TOMOGRAPHIC QUANTUM CRYPTOGRAPHY WITH BELL DIAGONAL STATES

by

Lim Jenn Yang

B.Sc. (Hons.), National University of Singapore

A thesis submitted for
the Degree of Master of Science

Supervisor
Asst. Prof. Dagomir Kaszlikowski

Department of Physics
National University of Singapore

2005

Abstract

In the first part of the thesis, a generalized version of the Tomographic Quantum Key Distribution protocol in which the two users Alice and Bob share a Bell diagonal mixed state of two qubits will be presented and its security analyzed. In particular, it will be shown that if an eavesdropper performs a coherent measurement on a number of ancilla states simultaneously, classical methods of secure key distillation are less effective than quantum distillation protocols. Furthermore, certain classes of Bell diagonal states that are resistant to eavesdropping attacks will be identified.

In the second part of this thesis, the security of the tomographic protocol using a source which produces entangled photons via an experimental scheme proposed in *Phys. Rev. Lett.*, **92**, *37903 (2004)* will be analyzed. The range of experimental parameters for which the protocol is secure will be determined.

Acknowledgements

To Dag, friend and teacher, for being with me in the “freakin’ foxhole”;

To Mum and Dad, for their hard work and sacrifice in bringing me to where I am today;

To my friends and mentors, for their valuable support and guidance;

To Yan, for being there for me.

Contents

List of Figures

List of Tables

Chapter 1
Introduction

The main goal of quantum cryptography, or quantum key distribution (QKD), is the establishment of a random, secure and perfectly correlated set of key between the two users Alice and Bob. The laws of quantum mechanics are exploited to achieve this purpose. In essence, Alice and Bob make use of entanglement and perform suitable measurements to generate random sets of keys for themselves. In the absence of interference from the environment, these two sets of keys for Alice and Bob will be perfectly correlated. Moreover, by making use of the *no-cloning theorem* [Wootters and Zurek, 1982], Alice and Bob can make sure that any attempt at eavesdropping can be detected so that they can always be certain about the security of their keys. The first QKD protocol was discovered by Bennett and Brassard in 1984 [Bennett and Brassard, 1984], and since then, a number of others have been proposed, such as the Ekert91 [Ekert, 1991], the B92 [Bennett, 1992] and in particular, the *Tomographic Quantum Key Distribution* scheme proposed by Liang *et al.* [Liang et al., 2003]. Experimentally, the field of QKD is sufficiently advanced so that there is already the possibility for commercialization of some of the QKD devices.

1.1 Overview

This thesis will consist of two parts. In the first part, the Tomographic QKD protocol will be presented and extended to a generalized scheme in which Alice and Bob share a *Bell diagonal mixed state* of two qubits. The security of the protocol will be analyzed based on the Csiszár-Körner (CK) theorem which guarantees that a secure key can be established

through classical communication and one-way error-correcting codes if the correlations between Alice and Bob's data are stronger than that between the eavesdropper Eve and either one of them.

Two scenarios will be considered. In the first scenario, Alice and Bob agree on a cryptographic key if the correlations between their data are stronger than that between Eve and one of them, under the assumption that Eve can only perform *incoherent* measurements. The CK theorem then guarantees a way of generating a secure key. In the second scenario, we consider the situation when Eve's correlations are initially stronger than Alice and Bob's so that the CK theorem is no longer valid. In this case, Alice and Bob can perform an intermediate step known as distillation to strengthen their correlation with respect to Eve's, and in doing so, make the CK theorem applicable once more. Two distillation protocols will be considered: a classical method known as *Advantage Distillation* (AD) and a quantum procedure known as *Entanglement Distillation* (ED). The security of the Tomographic QKD protocol under these two distillation procedures will be considered, and in particular it will be shown that if Eve performs coherent measurements, the classical method of key distillation is less effective than the quantum method. Finally, it will be shown that there exist certain classes of Bell diagonal states which are resistant to *any* attempt at eavesdropping.

In the second part of the thesis, the security of QKD protocols based on a particular scheme of generating polarization-entangled photons from a quantum dot single photon source will be considered. Such a method of producing entangled photons was first proposed by Fattal *et al.* [Fattal et al., 2004] and can be incorporated into QKD schemes based on shared entanglement, such as the Ekert91 and BBM92 [Bennett et al., 1992]. The security of the Tomographic QKD protocol based on such a source of photons will be analyzed in particular. The range of experimental parameters for which the protocol is secure against incoherent attacks will be determined in the analysis and certain observations which could also be applied to other QKD schemes will be made.

The main results of this thesis appear in *Phys. Rev. A*, **71**, *012309 (2005)* and *eprint arXiv /* `quant-ph` */ 0501051*.

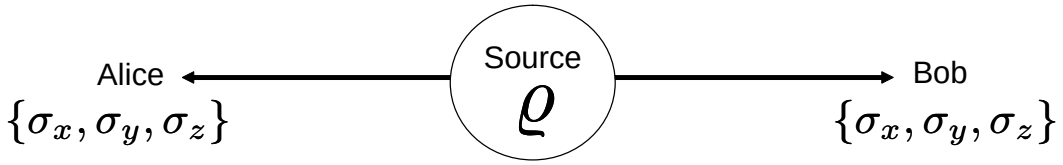
Chapter 2

Tomographic Quantum Key Distribution with Bell Diagonal States

In this chapter, the Tomographic QKD scheme based on Bell diagonal states will be presented. The protocol will first be described in general, after which we will apply the scheme to Bell diagonal states. We will then consider the situation where there is there is an eavesdropper Eve in the channel. Her optimal eavesdropping strategy in the situation where she is restricted only to incoherent attacks will be described, and the conditions for the protocol to be secure will be derived based on the Csiszár-Körner theorem.

2.1 Protocol

In the Tomographic QKD proocol [Liang et al., 2003], a central source distributes entangled qubit pairs to Alice and Bob (Fig. 2.1). For each qubit that they receive, Alice and Bob will independently and randomly choose one of the three Pauli observables $\{\sigma_x, \sigma_y, \sigma_z\}$ to measure their qubits. These observables have the important property of being *tomographically complete* in the sense that the probabilities for finding their eigenvalues as the results of measurements uniquely specify the statistical operator of the qubit pairs (see Appendix A). For each measurement they perform, Alice and Bob will separately record down the observables they have chosen as well as the results obtained.



$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Figure 2.1: Tomographic QKD setup. A central source distributes entangled qubit pairs described by density operator ϱ to Alice and Bob. For each qubit that they receive, Alice and Bob will independently and randomly choose one of the three tomograpically complete Pauli observables $\{\sigma_x, \sigma_y, \sigma_z\}$ to measure their qubits. After each measurement, Alice and Bob will keep separate records of the observables they have chosen as well as the results obtained. Here, the three Pauli matrices are expressed in the z basis.

In the ideal situation, Alice and Bob expect to receive the maximally entangled *singlet state* $|\psi_-\rangle$ from the source:

$$|\psi_-\rangle \quad = \quad \frac{1}{\sqrt{2}} \left(|z_0, z_1\rangle - |z_1, z_0\rangle \right). \tag{2.1}$$

Here, we have expressed Alice and Bob's two-qubit state in the z basis. The first ket entry refers to Alice's qubit while the second refers to Bob's qubit. If we express Eq. (2.1) in the other two bases, we see that the singlet state is invariant (up to a global phase) in those bases:

$$\begin{aligned} |\psi_-\rangle \quad &= \quad -\frac{1}{\sqrt{2}} \left(|x_0, x_1\rangle - |x_1, x_0\rangle \right) \\ &= \quad \frac{\mathrm{i}}{\sqrt{2}} \left(|y_0, y_1\rangle - |y_1, y_0\rangle \right). \end{aligned} \tag{2.2}$$

After all the qubits have been transmitted by the source and measured, Alice and Bob will proceed to the second step of the protocol where they process their data in the following way: They will first announce, over a public but authenticated channel, the observables they have measured for each qubit they receive. The results of the measurement are kept secret however. Based on this announcement, Alice and Bob will then proceed to divide their respective data into two groups. In the first group would be those results for which they have chosen the same observable to measure the same qubit pair, while in the second group would be those results for which they have chosen different observables.

For the first group, Alice and Bob's results will always be *perfectly anticorrelated* as well as *random*. For example, the probabilities for measurements performed in the x basis are

$$\begin{aligned} p^{(\mathrm{AB})}_{01|xx} &= \mathrm{Tr}\left[|x_0, x_1\rangle\langle x_0, x_1|\psi_-\rangle\langle\psi_-|\right] = \frac{1}{2} \\ p^{(\mathrm{AB})}_{10|xx} &= \frac{1}{2} \\ p^{(\mathrm{AB})}_{00|xx} &= p^{(\mathrm{AB})}_{11|xx} = 0 \end{aligned} \tag{2.3}$$

Here $p^{(\mathrm{AB})}_{kl|mm'}$ denotes the probability of Alice and Bob obtaining outcomes 'k' and 'l' respectively, given that they measured the observables σ_m and $\sigma_{m'}$ (where $m, m' = x, y$ or z) respectively. The data from this first group of matching bases can thus be used as a valid cryptographic key.

The second group of results for non-matching bases does not possess any useful correlations and is not useful for key generation. For example, we have

$$p^{(\mathrm{AB})}_{kl|xy} = \mathrm{Tr}\left[|x_k, y_l\rangle\langle x_k, y_l|\psi_-\rangle\langle\psi_-|\right] = \frac{1}{4}, \qquad \text{for all } k, l = 0, 1. \tag{2.4}$$

The results from this group of data are not completely useless however. What Alice and Bob will do in the next stage of the protocol is to make use of this group of data, together with some of the data from the first group, to perform a *state tomography* on the source. In this verification stage, Alice and Bob will exchange their data from the two groups and consider the frequencies at which various results arise. By doing this, they can in principle reconstruct any density operator describing the two-qubit state that they share (see Appendix A). If this reconstructed state is not of the form $|\psi_-\rangle\langle\psi_-|$ that they expect from the source, they will consider the channel insecure; they will discard their data and use another channel that fulfills their tomography requirement.

The tomographic protocol is summarized in Fig. 2.2.

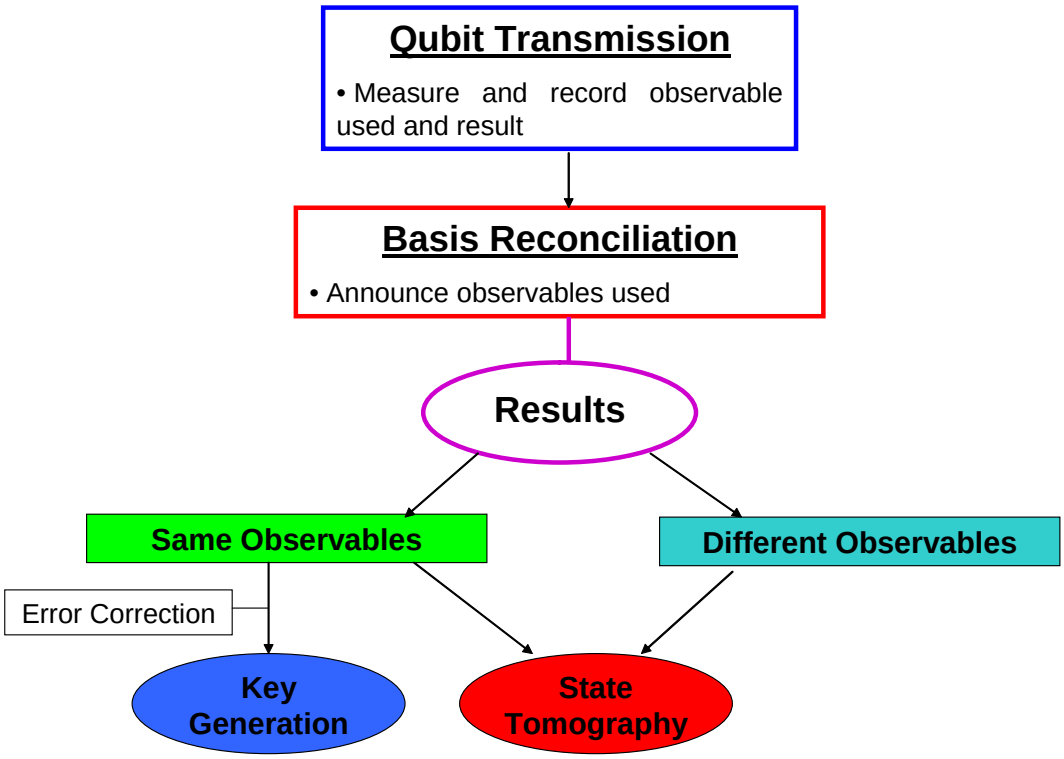


Figure 2.2: Tomographic QKD protocol.

2.1.1 Eavesdropping in a Perfect Channel

Suppose we have an eavesdropper Eve in the channel. It will be shown that the protocol will always be secure in the ideal situation of a noiseless channel, for which Alice and Bob always receive the singlet state $|\psi_-\rangle$ from the source. To be on the safe side, one must assume that Eve has full knowledge of the cryptographic protocol (the "Kerckhoff principle" of cryptology), and that she acquires as much knowledge about Alice and Bob's communication as is allowed by the laws of physics. In particular, it will be assumed that Eve has full control of the qubit distributing source.

