpha-\beta)^2/(3-2\alpha\beta)\end{aligned}$$

The values $p(0,0)$ and $p(1,1)$ are graphed in Fig. 5.1. Clearly, the bias term has a different effect on this protocol; in fact, this bias term can actually induce an error in A and B's raw key. We leave as an open question of some interest, as to whether or not it is possible to design a single state protocol which is either immune to this bias attack (which seems very unlikely), or which is less susceptible to it.

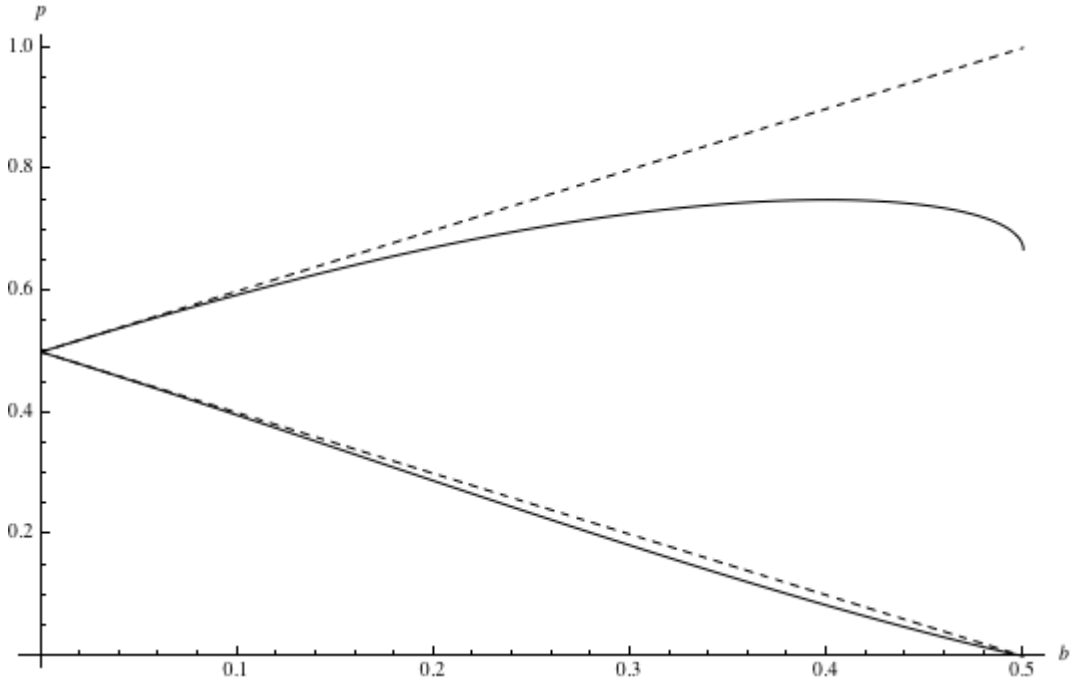

Figure 5.1: A graph of the distribution of the raw key if bias b (x-axis) is introduced in our new protocol. Top solid line plots $p(0,0)$ (the probability that Alice and Bob agree on 0), bottom solid line plots $p(1,1)$. The two dashed lines are the same quantities when Zou et al.'s protocol (see Chapter 4.3.1) is considered: namely $1/2 \pm b$.

5.4 Key Rate in the Asymptotic Scenario

We now turn our attention to bounding the maximum tolerated error rate of our new SQKD protocol. In particular, we will show an explicit attack that Eve may employ which, by introducing an error rate of 5.6% (that is, at most 5.6% of the qubits are flipped: $|i\rangle \to |1-i\rangle$ and $|+\rangle \to |-\rangle$), causes the key rate $r = S(A|E) - H(A|B)$ to become negative.

We will again consider a collective attack. From Theorem 4.2.1, we know the most general of these attacks is equivalent to Eve first sending the state $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ for $\alpha, \beta \in \mathbb{R}$. Let $\alpha = \sqrt{1/2+b}$ and $\beta = \sqrt{1/2-b}$ for some $b \in [-1/2, 1/2]$. Assume that she sends such a state to Bob who then will either reflect or measure and resend. We will use a similar method as in the proof of Theorem 5.2.1, however since we are only interested in the state whereby both Alice and Bob accept (if one of them rejects, the iteration is ignored), we might as well assume that Bob's register reads $|a\rangle$ (accept). Thus, the state of the system when Eve receives the return qubit is, from Equation 5.5:

$$\rho^{\text{accept}} = \frac{1}{2b+2}|e\rangle\langle e| \otimes |a,0\rangle\langle a,0|_B + \frac{2b+1}{2b+2}|0\rangle\langle 0| \otimes |a,1\rangle\langle a,1|_B .$$

Eve will now apply a unitary attack operator U, acting on the travel qubit and her own ancilla (prepared in some known state $|\chi\rangle$). This operator acts as follows:

$$\begin{aligned} U|0,\chi\rangle &= |U_0\rangle := |0,e_0\rangle + |1,e_1\rangle \\ U|1,\chi\rangle &= |U_1\rangle := |0,e_2\rangle + |1,e_3\rangle \\ U|e,\chi\rangle &= |U_e\rangle := |0,e_+\rangle + |1,e_-\rangle \end{aligned}$$

Where $|e_i\rangle$ are states in Eve's ancilla satisfying:

$$\begin{aligned}
&\langle e_0|e_0\rangle + \langle e_1|e_1\rangle = \langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1 \\
&\langle e_2|e_0\rangle + \langle e_3|e_1\rangle = \langle e_0|e_2\rangle + \langle e_1|e_3\rangle = 0 \\
&|e_+\rangle = \alpha\,|e_0\rangle + \beta\,|e_2\rangle \\
&|e_-\rangle = \alpha\,|e_1\rangle + \beta\,|e_3\rangle
\end{aligned} \tag{5.7}$$

The first two conditions follow from unitarity, the last two from linearity. After applying this operator, the system's state is:

$$\sigma^{\text{accept}} = \frac{1}{2b+2}\,|U_e\rangle\langle U_e| \otimes |0\rangle\langle 0|_B + \frac{2b+1}{2b+2}\,|U_0\rangle\langle U_0| \otimes |1\rangle\langle 1|_B\,.$$

The travel qubit is then forwarded to Alice who then measures in the X (accepting a key bit of 1 only if she measures a $|-\rangle$) or Z basis (accepting as a 0 only if she measures a $|1\rangle$). After this operation, and assuming she accepts, the joint system is in the state:

$$\sigma_{ATBE} = \frac{1}{2p}\left(\sigma_- \otimes |1\rangle\langle 1|_A + \sigma_1 \otimes |0\rangle\langle 0|_A\right), \tag{5.8}$$

where, defining $P(|\psi\rangle) = |\psi\rangle\langle\psi|$, we have:

$$\begin{aligned}
\sigma_- &= \tfrac{1}{2b+2} \cdot \tfrac{1}{2} P(|-\rangle (|e_+\rangle - |e_-\rangle)) \otimes |0\rangle \langle 0|_B \\
&+ \tfrac{2b+1}{2b+2} \cdot \tfrac{1}{2} P(|-\rangle (|e_0\rangle - |e_1\rangle)) \otimes |1\rangle \langle 1|_B
\end{aligned}$$

$$\sigma_1 = \tfrac{1}{2b+2} |1, e_-\rangle \langle 1, e_-| \otimes |0\rangle \langle 0|_B + \tfrac{2b+1}{2b+2} |1, e_1\rangle \langle 1, e_1| \otimes |1\rangle \langle 1|_B$$

$$\begin{aligned}
p &= \tfrac{1}{2} (tr(\sigma_-) + tr(\sigma_1)) \\
&= \tfrac{1}{4b+4} (\tfrac{1}{2} (\langle e_+|e_+\rangle + \langle e_-|e_-\rangle - \langle e_+|e_-\rangle - \langle e_-|e_+\rangle) \\
&+ \tfrac{2b+1}{2} (\langle e_0|e_0\rangle + \langle e_1|e_1\rangle - \langle e_0|e_1\rangle - \langle e_1|e_0\rangle) \\
&+ \langle e_-|e_-\rangle + (2b+1) \langle e_1|e_1\rangle).
\end{aligned}$$

We wish to compute $H(A|B)$ from $\sigma_{ABE} = tr_T(\sigma_{ATBE})$. Define $p(x, y)$ to be the probability that A's raw key bit is $x \in \{0, 1\}$ and that B's bit is $y \in \{0, 1\}$. From Equation 5.8, this is easy to compute:

$$\begin{aligned}
p(0,0) &= \tfrac{1}{2p(2b+2)} \langle e_-|e_-\rangle \\
p(1,1) &= \tfrac{2b+1}{2p(4b+4)} (\langle e_0|e_0\rangle + \langle e_1|e_1\rangle - \langle e_0|e_1\rangle - \langle e_1|e_0\rangle) \\
p(0,1) &= \tfrac{2b+1}{2p(2b+2)} \langle e_1|e_1\rangle \\
p(1,0) &= \tfrac{1}{2p(4b+4)} (\langle e_+|e_+\rangle + \langle e_-|e_-\rangle - \langle e_+|e_-\rangle + \langle e_-|e_+\rangle).
\end{aligned}$$

Also define $p(x)$ to be the probability that B's raw key bit is x. These values are:

$$\begin{aligned}
p(0) &= \tfrac{1}{2p(4b+4)} (\langle e_+|e_+\rangle + \langle e_-|e_-\rangle - \langle e_+|e_-\rangle - \langle e_-|e_+\rangle) + \tfrac{1}{2p(2b+2)} \langle e_-|e_-\rangle \\
p(1) &= \tfrac{2b+1}{2p(4b+4)} (\langle e_0|e_0\rangle + \langle e_1|e_1\rangle - \langle e_0|e_1\rangle - \langle e_1|e_0\rangle) + \tfrac{2b+1}{2p(2b+2)} \langle e_1|e_1\rangle .
\end{aligned}$$

Thus:

$$\begin{aligned} H(A|B) &= p(0,0)\log_2\left(\tfrac{p(0)}{p(0,0)}\right) + p(1,1)\log_2\left(\tfrac{p(1)}{p(1,1)}\right) \\ &+ p(0,1)\log_2\left(\tfrac{p(1)}{p(0,1)}\right) + p(1,0)\log_2\left(\tfrac{p(0)}{p(1,0)}\right) \end{aligned} \tag{5.9}$$

Up until this point we have been precise; we now however, for the remainder of this section, turn to numerical computations. In particular, the following attack operator was found using the search algorithm we designed in [21].

By the Stinespring Dilation Theorem [52], we can bound the dimension of $\mathcal{H}_E$ by four. Thus, fixing a basis for Eve's ancilla, we may write each state $|e_i\rangle$, for $i \in \{0,1,2,3\}$ as a dimension four vector. Now, consider the following attack operator U (note that the following numbers are approximations subject to precision error, however, since our goal in this section is to get a handle on this protocol's security properties, and not to compute a precise bound, this approximation suffices for our purposes):

$$\begin{aligned} |e_0\rangle &= \begin{pmatrix} -0.4821 + 0.3811i \\ -0.4188 - 0.4250i \\ -0.3895 + 0.2005i \\ 0.0019 + 0.1449i \end{pmatrix} \quad |e_1\rangle = \begin{pmatrix} 0.0801 - 0.0439i \\ -0.1489 - 0.1284i \\ -0.0108 - 0.0414i \\ -0.0664 + 0.0089i \end{pmatrix} \\ |e_2\rangle &= \begin{pmatrix} 0.0005 - 0.0438i \\ -0.0534 - 0.0268i \\ 0.0025 - 0.0897i \\ 0.1213 - 0.1569i \end{pmatrix} \quad |e_3\rangle = \begin{pmatrix} -0.5735 + 0.3219i \\ -0.4934 - 0.2124i \\ -0.2188 - 0.1283i \\ 0.3248 - 0.2371i \end{pmatrix} \end{aligned} \tag{5.10}$$

One may easily verify that this satisfies the requirements of Equation 5.7 to within

a small precision error:

$$\langle e_0|e_0\rangle + \langle e_1|e_1\rangle = 1.000$$
$$\langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1.000$$
$$|\langle e_0|e_2\rangle + \langle e_1|e_3\rangle| < 10^{-5}$$

Furthermore, assume for this attack, that Eve sets $b = 0.04$. Let $Q_{Z,i}$ be the probability that Bob measures a $|i\rangle$ and Alice measures a $|1-i\rangle$. Clearly we have:

$$Q_{Z,0} = \langle e_1|e_1\rangle = 0.053$$
$$Q_{Z,1} = \langle e_2|e_2\rangle = 0.0528$$

Thus we see this attack operator introduces an error rate of 5.3% in the Z basis. The error in the X basis (denoted Q_X) may be computed as:

$$Q_X = tr(|-\rangle\langle -|U_e\rangle\langle U_e|-\rangle\langle -|) = .056$$

To compute $S(\sigma_{AE})$, where $\sigma_{AE} = tr_{TB}(\sigma_{ATBE})$, we first compute the eight eigenvalues of this density matrix. These are found to be: $\{0.4607, 0.0455, 0.4551, 0.0385, 0, 0, 0, 0\}$. Thus: $S(\sigma_{AE}) = 1.4161$. We trace out A and compute the eigenvalues of the resulting density matrix σ_E; these are: $\{0.7760, 0.1788, 0.0443, 0.0009\}$. Thus, $S(\sigma_E) = 0.9359$ resulting in: $S(A|E) = 0.4801$.

Finally, using Equation 5.9, we compute $H(A|B) = 0.4863$. We may then conclude that $r = S(A|E) - H(A|B) = -0.0063$. We have thus shown, using numerical methods, an attack which introduces only 5.6% error (in the X basis - only 5.3% error in the Z basis) yet causes a negative key rate. This bound is of course not tight, but does demonstrate an upper-bound on the tolerated noise level of our protocol. Therefore, it shows that Alice should set her security threshold parameter to such a

value such that she aborts the protocol if she detects such an error rate. This is an upper-bound; in the next section, we will compute a lower bound.

5.5 Effects of Bias on the Key Rate

In this section, we adapt the technique used in Chapter 4.3.3, and apply it to our new protocol. In particular, given an attack operator U, we will compute a bound on the difference between key rate of our protocol when no bias is used, and when bias $b \in [-1/2, 1/2]$ is used. We will also show that, in the event $b = 0$, our protocol's key rate is equal to that of B92. Thus, the result of this chapter is a lower-bound on the key rate of our new SQKD protocol as a function of the key rate of B92, and the bias. This proves the unconditional security of our new SQKD protocol.

To simplify the analysis, we will first modify the protocol slightly. Instead of B randomly rejecting $1/2$ of those iterations he reflected, he will reject $1/2 - b$ of them, where b is E's initial bias (this is something B can estimate, given enough iterations of the protocol). To do so, of course, we must assume that B makes the decision to accept or reject after the protocol has completed. This modification symmetrizes B's key (before A's acceptance).

Let (b, U) be a restricted collective attack as described in Chapter 4. In this case, on each iteration the qubit arriving at B's system is: $|e\rangle_T = \sqrt{1/2 + b}\,|0\rangle + \sqrt{1/2 - b}\,|1\rangle$. Conditioning on the event that B accepts the iteration, the state of the system is:

$$\rho = \frac{1}{2}\,|0\rangle\langle 0|_B \otimes \mathcal{A}\left(U\,|e\rangle\langle e|\,U^*\right) + \frac{1}{2}\,|1\rangle\langle 1|_B \otimes \mathcal{A}\left(U\,|0\rangle\langle 0|\,U^*\right), \tag{5.11}$$

where $\mathcal{A}$ is A's operation (namely, her accepting if she measures $|-\rangle$ or $|1\rangle$ and setting her raw key bit accordingly; otherwise she rejects). Before describing the outcome of

$\mathcal{A}$, let us change basis and write $|e\rangle = \alpha |+\rangle + \beta |-\rangle$, where:

$$\alpha = \frac{1}{\sqrt{2}} \left(\sqrt{\frac{1}{2} + b} + \sqrt{\frac{1}{2} - b} \right)$$
$$\beta = \frac{1}{\sqrt{2}} \left(\sqrt{\frac{1}{2} + b} - \sqrt{\frac{1}{2} - b} \right).$$

Observe that:

$$\alpha^2 = \frac{1}{2} + \sqrt{\frac{1}{4} - b^2}$$
$$\beta^2 = \frac{1}{2} - \sqrt{\frac{1}{4} - b^2}$$
$$\alpha\beta = b.$$

Let U's action (recall U is E's attack operator) be described as follows:

$$U |0\rangle = |0, e_0\rangle + |1, e_1\rangle$$
$$U |+\rangle = |+, f_0\rangle + |1, f_1\rangle$$
$$U |-\rangle = |+, f_2\rangle + |-, f_3\rangle .$$

Thus, conditioning on the event that both A and B accept, Equation 5.11 becomes:

$$\begin{aligned} \rho_{ABE}(b) = \frac{1}{2N_b} \Bigg[& |00\rangle \langle 00|_{BA} \otimes \left(\frac{1}{2} P(\alpha |g_0\rangle + \beta |g_1\rangle) \right) \\ & + |01\rangle \langle 01|_{BA} \otimes P(\alpha |f_1\rangle + \beta |f_3\rangle) \\ & + |10\rangle \langle 10|_{BA} \otimes (|e_1\rangle \langle e_1|) \\ & + |11\rangle \langle 11|_{BA} \otimes \left(\frac{1}{2} P(|e_0\rangle - |e_1\rangle) \right) \Bigg], \end{aligned} \tag{5.12}$$

where $P(z) = zz^*$, $|g_0\rangle = |f_0\rangle - |f_1\rangle$, $|g_1\rangle = |f_2\rangle - |f_3\rangle$, and N_b is the normalization

term:

$$N_b = \frac{1}{2}\left(\frac{\alpha^2}{2}\langle g_0|g_0\rangle + \frac{\beta^2}{2}\langle g_1|g_1\rangle + bRe\langle g_0|g_1\rangle + \alpha^2\langle f_1|f_1\rangle + \beta^2\langle f_3|f_3\rangle \right.$$
$$\left. + 2bRe\langle f_1|f_3\rangle + \langle e_1|e_1\rangle + \frac{1}{2}(1 - 2Re\langle e_0|e_1\rangle)\right).$$

Note that N_b is exactly the probability that both A and B accept any particular iteration. We will assume throughout the rest of this section that $N_b > 0$. Otherwise, if $N_b = 0$, then no key is distilled and $r(b, U) = 0$.

Before continuing, we will require a small lemma, which is easily proven:

Lemma 5.5.1. Let $\sigma = |a\rangle\langle b| + |b\rangle\langle a|$, where $|a\rangle, |b\rangle \in \mathcal{H}$, for some finite dimensional Hilbert space $\mathcal{H}$ (neither states are necessarily normalized nor orthogonal). Then:

$$||\sigma|| \leq 4\sqrt{\langle a|a\rangle\langle b|b\rangle}.$$

Proof. Observe that σ is Hermitian, thus to compute $||\sigma||$, we must simply compute its eigenvalues. Write $|a\rangle = xe^{i\theta}|g\rangle$ and $|b\rangle = ye^{i\psi}|g\rangle + z|\zeta\rangle$ where $\langle g|g\rangle = 1$, $\langle g|\zeta\rangle = 0$, $x, y \in \mathbb{R}_{\geq 0}$, and $z \in \mathbb{C}$. Note that this implies:

$$x = \sqrt{\langle a|a\rangle} \tag{5.13}$$
$$\sqrt{y^2 + |z|^2} = \sqrt{\langle b|b\rangle}.$$

In this $\{|g\rangle, |\zeta\rangle\}$ basis, we may write σ as follows:

$$\sigma = \begin{pmatrix} 2xy\cos(\theta - \psi) & xe^{i\theta}z^* \\ xe^{-i\theta}z & 0 \end{pmatrix},$$

in which case the eigenvalues are simply:

$$\lambda_{\pm} = xy\cos(\theta-\psi) \pm \sqrt{x^2y^2\cos^2(\theta-\psi) + x^2|z^2|}.$$

Now:

$$\begin{aligned}
||\sigma|| = |\lambda_+| + |\lambda_-| &\leq 2xy|\cos(\theta-\psi)| + 2\sqrt{x^2y^2\cos^2(\theta-\psi) + x^2|z^2|} \\
&\leq 2xy + 2\sqrt{x^2y^2 + x^2|z|^2} = 2xy + 2\sqrt{x^2(y^2+|z|^2)} \\
&\leq 2\sqrt{\langle a|a\rangle\langle b|b\rangle} + 2\sqrt{\langle a|a\rangle\langle b|b\rangle} \\
&= 4\sqrt{\langle a|a\rangle\langle b|b\rangle}.
\end{aligned}$$

The last inequality follows from Equation 5.13 and the simple observation that, since $y \geq 0$, we have: $y = \sqrt{y^2} \leq \sqrt{y^2+|z|^2} = \sqrt{\langle b|b\rangle}$. □

We may now continue with our bound on the effects of E's bias attack on our new protocol. Let $r(b,U)$ be the key rate of this protocol, assuming E uses the attack (b,U). That is,

$$r(b,U) = S(B|E) - S(B|A) = S(\rho_{BE}(b)) - S(\rho_E(b)) - S(\rho_{BA}(b)) + S(\rho_A(b)).$$

(Note that we have used $S(B|A)$ above instead of $H(B|A)$; however since the system is classical, the two entropies are equal.)

Then, by the triangle inequality, we have:

$$\begin{aligned}
|r(0,U) - r(b,U)| \leq\ & |S(\rho_{BE}(0)) - S(\rho_{BE}(b))| + |S(\rho_E(0)) - S(\rho_E(b))| \\
&+ |S(\rho_{AB}(0)) - S(\rho_{AB}(b))| + |S(\rho_A(0)) - S(\rho_A(b))|.
\end{aligned} \tag{5.14}$$

Unfortunately, there is less structure in this state to take advantage of, as compared to the protocol considered in Chapter 4. Due to this, we are forced to bound each term separately using the Fannes-Audenaert inequality [51]. Recall that this inequality states, for any finite dimensional density operators ρ and σ (both of the same dimension D), it holds that:

$$|S(\rho) - S(\sigma)| \leq T \log(D-1) + h(T),$$

where $T = \frac{1}{2}||\rho - \sigma||$. Thus, our primary goal is to compute bounds on these trace distances.

We first compute a bound on $|S(\rho_{BE}(0)) - S(\rho_{BE}(b))|$. Let $\sigma = \rho_{BE}(0) - \rho_{BE}(b)$. This density operator is:

$$\begin{aligned}\sigma = &\frac{1}{2}|0\rangle\langle 0|_B \otimes \left[\frac{1}{2}\left(\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right)|g_0\rangle\langle g_0| - \frac{\beta^2}{2N_b}|g_1\rangle\langle g_1| - \frac{b}{2N_b}(|g_0\rangle\langle g_1| + |g_1\rangle\langle g_0|)\right.\\ &\left. + \left(\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right)|f_1\rangle\langle f_1| - \frac{\beta^2}{N_b}|f_3\rangle\langle f_3| - \frac{b}{N_b}(|f_1\rangle\langle f_3| + |f_3\rangle\langle f_1|)\right]\\ &+ \frac{1}{2}|1\rangle\langle 1|_B \otimes \left[\left(\frac{1}{N_0} - \frac{1}{N_b}\right)|e_1\rangle\langle e_1| + \frac{1}{2}\left(\frac{1}{N_0} - \frac{1}{N_b}\right)P(|e_0\rangle - |e_1\rangle)\right].\end{aligned}$$

Let $T_1 = \frac{1}{2}||\sigma||$. Using the triangle inequality and the fact that $||\,|i\rangle\langle i| \otimes \rho|| = ||\rho||$ for any density operator ρ, we have:

$$\begin{aligned}T_1 \leq &\frac{1}{8}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| \cdot ||\,|g_0\rangle\langle g_0|\,|| + \frac{\beta^2}{8N_b}||\,|g_1\rangle\langle g_1|\,|| + \frac{|b|}{8N_b}||\,|g_0\rangle\langle g_1| + |g_1\rangle\langle g_0|\,||\\ &+ \frac{1}{4}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| \cdot ||\,|f_1\rangle\langle f_1|\,|| + \frac{\beta^2}{4N_b}||\,|f_3\rangle\langle f_3|\,|| + \frac{|b|}{4N_b}||\,|f_1\rangle\langle f_3| + |f_3\rangle\langle f_1|\,||\\ &+ \frac{1}{4}\left|\frac{1}{N_0} - \frac{1}{N_b}\right| \cdot ||\,|e_1\rangle\langle e_1|\,|| + \frac{1}{8}\left|\frac{1}{N_0} - \frac{1}{N_b}\right| \cdot ||P(|e_0\rangle - |e_1\rangle)||.\end{aligned}$$

Let $\langle f_0|f_0\rangle = x$ (thus $\langle f_1|f_1\rangle = 1-x$ by unitarity of U). Using the Cauchy-Schwarz

inequality, we have $1 - 2Re\langle f_0|f_1\rangle \leq 1 + 2\sqrt{x(1-x)} \leq 2$. Similarly, $\langle g_0|g_0\rangle, \langle g_1|g_1\rangle$ are both less than 2. Then, using Lemma 5.5.1, and also the fact that $||M|| = trM$ for any positive operator M (in particular if $M = P(z)$ for some z):

$$T_1 \leq \frac{1}{4}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| + \frac{\beta^2}{4N_b} + \frac{|b|}{N_b} + \frac{1}{4}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| + \frac{\beta^2}{4N_b} + \frac{|b|}{N_b} + \frac{1}{2}\left|\frac{1}{N_0} - \frac{1}{N_b}\right|$$

$$= \frac{1}{2}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| + \frac{\beta^2}{2N_b} + \frac{2|b|}{N_b} + \frac{1}{2}\left|\frac{1}{N_0} - \frac{1}{N_b}\right|. \tag{5.15}$$

Observe that if $b = 0$, then $\alpha^2 = 1$ and $\beta^2 = 0$, thus $T_1 = 0$ as we would expect.