In order to obtain as much information as possible about the key generated by Alice and Bob, Eve entangles their qubits with ancilla states $|e_{ab}\rangle$ in her possession. The most general

state she can prepare*† is

$$|\psi_{ABE}\rangle \;=\; |\phi_+\rangle|e_{00}\rangle + |\phi_-\rangle|e_{01}\rangle + |\psi_+\rangle|e_{10}\rangle + |\psi_-\rangle|e_{11}\rangle, \tag{2.5}$$

where we have represented each of the four Bell states in the following way:

$$\begin{aligned} |\phi_\pm\rangle &= \frac{1}{\sqrt{2}}\left(|z_0, z_0\rangle \pm |z_1, z_1\rangle\right) \\ |\psi_\pm\rangle &= \frac{1}{\sqrt{2}}\left(|z_0, z_1\rangle \pm |z_1, z_0\rangle\right). \end{aligned} \tag{2.6}$$

Because Alice and Bob perform state tomography to ensure that their two-qubit state is always in a singlet state, Eve will also have to make sure that her prepared state appears to Alice and Bob in that form, that is we require that on tracing out Eve's degree of freedom in $|\psi_{ABE}\rangle\langle\psi_{ABE}|$, we recover the pure singlet state $|\psi_-\rangle\langle\psi_-|$:

$$\mathrm{Tr}_{\mathrm{E}}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] \;=\; |\psi_-\rangle\langle\psi_-|. \tag{2.7}$$

Here, $\mathrm{Tr}_{\mathrm{E}}\left[\cdot\right]$ denotes taking a partial trace over Eve's ancilla space. This tomography requirement imposes the following structure on Eve's ancillas:

$$\begin{aligned} \langle e_{00}|e_{00}\rangle = \langle e_{01}|e_{01}\rangle = \langle e_{10}|e_{10}\rangle &= 0 \\ \langle e_{11}|e_{11}\rangle &= 1, \end{aligned} \tag{2.8}$$

so that Eve is effectively restricted to the following preparation:

$$|\psi_{ABE}\rangle \;=\; |\psi_-\rangle|e_{11}\rangle. \tag{2.9}$$

The only state that Eve can prepare is *separable* and there is no useful entanglement between her ancillas and the qubit pairs that can provide her information about Alice and Bob's measurements. Eve will not be able to obtain any useful information from her ancillas in this ideal noiseless scenario and the protocol is secure.

*Since there is no advantage in generating a mixed state, it is sufficient to consider only such pure state preparations.

†More generally, one could consider coherent attacks in which Eve prepares entangled multi-qubit pair states rather than the single qubit pair state of Eq. (2.5). There would then be correlations appearing between different qubit pairs. We shall take for granted that Alice and Bob protect themselves by also looking for such correlations when they exchange information during state tomography, thus ruling out such a class of coherent attack.

2.2 Tomographic QKD with Bell Diagonal States

Although the Tomographic QKD protocol is perfectly secure in the noiseless situation, Alice and Bob cannot expect to obtain the pure singlet state $|\psi_-\rangle\langle\psi_-|$ in realistic situations because either the the source is not ideal, there is interference with the surroundings, or there is an eavesdropper tampering with the system. Their two-qubit state will be a *mixed state* in general.

Suppose now that Alice and Bob's QKD setup is non-ideal, so that instead of a pure singlet state, they expect to receive a Bell diagonal mixed state in the, say z basis:

$$\varrho \;=\; \sum_{a,b=0}^{1} p_{ab}|z_{ab}\rangle\langle z_{ab}|, \tag{2.10}$$

Following the nomenclature of [Bennett et al., 1996], each of the four Bell states in the z basis has been conveniently written here as

$$|z_{ab}\rangle \;=\; \frac{1}{\sqrt{2}}\sum_{k=0}^{1}\omega^{kb}|z_k, z_{k+a}\rangle, \tag{2.11}$$

where $\omega = -1$ and addition in the indices is performed modulo 2. We note that each Bell state is uniquely represented by two indices: an amplitude bit a which gives the parity of the two qubits (0 for even parity, 1 for odd) and a phase bit b (0 for '+' phase, 1 for '-' phase). Comparing with Eq. (2.6), we thus have

$$\begin{aligned} |z_{00}\rangle &\equiv |\phi_+\rangle \\ |z_{01}\rangle &\equiv |\phi_-\rangle \\ |z_{10}\rangle &\equiv |\psi_+\rangle \\ |z_{11}\rangle &\equiv |\psi_-\rangle. \end{aligned} \tag{2.12}$$

In Eq. (2.10), p_{ab} represents the proportion of the Bell state $|z_{ab}\rangle$ and they sum to 1, $\sum_{a,b=0}^{1} p_{ab} = 1$. The ideal situation for which Alice and Bob receive the pure singlet state $|z_{11}\rangle$ corresponds to the case where $p_{11} = 1$. Furthermore, we require one of the probabilities p_{ab} to be greater than $\frac{1}{2}$ as otherwise the two-qubit state Eq. (2.10) becomes separable and Alice and Bob will not be able to obtain a secure key from such a state (see

Chapter 3). Without loss of generality, it will be assumed here that $p_{11} > \frac{1}{2}$. The protocol for this mixed state scenario then proceeds as before and in the tomography stage of the protocol, Alice and Bob will accept their measurement data if and only if their reconstructed state is in the Bell diagonal form.

We note that the state $\sum_{a,b=0}^{1} p_{ab}|z_{ab}\rangle\langle z_{ab}|$ can be obtained from the singlet state $|z_{11}\rangle\langle z_{11}|$ by assuming that the travelling qubits undergo random bit and phase flips. The so-called Werner state (maximally entangled state admixed with white noise) is a special case where we have $p_{00} = p_{01} = p_{10} = \frac{1-p_{11}}{3}$. The Bell diagonal state considered here is thus more general than the one studied in [Liang et al., 2003; Brußet al., 2003] where only Werner states were considered.

It is convenient to express the state Eq. (2.10) in the x and y bases as well. This can be done by noting the transformation rules on the Bell states:

$$|z_{ab}\rangle = (-\mathrm{i})^a \omega^{ab} |y_{a+b+1\ a}\rangle = \omega^{ab}|x_{ba}\rangle. \tag{2.13}$$

We thus have the following equivalent forms in the different bases:

$$\varrho = \sum_{a,b=0}^{1} p_{ab}|z_{ab}\rangle\langle z_{ab}| = \sum_{a,b=0}^{1} p_{b\ a+b+1}|y_{ab}\rangle\langle y_{ab}| = \sum_{a,b=0}^{1} p_{ba}|x_{ab}\rangle\langle x_{ab}|. \tag{2.14}$$

If we have a Bell diagonal state in one of the bases, it will remain Bell diagonal in the other two bases.

If we compute the probability of Alice and Bob obtaining anticorrelated results in the event that they measure in matching bases, we have the following probabilities for each of the bases:

$$\begin{aligned}
p(\text{anticorrelation}|z\text{ basis}) &= \sum_{k=0}^{1} \mathrm{Tr}\left[|z_k, z_{k+1}\rangle\langle z_k, z_{k+1}|\varrho\right] \\
&= p_{10} + p_{11} \equiv p_1^{(z)}, \\
p(\text{anticorrelation}|y\text{ basis}) &= p_{00} + p_{11} \equiv p_1^{(y)}, \\
p(\text{anticorrelation}|x\text{ basis}) &= p_{01} + p_{11} \equiv p_1^{(x)}.
\end{aligned} \tag{2.15}$$

On the other hand, the probability of getting correlated results is given by

$$\begin{aligned} p(\text{correlation}|z \text{ basis}) &= \sum_{k=0}^{1} \text{Tr}\left[|z_k, z_k\rangle\langle z_k, z_k|\varrho\right] \\ &= p_{00} + p_{01} \equiv p_0^{(z)}, \\ p(\text{correlation}|y \text{ basis}) &= p_{01} + p_{10} \equiv p_0^{(y)}, \\ p(\text{correlation}|x \text{ basis}) &= p_{00} + p_{10} \equiv p_0^{(x)}. \end{aligned} \tag{2.16}$$

Since $p_{11} > \frac{1}{2}$, we see that Alice and Bob are more likely to obtain anticorrelated results in whichever basis they measure; they will thus make use of anticorrelation to generate their key sequence.

2.2.1 Eavesdropping

Let us now consider the security of the tomographic protocol based on Bell diagonal states. Unlike the ideal situation, the protocol will in general not always be secure as Eve can obtain some information about the key that Alice and Bob have established. However, by determining the values of the p_{ab}'s from state tomography, Alice and Bob can place an upper bound on the knowledge that Eve has about their key. The Csiszár-Körner theorem then guarantees them of a secure key that can be extracted from their raw key as long as their correlations are stronger than than that between Eve and either one of them. To place this upper bound on Eve's knowledge, we shall assume the worst-case scenario in which Eve has full control of the source and that all imperfections in the channel are due to her eavesdropping activities.

Ancilla Structure

As before, suppose Eve entangles Alice and Bob's qubits with ancilla states $|e_{ab}\rangle$ in the most general fashion:

$$|\psi_{ABE}\rangle = \sum_{a,b=0}^{1} \sqrt{p_{ab}}|z_{ab}\rangle|e_{ab}\rangle. \tag{2.17}$$

To satisfy the tomography requirement of the protocol, Eve has to prepare the entangled state in such a way that it appears Bell diagonal to Alice and Bob, ie. if we trace out Eve's degree of freedom, we must recover a two-qubit state that is Bell diagonal. This imposes the following structure on Eve's ancillas:

$$\langle e_{a'b'}|e_{ab}\rangle \quad = \quad \delta_{a',a}\delta_{b',b}. \tag{2.18}$$

Eq. (2.17) can be written in the following form when expressed in terms of Alice and Bob's individual qubits:

$$\begin{aligned}
|\psi_{ABE}\rangle &= \frac{1}{\sqrt{2}}\sum_{k,a=0}^{1}|z_k, z_{k+a}\rangle\left(\sum_{b=0}^{1}\sqrt{p_{ab}}\omega^{kb}|e_{ab}\rangle\right) \\
&= \frac{1}{\sqrt{2}}\sum_{k,a=0}^{1}|y_k, y_{k+a}\rangle\left(\sum_{b=0}^{1}\mathrm{i}^b\sqrt{p_{b\,a+b+1}}\omega^{(a+k)b}|e_{b\,a+b+1}\rangle\right) \\
&= \frac{1}{\sqrt{2}}\sum_{k,a=0}^{1}|x_k, x_{k+a}\rangle\left(\sum_{b=0}^{1}\sqrt{p_{ba}}\omega^{(a+k)b}|e_{ba}\rangle\right),
\end{aligned} \tag{2.19}$$

which can be more conveniently expressed as

$$\begin{aligned}
|\psi_{ABE}\rangle &= \sum_{a,k=0}^{1}\sqrt{\frac{p_a^{(z)}}{2}}|z_k, z_{k+a}\rangle|f_{ak}^{z}\rangle \\
&= \sum_{a,k=0}^{1}\sqrt{\frac{p_a^{(y)}}{2}}|y_k, y_{k+a}\rangle|f_{ak}^{y}\rangle \\
&= \sum_{a,k=0}^{1}\sqrt{\frac{p_a^{(x)}}{2}}|x_k, x_{k+a}\rangle|f_{ak}^{x}\rangle.
\end{aligned} \tag{2.20}$$

Here, the various probabilities $p_a^{(m)}$ in the mth basis ($m = x, y, z$) are given by Eqs. (2.15) and (2.16), and each ancilla $|f_{ak}^{m}\rangle$ has been characterized using two indices: a parity index a which gives the parity of the two-qubit state it is attached to, and an index k giving the

state of Alice's qubit. These ancillas are related to $|e_{ab}\rangle$ in the following way:

$$\begin{aligned}
|f^z_{ak}\rangle &= \frac{1}{\sqrt{p^{(x)}_a}} \sum_{b=0}^{1} \sqrt{p_{ab}}\omega^{kb}|e_{ab}\rangle \\
|f^y_{ak}\rangle &= \frac{1}{\sqrt{p^{(y)}_a}} \sum_{b=0}^{1} \mathrm{i}^b \sqrt{p_{b\,a+b+1}}\omega^{(a+k)b}|e_{b\,a+b+1}\rangle \\
|f^x_{ak}\rangle &= \frac{1}{\sqrt{p^{(x)}_a}} \sum_{b=0}^{1} \sqrt{p_{ba}}\omega^{(a+k)b}|e_{ba}\rangle.
\end{aligned} \tag{2.21}$$

Using Eq. (2.18), it can be shown that these ancillas are normalized and have the following structure:

$$\begin{aligned}
\langle f^z_{a0}|f^z_{a1}\rangle &= \frac{p_{a0}-p_{a1}}{p_{a0}+p_{a1}} \equiv \lambda^{(z)}_a \\
\langle f^y_{a0}|f^y_{a1}\rangle &= \frac{p_{0\,a+1}-p_{1a}}{p_{0\,a+1}+p_{1a}} \equiv \lambda^{(y)}_a \\
\langle f^x_{a0}|f^x_{a1}\rangle &= \frac{p_{0a}-p_{1a}}{p_{0a}+p_{1a}} \equiv \lambda^{(x)}_a,
\end{aligned} \tag{2.22}$$

while ancilla states with different a's are orthogonal.

Based on this structure, we can divide Eve's ancillas $|f^m_{ak}\rangle$ in each basis m into two groups according to the parity bit a. The first group corresponds to $a = 0$ and refers to the situation when Alice and Bob obtain correlated results in the mth basis. The second group corresponds to the case $a = 1$, for which Alice and Bob obtain anticorrelated results. The $a = 0$ group occurs with probability $p^{(m)}_0$ while the $a = 1$ group occurs with probability $p^{(m)}_1$. The ancillas in the $a = 0$ group are orthogonal to those in the $a = 1$ group. Within each group however, the ancillas with different k's are non-orthogonal in general and have mutual inner product $\langle f^m_{a0}|f^m_{a1}\rangle = \lambda^{(m)}_a$. The structure of the ancillas is summarized graphically in Fig. 2.3.

2.2.2 General Strategy

Eve's strategy is as follows. She will wait for Alice and Bob to perform their measurement and announce their measurement bases as well as the qubits they intend to use for key generation. By eavesdropping on this classical communication between Alice and Bob,

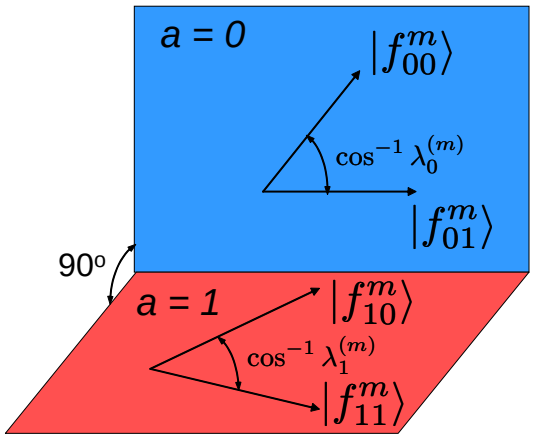


Figure 2.3: Structure of the ancillas $|f_{ak}^m\rangle$ in the mth basis. Ancillas with different parity bit a reside in orthogonal subspaces. Within each subspace, ancillas with different values of k have inner product $\lambda_a^{(m)}$ and are in general nonorthogonal.

Eve can identify the qubit pairs as well as the measurement bases in which to perform her attack. Her ancilla corresponding to each of those contributing pairs will then be a mixture of four possible states:

$$\varrho_E^m \;=\; \mathrm{Tr}_{\mathrm{AB}}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \sum_{a,k=0}^{1} \frac{p_a^{(m)}}{2} |f_{ak}^m\rangle\langle f_{ak}^m|, \tag{2.23}$$

where $m = x, y, z$ is the chosen basis of Alice and Bob and $\mathrm{Tr}_{\mathrm{AB}}\left[\cdot\right]$ denotes taking partial trace over Alice and Bob's degrees of freedom. Formally, this can be viewed as a transmission of information from Alice and Bob to Eve, with the information encoded in the quantum state ϱ_E^m of Eve's ancilla. Eve's optimal eavesdropping strategy is then to maximize this information transfer by choosing a suitable generalized measurement, known as a *Positive Operator Valued Measure* (POVM), to perform on her ancilla. A brief discussion of POVMs and their properties is given in Appendix B.

Another way to understand this transfer of information from Alice and Bob to Eve is as follows. From Eq. (2.20), the entangled state prepared by Eve in the mth basis is of the form

$$|\psi_{ABE}\rangle \;=\; \sum_{a,k=0}^{1} \sqrt{\frac{p_a^{(m)}}{2}} |m_k, m_{k+a}\rangle |f_{ak}^m\rangle, \tag{2.24}$$

while Alice and Bob's two-qubit state is given by

$$\varrho_{AB}^{m} \;=\; \mathrm{Tr_E}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \sum_{a,k,k'=0}^{1} \frac{p_a^{(m)}}{2} |m_k, m_{k+a}\rangle\langle m_{k'}, m_{k'+a}|. \quad (2.25)$$

When Alice and Bob measure their respective qubits, they will collapse Eve's ancilla space into an appropriate state. For those qubit pairs that contribute to key generation, the collapsed state will be one of the $|f_{ak}^m\rangle$'s, where m is the chosen basis. Specifically, if Alice and Bob measure k and $k+a$ respectively, Eve's collapsed state will be $|f_{ak}^m\rangle$. This occurs with probability $\langle m_k, m_{k+a}|\varrho_{AB}^m|m_k, m_{k+a}\rangle = \frac{p_a^{(m)}}{2}$. By determining the identity of this collapsed state, Eve will be able to deduce Alice and Bob's measurement results. Overall this is equivalent to saying that Alice and Bob sends the quantum mixed state $\varrho_E^m = \sum_{a,k=0}^{1} \frac{p_a^{(m)}}{2} |f_{ak}^m\rangle\langle f_{ak}^m|$ to Eve whose goal is to extract the maximum information possible from this mixed state to help her determine Alice and Bob's measurement results. This maximum amount of information available to Eve is also known in literature as the *accessible information* [Nielsen and Chuang, 2000].

2.2.3 Incoherent Attack

We shall assume that Eve carries out an *incoherent* attack in which she measures her ancillas one at a time. In contrast, in a *coherent* attack, she would measure some joint observable of more than one ancilla at a time, or construct Eq. (2.20) so that more than one pair of qubits are entangled with each ancilla[‡]. We shall give an example of how Eve can carry out the first type of coherent attack later on in Chapter 4.

We can rewrite the statistical operator describing Eve's state in the mth basis in Eq. (2.23) as follows:

$$\begin{aligned} \varrho_E^m &= \sum_{a=0}^{1} p_a^{(m)} \rho_a^m \\ &= p_0^{(m)} \rho_0^m + p_1^{(m)} \rho_1^m, \end{aligned} \quad (2.26)$$

[‡]As pointed out before, we assume that Alice and Bob protect themselves from this second possibility by checking for correlations between qubit pairs during state tomography.

where

$$\rho_0^m = \frac{1}{2}|f_{00}^m\rangle\langle f_{00}^m| + \frac{1}{2}|f_{01}^m\rangle\langle f_{01}^m| \tag{2.27}$$

describes Eve's ancilla in the situation where Alice and Bob obtain correlated results in the mth basis, which occurs with probability $p_0^{(m)}$, while

$$\rho_1^m = \frac{1}{2}|f_{10}^m\rangle\langle f_{10}^m| + \frac{1}{2}|f_{11}^m\rangle\langle f_{11}^m|. \tag{2.28}$$

describes her state for anticorrelated results, which occurs with probability $p_1^{(m)}$. Since ρ_0^m and ρ_1^m reside in orthogonal subspaces, Eve can discriminate between the two situations unambiguously.

The POVM measurement that optimizes the information transferred by Alice and Bob to Eve via the state ϱ_E^m will now be presented. The proof of optimality is given in Appendix C.

Optimal POVM

In the first step of the measurement, Eve projects her mixture of ancillas into one of the two orthogonal subspaces corresponding to the parity index a. The subspace that she projects into depends on the result of Alice and Bob's measurement. If Alice and Bob obtain correlated results, Eve will project into the $a = 0$ subspace and end up with the mixed state ρ_0^m; if they obtain anticorrelated results, she projects into the $a = 1$ subspace instead and ends up with ρ_1^m.

Next, she applies the measurement that maximizes the information she can extract from the mixed state ρ_a^m obtained in the first step. Now, ρ_a^m is composed of an equiprobable mixture of pure states. For example,

$$\rho_0^x = \frac{1}{2}|f_{00}^x\rangle\langle f_{00}^x| + \frac{1}{2}|f_{01}^x\rangle\langle f_{01}^x|, \tag{2.29}$$

which is an equal mixture of the pure states $|f_{00}^x\rangle$ and $|f_{01}^x\rangle$. The optimum measurement which maximizes the information she can extract from such a mixture is known in literature and is given by the so-called *square-root measurement* [Chefles, 2000a; Helstrom, 1976].

Square-Root Measurement

The square-root measurement[§] for Eve's projected mixed state $\rho_a^m = \sum_{k=0}^{1} \frac{1}{2}|f_{ak}^m\rangle\langle f_{ak}^m|$ is in fact the one that minimizes Eve's error in distinguishing between the two nonorthogonal states $|f_{a0}^m\rangle$ and $|f_{a1}^m\rangle$. The measurement is given by the set of POVM $\{|\omega_{ak}^m\rangle\langle\omega_{ak}^m|\}_{k=0,1}$, where

$$|\omega_{ak}^m\rangle \;=\; \frac{1}{\sqrt{2\rho_a^m}}|f_{ak}^m\rangle. \tag{2.30}$$

Given a state $|f_{ak}^m\rangle$ in the mth basis, the probability of inferring it correctly using the square-root measurement is then given by

$$\begin{aligned} p(\omega_{ak}^m|f_{ak}^m) &= \mathrm{Tr}\left[|\omega_{ak}^m\rangle\langle\omega_{ak}^m|f_{ak}^m\rangle\langle f_{ak}^m|\right] \\ &= |\langle f_{ak}^m|\omega_{ak}^m\rangle|^2 \equiv \eta_a^{(m)}. \end{aligned} \tag{2.31}$$

The probability of a wrong guess is $1-\eta_a^{(m)}$.

For the purpose of obtaining the probability in Eq. (2.31), we note that ρ_a^m has the eigenkets $|r_a^m\rangle = \frac{1}{\sqrt{2(1+\lambda_a^{(m)})}}\left(|f_{a0}^m\rangle + |f_{a1}^m\rangle\right)$ and $|s_a^m\rangle = \frac{1}{\sqrt{2(1-\lambda_a^{(m)})}}\left(|f_{a0}^m\rangle - |f_{a1}^m\rangle\right)$, with corresponding eigenvalues $1+\lambda_a^{(m)}$ and $1-\lambda_a^{(m)}$. We can then write out the diagonal form of $\frac{1}{\sqrt{\rho_a^m}}$ as follows:

$$\frac{1}{\sqrt{\rho_a^m}} \;=\; \frac{1}{\sqrt{1+\lambda_a^{(m)}}}|r_a^m\rangle\langle r_a^m| + \frac{1}{\sqrt{1-\lambda_a^{(m)}}}|s_a^m\rangle\langle s_a^m|. \tag{2.32}$$

Using the relation $\langle f_{ak}^m|f_{ak'}^m\rangle = \lambda_a^{(m)} + \delta_{k,k'}(1-\lambda_a^{(m)})$, we find that

$$\begin{aligned} \langle f_{ak}^m|r_a^m\rangle &= \sqrt{1+\lambda_a^{(m)}} \\ \langle f_{ak}^m|s_a^m\rangle &= (\delta_{k,0}-\delta_{k,1})\sqrt{1-\lambda_a^m}, \end{aligned} \tag{2.33}$$

and thus

$$\langle f_{ak}^m|\omega_{ak}^m\rangle \;=\; \frac{1}{\sqrt{2}}\left(\sqrt{1+\lambda_a^{(m)}} + \sqrt{1-\lambda_a^{(m)}}\right). \tag{2.34}$$

[§] See also Appendix B.3.

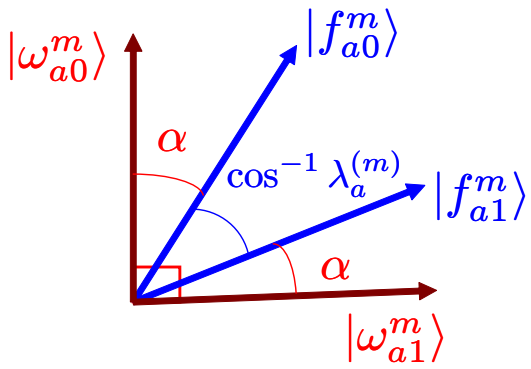


Figure 2.4: Geometrical interpretation of the square-root measurement.

Using the above result, we arrive at the following expression for Eq. (2.31):

$$\eta_a^{(m)} = \frac{1}{2}\left(1+\sqrt{1-(\lambda_a^{(m)})^2}\right). \tag{2.35}$$

Eq. (2.35) tells us that if Eve's ancillas $|f_{a0}^m\rangle$ and $|f_{a1}^m\rangle$ are orthogonal ($\lambda_a^{(m)} = 0$), she can distinguish them without error ($\eta_a^{(m)} = 1$); if her ancillas are parallel/antiparallel ($\lambda_a^{(m)} = \pm 1$), and hence indistinguishable, the best she can do is to resort to random guessing ($\eta_a^{(m)} = \frac{1}{2}$). These results are what we would expect intuitively.

We note that the square-root measurement has the following geometrical interpretation which we will find useful later on: Suppose we picture the two ancillas $|f_{a0}^m\rangle$ and $|f_{a1}^m\rangle$ being aligned at an angle of $\cos^{-1}\lambda_a^{(m)}$. The square-root measurement will then be a projective measurement whose projected states $|\omega_{a0}^m\rangle$ and $|\omega_{a1}^m\rangle$ are orthogonal to each other (ie. a *von Neumann measurement*) and have geometrical relations with the ancilla states as shown in Fig. 2.4. We can then express the ancilla states in terms of the square-root states as follows:

$$\begin{aligned} |f_{a0}^m\rangle &= \cos\alpha|\omega_{a0}^m\rangle + \sin\alpha|\omega_{a1}^m\rangle \\ |f_{a1}^m\rangle &= \sin\alpha|\omega_{a0}^m\rangle + \cos\alpha|\omega_{a1}^m\rangle. \end{aligned} \tag{2.36}$$

Furthermore, since $\langle f_{a0}^m|f_{a1}^m\rangle = \lambda_a^{(m)}$, we have

$$\cos^2\alpha = \frac{1}{2}\left(1+\sqrt{1-(\lambda_a^{(m)})^2}\right). \tag{2.37}$$

The probability of inferring a state correctly is then given by the probability of projecting the state into the correct square-root state, so that we have

$$\begin{aligned} \eta_a^{(m)} &= \cos^2\alpha \\ &= \frac{1}{2}\left(1+\sqrt{1-(\lambda_a^{(m)})^2}\right), \end{aligned} \tag{2.38}$$

as before.

Probabilities

For the purpose of determining the criteria for security, we summarize the probabilities of Alice, Bob and Eve getting the various results. Since Alice and Bob generate their cryptographic key only if their bases match, we shall consider only the situation where Alice and Bob have matching bases.