Note that, the same process may be used to bound $T_2 = \frac{1}{2}||\rho_E(0) - \rho_E(b)||$ (here, we no longer need the fact that $||\,|i\rangle\langle i| \otimes \sigma|| = ||\sigma||$). Thus, all that remains is to bound the change in $S(B|A)$.

We will first bound $|S(\rho_{AB}(0)) - S(\rho_{AB}(b))|$. Let $p_b(x, y)$ be the probability that B's key bit is x and A's key is y if bias b is used. From Equation 5.12, these values are:

$$\begin{aligned}
p_b(0,0) &= \frac{1}{4N_b}\left(\alpha^2\langle g_0|g_0\rangle + \beta^2\langle g_1|g_1\rangle + 2bRe\langle g_0|g_1\rangle\right) \\
p_b(0,1) &= \frac{1}{2N_b}\left(\alpha^2\langle f_1|f_1\rangle + \beta^2\langle f_3|f_3\rangle + 2bRe\langle f_1|f_3\rangle\right) \\
p_b(1,0) &= \frac{1}{2N_b}\langle e_1|e_1\rangle \\
p_b(1,1) &= \frac{1}{4N_b}(1 - 2Re\langle e_0|e_1\rangle)
\end{aligned}$$

Let $T_2 = \frac{1}{2}||\rho_{AB}(0) - \rho_{AB}(b)|| = \frac{1}{2}\sum_{x,y}|p_0(x,y) - p_b(x,y)|$. Thus, to bound T_2, we must bound $\delta_b(x,y) = |p_0(x,y) - p_b(x,y)|$ for all $x, y \in \{0,1\}$. These bounds are computed as follows:

$$\delta_b(0,0) \leq \left|\frac{1}{4N_0} - \frac{\alpha^2}{4N_b}\right| \langle g_0|g_0\rangle + \left|\frac{\beta^2}{4N_B}\right| \langle g_1|g_1\rangle + \left|\frac{b}{2N_b}\right| \cdot |Re\,\langle g_0|g_1\rangle\,|$$
$$\leq \frac{1}{2}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| + \frac{1}{2}\left|\frac{\beta^2}{N_b}\right| + \left|\frac{b}{N_b}\right|$$

$$\delta_b(0,1) \leq \left|\frac{1}{2N_0} - \frac{\alpha^2}{2N_b}\right| \langle f_1|f_1\rangle + \left|\frac{\beta^2}{2N_b}\right| \langle f_3|f_3\rangle + \left|\frac{b}{N_b}\right| \cdot |Re\,\langle f_1|f_3\rangle\,|$$
$$\leq \frac{1}{2}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| + \frac{1}{2}\left|\frac{\beta^2}{N_b}\right| + \left|\frac{b}{N_b}\right|$$

$$\delta_b(1,0) \leq \left|\frac{1}{2N_0} - \frac{1}{2N_b}\right| \langle e_1|e_1\rangle \leq \frac{1}{2}\left|\frac{1}{N_0} - \frac{1}{N_b}\right|$$

$$\delta_b(1,1) \leq \left|\frac{1}{4N_0} - \frac{1}{4N_b}\right| \cdot |1 - 2Re\,\langle e_0|e_1\rangle\,| \leq \frac{1}{2}\left|\frac{1}{N_0} - \frac{1}{N_b}\right|.$$

Thus:

$$T_2 = \frac{1}{2}\sum_{x,y} \delta_b(x,y) \leq \frac{1}{2}\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| + \frac{1}{2}\left|\frac{\beta^2}{N_b}\right| + \left|\frac{b}{N_b}\right| + \frac{1}{2}\left|\frac{1}{N_0} - \frac{1}{N_b}\right|. \tag{5.16}$$

It is not difficult to show that $\frac{1}{2}||\rho_A(0) - \rho_A(b)||$ may be upper bounded by the same quantity (by use of the triangle inequality). Thus we have:

$$|S(\rho_{BE}(0)) - S(\rho_{BE}(b))| \leq T_1 \log 7 + h(T_1)$$
$$|S(\rho_{E}(0)) - S(\rho_{E}(b))| \leq T_1 \log 3 + h(T_1)$$
$$|S(\rho_{AB}(0)) - S(\rho_{AB}(b))| \leq T_2 \log 3 + h(T_2)$$
$$|S(\rho_{A}(0)) - S(\rho_{A}(b))| \leq T_2 \log 1 + h(T_2) = h(T_2),$$

and so, from Equation 5.14:

$$|r(U,0) - r(U,b)| \leq T_1 \log 21 + T_2 \log 3 + 2h(T_1) + 2h(T_2), \tag{5.17}$$

where T_1 is bounded by Equation 5.15 and T_2 is bounded by Equation 5.16. So long as these upper-bounds are no greater than $1/2$, they may be used to upper bound Equation 5.17; if they are larger than $1/2$, they may be capped at that value (the binary entropy function $h(x)$ taking its maximum when $x = 1/2$).

In practice, this should be sufficient to generate a bound on the key rate, as the quantity N_b may be estimated directly (N_0 may be estimated as described below). However, if we wish to compute a bound based only on the bias b, we must continue forward and bound those terms which appear in T_1 and T_2 which rely on N_b.

First, since we are assuming N_0 and N_b are both non zero, we have:

$$\left|\frac{1}{N_0} - \frac{\alpha^2}{N_b}\right| = \frac{1}{N_0 N_b}|N_b - \alpha^2 N_0|$$
$$\left|\frac{1}{N_0} - \frac{1}{N_b}\right| = \frac{1}{N_0 N_b}|N_b - N_0|.$$

From this, we may bound:

$$\begin{aligned}
|N_b - \alpha^2 N_0| &= \left| \frac{\beta^2}{4} \langle g_1|g_1\rangle + \frac{b}{2} Re\,\langle g_0|g_1\rangle + \frac{\beta^2}{2} \langle f_3|f_3\rangle + bRe\,\langle f_1|f_3\rangle \right. \\
&\quad \left. + \frac{1}{2}(1-\alpha^2)\langle e_1|e_1\rangle + \frac{1}{4}(1-\alpha^2)(1-2Re\,\langle e_0|e_1\rangle) \right| \\
&\leq \beta^2 \left| \frac{1}{4}\langle g_1|g_1\rangle + \frac{1}{2}\langle f_3|f_3\rangle + \frac{1}{2}\langle e_1|e_1\rangle + \frac{1}{4}(1-2Re\,\langle e_0|e_1\rangle) \right| \\
&\quad + b \left| \frac{1}{2} Re\,\langle g_0|g_1\rangle + Re\,\langle f_1|f_3\rangle \right| \\
&\leq 2\beta^2 + 2|b|,
\end{aligned}$$

where the first inequality follows from the fact that $\alpha^2 + \beta^2 = 1 \Rightarrow \beta^2 = 1 - \alpha^2$. Similar algebra yields:

$$|N_b - N_0| \leq 2\beta^2 + 2|b|. \tag{5.18}$$

All that remains is to lower bound N_b (thus upper-bounding $1/N_0N_b$). Observe that N_b may be written as the sum of four non-negative values: $N_b = p_{00} + p_{01} + p_{10} + p_{11}$, where p_{ij} is the probability that A and B's raw key bit is j, i respectively, conditioning on the event they both accept. That is (from Equation 5.12):

$$
\begin{aligned}
p_{00} &= \frac{\alpha^2}{4}\langle g_0|g_0\rangle + \frac{\beta^2}{4}\langle g_1|g_1\rangle + \frac{b}{2}Re\langle g_0|g_1\rangle \\
p_{01} &= \frac{\alpha^2}{2}\langle f_1|f_1\rangle + \frac{\beta^2}{2}\langle f_3|f_3\rangle + bRe\langle f_1|f_3\rangle \\
p_{10} &= \frac{1}{2}\langle e_1|e_1\rangle \\
p_{11} &= \frac{1}{4}(1 - 2Re\langle e_0|e_1\rangle).
\end{aligned}
$$

By unitarity of U, these quantities are non-negative. Thus, we may trivially bound:

$$N_b \geq p_{10} + p_{11} \geq \frac{1}{2}Q + \frac{1}{4}(1 - 2\sqrt{Q(1-Q)}),$$

where $Q = \langle e_1|e_1\rangle$ is the probability of a $|0\rangle$ flipping to a $|1\rangle$ in the return channel. (Note that we used the Cauchy-Schwarz inequality to bound $Re\langle e_0|e_1\rangle \geq -\sqrt{Q(1-Q)}$.) It is not difficult to show numerically that this function is lower bounded by .146, thus giving us a bound on the quantities T_1 and T_2 (and thus a bound on the difference in the key rate $r(b, U)$) as functions only of b.

As future work, it might be possible to improve this bound. In practice, however, one may simply estimate N_b exactly (this is simply the probability of accepting an iteration) and use Equation 5.18 to determine bounds on T_1 and T_2.

It is not difficult to see that, in the absence of bias (i.e., $b = 0$), the protocol is similar to B92 [2]. Indeed, in this case, the state leaving B is $|+\rangle$ with probability 1/2 or $|0\rangle$ with probability 1/2. The only difference between the two protocols is that the users of our semi-quantum version may estimate the values of $|e_i\rangle$ directly for all $i = 0, 1, 2, 3$ (whereas in B92, only $|e_0\rangle$ and $|e_1\rangle$ may be estimated). Thus, the key rate can be no worse than B92 in this instance, and, therefore, a user of our protocol may use the techniques from [22] to first bound $r(0, U)$ (no exact equation for B92

exists as far as we are aware - unlike the three state BB84 case considered earlier) followed by the procedure described at the end of Chapter 4.3.3 to lower bound r_b, the key rate of our protocol optimized over all possible attack operators U. So long as this bound is greater than zero, A and B need not abort.

Chapter 6

Mediated Semi-Quantum Key Distribution

Up until now, we have considered the following scenario: there are two users A and B who wish to establish a secret key, secure against an all-powerful adversary E. Further, while the user A is fully quantum, the user B is "classical" or semi-quantum. In this chapter, we consider the case when both A and B are classical in nature.

Clearly this cannot be done without some form of additional quantum resources (otherwise A and B might as well use a standard classical channel). Thus, we add to this picture a third party: a quantum server or center C which is capable of producing and working with quantum resources (e.g., he is able to produce and measure qubits in a variety of bases). We call such a protocol a *mediated semi-quantum key distribution protocol*. This task would be trivial if C were trusted; instead we are going to assume that C is adversarial. We will also assume that there may be an additional third-party attacker E (independent of A, B, and C). Despite this, we will show it is possible for classical A and B to distill a secure secret key. See Figure 6.1 for a diagram of the situation we consider in this chapter.

In this chapter, we will first discuss our protocol. Following this, we will show its unconditional security by computing a lower-bound on its key rate in the asymptotic scenario. This bound will be a function of several parameters which may be estimated by A and B. The information in this chapter is derived from a paper we submitted in [53].

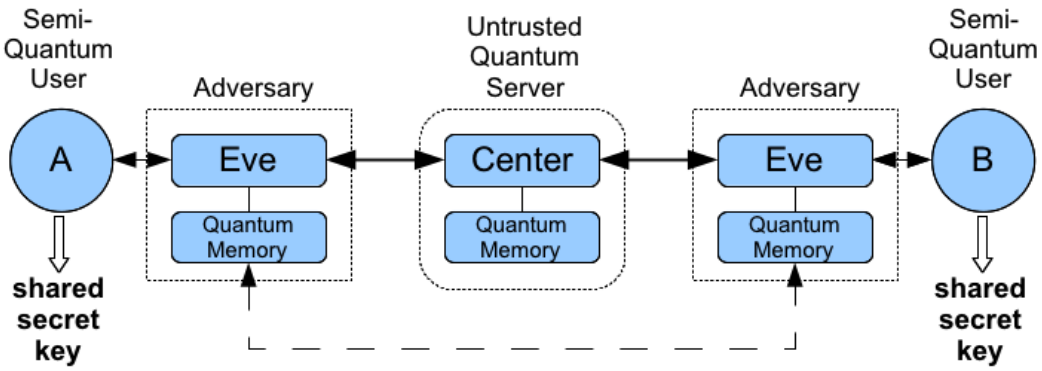

Figure 6.1: A diagram of the situation we consider in this chapter. Here, there are two semi-quantum users A and B. A quantum communication line connects these users to an untrusted and adversarial quantum server. Furthermore, there may be additional eavesdroppers attacking each of the quantum channels.