The probability of Alice getting result k and Bob measuring l in the same mth basis is

$$p^{(\mathrm{AB})}_{k,l|\text{basis } m} = \frac{p_0^{(m)}}{2}\delta_{k,l} + \frac{p_1^{(m)}}{2}(1-\delta_{k,l}). \tag{2.39}$$

The probability of Alice measuring k and Eve getting outcome ω_{al}^m for the square-root measurement (in the mth basis) can be expressed as

$$p^{(\mathrm{AE})}_{k,al|\text{basis } m} = \frac{p_a^{(m)}}{2}\left[\delta_{k,l}\eta_a^{(m)} + (1-\delta_{k,l})(1-\eta_a^{(m)})\right]. \tag{2.40}$$

The corresponding probability for Bob and Eve, $p^{(\mathrm{BE})}_{k,al|\text{basis } m}$, has a similar expression.

2.2.4 Security Criterion

Let us now derive the conditions for which our protocol is secure under an incoherent eavesdropping attack.

Intuitively, Alice and Bob are able to obtain a secure key if the information that they share

in terms of their bit correlation is greater than the information that Eve can obtain from them via her ancillas. A quantitative measure of the information shared between two parties is given by the so-called *mutual information* [Cover and Thomas, 1991]. The mutual information between two parties, say Alice and Bob, is given by

$$\mathcal{I}_{AB} \;=\; \sum_{k,l} p_{k,l}^{(\mathrm{AB})} \log_2 \frac{p_{k,l}^{(\mathrm{AB})}}{p_k^{(\mathrm{A})} p_l^{(\mathrm{B})}}, \tag{2.41}$$

where $p_{k,l}^{(\mathrm{AB})}$ is the joint probability of Alice and Bob having outcomes k and l respectively while $p_k^{(\mathrm{A})} = \sum_l p_{k,l}^{(\mathrm{AB})}$ and $p_l^{(\mathrm{B})} = \sum_k p_{k,l}^{(\mathrm{AB})}$ are the respective marginals. The mutual information is non-negative. It is 0 when Alice and Bob's outcomes are independent ($p_{k,l}^{(\mathrm{AB})} = p_k^{(\mathrm{A})} p_l^{(\mathrm{B})}$) and has a maximum value when Alice and Bob's outcomes are perfectly correlated. In the case of binary outcomes ($k, l = 0, 1$), $\mathcal{I}_{AB}$ has a maximum value of 1 for perfect correlation. Appendix D gives an intuitive argument as to why the mutual information can be used to quantify the amount of correlation between two ensembles.

Using the expression for Alice and Bob's joint probability in Eq. (2.39), we can compute the mutual information between Alice and Bob's data established in the mth basis. Doing so, we obtain the following:

$$\begin{aligned} \mathcal{I}_{AB}^{(m)} &= 1 + p_0^{(m)} \log_2 p_0^{(m)} + p_1^{(m)} \log_2 p_1^{(m)} \\ &= 1 - \mathrm{H}(p_0^{(m)}). \end{aligned} \tag{2.42}$$

We have expressed the final expression more conveniently in terms of the *binary entropy*, defined as $\mathrm{H}(p) = -p \log_2 p - (1-p) \log_2 (1-p)$. The entropy gives an indication of how random the events are in a probability distribution [Cover and Thomas, 1991]. In the case of binary probability distributions, the binary entropy $\mathrm{H}(p)$ has a maximum of 1 when $p = \frac{1}{2}$ (all events are equiprobable), and a minimum of 0 when $p = 0$ or 1 (one of the events always occurs).

Likewise, the mutual information between Alice and Eve in the mth basis computed using the expression for their joint probability in Eq. (2.40) is given by

$$\mathcal{I}_{AE}^{(m)} \;=\; 1 - \sum_{a=0}^{1} p_a^{(m)} \mathrm{H}(\eta_a^{(m)}). \tag{2.43}$$

Due to the symmetric nature of the quantum channel, the mutual information between Bob and Eve, $\mathcal{I}_{BE}^{(m)}$, is the same as that between Alice and Eve.

Csiszár-Körner Theorem

The condition for the tomographic protocol to be secure is given by the Csiszár-Körner (CK) theorem [Csiszár and Körner, 1978] which says that Alice and Bob can generate a secure key from their raw key sequence by means of a suitably chosen error-correcting code and classical two-way communication if the mutual information between them exceeds that between Eve and either one of them, i.e. security is assured as long as we are in the following *CK regime*:

$$\mathcal{I}_{AB} \quad > \quad \{\mathcal{I}_{AE}, \mathcal{I}_{BE}\}. \tag{2.44}$$

Note that due to the symmetric nature of the protocol, we have $\mathcal{I}_{AE} = \mathcal{I}_{BE}$. Furthermore, the *CK yield* is given by

$$\nu \quad = \quad \max\{\mathcal{I}_{AB} - \mathcal{I}_{AE}, 0\} \tag{2.45}$$

and it defines the rate at which a secure key can be generated in the CK theorem: a secure key of length νL can be obtained from a raw key sequence of length L by applying the CK theorem.

Now for each basis $m = x, y$ or z, we can define a corresponding CK yield for the rate at which a secure key can be generated using the data measured in that basis alone:

$$\nu_m \quad = \quad \max\{\mathcal{I}_{AB}^{(m)} - \mathcal{I}_{AE}^{(m)}, 0\}. \tag{2.46}$$

The yield for different bases will in general be different. It will be assumed here that Alice and Bob make use of data only from those bases that give them positive yield to establish their key while rejecting the data obtained from the remaining bases that give them zero

yield[¶]. The *average yield* for Alice and Bob's key in this case is then given by

$$\nu = \frac{1}{3}\nu_x + \frac{1}{3}\nu_y + \frac{1}{3}\nu_z. \tag{2.47}$$

2.2.5 Discussion

A Bell diagonal density matrix is characterized by four probabilities $\{p_{00}, p_{01}, p_{10}, p_{11}\}$ together with the normalization condition $p_{00} + p_{01} + p_{10} + p_{11} = 1$, so that only three of the probabilities are independent. Let us thus parameterize the probabilities using p_{11} (the proportion of $|z_{11}\rangle$ in the Bell mixture) and two angles θ, ϕ in the following way:

$$\begin{aligned} p_{00} &= (1 - p_{11}) \cos^2\theta \cos^2\phi \\ p_{01} &= (1 - p_{11}) \sin^2\theta \cos^2\phi \\ p_{10} &= (1 - p_{11}) \sin^2\phi. \end{aligned} \tag{2.48}$$

By considering the average yield ν over different values of p_{11}, θ and ϕ, we can determine those states for which the protocol is secure (the CK regime): these states have $\nu > 0$ so that a secure key can be extracted from them using the CK theorem. In Fig. 2.5, the CK regime for fixed p_{11} is shown over all possible values of θ and ϕ.

First, we note that as long as $p_{11} \gtrsim 0.765$, all Bell diagonal states will be secure. When p_{11} drops below this threshold, insecure states will start to appear. In fact, the first insecure state that appears is the Werner state $\frac{4p_{11}-1}{3}|z_{11}\rangle\langle z_{11}| + \frac{1-p_{11}}{3} 1 \otimes 1$. The Werner state was considered in the protocol of [Liang et al., 2003] and the same threshold of 0.765 was obtained. As p_{11} decreases further, fewer and fewer states remain secure until finally when we reach $p_{11} = \frac{1}{2}$, the Bell diagonal mixture becomes separable (see Chapter 3) and no secret bits can be obtained.

[¶]From their state tomography, Alice and Bob can determine the parameters p_{ab} and can thus agree beforehand on those bases which will give them positive yield.

Resistant States

From the figures, we can also identify certain states that remain secure against incoherent attacks as long as $p_{11} > \frac{1}{2}$. These resistant states are the *rank 2* states, given by

$$\begin{aligned}
&\text{‘00’ resistant state:} \quad (1-p_{11})|z_{00}\rangle\langle z_{00}| + p_{11}|z_{11}\rangle\langle z_{11}| \quad (\text{for which } \theta = 0, \phi = 0);\\
&\text{‘01’ resistant state:} \quad (1-p_{11})|z_{01}\rangle\langle z_{01}| + p_{11}|z_{11}\rangle\langle z_{11}| \quad (\theta = \tfrac{\pi}{2}, \phi = 0);\\
&\text{‘10’ resistant state:} \quad (1-p_{11})|z_{10}\rangle\langle z_{10}| + p_{11}|z_{11}\rangle\langle z_{11}| \quad (\phi = \tfrac{\pi}{2}).
\end{aligned} \tag{2.49}$$

For these rank 2 states, it can be shown that there are certain bases for which Eve is not able to extract any useful information from her ancilla. For example, consider the ‘00’ resistant state. The ancilla structure in the different bases are:

$$\begin{aligned}
|\langle f^z_{00}|f^z_{01}\rangle| = 1 \quad &, \quad |\langle f^z_{10}|f^z_{11}\rangle| = 1\\
|\langle f^y_{00}|f^y_{01}\rangle| = 1 \quad &, \quad |\langle f^y_{10}|f^y_{11}\rangle| = 2p_{11} - 1\\
|\langle f^x_{00}|f^x_{01}\rangle| = 1 \quad &, \quad |\langle f^x_{10}|f^x_{11}\rangle| = 1.
\end{aligned} \tag{2.50}$$

Hence for the x and z bases, Eve will not be able to distinguish between the ancilla states with different k values lying in the same a subspace. It follows that for the ‘00’ resistant state, if Alice and Bob only use data from the x and z bases to generate the key, Eve cannot extract any useful information about their key from her ancilla[‖]. In this sense, the ‘00’ state provides not just security against incoherent attacks, but *unconditional security* as it remains secure against any attack that Eve performs. Similarly for the ‘01’ resistant state, we have unconditional security in the y and z bases, while for the ‘10’ resistant state, we have unconditional security in the x and y bases.

[‖] This is because Eve knows only the parity index a characterizing Alice and Bob’s measurement but she is not able to determine the index k corresponding to Alice’s result — both indices are needed to deduce both Alice and Bob’s results

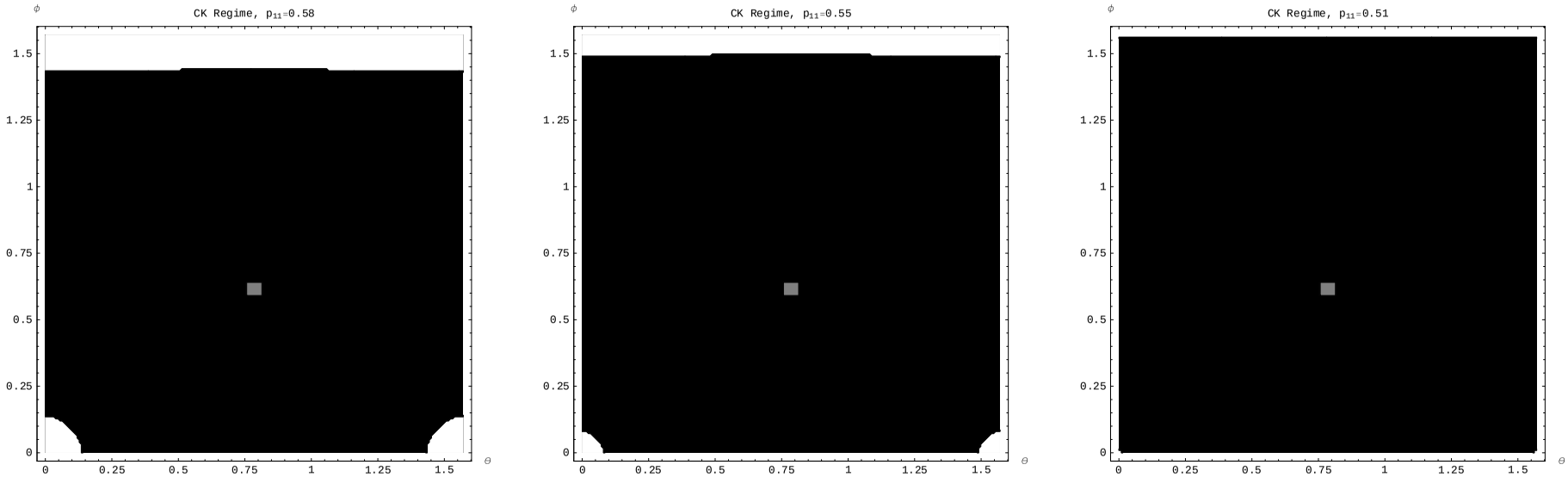


Figure 2.5: Comparison of secure regions for different values of p_{11}. White regions represent states which are secure. As a reference, the Werner state for which $p_{00} = p_{01} = p_{10} = \frac{1-p_{11}}{3}$ is indicated by the square.

2.2.6 Distillation

Based on the CK theorem, we can determine those Bell diagonal states which would give Alice and Bob a secure set of key. If there is too much noise in the channel however, it is possible for Eve to extract enough information from her ancilla so that her mutual information is higher than that between Alice and Bob. In this case, the CK theorem is not immediately applicable in obtaining a secure key. However, Alice and Bob may perform auxiliary steps so as to strengthen the correlation between their keys in order for the CK theorem to be applicable again. This procedure is known as *distillation* and will be the subject of the next two chapters. In general, Alice and Bob can opt to perform *classical distillation* whereby they select a subsequence of their established bit values in a systematic way, or carry out *quantum distillation* in which they pre-process their two-qubit state before measuring. We will apply both methods of distillation to the tomographic protocol and investigate the conditions for the methods to be successful.