6.1 The Protocol

Our protocol requires a quantum communication channel connecting the quantum server/center C to A and also to B (there is no need for a channel connecting A directly to B). We also assume an authenticated classical channel connecting A to B and an unauthenticated classical channel connecting C to one of A or B (possibly both). Any message that the server sends to A or B is automatically forwarded by that party to the other user via the authenticated channel (e.g., if C sends a message to A, she will then forward it to B over the authenticated channel). This ensures that C cannot send different messages to each user separately (without being caught in which case A and B will simply abort). In fact, from now on, we will simply assume that C sends a single message to both parties.

Note that the channel connecting the server to A and/or B is not required to be authenticated. Indeed, at first, we will assume that C is the only adversary in which case it makes no sense for his messages to be authenticated. Later, when we consider third-party attackers E, these users may arbitrarily alter C's messages. However,

in this case, their attack may be "absorbed" into C's attack and thus the security bounds we prove hold even then. There may be more optimistic security bounds, however, if we assume C is trusted and his channel is authenticated - a scenario we will consider later.

Our protocol requires preparation and measurements in the Bell basis, the states of which are defined as:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$
$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

We will describe our protocol first assuming the center C is perfectly honest and trustworthy. In this case, the protocol repeats the following procedure:

1. C will prepare the Bell state $|\Phi^{+}\rangle$ and send one particle to A, the other to B.

2. A will choose randomly either to reflect the qubit (this with probability p_R^A) or to measure and resend it (this with probability $p_M^A = 1 - p_R^A$). If A measures and resends, the measurement result is saved as her potential raw key bit for this iteration.

3. B will also choose randomly, and independently of A, to reflect or measure and resend (with probabilities p_R^B and p_M^B respectively). If B measures and resends, the measurement result is saved as his potential raw key bit for this iteration.

4. C receives both qubits back from A and B (neither of whom have yet divulged their choice to reflect or measure and resend). He will then perform a Bell measurement. If his result is $|\Phi^{-}\rangle$ he will send to A and B the classical message "-1". For any other measurement result, C will send the message "$+1$".

5. A and B will now disclose (over the authenticated channel) their choice to reflect or measure and resend:

   - If they both measured and resent, and if C sent "-1", they will keep their raw key bits; otherwise this iteration is discarded
   - If A and B both reflected, C should have sent the message "$+1$" - if C sent the message "-1", they will count this round as an error.

Notice that this protocol only uses those iterations where both A and B measure and resend and C sends "-1". Assuming an honest C and no additional noise, this implies that, after repeating the process above N times, the size of the raw key is expected to be $Np_M^A p_M^B/2$. Of course, following the example of [50], we may set p_M^A and p_M^B arbitrarily close to one improving the raw key size to roughly $N/2$. It is an open question as to whether or not a mediated SQKD protocol may be developed which attains a greater efficiency.

As is usual, after running the above process, A and B will divulge certain measurement results permitting them to gauge various statistics of the quantum channel (and C's attack). If the error rate is low enough (to be determined), they will then run an error correction and privacy amplification protocol to distill a final, secure, secret key.

6.2 Collective Attacks

We now consider the security of our protocol assuming an untrusted and adversarial center. In this case, the center C will prepare any arbitrary state in step (1) of the protocol (though we will assume he is limited to sending a single qubit each iteration to each party - an assumption used in the proofs of other SQKD protocols up to now). This state may possibly be entangled with his private ancilla. Then, on

step (4), C will perform any arbitrary operation of his choice allowed by the laws of physics. This operation may include additional, unmeasured, information in quantum memory. However, he is restricted to sending only a single message "+1" or "−1" to each user A and B, and this message must be the same for both parties.

We will first consider collective attacks. In this case, the center will perform the same attack operation each iteration. This attack will be modeled as follows: on step (1), C will not necessarily send $|\Phi^+\rangle$, but instead any arbitrary state of his choosing $|\psi_0\rangle \in \mathcal{H}$, where:

$$\mathcal{H} = \mathcal{H}_{T_A} \otimes \mathcal{H}_{T_B} \otimes \mathcal{H}_C.$$

We use the two dimensional Hilbert spaces $\mathcal{H}_{T_A}$ and $\mathcal{H}_{T_B}$ to model the qubit sent (or "transmitted") to A and B respectively. $\mathcal{H}_C$ will be used to model C's private ancilla which, without loss of generality, we may assume to be finite dimensional.

We may assume, also without loss of generality, that the state C sends is pure (otherwise C may purify it). In this case, this state $|\psi_0\rangle$ may be written as:

$$|\psi_0\rangle = \sum_{i,j\in\{0,1\}} \alpha_{i,j} \, |i,j\rangle_{T_A,T_B} \otimes |c_{i,j}\rangle_C \,, \tag{6.1}$$

where each $\alpha_{i,j} \in \mathbb{C}$ such that $\sum_{i,j} |\alpha_{i,j}|^2 = 1$. The states $|c_{i,j}\rangle$ we take to be normalized, but not necessarily orthogonal.

When the qubits return to C on step (4) (after A and B's operations), we allow C to perform any operation of his choice on the entire system living in $\mathcal{H}$. Since he must additionally send a single classical bit (his message to A and B), we will model this attack as a *quantum instrument* [54]. This instrument, denoted $\mathcal{I}$ acts on density

matrices ρ as follows:

$$\mathcal{I}(\rho) = \sum_{k=1}^{N_0} E_{k,0}\rho E_{k,0}^* \otimes |+1\rangle\langle+1|_{cl} + \sum_{k=1}^{N_1} E_{k,1}\rho E_{k,1}^* \otimes |-1\rangle\langle-1|_{cl}\,, \tag{6.2}$$

such that:

$$\sum_{k=1}^{N_0} E_{k,0}^* E_{k,0} + \sum_{k=1}^{N_1} E_{k,1}^* E_{k,1} = I.$$

We may assume, in our case, that N_0 and N_1 are both finite.

Observe that, in the above, we have expanded our Hilbert space by adding the subspace $\mathcal{H}_{cl}$ spanned by orthonormal basis $\{|+1\rangle_{cl}, |-1\rangle_{cl}\}$. This will be used to model C's classical message, sent to A and B. Since C cannot send different messages to different users (without being caught and thus causing the protocol to abort), this is sufficient.

6.2.1 An Unentangled Initial State

The first step of the proof is to simplify the state $|\psi_0\rangle$ that C initially sends in step (1) (Equation 6.1). We will show, using a technique similar to the proof of Theorem 4.2.1, that, without any loss of power to C, he may instead send the far simpler state $|\psi_0'\rangle = \sum_{i,j} \alpha_{i,j} |i,j\rangle$ (which is unentangled with his private ancilla).

Indeed, assume that C initially sends the state $|\psi_0\rangle$ from Equation 6.1. Also assume that either both A and B reflected, or they both measured and resent (any other case is discarded by our protocol). Then, on step (4), when he receives the qubits back, the system is in the mixed state (up to a normalization term):

$$\rho = p_R^A \cdot p_R^B |\psi_0\rangle\langle\psi_0| + p_M^A \cdot p_M^B \left(\sum_{i,j\in\{0,1\}} |\alpha_{i,j}|^2 |i,j,c_{i,j}\rangle\langle i,j,c_{i,j}| \right),$$

If, however, C sends the simpler state $|\psi_0'\rangle$, the state on step (4) is, again up to the same normalization term as before:

$$\rho' = p_R^A p_R^B \left|\psi_0'\right\rangle \left\langle\psi_0'\right| \otimes |0\rangle \langle 0|_C + p_M^A \cdot p_M^B \left(\sum_{i,j} |\alpha_{i,j}|^2 |i,j\rangle \langle i,j| \otimes |0\rangle \langle 0|_C \right).$$

(Note that we have assumed C's ancilla is cleared to some known "zero" state $|0\rangle_C$; this is without loss of generality.)

From this point, a unitary operator V may be constructed which sends $|i,j,0\rangle$ to $|i,j,c_{i,j}\rangle$. Clearly $V\rho'V^* = \rho$ and so, there is no advantage to C sending $|\psi_0\rangle$ initially.

6.2.2 A Unitary Attack Operator

The next step in the proof is to simplify C's attack on step (4) by showing it is equivalent to a unitary attack operator. To do this, we will use standard techniques (such as in [23, 55]) to represent the quantum instrument $\mathcal{I}$ as a unitary operator acting on a larger Hilbert space. Giving C access to this larger space, only increases his power, thus providing us with a lower-bound on the security of our protocol.

Let $\mathcal{I}$ be C's quantum instrument (see Equation 6.2). Define the isometry $U_{\mathcal{I}}$ in the following manner:

$$U_{\mathcal{I}} := \sum_{k=1}^{N_0} E_{k,0} \otimes |k\rangle_{E_1} |0\rangle_{E_2} |+1\rangle_{cl} + \sum_{k=1}^{N_1} E_{k,1} \otimes |N_0 + k\rangle_{E_1} |1\rangle_{E_2} |-1\rangle_{cl}.$$

It is not difficult to show that $U_{\mathcal{I}}$ is an isometry mapping $\mathcal{H}$ to $\mathcal{H} \otimes \mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2} \otimes \mathcal{H}_{cl}$, where the subspace $\mathcal{H}_{E_1}$ is spanned by the orthonormal basis $\{|i\rangle_{E_1} \mid i = 1, \cdots, N_0 + N_1\}$ and $\mathcal{H}_{E_2}$ is the subspace spanned by orthonormal basis $\{|0\rangle_{E_2}, |1\rangle_{E_1}\}$. It is also

not difficult to show that it is an isometry:

$$\begin{aligned} U_{\mathcal{I}}^* U_{\mathcal{I}} &= \left(\sum_{k=1}^{N_0} E_{k,0}^* \otimes \langle k,0,+1| + \sum_{k=1}^{N_1} E_{k,1}^* \otimes \langle N_0+k,1,-1|\right) \\ &\cdot \left(\sum_{k=1}^{N_0} E_{k,0} \otimes |k,0,+1\rangle + \sum_{k=1}^{N_1} E_{k,1} \otimes |N_0+k,1,-1\rangle\right) \\ &= \sum_{k=1}^{N_0} E_{k,0}^* E_{k,0} \otimes \langle k,0,+1|k,0,+1\rangle \\ &+ \sum_{k=1}^{N_1} E_{k,1}^* E_{k,1} \otimes \langle N_0+k,1,-1|N_0+k,1,-1\rangle \\ &= \sum_{k=1}^{N_0} E_{k,0}^* E_{k,0} + \sum_{k=1}^{N_1} E_{k,1}^* E_{k,1} = I. \end{aligned}$$

Finally, given $|\psi\rangle \in \mathcal{H}$, it is clear that:

$$tr_{E_1,E_2}(U_{\mathcal{I}} |\psi\rangle \langle\psi| U_{\mathcal{I}}^*) \equiv \mathcal{I}(|\psi\rangle \langle\psi|).$$

(Due to linearity, this is also true for any mixed state.)

Now, assume that C has access to the subspace $\mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2}$ (this can only increase his power). We may also assume, without loss of generality, that on step (4), when C receives the qubits from A and B, that the entire quantum system may be described by the state $|\psi,0,0,0,0\rangle \in \mathcal{H} \otimes \mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2} \otimes \mathcal{H}_{cl}$. That is, this "ancilla" $\mathcal{H}_C \otimes \mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2} \otimes \mathcal{H}_{cl}$ is cleared to an arbitrary "zero" state.

Lastly, the isometry $U_{\mathcal{I}}$ may be extended to a unitary operator, which we denote $\mathcal{U}_{\mathcal{I}}$ in such a manner so that $\mathcal{U}_{\mathcal{I}} |\psi,0,0,0,0\rangle \equiv U_{\mathcal{I}} |\psi,0\rangle$. Its action on states $|\psi,k,i,j,l\rangle$ for $k,i,j,l \neq 0$ is not relevant.

We therefore have:

$$tr_{E_1,E_2}\left(\mathcal{U}_{\mathcal{I}} |\psi,0,0,0,0\rangle \langle\psi,0,0,0,0| \mathcal{U}_{\mathcal{I}}^*\right) = tr_{E_1,E_2}\left(U_{\mathcal{I}} |\psi\rangle \langle\psi| U_{\mathcal{I}}^*\right) = \mathcal{I}(|\psi\rangle \langle\psi|),$$

and so we conclude that it is sufficient to consider only unitary attack operators on step (4) when proving the security of our protocol. If C sends the classical message "+1", this is equivalent to projecting the above state's $\mathcal{H}_{cl}$ portion to $|+1\rangle_{cl}$. Likewise for C sending the message "-1". Thus, C's choice determining which message to send to A and B, followed by the state resulting from such a decision (Equation 6.2), is equivalent to a projective measurement of the $\mathcal{H}_{cl}$ subspace in the $\{|+1\rangle_{cl}, |-1\rangle_{cl}\}$ basis. From here on, we will also absorb the auxiliary subspaces $\mathcal{H}_{E_1}$ and $\mathcal{H}_{E_2}$ into $\mathcal{H}_C$.