Chapter 3

Entanglement Distillation

In the quantum method of distillation known as Entanglement Distillation (ED), Alice and Bob produce a smaller number of more strongly entangled qubit pairs from weakly entangled ones by means of local operations and classical communication [Deutsch et al., 1996; Alber et al., 2001]. In this chapter, the ED protocol will be described and the condition for the procedure to be successful in generating a secure key for Alice and Bob will be obtained.

3.1 ED Protocol

Suppose Alice and Bob initially share a large number n of qubit pairs sent from the source, each pair being in the same Bell diagonal state ϱ, so that the total state is $\varrho^{\otimes n}$. The proportion of the singlet state $|z_{11}\rangle$ present in each state ϱ (ie. the *singlet fraction*) is given by $\langle z_{11}|\varrho|z_{11}\rangle = p_{11}$. Their aim is to obtain a smaller number of pairs $\tilde{\varrho}^{\otimes m}$ ($m < n$) with a higher proportion of singlet fraction, $\langle z_{11}|\tilde{\varrho}|z_{11}\rangle > p_{11}$. To achieve this, Alice and Bob can carry out the following sequence of steps iteratively on their qubit pairs:

1. They pick two pairs, apply to each of them $U \otimes U^*$ *twirling*, ie. random unitary transformation of the form $U \otimes U^*$: Alice picks at random a unitary transformation U, applies it, and communicates to Bob which transformation she chooses; Bob will then follow up with U^* to his qubit. The net effect is transformation from ϱ to another

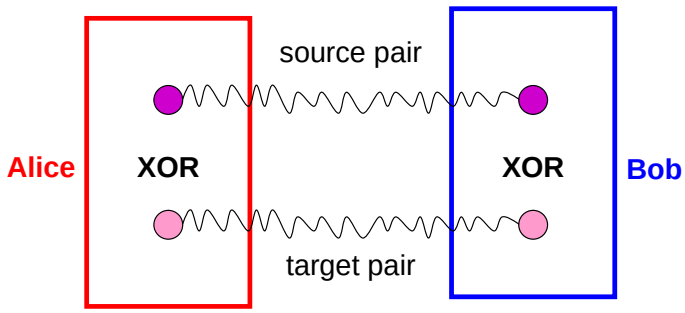


Figure 3.1: Bilateral quantum XOR operation.

state ϱ' whose singlet fraction remains unchanged:

$$\varrho \otimes \varrho \longrightarrow \varrho' \otimes \varrho'.$$

2. Each party performs unitary XOR on their respective qubits (see Fig. 3.1). The transformation is given by

$$\overset{\text{control}}{|z_k\rangle}\ \overset{\text{target}}{|z_{k'}\rangle} \quad \overset{\text{XOR}}{\longrightarrow} \quad \overset{\text{control}}{|z_k\rangle}\ \overset{\text{target}}{|z_{k\oplus k'}\rangle}\ .$$

   The first qubit is called the source qubit and the second one is the target qubit. They will obtain some complicated state $\hat{\varrho}$ after the operation.

3. Alice and Bob then perform a local measurement on their respective target qubits in the $\{|z_0\rangle, |z_1\rangle\}$ basis. They communicate the results of their measurement and if they obtain the same outcome, they will keep the source pair. The final state of the kept source pair is given by

$$\tilde{\varrho} \;=\; \frac{1}{\mathcal{N}} \mathrm{Tr}_{\mathcal{H}_t} \left[P_t \otimes 1_s \hat{\varrho} P_t \otimes 1_s \right], \tag{3.1}$$

   where the partial trace is perform over the Hilbert space $\mathcal{H}_t$ of the target pair, 1_s is the identity on the space of the source pair (since it is not measured), while $P_t = |z_0, z_0\rangle\langle z_0, z_0| + |z_1, z_1\rangle\langle z_1, z_1|$ acts on the target pair space and corresponds to the case where Alice and Bob's results agree. The normalization constant $\mathcal{N}$ is given by $\mathrm{Tr}\left[P_t \otimes 1_s \hat{\varrho} P_t \otimes 1_s\right]$. On the other hand, if the results of Alice and Bob's measurement disagree, the source pair is discarded.

It can be shown [Alber et al., 2001] that as long as the initial two-qubit state ϱ is entangled, Alice and Bob's distilled state $\tilde{\varrho}$ will have a higher singlet fraction than before. They may then apply the distillation procedure to the surviving distilled states again to obtain states with higher singlet fraction, and so on. Hence, by applying the protocol repeatedly to every surviving qubit pair, Alice and Bob can eventually drive the singlet fraction to 1 so that each of the surviving two-qubit states must individually approach the pure state $|z_{11}\rangle\langle z_{11}|$.

3.1.1 Peres-Horodecki Criterion

As pointed out earlier, the ED protocol will be successful as long as the initial pair of qubits are entangled. In the case of qubits, such a condition can also be expressed by the Peres-Horodecki Partial Transposition criterion [Peres, 1996]: A two-qubit state ϱ is quantum distillable if and only if it is a *non-positive partial transposed* (NPPT) state. A state ϱ is NPPT if $\varrho^{T_B} \not\geqslant 0$ so that it has at least one negative eigenvalue. Here, ϱ^{T_B} denotes partial transposition of ϱ with respect to Bob's basis only, ie. $\varrho = \sum_{k,l,m,n=0}^{1} \rho_{kl,mn}|z_k, z_l\rangle\langle z_m, z_n| \stackrel{[\cdot]^{T_B}}{\longrightarrow} \varrho^{T_B} = \sum_{k,l,m,n=0}^{1} \rho_{kl,mn}|z_k, z_n\rangle\langle z_m, z_l|$.

Taking the partial transpose of each of the Bell states, we have

$$|z_{ab}\rangle\langle z_{ab}| \quad \stackrel{[\cdot]^{T_B}}{\longrightarrow} \quad \frac{1}{2} - |z_{a+1\ b+1}\rangle\langle z_{a+1\ b+1}|. \tag{3.2}$$

so that partial transposition of Eq. (2.10) gives

$$\varrho^{T_B} \quad = \quad \sum_{a,b=0}^{1} \left(\frac{1}{2} - p_{a+1\ b+1}\right) |z_{ab}\rangle\langle z_{ab}|. \tag{3.3}$$

The eigenvalues of ϱ^{T_B} are thus $\left\{\frac{1}{2} - p_{ab}\right\}_{a,b=0}^{1}$. Applying the Peres-Horodecki criterion, we find that the state Eq. (2.10) is quantum distillable provided that

$$\max_{ab} p_{ab} \quad > \quad \frac{1}{2}. \tag{3.4}$$

As is evident from the nature of the ED protocol, this threshold is independent of the kind of eavesdropping attack Eve performs on the quantum channel.

The Peres-Horodecki criterion also gives the condition for a quantum state to be separable:

a state which is non-NPPT is separable. In our case, if $\max_{ab} p_{ab} \not> \frac{1}{2}$, Alice and Bob's two-qubit state ϱ becomes separable and can be written as a convex sum of product states:

$$\varrho \;=\; \sum_i p_i \varrho_i^{(A)} \otimes \varrho_i^{(B)}. \tag{3.5}$$

Eve can then blend the state ϱ from product states by sending each product state $\varrho_i^{(A)} \otimes \varrho_i^{(B)}$ to Alice and Bob respectively with probability p_i, and by doing so, ensure that no useful mutual information between Alice and Bob can be established for them to generate a secure key. This observation motivates us to require at least one of the p_{ab}'s in Eq. (2.10) to be more than $\frac{1}{2}$ in the protocol.

The ED procedure presented here is rather wasteful in terms of discarded particles – at least half of the particles (those used as targets) are lost at every iteration. In the next chapter, we shall look at another distillation method available for Alice and Bob — a classical method of post-selecting their measured bit values and processing them via two-way communication to obtain a distilled key sequence with stronger correlations. The classical method of distillation can be more attractive than ED by nature of its simplicity. There are quite a number of classical distillation methods, such as the parity-check procedure discussed in [Kaszlikowski et al., 2004]. We will be considering a protocol known as *Advantage Distillation* in the next chapter. The argument employed there can also be adopted for other classical distillation protocols.

Chapter 4

Classical Advantage Distillation

In Classical Advantage Distillation (AD) Alice and Bob process their bit values by means of classical two-way communication to obtain a distilled key sequence possessing stronger correlations. In this chapter, the AD protocol will be described, after which the condition for the protocol to be successful will be derived.

Earlier, we have applied Quantum Entanglement Distillation to the tomographic protocol and derived conditions for distillation to be successful. An important question that naturally arises is whether quantum methods of distillation are equivalent to classical ones in the sense that both offer the same amount of security. It will be shown at the end of this chapter that if an eavesdropper performs a coherent measurement on many quantum states simultaneously, classical methods of distillation are less effective than quantum ones. The same conclusion was obtained in [Kaszlikowski et al., 2003].

4.1 Protocol

We noted in Chapter 2 that in the prefect situation of $p_{11} = 1$, the tomographic protocol will always give Alice and Bob perfectly anticorrelated sets of keys. In non-ideal situations however, errors will arise so that their keys will no longer be perfectly anticorrelated.

To strengthen the correlation between their keys, Alice and Bob can perform AD by following the series of steps: They first divide their respective keys into blocks of length L. For each L-block, Alice rolls a 2-sided die. She adds (modulo 2) the value obtained to each bit

entry in her block. After that, she sends the processed block to Bob via a classical channel. Bob then subtracts (modulo 2) his corresponding L-block from Alice's processed block and examine the resulting string of bits.

If Bob ends up with a string of identical bits, he will accept that bit value into his distilled key sequence. He then communicates his decision to Alice so that she also enters the value she has rolled into her own set of distilled bits. This situation occurs when Alice and Bob

- start off with raw blocks that are perfectly anticorrelated, ie. blocks that differ by a constant shift, or
- start with identical raw blocks.

However, if any of the bits in Bob's subtracted sequence is different from the rest, he will reject that particular block and communicate his decision to Alice; she will likewise reject the bit value she had rolled for that block.

The protocol is summarized in Fig. 4.1

4.1.1 Probabilities

For those accepted blocks, we can identify two cases:

(I) Alice and Bob end up with different distilled bits. In this case, the raw blocks that they start out with must have been the perfectly anticorrelated;

(II) Alice and Bob end up with the same distilled bit. In this case, they start out with identical raw blocks.

Since Alice and Bob aim to establish anticorrelated sets of keys, Case (II) would give rise to errors in the distilled key sequence. Let us consider the rate at which the cases occur.

For large L, the Law of Large Numbers tells us that there will be approximately $\frac{L}{3}$ bits in the good block that result from Alice and Bob's z basis measurement. For the σ_z measurement, $p_1^{(z)}$ is the probability that Alice and Bob obtain anti-correlated results while $p_0^{(z)}$ is the probability that they obtain correlated results. Similarly, $\frac{L}{3}$ bits will result from y (x) basis

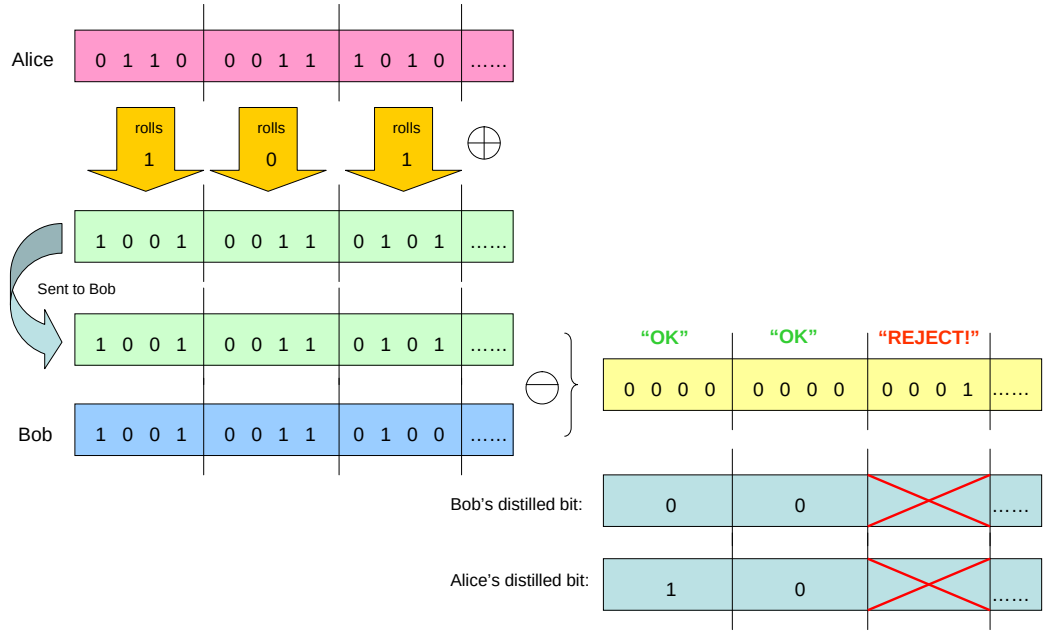


Figure 4.1: AD protocol for $L = 4$. Suppose Alice and Bob start out with the anticorrelated raw key sequences "0110" and "1001" respectively. Alice rolls the value '1', adds it to each entry in her block and obtains the processed sequence "1001". She sends this block over a classical channel to Bob who, after subtracting his block, obtains the distilled sequence "0000". Since all bits are the same, he will accept '0' into his distilled key sequence and communicate his decision to accept the nit to Alice. Alice will then keep her rolled value '1'. Alice and Bob thus end up with the anticorrelated distilled bits. Similarly if Alice and Bob start out with the same raw key sequence, they will end up with the same distilled bit. On the other hand, if any bit in Bob's subtracted sequence is different from all others, he will reject that particular block and communicate his decision to Alice; she will likewise reject that particular block.

measurement, and $p_1^{(y)}$ ($p_1^{(x)}$) is the probability that Alice and Bob obtain anti-correlated results while $p_0^{(y)}$ ($p_0^{(x)}$) is the probability that they obtain correlated results. Thus for an accepted block, Case (I) occurs with probability $\frac{(p_1^{(x)}p_1^{(y)}p_1^{(z)})^{L/3}}{(p_0^{(x)}p_0^{(y)}p_0^{(z)})^{L/3}+(p_1^{(x)}p_1^{(y)}p_1^{(z)})^{L/3}}$ while Case (II) occurs with probability $\frac{(p_0^{(x)}p_0^{(y)}p_0^{(z)})^{L/3}}{(p_0^{(x)}p_0^{(y)}p_0^{(z)})^{L/3}+(p_1^{(x)}p_1^{(y)}p_1^{(z)})^{L/3}}$. The *error rate* for Alice and Bob refers to the proportion of Case (II) blocks and is thus given by

$$E_{AB} = \frac{(p_0^{(x)}p_0^{(y)}p_0^{(z)})^{L/3}}{(p_0^{(x)}p_0^{(y)}p_0^{(z)})^{L/3} + (p_1^{(x)}p_1^{(y)}p_1^{(z)})^{L/3}}, \tag{4.1}$$

which, for $L \gg 1$ and $p_1^{(m)} > p_0^{(m)}$ for $m = x, y$ or z (since $p_{11} > \frac{1}{2}$), can be approximated by

$$E_{AB} \approx \left(\frac{p_0^{(x)} p_0^{(y)} p_0^{(z)}}{p_1^{(x)} p_1^{(y)} p_1^{(z)}} \right)^{L/3}. \tag{4.2}$$

For large L we have $E_{AB} \to 0$ so that the error rate in Alice's and Bob's distilled key decreases and their distilled key becomes perfectly anticorrelated as the block length becomes large.

In the case of Eve, it is possible for her to intercept the processed blocks that Alice sends to Bob via the classical channel. She can also eavesdrop on their communication to find out which of the blocks are accepted or rejected. For those accepted blocks, her goal is to deduce the distilled bit for each block. We shall consider two strategies at her disposal: incoherent and coherent attacks.

4.2 Incoherent Attack on AD

For each raw block of length L, Eve has in her possession ancillas corresponding to each of Alice and Bob's measurements that give rise to the block. In an incoherent attack, she distinguishes those ancillas one by one to deduce Alice and Bob's bit values for each entry in the raw block. Like Bob, she will then subtract Alice's processed block from her own to obtain the distilled bit*. Typically, Eve's block will be inhomogeneous after subtraction so she decides by majority voting which bit value to assign to a particular block, i.e. she chooses the value which occurs most frequently in her subtracted block, and if there are the same number of 0s as 1s, she picks one of them at random. To obtain the condition for AD to be successful under an incoherent attack by Eve, we will compare Eve's error rate to Alice and Bob's error rate E_{AB} derived earlier.

Consider first the Case (I) blocks. For this case, Alice and Bob start out with anticorrelated raw blocks. Eve's corresponding ancillas will then reside in the $a = 1$ subspace. To distinguish the individual ancillas, we assume that Eve performs a square-root measurement on each of them as such a measurement gives her the least probability of error in her

*Eve is able to intercept Alice's block as it is transmitted over a classical channel.

state discrimination. Eve thus guesses each entry in a block correctly with the following probabilities:

- $\eta_1^{(x)}$ if Alice and Bob measure in the x basis;
- $\eta_1^{(y)}$ if they measure in the y basis;
- $\eta_1^{(z)}$ if they measure in the z-basis,

while she guesses an entry incorrectly with the probabilities

- $1-\eta_1^{(x)}$ if Alice and Bob measure in the x basis;
- $1-\eta_1^{(y)}$ if they measure in the y basis;
- $1-\eta_1^{(z)}$ if they measure in the z-basis.

Since Eve applies majority voting, she will assign the wrong distilled bit whenever she guesses more than half of the entries in the block wrongly. If the same number of 0s and 1s appear in her guesses, she picks one of them at random and makes errors half of the time. Eve's error rate is thus given by:

$$\begin{aligned} E_{BE}^{(I)} \;=\; & \sum_{\sum_i e_i > \frac{L}{2}} \left(\begin{array}{c} \frac{L}{3} \\ e_x \end{array} \right) (1-\eta_1^{(x)})^{e_x} (\eta_1^{(x)})^{\frac{L}{3}-e_x} \left(\begin{array}{c} \frac{L}{3} \\ e_y \end{array} \right) (1-\eta_1^{(y)})^{e_y} (\eta_1^{(y)})^{\frac{L}{3}-e_y} \\ & \times \left(\begin{array}{c} \frac{L}{3} \\ e_z \end{array} \right) (1-\eta_1^{(z)})^{e_z} (\eta_1^{(z)})^{\frac{L}{3}-e_z} \\ & + \frac{1}{2} \sum_{\sum_i e_i = \frac{L}{2}} \left(\begin{array}{c} \frac{L}{3} \\ e_x \end{array} \right) (1-\eta_1^{(x)})^{e_x} (\eta_1^{(x)})^{\frac{L}{3}-e_x} \left(\begin{array}{c} \frac{L}{3} \\ e_y \end{array} \right) (1-\eta_1^{(y)})^{e_y} (\eta_1^{(y)})^{\frac{L}{3}-e_y} \\ & \times \left(\begin{array}{c} \frac{L}{3} \\ e_z \end{array} \right) (1-\eta_1^{(z)})^{e_z} (\eta_1^{(z)})^{\frac{L}{3}-e_z}, \end{aligned} \tag{4.3}$$

where e_i is the number of errors made in the i^{th} basis. The second summation arises from the situation when Eve has to assign 0 or 1 at random to the block in the event that the number of 0s and 1s in the block are equal.

For large L, we can approximate the summations in Eq. (4.3) by the main contributing

terms, so that

$$E_{AE}^{(I)} \sim \left(\begin{array}{c} \frac{L}{3} \\ \frac{L}{6} \end{array} \right) (1-\eta_1^{(x)})^{\frac{L}{6}} (\eta_1^{(x)})^{\frac{L}{6}} \times \left(\begin{array}{c} \frac{L}{3} \\ \frac{L}{6} \end{array} \right) (1-\eta_1^{(y)})^{\frac{L}{6}} (\eta_1^{(y)})^{\frac{L}{6}} \times \left(\begin{array}{c} \frac{L}{3} \\ \frac{L}{6} \end{array} \right) (1-\eta_1^{(z)})^{\frac{L}{6}} (\eta_1^{(z)})^{\frac{L}{6}}. \quad (4.4)$$

By applying Stirling's approximation we have $\left(\begin{array}{c} \frac{L}{3} \\ \frac{L}{6} \end{array} \right) \sim 2^{\frac{L}{3}}$, so that we can approximate Eq. (4.4) by

$$E_{AE}^{(I)} \sim 2^L \left[\eta_1^{(x)} \eta_1^{(y)} \eta_1^{(z)} (1-\eta_1^{(x)})(1-\eta_1^{(y)})(1-\eta_1^{(z)}) \right]^{\frac{L}{6}}. \quad (4.5)$$

Similarly for Case (II) where Alice and Bob start out with correlated raw blocks, the error rate for Eve is given by:

$$E_{AE}^{(II)} \sim 2^L \left[\eta_0^{(x)} \eta_0^{(y)} \eta_0^{(z)} (1-\eta_0^{(x)})(1-\eta_0^{(y)})(1-\eta_0^{(z)}) \right]^{\frac{L}{6}}. \quad (4.6)$$

The *total* error rate for Eve is thus given by

$$\begin{aligned} E_{AE} &= p(\text{Case I}) \cdot E_{BE}^{(I)} + p(\text{Case II}) \cdot E_{BE}^{(II)} \\ &\sim \frac{(p_1^{(x)} p_1^{(y)} p_1^{(z)})^{L/3}}{(p_0^{(x)} p_0^{(y)} p_0^{(z)})^{L/3} + (p_1^{(x)} p_1^{(y)} p_1^{(z)})^{L/3}} E_{BE}^{(I)} \\ &\quad + \frac{(p_0^{(x)} p_0^{(y)} p_0^{(z)})^{L/3}}{(p_0^{(x)} p_0^{(y)} p_0^{(z)})^{L/3} + (p_1^{(x)} p_1^{(y)} p_1^{(z)})^{L/3}} E_{BE}^{(II)} \end{aligned} \quad (4.7)$$

Since $p(\text{Case I})$ goes to 1 while $p(\text{Case II})$ goes to 0 for large L, we can approximate Eq. (4.7) by the first term only:

$$E_{BE} \approx 2^L \left[\eta_1^{(x)} \eta_1^{(y)} \eta_1^{(z)} (1-\eta_1^{(x)})(1-\eta_1^{(y)})(1-\eta_1^{(z)}) \right]^{\frac{L}{6}}. \quad (4.8)$$

By comparing error rates [Maurer, 1993], we can obtain the condition for AD to be success-

ful under an incoherent attack. This condition is given by

$$\lim_{L\to\infty} \frac{E_{AB}}{E_{AE}} \quad < \quad 1, \tag{4.9}$$

which reduces to

$$\frac{p_0^{(x)}}{p_1^{(x)}}\frac{p_0^{(y)}}{p_1^{(y)}}\frac{p_0^{(z)}}{p_1^{(z)}} \quad < \quad 8\sqrt{\eta_1^{(x)}\eta_1^{(y)}\eta_1^{(z)}(1-\eta_1^{(x)})(1-\eta_1^{(y)})(1-\eta_1^{(z)})}. \tag{4.10}$$

For the special case of Werner states, we have $p_{00} = p_{01} = p_{10} = \frac{1-p_{11}}{3}$, so that $p_0^{(x)} = p_0^{(y)} = p_0^{(z)}$, $p_1^{(x)} = p_1^{(y)} = p_1^{(z)}$ and $\eta_1^{(x)} = \eta_1^{(y)} = \eta_1^{(z)}$. Eq. (4.10) then reduces to

$$\frac{p_0^{(z)}}{p_1^{(z)}} \quad < \quad 2\sqrt{\eta_1^{(z)}(1-\eta_1^{(z)})}. \tag{4.11}$$

A similar result was obtained in [Brußet al., 2003].

4.3 Coherent Attack on AD

As pointed out before in Chapter 2, the tomography requirement of Alice and Bob ensures that Eve cannot prepare a state that would give her some additional correlations across different qubit pairs as such correlations would appear in Alice and Bob's data and can be picked up by them. This considerably reduces the number of coherent eavesdropping strategies Eve can use. In fact, the only possibility of a coherent attack for Eve is to collect her ancillas and perform some collective measurements on them. We shall consider such attacks in this section. To illustrate the possible advantages that such coherent attacks have over incoherent ones, we shall make use of a particularly simple scheme of attack that was presented in [Kaszlikowski et al., 2003]. Instead of measuring her set of L ancillas one-by-one as in an incoherent attack, Eve will perform a collective measurement on *all* the L ancillas. It will be shown that by further eavesdropping on the communication between Alice and Bob during the distillation process, Eve will be able to learn much more about the distilled bit than if she were to measure her ancillas one by one.

Consider first a Case (I) block. As an example, suppose that Alice and Bob start out with the blocks '0110' and '1001' respectively for $L = 4$, and that Alice's random bit is 1.

After addition (modulo 2), she sends the processed block '1001' to Bob via a classical channel. Eve is able to intercept this piece of information. Furthermore, she can project her corresponding block of ancilla states into the appropriate a-subspace corresponding to Alice and Bob having a correlated or anticorrelated block. Doing this, she knows that Alice and Bob start out with anticorrelated raw blocks (i.e. Case (I) blocks). Eve then proceeds to deduce the following possibilities:

1. If Alice's random bit is '0' (and since the intercepted processed block is '1001'), Alice and Bob must have started out with raw blocks '1001' and '0110' respectively. Furthermore, by by eavesdropping on the information exchanged during the basis reconciliation stage, Eve knows the bases that Alice and Bob used for each entry in the block. Suppose Alice and Bob had measured in the bases x, y, x, z for the respective entries in the block. The corresponding ancilla state that she holds in this case will then be $|f^x_{11}\rangle|f^y_{10}\rangle|f^x_{10}\rangle|f^z_{11}\rangle$.

2. If Alice's random bit is '1', Alice and Bob must have started out with raw blocks '0110' and '1001' respectively. If the measurement bases had been x, y, x, z respectively, the ancilla state that Eve holds will then be $|f^x_{10}\rangle|f^y_{11}\rangle|f^x_{11}\rangle|f^z_{10}\rangle$.

The two possible Case (I) ancilla states occur with equal probability, and their mutual inner product is

$$(\lambda_1^{(x)})^{n_x}(\lambda_1^{(y)})^{n_y}(\lambda_1^{(z)})^{n_z},$$

where n_m is the number of times the basis m was measured. In the above example, this gives $(\lambda_1^{(x)})^2\lambda_1^{(y)}\lambda_1^{(z)}$. The optimal measurement to distinguish these two equiprobable states is then given by the square root measurement and the probability of a correct inference given by

$$\frac{1}{2}\left(1+\sqrt{1-\left[(\lambda_1^{(x)})^{n_x}(\lambda_1^{(y)})^{n_y}(\lambda_1^{(z)})^{n_z}\right]^2}\right).$$

In general, for each Case (I) block of length L, Eve needs to distinguish just two equiprobable L-ancilla states with mutual inner product $(\lambda_1^{(x)})^{n_x}(\lambda_1^{(y)})^{n_y}(\lambda_1^{(z)})^{n_z}$. In contrast for an incoherent strategy, Eve would have 2^L possible states to distinguish, which scales exponentially with block length L.