6.2.3 Bounding the Key Rate

Recall that the key rate of a QKD protocol (semi-quantum or otherwise) in the asymptotic scenario is defined to be:

$$r = \lim_{N\to\infty} \frac{\ell(N)}{N},$$

where N is the size of the raw key and $\ell(N)$ is the size of the secure secret key (possibly zero). It was shown in [29, 22] that, assuming collective attacks:

$$r = I(A:B) - I(A:C),$$

where $I(A:C)$ is the quantum mutual information held between A and C. This is defined to be:

$$I(A:C) = S(\rho_A) + S(\rho_C) - S(\rho_{AC}).$$

Similarly, $I(A:B)$ is the (classical) mutual information held between A and B. Note that this equation is exactly equivalent to Equation 2.6 which we used in previous chapters. However, for this mediated protocol, it turns out the mutual information

version is easier to work with.

Note that, after the completion of the quantum communication stage, after parameter estimation, but before error correction and privacy amplification, a single iteration of our protocol may be described by the following state:

$$\rho_{ABC} = \sum_{x,y \in \{0,1\}} p(x,y) \left|x,y\right\rangle \left\langle x,y\right| \otimes \rho_C^{(x,y)},$$

where $p(x,y)$ denotes the probability that A and B's raw key bits are x and y respectively, and $\rho_C^{(x,y)}$ represents the state of C's ancilla in this event (which depends on the protocol and C's attack). For such a state, it is not difficult to show that:

$$I(A:C) = S(\rho_C) - \sum_{x \in \{0,1\}} p(x) S\left(\rho_C^{(x)}\right).$$

(In the above, we have traced out B's system.)

Recall that, given a matrix A, we denote its trace norm by $||A||$. Furthermore, if A is an $n \times n$ Hermitian matrix with eigenvalues $\{\lambda_i\}_{i=1}^n$, then $||A|| = \sum_{i=1}^n |\lambda_i|$. Using a result from [56], which claims that:

$$S(\rho_C) - \frac{1}{2} S\left(\rho_C^{(0)}\right) - \frac{1}{2} S\left(\rho_C^{(1)}\right) \leq \frac{1}{2} \left|\left|\rho_C^{(0)} - \rho_C^{(1)}\right|\right|, \tag{6.3}$$

we can bound $I(A:C)$ as follows:

$$I(A:C) = S(\rho_C) - \frac{1}{2} S\left(\rho_C^{(0)}\right) - \frac{1}{2} S\left(\rho_C^{(1)}\right) \leq \frac{1}{2} \left|\left|\rho_C^{(0)} - \rho_C^{(1)}\right|\right|. \tag{6.4}$$

We will use this bound shortly.

6.2.4 Bounding $I(A:C)$

Before we can continue, we require a small lemma:

Lemma 6.2.1. Let $\rho = |a\rangle\langle b| + |b\rangle\langle a|$, where $|a\rangle, |b\rangle \in \mathcal{H}_D$ for some D-dimensional Hilbert space $\mathcal{H}_D$ ($D < \infty$). We place no restrictions on $|a\rangle$ and $|b\rangle$ besides that $tr\rho = 0$. Then it holds that:

$$||\rho|| \leq 2\sqrt{\langle a|a\rangle\langle b|b\rangle}.$$

Proof. Since ρ is Hermitian, to compute $||\rho||$, we must find its eigenvalues. Write $|a\rangle = \alpha|\tilde{a}\rangle$, and $|b\rangle = x|\tilde{a}\rangle + y|\zeta\rangle$ where $\alpha, x, y \in \mathbb{C}$ and $|\tilde{a}\rangle$ and $|\zeta\rangle$ are orthonormal. Clearly this implies $|\alpha|^2 = \langle a|a\rangle$, $|x|^2 + |y|^2 = \langle b|b\rangle$, and $\langle a|b\rangle = \alpha^* x$. Also note that since ρ has trace zero, this implies $\langle a|b\rangle + \langle b|a\rangle = \alpha^* x + x^*\alpha = 0$.

Choosing a suitable basis for $\mathcal{H}_D$, the first two entries of which are $\{|\tilde{a}\rangle, |\zeta\rangle\}$, we may write ρ as:

$$\rho \equiv \begin{pmatrix} \sigma & 0 \\ 0 & 0 \end{pmatrix},$$

where the 2×2 matrix σ is defined as:

$$\sigma = \begin{pmatrix} 0 & \alpha y^* \\ \alpha^* y & 0 \end{pmatrix}.$$

From this, we see there are two non-zero eigenvalues of ρ:

$$\lambda_\pm = \pm\sqrt{|\alpha|^2|y|^2} = \pm\sqrt{\langle a|a\rangle(\langle b|b\rangle - |x|^2)},$$

and so:

$$||\rho|| = |\lambda_-| + |\lambda_+| = 2\lambda_+ = 2\sqrt{\langle a|a\rangle\left(\langle b|b\rangle - |x|^2\right)} \leq 2\sqrt{\langle a|a\rangle\,\langle b|b\rangle}, \tag{6.5}$$

where the inequality follows from the observation that $|x|^2$ and $\langle a|a\rangle$ are non-negative.

□

This result will be useful later. Note the difference between this result, and Lemma 5.5.1; the latter did not require the operator to be of trace zero. We can now return to our protocol.

Define $p_{i,j}$ to be the probability that, if A and B perform a measurement (on step (2) and (3) of the protocol), the joint outcome is $|i,j\rangle$. As in [57] (where the B92 [2] protocol was proved secure), we may restrict our attention to "symmetric" attacks and enforce the condition that $p_{0,0} = p_{1,1} = (1-Q)/2$ and $p_{0,1} = p_{1,0} = Q/2$. Here Q is used to represent the probability that A and B's measurement results are different.

Let $U = \mathcal{U}_{\mathcal{I}}$ be C's unitary attack operator used on step (4) (collective attacks imply the same operator is used each iteration). From our discussion in a previous section, we may, without loss of power to C, assume that the state he initially sends on step (1) of the protocol is unentangled with his private ancilla. Thus, we only need to describe U's action on the four dimensional space $\mathcal{H}_{T_A} \otimes \mathcal{H}_{T_B}$. The action may be described as follows:

$$\begin{aligned}
U\,|\Phi^+\rangle &= |e_0\rangle\,|{+1}\rangle + |f_0\rangle\,|{-1}\rangle \\
U\,|\Phi^-\rangle &= |e_1\rangle\,|{+1}\rangle + |f_1\rangle\,|{-1}\rangle \\
U\,|\Psi^+\rangle &= |e_2\rangle\,|{+1}\rangle + |f_2\rangle\,|{-1}\rangle \\
U\,|\Psi^-\rangle &= |e_3\rangle\,|{+1}\rangle + |f_3\rangle\,|{-1}\rangle\,,
\end{aligned} \tag{6.6}$$

where each $|e_i\rangle$ and $|f_i\rangle$ are arbitrary states (not necessarily normalized nor orthogonal) in $\mathcal{H}_{T_A} \otimes \mathcal{H}_{T_B} \otimes \mathcal{H}_C$. Of course unitarity imposes certain restrictions on these states which we will make use of later.

By linearity of U, it holds that:

$$\begin{aligned}
U|00\rangle &= \frac{1}{\sqrt{2}}(|e_0\rangle + |e_1\rangle)|+1\rangle + \frac{1}{\sqrt{2}}(|f_0\rangle + |f_1\rangle)|-1\rangle \\
U|11\rangle &= \frac{1}{\sqrt{2}}(|e_0\rangle - |e_1\rangle)|+1\rangle + \frac{1}{\sqrt{2}}(|f_0\rangle - |f_1\rangle)|-1\rangle \\
U|01\rangle &= \frac{1}{\sqrt{2}}(|e_2\rangle + |e_3\rangle)|+1\rangle + \frac{1}{\sqrt{2}}(|f_2\rangle + |f_3\rangle)|-1\rangle \\
U|10\rangle &= \frac{1}{\sqrt{2}}(|e_2\rangle - |e_3\rangle)|+1\rangle + \frac{1}{\sqrt{2}}(|f_2\rangle - |f_3\rangle)|-1\rangle .
\end{aligned}$$

At this point, we will make one more assumption regarding the symmetry of C's attack. In addition to assuming $p_{0,0} = p_{1,1}$ and $p_{0,1} = p_{1,0}$, we will also assume that the probability of C sending the message "-1" in case A and B's measurement result was $|0,0\rangle$ is equal to the probability of him sending that same message if their measurement result was $|1,1\rangle$. We will make a similar assumption in the event A and B's measurement results differ. These statistics can easily be estimated by A and B and can be enforced. Further, we will show later that these are not unreasonable assumptions. In particular, however, this assumption implies that $Re\,\langle f_0|f_1\rangle = Re\,\langle f_2|f_3\rangle = 0$.

Now, denote by p_a, the probability that C sends the message "-1" on any particular iteration assuming that A and B both measured. Taking into account the above assumptions, this value is:

$$p_a = \frac{1}{2}(1-Q)(\langle f_0|f_0\rangle + \langle f_1|f_1\rangle) + \frac{1}{2}Q(\langle f_2|f_2\rangle + \langle f_3|f_3\rangle). \tag{6.7}$$

We can now prove an upper-bound on the quantity $I(A:C)$.

Theorem 6.2.1. Using the above notation, and given the above discussed assumptions, it holds that:

$$I(A:C) \leq \frac{(1-Q)}{p_a}\sqrt{\langle f_0|f_0\rangle \langle f_1|f_1\rangle} + \frac{Q}{p_a}\sqrt{\langle f_2|f_2\rangle \langle f_3|f_3\rangle} \tag{6.8}$$

$$\leq \frac{(1-Q)}{p_a}\sqrt{\langle f_0|f_0\rangle} + \frac{Q}{p_a}. \tag{6.9}$$

Proof. Let ρ_{ABC} be the density operator describing the state of the quantum system in the event that both A and B measured and resent (otherwise the iteration is not used for the raw key, so there is nothing to learn), after C has attacked with U, but before he sends a message (i.e., before he measures $\mathcal{H}_{cl}$). This state is:

$$\rho_{ABC} = \left(\frac{1-Q}{2}\right)(U_{00} + U_{11}) + \left(\frac{Q}{2}\right)(U_{01} + U_{10}),$$

where:

$$U_{ij} = |i,j\rangle \langle i,j|_{AB} \otimes U\,|i,j\rangle \langle i,j|\,U^*$$

(above the state $|i,j\rangle \langle i,j|_{AB}$ are A and B's private registers used to store their raw key bit for this particular iteration). Now assume that C sends the message "-1" (otherwise, again, the iteration is discarded and there is nothing to learn). From our earlier discussion, the resulting state is the projection of ρ_{ABC} to $|-1\rangle \langle -1|_{cl}$ which

yields:

$$\begin{aligned}\rho'_{ABC} = &\frac{1}{p}\left(\left(\frac{1-Q}{2}\right)|0,0\rangle\langle 0,0|_{AB} \otimes P(|f_0\rangle + |f_1\rangle)\right) \\ &+ \frac{1}{p}\left(\left(\frac{1-Q}{2}\right)|1,1\rangle\langle 1,1|_{AB} \otimes P(|f_0\rangle - |f_1\rangle)\right) \\ &+ \frac{1}{p}\left(\frac{Q}{2}|0,1\rangle\langle 0,1|_{AB} \otimes P(|f_2\rangle + |f_3\rangle)\right) \\ &+ \frac{1}{p}\left(\frac{Q}{2}|1,0\rangle\langle 1,0|_{AB} \otimes P(|f_2\rangle - |f_3\rangle)\right),\end{aligned}$$

where we use the notation $P(z) = zz^*$ for any vector z. We also defined $p = 2p_a$ (see Equation 6.7).

Next, we trace out B's system resulting in the state:

$$\begin{aligned}\rho'_{AC} = &\frac{1}{2}|0\rangle\langle 0|_A \otimes \overbrace{\left(\frac{1-Q}{p}P(|f_0\rangle + |f_1\rangle) + \frac{Q}{p}P(|f_2\rangle + |f_3\rangle)\right)}^{\rho_C^{(0)}} \\ &+ \frac{1}{2}|1\rangle\langle 1|_A \otimes \underbrace{\left(\frac{1-Q}{p}P(|f_0\rangle - |f_1\rangle) + \frac{Q}{p}P(|f_2\rangle - |f_3\rangle)\right)}_{\rho_C^{(1)}}.\end{aligned}$$

By our symmetry assumptions, it holds that $Re\langle f_0|f_1\rangle = Re\langle f_2|f_3\rangle = 0$. This further implies that $tr\rho_C^{(0)} = tr\rho_C^{(1)} = 1$.