Now, for large L, we have $n_x, n_y, n_z \approx \frac{L}{3}$. Eve's probability of correctly inferring a partic-

ular Case (I) L-ancilla state is then given by

$$\frac{1}{2}\left(1+\sqrt{1-(\lambda_1^{(x)}\lambda_1^{(y)}\lambda_1^{(z)})^{\frac{2L}{3}}}\right) \approx 1-\frac{1}{4}(\lambda_1^{(x)}\lambda_1^{(y)}\lambda_1^{(z)})^{\frac{2L}{3}}. \tag{4.12}$$

Her error rate for Case (I) blocks is thus

$$E_{BE}^{(I)} \approx \frac{1}{4}(\lambda_1^{(x)}\lambda_1^{(y)}\lambda_1^{(z)})^{\frac{2L}{3}}. \tag{4.13}$$

For large L, this error rate goes to 0 because Eve's L-ancilla states approach orthogonality with increasing L. Contrast this with the incoherent case where Eve's ancillas does not become easier to distinguish with increasing L.

For Case (II) blocks, we can invoke a similar argument and arrive at the corresponding expression for Eve's error rate:

$$E_{BE}^{(II)} \approx \frac{1}{4}(\lambda_0^{(x)}\lambda_0^{(y)}\lambda_0^{(z)})^{\frac{2L}{3}}. \tag{4.14}$$

As before, Eve's *total* error rate is given by

$$\begin{aligned} E_{AE} &= p(\text{Case I})\cdot E_{BE}^{(I)} + p(\text{Case II})\cdot E_{BE}^{(II)} \\ &\approx E_{BE}^{(I)} \\ &\approx \frac{1}{4}(\lambda_1^{(x)}\lambda_1^{(y)}\lambda_1^{(z)})^{\frac{2L}{3}}. \end{aligned} \tag{4.15}$$

Finally, we can obtain the condition for AD to be possible by comparing error rates:

$$\begin{aligned} \lim_{L\to\infty}\frac{E_{AB}}{E_{AE}} &< 1 \\ \Rightarrow \frac{p_0^{(x)}}{p_1^{(x)}}\frac{p_0^{(y)}}{p_1^{(y)}}\frac{p_0^{(z)}}{p_1^{(z)}} &< \left(\lambda_1^{(x)}\lambda_1^{(y)}\lambda_1^{(z)}\right)^2. \end{aligned} \tag{4.16}$$

4.4 Discussion

To determine those Bell diagonal sates for which AD can be successfully carried out to give Alice and Bob a secure set of key, we can fix p_{11} as before and parameterize the remaining

probabilities as follows

$$\begin{aligned} p_{00} &= (1-p_{11})\cos^2\theta\cos^2\phi \\ p_{01} &= (1-p_{11})\sin^2\theta\cos^2\phi \\ p_{10} &= (1-p_{11})\sin^2\phi. \end{aligned} \tag{4.17}$$

4.4.1 Coherent vs Incoherent Attack

For an incoherent attack on AD, we can use Eq. (4.10) to verify numerically that AD is successful as long as $p_{11} > \frac{1}{2}$. This result was in fact proven in [Acín et al., 2003].

On the other hand, if Eve carries out a coherent attack, we can see from Fig. 4.2 that certain states which are secure under an incoherent attack will no longer be so when Eve carries out coherent eavesdropping. This is because coherent attacks can provide Eve with a lot more information than an incoherent one, thereby causing certain states which are secure under incoherent eavesdropping to become insecure under the coherent attack. Coherent attacks are thus more powerful than incoherent ones.

In addition, we can notice certain states that remain secure under both coherent and incoherent attacks (as long as $p_{11} > \frac{1}{2}$). These are the rank 2 resistant states that were seen in Chapter 2 to be unconditionally secure (in certain bases) regardless of the kind of attack carried out by Eve.

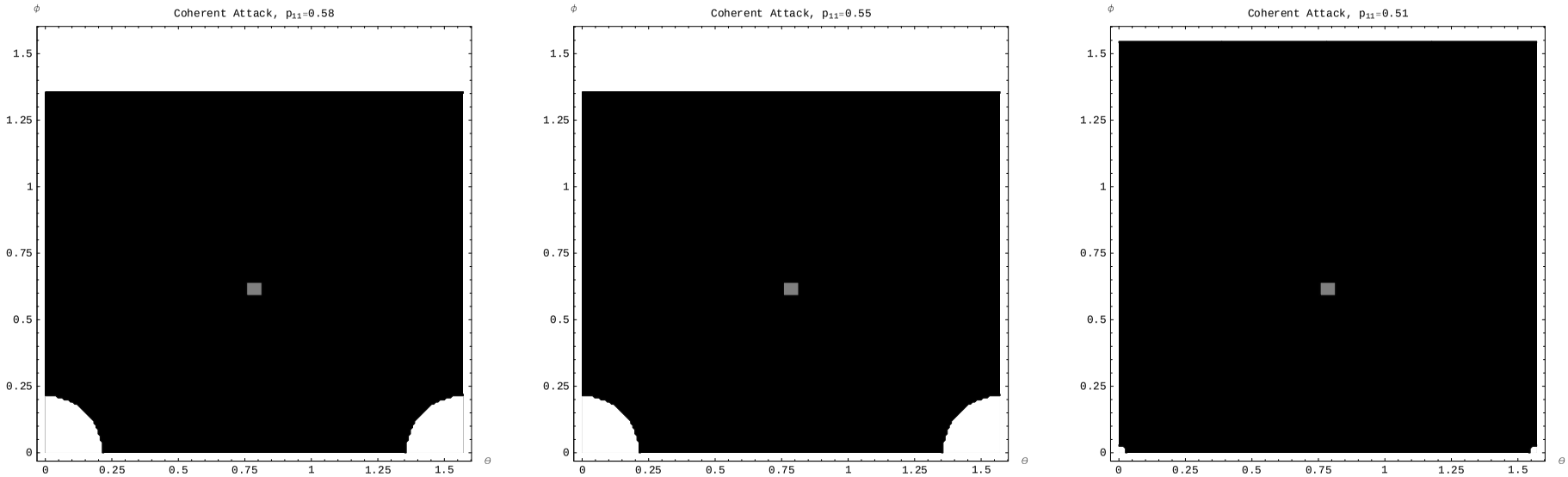


Figure 4.2: Comparison of secure regions in Advantage Distillation for different values of p_{11} under a coherent attack. White regions represent states which are secure. As a reference, the Werner state for which $p_{00} = p_{01} = p_{10} = \frac{1-p_{11}}{3}$ is indicated by the square.

4.4.2 Quantum and Classical Distillation Are Not Equivalent

The criteria for AD and ED to be successful are summarized below

$$\begin{aligned} \text{ED} &: p_{11} > \frac{1}{2} \\ \text{AD (incoherent attack)} &: p_{11} > \frac{1}{2} \\ \text{AD (coherent attack)} &: \frac{p_0^{(x)}}{p_1^{(x)}}\frac{p_0^{(y)}}{p_1^{(y)}}\frac{p_0^{(z)}}{p_1^{(z)}} < \left(\lambda_1^{(x)}\lambda_1^{(y)}\lambda_1^{(z)}\right)^2 \quad \text{(see Fig. 4.2).} \end{aligned} \tag{4.18}$$

If Eve is restricted only to incoherent attacks, we see that ED is equivalent to AD. As long as $p_{11} > \frac{1}{2}$, Alice and Bob do not need ED because AD works equally well and does not require the collective operations on qubits that ED requires and which are difficult to realize experimentally.

However, if Eve is capable of carrying out a coherent attack, ED will be more powerful than AD because ED is effective over a larger set of Bell diagonal states than AD. This can be seen from Fig. 4.2 where more and more states fall into the black regions where AD fails and only ED is possible, as p_{11} approaches $\frac{1}{2}$.

Although we have considered only two specific protocols to illustrate the inequivalence of the classical and quantum methods of key distillation, argument along a similar line can be applied to other distillation protocols (see for example the parity check protocol presented in [Kaszlikowski et al., 2004]). We thus conclude that classical methods of secure key distillation are less effective than quantum entanglement distillation protocols if an eavesdropper performs a coherent measurement on many quantum ancilla states simultaneously. The same conclusion was arrived at in [Acín et al., 2003].

Chapter 5

Tomographic Quantum Cryptography with a Quantum Dot Single Photon Source

In the final part of this thesis, the practical aspect of QKD will be considered. Experimental quantum cryptography is a sufficiently advanced field so that there is already the possibility for commercialization of some of the QKD devices. However, security analysis of such generic devices is not always straightforward.

Recently, there was a scheme proposed by Fattal *et al.* [Fattal et al., 2004] to generate polarization entangled photons by pulsed laser excitation of a single quantum dot. Such a method has the advantage of producing entangled photons that are triggered on demand and is particularly suitable as a source of photons in quantum cryptography schemes based on shared entanglement such as the Ekert91 and BBM92. In this chapter, we apply this scheme as a source of photons for our tomographic protocol and analyze its security.

5.1 Setup

The whole idea behind Fattal's scheme lies in generating triggered single photons from a quantum dot, using a method proposed by Santori *et al.* [Santori et al., 2001]. Such a method involves pulsed optical excitation of a single quantum dot followed by spectral

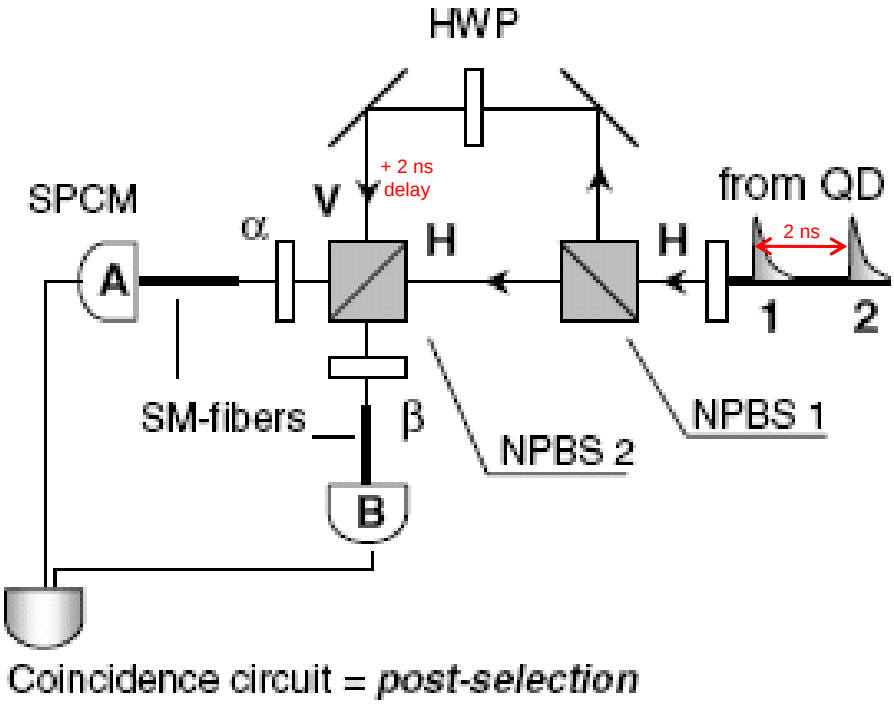


Figure 5.1: Experimental setup: Single photons produced in pairs separated by 2ns from a quantum dot microcavity device are sent through a single mode fiber and have their polarization rotated to H. They are split by a nonpolarizing beamsplitter (NPBS 1). The polarization is changed to V in the longer arm of the Mach-Zehnder configuration. The two paths of the interferometer merge at a second nonpolarizing beamsplitter (NPBS 2). One time out of four, the first emitted photon takes the long path while the second photon takes the short path, in which case their wave functions overlap at NPBS2. The output modes of NPBS 2 are matched to single mode (SM) fibers for subsequent detection. The detectors are linked to a time-to-amplitude converter for a record of coincidence counts, effectively implementing the post-selection.

filtering to remove all but the last emitted photons. The main advantages of this method are that multiphoton pulses can be suppressed and it allows one to generate consecutively two photons that are quantum mechanically indistinguishable.

This idea of obtaining triggered single photons can be extended to a scheme for producing polarization-entangled photons by incorporating it into the setup shown in Fig. 5.1. Suppose we wish to produce polarization-entangled photons in the singlet state:

$$|z_{11}\rangle \quad = \quad |z_0, z_1\rangle - |z_1, z_0\rangle, \tag{5.1}$$

where the '0' and '1' stand for horizontal and vertical polarization respectively. In the setup,

triggered photons are generated in pairs from the single-photon source using laser pulses. The photon pairs are then sent through a Mach-Zehnder type interferometer setup. The idea is to "collide" these photons with orthogonal polarizations at two conjugated input ports of a nonpolarizing beam splitter (NPBS). Quantum interference effect ensures that photons simultaneously detected at different output ports of the NPBS will ideally be entangled in the form Eq. (5.1).

This method of generating entangled photons has the particular advantage of allowing the users to generate entangled photons on demand and is particularly suitable as a source of photons in quantum cryptography schemes based on shared entanglement. Let us apply this scheme as a source of entangled qubits for our Tomographic QKD protocol. The aim here is to analyze the security of the protocol based on this scheme of generating entangled photons, thereby obtaining some useful results that could also be applied to other QKD schemes based on such a photon source.