Define $\tilde{\rho} = \rho_C^{(0)} - \rho_C^{(1)}$. This state is:

$$\widetilde{\rho} = \frac{2}{p}((1-Q)|f_0\rangle\langle f_1| + (1-Q)|f_1\rangle\langle f_0| + Q|f_2\rangle\langle f_3| + Q|f_3\rangle\langle f_2|). \tag{6.10}$$

Define $T = \frac{1}{2}||\widetilde{\rho}||$. This value is:

$$\begin{aligned} T &= \frac{1}{p}||(1-Q)\,|f_0\rangle\langle f_1| + (1-Q)\,|f_1\rangle\langle f_0| + Q\,|f_2\rangle\langle f_3| + Q\,|f_3\rangle\langle f_2|\,|| \\ &\leq \frac{1-Q}{2p_a}||\,|f_0\rangle\langle f_1| + |f_1\rangle\langle f_0|\,|| + \frac{Q}{2p_a}||\,|f_2\rangle\langle f_3| + |f_3\rangle\langle f_2|\,||. \end{aligned}$$

Let $\sigma_0 = |f_0\rangle\langle f_1| + |f_1\rangle\langle f_0|$ and also $\sigma_1 = |f_2\rangle\langle f_3| + |f_3\rangle|f_2\rangle$. To bound T, we must bound $||\sigma_i||$. Due to our symmetry assumptions, $Re\langle f_0|f_1\rangle = Re\langle f_2|f_3\rangle = 0$ which implies $tr\sigma_0 = tr\sigma_1 = 0$ and, therefore, Lemma 6.2.1 can be applied yielding:

$$T \leq \frac{1-Q}{p_a}\sqrt{\langle f_0|f_0\rangle\langle f_1|f_1\rangle} + \frac{Q}{p_a}\sqrt{\langle f_2|f_2\rangle\langle f_3|f_3\rangle}. \tag{6.11}$$

Combining this bound, with Equation 6.4 proves the first claim (Equation 6.8). The second claim (Equation 6.9) follows immediately simply by observing that $\langle f_i|f_i\rangle$ is less than 1 for all i. □

This theorem shows that, in order to upper-bound $I(A:C)$ (thus lower-bounding the key rate r), A and B must estimate the quantities $\langle f_i|f_i\rangle$. These values are the probabilities that C sends the classical message "-1" based on which one of the four Bell states was received by him in step (4). Of course, A and B, being semi-quantum, cannot prepare Bell states and so are unable to measure these quantities directly. As we demonstrate next section, however, they are able to form reasonable estimates for them providing us with a lower-bound on our mediated protocol's key rate.

6.2.5 First Bound: An Honest Center

In this section we will use our bound on $I(A:C)$, from last section, to compute a lower-bound on the key rate of our mediated protocol in two different scenarios. First, in order to justify our symmetry assumptions earlier, we will consider the case

of an honest center with a noisy channel. Here, the noise in the quantum channel will be modeled as a depolarization channel. The bound we compute here can also be applied in the event C is "semi-honest" (that is, he follows the protocol description on step (1) and (4), but after sending his message, he is allowed to do whatever he likes with the information he has). After this example, we will consider the worst case: that C is adversarial.

To model the noisy channel, assume that C prepares the state $\rho \in \mathcal{H}_{T_A} \otimes \mathcal{H}_{T_B}$. Then, the joint state, after passing through the quantum channel, will be described by the mixed state $(1-p)\rho + \frac{p}{4}I$, where I is the identity operator. Similarly, if the joint state leaving the two users A and B is σ, the state arriving at C is the mixed state $(1-q)\sigma + \frac{q}{4}I$.

To simplify our notation, in this example, we will relabel the Bell states as follows: $|\phi_0\rangle = |\Phi^+\rangle$, $|\phi_1\rangle = |\Phi^-\rangle$, $|\phi_2\rangle = |\Psi^+\rangle$, and $|\phi_3\rangle = |\Psi^-\rangle$. Assuming an honest C in this example, we know that he initially prepares and sends the state $\rho = |\phi_0\rangle\langle\phi_0|$ and, from the above discussion, when it arrives at the users A and B, the joint system can be described by the state:

$$\rho = (1-p)\,|\phi_0\rangle\langle\phi_0| + \frac{p}{4}\sum_{i=0}^{3}|\phi_i\rangle\langle\phi_i|\,. \tag{6.12}$$

From this, the probability that A measures $|i\rangle$ and B measures $|j\rangle$ (denoted $p_{i,j}$ as in the previous section) are:

$$p_{0,0} = p_{1,1} = \frac{1}{2} - \frac{p}{4}$$
$$p_{0,1} = p_{1,0} = \frac{p}{4}$$

From the previous section, we define $Q/2 = p_{0,1} = p_{1,0}$ which implies $Q = \frac{p}{2}$. It is

clear that this fits our first requirement of a symmetric attack. This value p (and therefore the quantity Q) are parameters that A and B may estimate.

Now, assume that both A and B reflect their qubits. In this case, the state arriving back to C can be described by the mixed state:

$$\rho' = (1-q)\rho + \frac{q}{4}\sum_{i=0}^{3} |\phi_i\rangle \langle\phi_i| \tag{6.13}$$

$$= (1-q)\left[(1-p)\,|\phi_0\rangle \langle\phi_0| + \frac{p}{4}\sum_{i=0}^{3} |\phi_i\rangle \langle\phi_i|\right] + \frac{q}{4}\sum_{i} |\phi_i\rangle \langle\phi_i|\,. \tag{6.14}$$

We are assuming, for now, that C is honest and so he will always send the message "+1" if he measures $|\phi_i\rangle \langle\phi_i|$ for $i \neq 1$. It is clear, from the above equation, that the value p_w (which represents the probability that C sends "-1" if both A and B reflect) is:

$$p_w = \frac{(1-q)p}{4} + \frac{q}{4}, \tag{6.15}$$

which allows the users A and B to determine the value of q:

$$q = \frac{4p_w - p}{1-p} \tag{6.16}$$

This provides us with enough information to estimate the values $\langle f_i|f_i\rangle$: the probability that C sends the message "-1" when the state leaving A and B is $|\phi_i\rangle$. After

C's operation on the returned qubits, the joint system may be described as follows:

$$
\begin{aligned}
|\phi_0\rangle\langle\phi_0| &\to \left((1-q)+\frac{3q}{4}\right)\sigma_{+1}^{(0)}\otimes|+1\rangle\langle+1|_{cl}+\left(\frac{q}{4}\right)\sigma_{-1}^{(0)}\otimes|-1\rangle\langle-1|_{cl}\\
|\phi_1\rangle\langle\phi_1| &\to \left(\frac{3q}{4}\right)\sigma_{+1}^{(1)}\otimes|+1\rangle\langle+1|_{cl}+\left((1-q)+\frac{q}{4}\right)\sigma_{-1}^{(1)}\otimes|-1\rangle\langle-1|_{cl}\\
|\phi_2\rangle\langle\phi_2| &\to \left((1-q)+\frac{3q}{4}\right)\sigma_{+1}^{(2)}\otimes|+1\rangle\langle+1|_{cl}+\left(\frac{q}{4}\right)\sigma_{-1}^{(2)}\otimes|-1\rangle\langle-1|_{cl}\\
|\phi_3\rangle\langle\phi_3| &\to \left((1-q)+\frac{3q}{4}\right)\sigma_{+1}^{(3)}\otimes|+1\rangle\langle+1|_{cl}+\left(\frac{q}{4}\right)\sigma_{-1}^{(3)}\otimes|-1\rangle\langle-1|_{cl}\,.
\end{aligned}
$$

We have written the effect of C's operation with respect to the Bell basis in keeping with Equation 6.6. Each $\sigma_{\pm1}^{(i)}$ is a density operator which represents the state of C's system in the event the joint system leaving A and B was $|\phi_i\rangle$ and C's message was "±1". For an honest C, these systems are all equal; for a semi-honest C, they may provide some information to the center. The reader may easily verify, by performing the same computation as above for the case that the state leaving A and B is $|i,j\rangle\langle i,j|$ (for $i,j\in\{0,1\}$), the probability that C sends the message "-1" in the event both A and B measure zero, is equal to the probability of him sending the same message if the users both measure one (likewise for the case when their measurement results differ). Thus, this scenario fits our symmetry assumptions. Further this shows our symmetry assumptions to not penalize an honest server running on a noisy channel.

Of course the state leaving A and B is never, for example, $|\phi_2\rangle$. But this is irrelevant. The point is that *if* the state were $|\phi_2\rangle$, then this would be the result and, assuming a depolarization channel and honest C, A and B may estimate these states thus producing a lower-bound on the key rate using the results from the previous section. In particular, they may estimate the quantity $\langle f_1|f_1\rangle = (1-q)+\frac{q}{4}$ and $\langle f_i|f_i\rangle = \frac{q}{4}$ (for $i=0,2,3$).

Using our results from the previous section, we may bound $I(A:C)$ using Theorem

6.2.1. To estimate the key rate all that remains is to compute $I(A:B)$. Denote by Q_Z, the probability that A and B's measurement results are different assuming that C sent the message "-1" (this may be very different from Q). This value, for any scenario, is:

$$Q_Z = \frac{Q(\langle f_2|f_2\rangle + \langle f_3|f_3\rangle)}{2p_a}, \tag{6.17}$$

which in our case, with an honest center and noisy channel, is:

$$Q_Z = \frac{pq}{8p_a}. \tag{6.18}$$

It is trivial to show that $I(A:B) = 1 - h(Q_Z)$. This provides us with enough information to estimate the key rate. For example, in the event $p = q$ (the noise in the forward directing is equal to the noise in the reverse channel), we see our protocol maintains a positive key rate for all $Q \leq 19.9\%$ (see Figure 6.2; also see Figure 6.3 which shows how the values p_w, p_a, and Q_Z are affected by p). This is a much higher tolerated noise threshold than BB84 (which supports up to 11% error [22]). This is due to the fact that Q_Z is very small, even for large Q (see Figure 6.3) thanks to the honest server "throwing out" the majority of iterations where A and B's measurement results are different. In this case, $I(A:B)$ remains large - that is to say, little information leaks due to error correction.

6.2.6 Second Bound: An Adversarial Center

We now consider the worst-case scenario: C is fully adversarial, and all noise is induced by C's attack. Let $|\psi_0\rangle = \sum_{i,j} \alpha_{i,j} |i,j\rangle$ be the state C initially prepares for sending in step (1) of the protocol. As we consider only symmetric attacks, it is forced that $|\alpha_{0,0}|^2 = |\alpha_{1,1}|^2 = (1-Q)/2$ and $|\alpha_{0,1}|^2 = |\alpha_{1,0}|^2 = Q/2$. Our first claim is that, without any loss of power to the center C, we may assume that C prepares

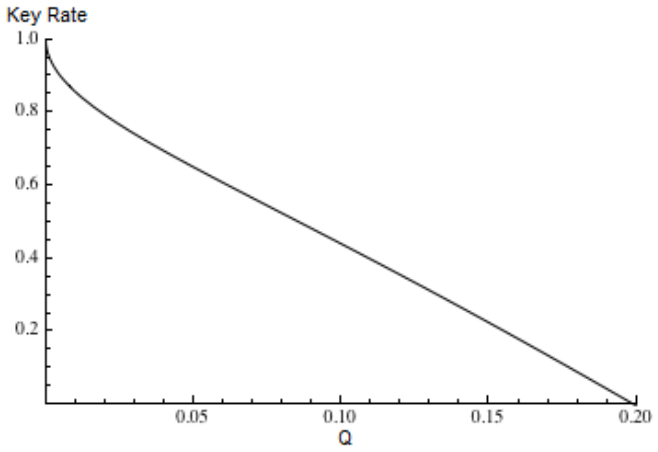

Figure 6.2: Showing the key rate of our protocol when the center is honest (or semi-honest) with two independent depolarizing channels modeling the noise in both channels (one with parameter p and the second with parameter q). The key rate in this figure is plotted as a function of $Q = p/2$ which is the error rate of A and B's measurements. In the above graph, we assume $p = q$ - i.e., the noise in both directions of the quantum channel is equal. Notice that the key rate remains positive for all $Q \leq 19.9\%$.

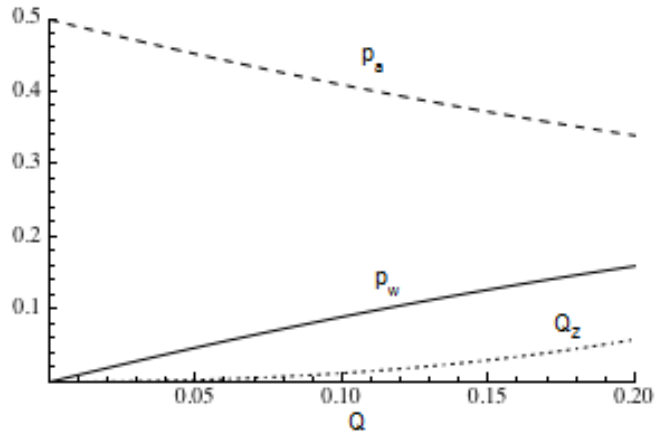

Figure 6.3: Showing various statistics of the depolarization example with honest (or semi-honest) center, when $p = q$. Note that $Q = p/2$ is the error rate of A and B's measurement results. The solid line graphs the value of p_w; the dashed line (top) plots p_a; finally, Q_Z is the dotted line. Observe that, as Q increases, Q_Z remains small due to the fact that the quantum server is discarding most iterations where A and B's measurement results differ. While this decreases the value of p_a, less information is leaked due to error correction.

the initial state $|\psi_0'\rangle = \sqrt{1-Q}\,|\Phi^+\rangle + \sqrt{Q}\,|\Psi^+\rangle$.

Assume, first, that C sends the state $|\psi_0\rangle$. As we are assuming all noise is induced by C's attack, the state of the system arriving back to C (after A and B either both reflect or both measure and resend - any other case is discarded), is (up to a normalization term):

$$\rho = p_R\,|\psi_0\rangle\langle\psi_0| + p_M\left(\sum_{i,j}|\alpha_{i,j}|^2\,|i,j\rangle\langle i,j|\right),$$

where p_R denotes the probability that both users A and B reflect and p_M is the probability they both measure and resend. However, if instead C were to send $|\psi_0'\rangle$, the state arriving back to C (after A and B's operation and again up to the same normalization term as before) is:

$$\rho' = p_R\,|\psi_0'\rangle\langle\psi_0'| + p_M\left(\frac{1-Q}{2}\,|0,0\rangle\langle 0,0| + \frac{1-Q}{2}\,|1,1\rangle\langle 1,1| + \frac{Q}{2}\,|0,1\rangle\langle 0,1| + \frac{Q}{2}\,|1,0\rangle\langle 1,0|\right).$$

Write each $\alpha_{j,k} = e^{i\theta_{j,k}}p_{j,k}$ where:

$$p_{j,k} = \begin{cases} \sqrt{\frac{1-Q}{2}} & \text{if } j = k \\ \sqrt{\frac{Q}{2}} & \text{if } j \neq k \end{cases}$$

Define the unitary operator: $V = \sum_{j,k} e^{i\theta_{j,k}}\,|j,k\rangle\langle j,k|$. Then it is clear that $V\rho'V^* = \rho$. We conclude, therefore, that if there were an advantage for C in sending the state $|\psi_0\rangle$ initially in step (1), C may instead simply prepare and send $|\psi_0'\rangle$ and apply this operator V on step (4) without any loss of power. Therefore, to simplify our analysis, we will assume that C sends the state $|\psi_0'\rangle$ on step (1).

Denote C's unitary attack operator, as described by Equation 6.6, by U. By linearity, we have:

$$U\left|\psi_0'\right\rangle = (\sqrt{1-Q}\left|e_0\right\rangle + \sqrt{Q}\left|e_2\right\rangle)\left|+1\right\rangle_{cl} + (\sqrt{1-Q}\left|f_0\right\rangle + \sqrt{Q}\left|f_2\right\rangle)\left|-1\right\rangle_{cl}.$$

We will again denote by p_w the probability that C sends the message "-1" if both A and B reflect. In this case, using the above equation, we find this value to be:

$$p_w = (1-Q)\left\langle f_0|f_0\right\rangle + Q\left\langle f_2|f_2\right\rangle + 2\sqrt{Q(1-Q)}Re\left\langle f_0|f_2\right\rangle. \tag{6.19}$$

It is not difficult to see that if Q and p_w are both small, then so must be $\langle f_0|f_0\rangle$. Our goal is to upper-bound this quantity, thus providing us with an upper-bound on $I(A:C)$ using Theorem 6.2.1. Obviously, we must bound this value using only statistics that A and B may estimate.

Write $\left|f_0\right\rangle = x\left|\tilde{f}_0\right\rangle$ and $\left|f_2\right\rangle = ye^{i\theta}\left|\tilde{f}_0\right\rangle + z\left|\zeta\right\rangle$, where $x, y, z \in \mathbb{R}_{\geq 0}$, $\langle\tilde{f}_0|\tilde{f}_0\rangle = \langle\zeta|\zeta\rangle = 1$ and $\langle\tilde{f}_0|\zeta\rangle = 0$. Clearly this implies $x = \sqrt{\langle f_0|f_0\rangle}$, $x^2 + y^2 = \langle f_2|f_2\rangle$, and $xye^{i\theta} = \langle f_0|f_2\rangle$. Adopting this notation, we may rewrite Equation 6.19 as:

$$p_w = (1-Q)x^2 + Q(y^2+z^2) + 2\sqrt{Q(1-Q)}xy\cos\theta. \tag{6.20}$$

This we may solve for x which, taking the larger solution, yields:

$$x = \sqrt{f_0|f_0} = \frac{-\sqrt{Q(1-Q)}y\cos\theta}{1-Q} + \frac{\sqrt{Q(1-Q)y^2\cos^2\theta - Q(1-Q)(y^2+z^2) + p_w(1-Q)}}{1-Q}$$

$$= \frac{-\sqrt{Q(1-Q)}y\cos\theta}{1-Q} + \frac{\sqrt{Q(1-Q)y^2(\cos^2\theta - 1) - Q(1-Q)z^2 + p_w(1-Q)}}{1-Q}.$$

It is not difficult to see that this function is maximal when $y = \sqrt{\langle f_2|f_2\rangle}$ (which is the maximum value y can attain), $\theta = \pi$, and $z = 0$. These values produce:

$$\sqrt{f_0|f_0} \leq \frac{\sqrt{1-Q}(\sqrt{Q\,\langle f_2|f_2\rangle} + \sqrt{p_w})}{1-Q} \tag{6.21}$$

$$\leq \frac{\sqrt{1-Q}(\sqrt{Q} + \sqrt{p_w})}{1-Q}. \tag{6.22}$$

Using this bound with Equation 6.9 (from Theorem 6.2.1), yields the following lower-bound on the key rate:

$$r \geq 1 - h(Q_Z) - \frac{1}{p_a}\left(\sqrt{1-Q}\left(\sqrt{Q} + \sqrt{p_w}\right) + Q\right), \tag{6.23}$$

where Q_Z is the probability that A and B's measurement results are different in the event C sends "-1". These values, Q_Z, Q, p_w, and p_a can all be easily estimated by A and B. As an example of this bound, assuming $Q_Z = Q$, $p_w = Q$, and $p_a = 1/2$, the key rate remains positive for all $Q \leq 3.35\%$ as shown in Figure 6.4.

This bound may be improved, however, by considering the values of $\langle f_2|f_2\rangle$ and $\langle f_3|f_3\rangle$, which may be estimated using the probability that C sends "-1" if A and

B's measurement results are different. Call this probability $p_{-1}(A \neq B)$ and it may be estimated by A and B. Using our symmetry assumptions (and also the fact that $\langle x|x\rangle \geq 0$ for any vector x), we have:

$$\frac{1}{2}\langle f_2|f_2\rangle \leq \frac{1}{2}(\langle f_2|f_2\rangle + \langle f_3|f_3\rangle) = p_{-1}(A \neq B).$$

The same may be said for $\langle f_3|f_3\rangle$.

To demonstrate how this improves our bound, assume that both $\langle f_2|f_2\rangle$ and $\langle f_3|f_3\rangle$ are no greater than Q (considering the analysis in the previous section, this is reasonable). Then, using Equation 6.8 from Theorem 6.2.1, with $\langle f_1|f_1\rangle = 1$, we have the following key rate bound:

$$r \geq 1 - h(Q_Z) - \frac{1}{p_a}\left(\sqrt{1-Q}\,(Q + \sqrt{p_w}) + Q^2\right). \tag{6.24}$$

In this scenario, $Q_Z = Q^2/p_a$ and a graph of this bound is shown in Figure 6.5. Now we see that, when $p_a = 1/2$, our protocol maintains a positive key rate for all $Q \leq 10.65\%$: this is almost comparable to BB84. When $p_a = .3$ (which was the smallest value of p_a we observed in the previous depolarization example), the key rate remains positive for all $Q \leq 5.25\%$ which is better than the three state BB84 (which allows up to 4.25% error [3]).

Better bounds may be determined by taking into account the relation between p_a and $\langle f_i|f_i\rangle$. Observe that, as the former drops, so do the latter. Our bounds treat these two interdependent quantities independently. While this yields a "worst-case" bound, more optimistic bounds may be found in the future, perhaps, by deriving the relationship between the two.

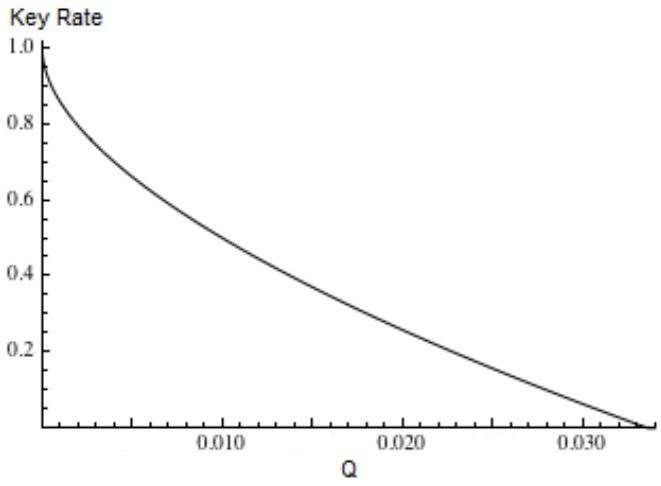

Figure 6.4: A graph of the key rate of our protocol in the worst case scenario, when the server is adversarial and A and B use only the value of p_w to bound $I(A:C)$ (Equation 6.23). Note the key rate is positive for all $Q \leq 3.35\%$.

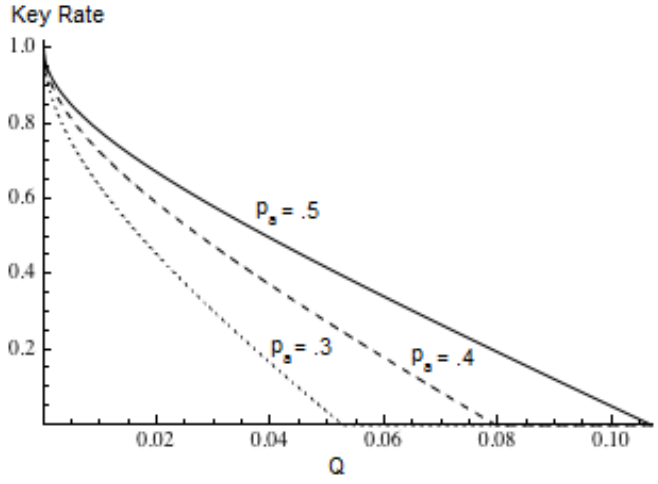

Figure 6.5: Showing the key rate of our protocol when the server is adversarial and A and B use p_w and $p_{-1}(A \neq B)$ to bound $I(A:C)$ (Equation 6.24). In particular, they observe (or enforce) $\langle f_2|f_2\rangle, \langle f_3|f_3\rangle \leq Q$. Here we also assume $p_w = Q$. The solid line plots the key rate if $p_a = .5$; the dashed line graphs the key rate when $p_a = .4$; finally the dotted line is when $p_a = .3$. When $p_a = .5$, the key rate remains positive for all $Q \leq 10.65\%$. When $p_a = .3$, it is positive for $Q \leq 5.25\%$. See the text for some observations on how the effect of p_a may be better bounded.

6.2.7 General Attacks and Third-Party Eavesdroppers

In the above, we have only considered an adversarial center. However, we may also face the situation where there are additional attackers, independent of the center (see 6.1). In this case, though, any such attack performed by these attackers may simply be "absorbed" into the center's unitary attack operator U considered in the previous section. This includes any strategy where these independent attackers alter C's messages (since C's classical channel is not assumed to be authenticated). Thus, our bound from the previous section applies even in this case.

Note that, if C's channel is authenticated so that E cannot alter his messages, and if we model these independent attacker's strategy as a depolarization channel (as was done when analyzing the key rate of B92 [22]), then our analysis in the first example shows our protocol's key rate remains positive so long as the noise is no greater than 19.9%. Compare this with B92's depolarization noise level of 6.5% [58].

Our security analysis above, considered only collective attacks. However, as was shown in [17, 18], for permutation invariant protocols, proving security against collective attacks is sufficient to show security against general attacks (those where the attacker is allowed to perform any operation within the laws of physics). Our mediated protocol may be made permutation invariant using the standard technique of adding an extra communication stage, immediately after the quantum communication stage (before parameter estimation). This involves A choosing a random permutation and disclosing it to B (over the authenticated channel). Both A and B then permute their measurement results using the permutation. This gives us permutation invariance and so security against general attacks. Furthermore, since we are working only with the asymptotic scenario, our security bound proven above is exactly the same in this case.

Chapter 7

Closing Remarks and Future Work

In this dissertation, we have studied the problem of semi-quantum key distribution. This field of research was started in 2007 by Boyer et al. [13], however, despite the fact that many protocols have been developed since then, their security against general attacks was in question. Up until our work, the majority of semi-quantum protocols were proven *robust*: that is, *if* there is an attack against the protocol, it can be detected. While this is a good first-start towards security, it leaves a lot to be desired. In particular, it says nothing about how many secure key bits, after privacy amplification, can be distilled given a certain level of noise in the quantum channel (i.e., the key rate of a protocol in, for instance, the asymptotic scenario). While all SQKD protocols described to date have a command to "abort if the noise is over threshold τ," no one knew what value to set τ.

Our work has, for the first time, given conclusive answers to this question for many SQKD protocols. We first proved that, for any single-state protocol (one where A is limited to sending only a single, publicly known state each iteration), E's most general collective attack, consisting of two unitary attack operators, is equivalent to a restricted attack where she biases A's superposition, and then attacks with a single unitary operator. Using this, we were able to bound the key rate of two different SQKD protocols, as functions of this bias term, with the key rate bound of two other fully quantum protocols: a three state BB84 [3] and B92 [2]. This also shows that, for small bias, the key rate of these SQKD protocols is similar to fully quantum ones.

We designed a new SQKD protocol and proved its security. This is also the first semi-quantum protocol which permitted X basis states to contribute to the raw key

(as opposed to being used only for security purposes) - a theoretically interesting result. Since it is a single state protocol, it allowed us to utilize our previous results in order to prove its unconditional security.

Finally, we have designed a new form of SQKD protocol: a *mediated* semi-quantum protocol. Now, both A and B are limited/classical. In order to establish a secure key, they must utilize the services of a quantum server: a service which is able to produce quantum resources and measure in alternative bases. Our protocol, as we have proven, is secure even when this server is untrusted. Indeed, if the server is adversarial, our mediated protocol maintains a positive key rate for all noise levels less than 10.65%. If the server is trusted, the protocol maintains a positive key rate for noise levels less than 19.9%. This is a theoretically interesting result, however it also has possible practical benefits. One can envision a future where there are several limited semi-quantum users, establishing keys with one another, using the services of a quantum server - our protocol has shifted the complexity of quantum key distribution from the end-users to this single quantum server.

While we have greatly advanced the field of semi-quantum key distribution, much future work remains. In particular, while we have proven the unconditional security of several SQKD protocols (and devised techniques which can be applied to others), there are still many other SQKD protocols which remain unconsidered. We have already started in this direction [59], proving a lower-bound on the key rate of the multi-state protocol of [13]. However, much work remains in this regard.

Also of interest would be to consider more practical attacks on semi-quantum key distribution protocols: for instance multi-photon attacks [5] and the photon tagging attack described in [60, 61]. While the first was considered partially in [62] (though their analysis can be improved), designing a protocol secure against the second is still an open question. We believe our new single-state SQKD protocol may actually be

used for this purpose, however a proof of security remains elusive.

Finally, we would like to improve on our mediated protocol. The requirements on the sever at the moment are practical, though extreme - it would be preferable to design a protocol which required the server to prepare and measure single qubit states as opposed to the current Bell states. We have a protocol which appears to work, however a proof of its unconditional security is still required.

Semi-quantum key distribution asks the question "how quantum does a protocol need to be in order to gain an advantage over a classical one in cryptographic applications." It is of great theoretical interest, but it also has great practical potential. Indeed, it might lead to systems which require far simpler hardware for end-users. In the future, if quantum computers become widely available, it will be vital to establish an infrastructure allowing users to securely establish shared secret keys; semi-quantum protocols may be the way forward in this direction and our work in this dissertation greatly contributes to this effort.

Bibliography

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

[2] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[3] Chi-Hang Fred Fung and Hoi-Kwong Lo. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Phys. Rev. A*, 74:042342, Oct 2006.

[4] Antonio Acin, Nicolas Gisin, and Valerio Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, 69:012309, Jan 2004.

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

[6] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[7] Frank Jordans. Swiss call new vote encryption system unbreakable. http://web.archive.org/web/20071209214958/http:// www.technewsworld.com /story /59793.html, 2007. Accessed: January 21, 2015.

[8] Anton Zeilinger. World premiere: Bank transfer via quantum cryptography based on entangled photons. http://www.secoqc.net/ downloads/pressrelease/ Banktransfer_english.pdf, 2004. Accessed: February 5, 2015.

[9] Will Knight. Quantum cryptography network gets wireless link. http://www.newscientist.com/article/dn7484, 2005. Accessed: January 21, 2015.

[10] 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.

[11] Roland Pease. Unbreakable encryption unveiled. http://news.bbc.co.uk/2/hi/ science/nature/7661311.stm, 2008. Accessed: February 5, 2015.

[12] Tokyo qkd network. http://www.uqcc2010.org/highlights/index.html, 2010. Accessed: February 5, 2015.

[13] Michel Boyer, D. Kenigsberg, and T. Mor. Quantum key distribution with classical Bob. In *Quantum, Nano, and Micro Technologies, 2007. ICQNM '07. First International Conference on*, pages 10–10, 2007.

[14] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. *Phys. Rev. A*, 79:032341, Mar 2009.

[15] Takayuki Miyadera. Relation between information and disturbance in quantum key distribution protocol with classical Alice. *Int. J. of Quantum Information*, 9, 2011.

[16] Hua Lu and Qing-Yu Cai. Quantum key distribution with classical Alice. *International Journal of Quantum Information*, 6(06):1195–1202, 2008.

[17] Matthias Christandl, Robert Konig, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.

[18] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[19] Walter O. Krawec. Restricted attacks on semi-quantum key distribution protocols. *Quantum Information Processing*, 13(11):2417–2436, 2014.

[20] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A*, 79:052312, May 2009.

[21] Walter O Krawec. Using evolutionary techniques to analyze the security of quantum key distribution protocols. In *Proceedings of the 2014 conference companion on Genetic and evolutionary computation companion*, pages 171–172. ACM, 2014.

[22] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.

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

[24] P. A. M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(3):416–418, 1939.

[25] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59:4238–4248, Jun 1999.

[26] Helle Bechmann-Pasquinucci and Asher Peres. Quantum cryptography with 3-state systems. *Phys. Rev. Lett.*, 85:3313–3316, Oct 2000.

[27] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.

[28] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501, Aug 2005.

[29] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 461(2053):207–235, 2005.

[30] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way post-processing. *Physical review letters*, 100(20):200501, 2008.

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

[32] Zhi-Wei Sun, Rui-Gang Du, and Dong-Yang Long. Quantum key distribution with limited classical Bob. *International Journal of Quantum Information*, 11(01), 2013.

[33] Wang Jian, Zhang Sheng, Zhang Quan, and Tang Chao-Jing. Semiquantum key distribution using entangled states. *Chinese Physics Letters*, 28(10):100301, 2011.

[34] Kun-Fei Yu, Chun-Wei Yang, Ci-Hong Liao, and Tzonelih Hwang. Authenticated semi-quantum key distribution protocol using bell states. *Quantum Information Processing*, pages 1–9, 2014.

[35] Zhang Xian-Zhou, Gong Wei-Gui, Tan Yong-Gang, Ren Zhen-Zhong, and Guo Xiao-Tian. Quantum key distribution series network protocol with m-classical Bobs. *Chinese Physics B*, 18(6):2143, 2009.

[36] Qin Li, W. H. Chan, and Dong-Yang Long. Semiquantum secret sharing using entangled states. *Phys. Rev. A*, 82:022303, Aug 2010.

[37] Lvzhou Li, Daowen Qiu, and Paulo Mateus. Quantum secret sharing with classical Bobs. *Journal of Physics A: Mathematical and Theoretical*, 46(4):045304, 2013.

[38] Jian Wang, Sheng Zhang, Quan Zhang, and Chao-Jing Tang. Semiquantum secret sharing using two-particle entangled state. *International Journal of Quantum Information*, 10(05), 2012.

[39] Chun-Wei Yang and Tzonelih Hwang. Efficient key construction on semi-quantum secret sharing protocols. *International Journal of Quantum Information*, 11(05), 2013.

[40] Simon JD Phoenix, Stephen M Barnett, Paul D Townsend, and KJ Blow. Multi-user quantum cryptography on optical networks. *Journal of modern optics*, 42(6):1155–1163, 1995.

[41] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Physical Review A*, 54(4):2651, 1996.

[42] Peng Xue, Chuan-Feng Li, and Guang-Can Guo. Conditional efficient multiuser quantum cryptography network. *Physical Review A*, 65(2):022317, 2002.

[43] Li Chun-Yan, Zhou Hong-Yu, Wang Yan, and Deng Fu-Guo. Secure quantum key distribution network with bell states and local unitary operations. *Chinese Physics Letters*, 22(5):1049, 2005.

[44] Wei Huang, Hui-Juan Zuo, and Yan-Bing Li. Cryptanalysis and improvement of a multi-user quantum communication network using χ-type entangled states. *International Journal of Theoretical Physics*, 52(4):1354–1361, 2013.

[45] Song Lin, Chuan Huang, and Xiao-Fen Liu. Multi-user quantum key distribution based on bell states with mutual authentication. *Physica Scripta*, 87(3):035008, 2013.

[46] Chang Ho Hong, Jin O Heo, Jong In Lim, and Hyung Jin Yang. Multi-user quantum network system and quantum communication using χ-type entangled states. *Journal of the Korean Physical Society*, 61(1):1–5, 2012.

[47] Chang Ho Hong, Jin O Heo, Gyong Luck Khym, Jongin Lim, Suc-Kyung Hong, and Hyung Jin Yang. N quantum channels are sufficient for multi-user quantum key distribution protocol between n users. *Optics Communications*, 283(12):2644–2646, 2010.

[48] Chia-Wei Tsai, Shih-Hsueh Wang, and Tzonelih Hwang. Comment on "n quantum channel are sufficient for multi-user quantum key distribution protocol between n users". *Optics Communications*, 283(24):5285–5286, 2010.

[49] Tian-Yin Wang, Qiao-Yan Wen, and Xiu-Bo Chen. Cryptanalysis and improvement of a multi-user quantum key distribution protocol. *Optics Communications*, 283(24):5261–5263, 2010.

[50] Hoi-Kwong Lo, Hoi-Fung Chau, and M Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18(2):133–165, 2005.

[51] Koenraad MR Audenaert. A sharp continuity estimate for the von Neumann entropy. *Journal of Physics A: Mathematical and Theoretical*, 40(28):8127, 2007.

[52] W Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[53] Walter O. Krawec. Mediated semiquantum key distribution. *Phys. Rev. A*, 91:032323, Mar 2015.

[54] E.B. Davies and J.T. Lewis. An operational approach to quantum probability. *Communications in Mathematical Physics*, 17(3):239–260, 1970.

[55] Mark M Wilde. From classical to quantum Shannon theory. *arXiv preprint arXiv:1106.1445*, 2011.

[56] Jop Briët and Peter Harremoës. Properties of classical and quantum Jensen-Shannon divergence. *Physical review A*, 79(5):052311, 2009.

[57] Matthias Christandl, Renato Renner, and Artur Ekert. A generic security proof for quantum key distribution. *arXiv preprint quant-ph/0402131*, 2004.

[58] Ryutaroh Matsumoto. Improved asymptotic key rate of the B92 protocol. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 351–353. IEEE, 2013.

[59] Walter O Krawec. Security proof of a semi-quantum key distribution protocol. *to appear, Proc. IEEE ISIT '15 - preprint available online: arXiv:1412.0282*, 2015.

[60] Yong-gang Tan, Hua Lu, and Qing-yu Cai. Comment on quantum key distribution with classical Bob. *Phys. Rev. Lett.*, 102:098901, Mar 2009.

[61] Michel Boyer, Dan Kenigsberg, and Tal Mor. Boyer, kenigsberg, and mor reply:. *Phys. Rev. Lett.*, 102:098902, Mar 2009.

[62] Michel Boyer and Tal Mor. On the robustness of (photonic) quantum key distribution with classical Alice. *arXiv preprint arXiv:1012.2418*, 2010.

Vita

Walter O. Krawec

Address PO Box 732 Bloomingburg NY

Email walter.krawec@gmail.com

Education

Stevens Institute of Technology, Hoboken, NJ
Doctoral Candidate in Computer Science
expected date of graduation, May 2015

University at Albany (SUNY), Albany NY
MA Mathematics
Graduated May 2010

Experience

Stevens Institute of Technology
Research Assistant (2011 - present)
Assisted with research and development of the Icing Project (part of the NSF funded Nebula Future Internet Architecture project)

University at Albany (SUNY)
Instructor (2010-2011)
Instructor of Record for Pre-Calculus and Calculus I classes (30-40 students each).

Publications

W.O. Krawec. Restricted attacks on semi-quantum key distribution protocols.
Quantum Information Processing, 13 (11): 2417-2436 (2014).

W.O. Krawec. Mediated Semi-Quantum Key Distribution.
Phys. Rev. A, 91 032323 (2015).

W.O. Krawec. Security Proof of a Semi-Quantum Key Distribution Protocol.
to appear, *Proc. IEEE ISIT*, 2015.

Honors

Robert Crooks Stanley Graduate Fellowship, 2014