Due to imperfections in the experimental setup, the two-photon state produced from the source is not a pure singlet state in general, but will instead be of the following form in the say, z basis [Fattal et al., 2004]:

$$\varrho^z = \frac{1}{2}\begin{pmatrix} 2\alpha & & & \\ & \beta_1+\beta_2+2\gamma & \beta_1-\beta_2 & \\ & \beta_1-\beta_2 & \beta_1+\beta_2-2\gamma & \\ & & & 2\alpha \end{pmatrix}, \tag{5.2}$$

where

$$\begin{aligned} \alpha &= \frac{2g}{\frac{R}{T}+\frac{T}{R}+4g} \\ \beta_1 &= \frac{\frac{R}{T}+\frac{T}{R}-2V}{2(\frac{R}{T}+\frac{T}{R})+8g} \\ \beta_2 &= \frac{\frac{R}{T}+\frac{T}{R}+2V}{2(\frac{R}{T}+\frac{T}{R})+8g} \\ \gamma &= \frac{\frac{R}{T}-\frac{T}{R}}{2(\frac{R}{T}+\frac{T}{R})+8g}. \end{aligned} \tag{5.3}$$

The significance of the experimentally accessible parameters R, T, V and g is as follows: R (T) denotes the reflectivity (transmittivity) of the beamsplitters in the Mach-Zehnder

interferometer used in the experiment. The parameter V denotes the overlap of the wave packets of two consecutive photons that give rise to coincidence events in the experiment, and g is the equal time second-order correlation function, and is related to the probability of obtaining unwanted coincidence counts due to residual two-photon pulses from the quantum dot. In the ideal situation, we have $R = T$ (perfect beamsplitters), $V = 1$ and $g = 0$. Furthermore, in order for entanglement to exist in the two photon state, we require $V > 2g$ from the Peres-Horodecki Partial Transposition criterion (see Chapter 3).

We can also express the density matrix Eq. (5.2) in the Bell basis $\{|m_{ab}\rangle\}_{a,b=0,1}$. As before, $|m_{ab}\rangle = \sum_{k=0}^{1} \frac{1}{\sqrt{2}} \omega^{kb} |m_k \; m_{k+a}\rangle$ (where $\omega = -1$) denotes the Bell state in the mth basis ($m = x, y, z$). We then have

$$\begin{aligned} \varrho_{\text{Bell}}^{(z)} &= \begin{pmatrix} \alpha & & & \\ & \alpha & & \\ & & \beta_1 & \gamma \\ & & \gamma & \beta_2 \end{pmatrix} \\ \varrho_{\text{Bell}}^{(y)} = \varrho_{\text{Bell}}^{(x)} &= \begin{pmatrix} \alpha & & & \\ & \beta_1 & & -\gamma \\ & & \alpha & \\ & -\gamma & & \beta_2 \end{pmatrix} \end{aligned} \tag{5.4}$$

for the z, y and x Bell state representation respectively.

From their state tomography, Alice and Bob can make sure that their two-photon state is always in the form Eq. (5.4). Furthermore, they can determine the parameters $\frac{R}{T}$, g and V that affect the security of their key. From these parameters, they can compute, for each basis, the maximal strength of correlations between Eve and any one of them. The Csiszár-Körner theorem then guarantees that if the correlations between Alice and Bob are stronger than those between Eve and either of them, a secure key can be established through one-way error correcting codes, with efficiency given by the CK yield. For each basis, there is a CK yield for Alice and Bob's bit data, and they can find out which basis will give them a positive CK yield. They will then make use of data only from those bases with positive yield to establish their key, rejecting the bits obtained from the remaining measurements.

5.2 Eavesdropping

We now consider Eve's attack on the protocol. As before, we assume the worst-case scenario in which she is in full control of the photon-distributing source, and that all the factors that contribute to experimental imperfections (parameters R, T, g and V) are due to her eavesdropping activities.

In order to obtain as much information as possible about the key generated by Alice and Bob, Eve entangles their photons with ancilla states $|e_{ab}\rangle$ in her possession. She prepares the following state:

$$|\psi_{ABE}\rangle \quad = \quad \sqrt{\alpha}|z_{00}\rangle|e_{00}\rangle + \sqrt{\alpha}|z_{01}\rangle|e_{01}\rangle + \sqrt{\beta_1}|z_{10}\rangle|e_{10}\rangle + \sqrt{\beta_2}|z_{11}\rangle|e_{11}\rangle, \tag{5.5}$$

where

$$\langle e_{a'b'}|e_{ab}\rangle \quad = \quad \begin{cases} \delta_{a,a'}\delta_{b,b'}, & \text{if } a = 0; \\ \delta_{a,a'}(1-\delta_{b,b'})\frac{\gamma}{\sqrt{\beta_1\beta_2}} + \delta_{a,a'}\delta_{b,b'}, & \text{if } a = 1. \end{cases} \tag{5.6}$$

Tracing out Eve's degree of freedom in $|\psi_{ABE}\rangle\langle\psi_{ABE}|$ gives the mixed state Eq. (5.4) that Alice and Bob expect, and this purification is the most general one as far as eavesdropping is concerned. As before, we note that because of the tomography requirement of Alice and Bob, Eve cannot prepare a state that would give her some additional correlations across different photon pairs emitted by the source as such correlations would appear in Alice and Bob's data and can be picked up by them (we assume that they look out for such correlations in their state tomography). This considerably reduces the number of coherent eavesdropping strategies Eve can use. The only possibility of a coherent attack for Eve is to collect her ancillas and perform some collective measurements on them. We shall only consider here the case where Eve measures her ancillas one by one, although the treatment of a strategy based on collective measurements can be done using the approach presented in Chapter 4.

Eve's purification Eq. (5.5), when expressed in the x, y and z bases, reads

$$\begin{aligned}
|\psi_{ABE}\rangle &= \sum_{k,a=0}^{1} \sqrt{\mu_{ak}^{(z)}}|z_k,\ z_{k+a}\rangle|f_{ak}^{z}\rangle \\
&= \sum_{k,a=0}^{1} \sqrt{\mu_{ak}^{(y)}}|y_k,\ y_{k+a}\rangle|f_{ak}^{y}\rangle \\
&= \sum_{k,a=0}^{1} \sqrt{\mu_{ak}^{(x)}}|x_k,\ x_{k+a}\rangle|f_{ak}^{x}\rangle,
\end{aligned} \tag{5.7}$$

where the normalization constants $\mu_{ak}^{(m)}$ are given by

$$\begin{aligned}
\mu_{ak}^{(z)} &= \delta_{a,0}\alpha + \delta_{a,1}\left[(\delta_{k,0}-\delta_{k,1})\gamma + \frac{\beta_1+\beta_2}{2}\right] \\
\mu_{ak}^{(x)} = \mu_{ak}^{(y)} &= \delta_{a,0}\frac{\alpha+\beta_1}{2} + \delta_{a,1}\frac{\alpha+\beta_2}{2}.
\end{aligned} \tag{5.8}$$

The ancilla states have the following inner product

$$\begin{aligned}
\langle f_{a'k'}^{z}|f_{ak}^{z}\rangle &= \begin{cases} \delta_{k,k'}, & \text{if } a=a'=0, \\ \delta_{k,k'} + (1-\delta_{k,k'})\frac{\beta_1-\beta_2}{\sqrt{(\beta_1+\beta_2)^2-4\gamma^2}}, & \\ & \text{if } a=a'=1, \\ 0, & \text{if } a\neq a'. \end{cases} \\
\langle f_{a'k'}^{x}|f_{ak}^{x}\rangle &= \langle f_{a'k'}^{y}|f_{ak}^{y}\rangle \\
&= \begin{cases} \delta_{k,k'} + (1-\delta_{k,k'})\frac{\alpha-\beta_1}{\alpha+\beta_1}, & \text{if } a=a'=0; \\ \delta_{k,k'} + (1-\delta_{k,k'})\frac{\alpha-\beta_2}{\alpha+\beta_2}, & \text{if } a=a'=1; \\ -\frac{\gamma}{\sqrt{(\alpha+\beta_1)(\alpha+\beta_2)}}\omega^{k+k'}, & \text{if } a\neq a'. \end{cases}
\end{aligned} \tag{5.9}$$

Eve's strategy is then as follows. After the basis reconciliation stage, Eve knows which pairs of photons contribute to the key and the basis that each pair was measured in. Her ancilla for each of those pairs (measured in the mth basis) will then be a mixture of four possible states:

$$\varrho_E^m = \sum_{a,k=0}^{1} \mu_{ak}^{(m)}|f_{ak}^{m}\rangle\langle f_{ak}^{m}|. \tag{5.10}$$

As pointed out in Chapter 2, this can be viewed as a transmission of information from Alice

and Bob to Eve encoded in the quantum state of Eve's ancilla and the optimal eavesdropping strategy is one which maximizes this information transfer through a suitable Positive Operator Valued Measure (POVM) [Davies, 1976]. This maximum information that can be extracted by Eve is known as the accessible information.

5.3 Optimal POVM

In this section, the optimal POVM that achieves the accessible information will be presented. Due to the asymmetric nature of the bases, the optimal POVM is different for the z and x/y bases. The optimality of these POVMs was deduced, and confirmed numerically, using the algorithms presented in [Willeboordse, 2005] and [Reh$\acute{a}$cek et al., 2004].

5.3.1 z Basis

Suppose Eve receives a state in the z basis:

$$\varrho_E^z = \sum_{k,a=0}^{1} \mu_{ak}^{(z)} |f_{ak}^z\rangle\langle f_{ak}^z|, \tag{5.11}$$

where the kets have the structure given in Eq. (5.9). Ancillas from the correlation subspace ($a = 0$) are orthogonal to all other states; those from the anticorrelation subspace ($a = 1$) are in general non-orthogonal among themselves.

In the first step, Eve sorts the mixture of the ancillas into two sub-ensembles according to the parity index a. This is done using a projective measurement. After that, depending on the outcome of the projection ($a = 0$ or $a = 1$), Eve will have a mixture of two ancilla states

$$\rho_a^z = \frac{\sum_{k=0}^{1} \mu_{ak}^{(z)} |f_{ak}^z\rangle\langle f_{ak}^z|}{\sum_{k=0}^{1} \mu_{ak}^{(z)}}. \tag{5.12}$$

If she projects into the $a = 0$ subspace, Eve will possess a mixture of equiprobable orthogonal ancilla states

$$\rho_{a=0}^z = \frac{1}{2}|f_{00}^z\rangle\langle f_{00}^z| + \frac{1}{2}|f_{01}^z\rangle\langle f_{01}^z|, \tag{5.13}$$

which she can distinguish perfectly.

On the other hand, if she projects into the $a = 1$ subspace, she will obtain a mixture of non-orthogonal ancilla states:

$$\rho^z_{a=1} = \left(\frac{1}{2} + \frac{\gamma}{2\alpha+\beta_1+\beta_2}\right)|f^z_{10}\rangle\langle f^z_{10}| + \left(\frac{1}{2} - \frac{\gamma}{2\alpha+\beta_1+\beta_2}\right)|f^z_{11}\rangle\langle f^z_{11}|. \tag{5.14}$$

For simplicity, we shall denote the inner product $\langle f^z_{10}|f^z_{11}\rangle$ by $\lambda \equiv \frac{\beta_1-\beta_2}{\sqrt{(\beta_1+\beta_2)^2-4\gamma^2}}$.

Now, if the states $|f^z_{10}\rangle, |f^z_{11}\rangle$ in Eq. (5.14) are equiprobable (which happens if $\gamma = 0$, or $R = T$), the optimal measurement for Eve would be the square-root measurement (see Chapter 2). Its POVM is given by $\{|\omega_{10}\rangle\langle\omega_{10}|, |\omega_{11}\rangle\langle\omega_{11}|\}$, where

$$\begin{aligned} |\omega_{10}\rangle &= \frac{1}{1-2\eta}\left(-\sqrt{\eta}|f^z_{10}\rangle + \sqrt{1-\eta}|f^z_{11}\rangle\right) \\ |\omega_{11}\rangle &= \frac{1}{1-2\eta}\left(\sqrt{1-\eta}|f^z_{10}\rangle - \sqrt{\eta}|f^z_{11}\rangle\right), \end{aligned} \tag{5.15}$$

with $\eta = \frac{1}{2}(1+\sqrt{1-\lambda^2})$ being the probability of determining a given state correctly.

In general, the ancilla states will not occur with the same probability, and the optimal measurement for Eve will then not be the square-root measurement. Consider the following POVM $\{|\tilde{\omega}_{10}\rangle\langle\tilde{\omega}_{10}|, |\tilde{\omega}_{11}\rangle\langle\tilde{\omega}_{11}|\}$, where the states

$$\begin{aligned} |\tilde{\omega}_{10}\rangle &= \cos\theta|\omega_{10}\rangle - \sin\theta|\omega_{11}\rangle \\ |\tilde{\omega}_{11}\rangle &= \sin\theta|\omega_{10}\rangle + \cos\theta|\omega_{11}\rangle \end{aligned} \tag{5.16}$$

are *rotated* from the square-root measurement states $\{|\omega_{10}\rangle, |\omega_{11}\rangle\}$ by an angle θ (see Fig. 5.2). We then have the following conditional probabilities

$$\begin{aligned} p(\tilde{\omega}_{10}|f^z_{10}) &= \left(\sqrt{\eta}\cos\theta - \sqrt{1-\eta}\sin\theta\right)^2 \\ p(\tilde{\omega}_{11}|f^z_{10}) &= \left(\sqrt{\eta}\sin\theta + \sqrt{1-\eta}\cos\theta\right)^2 \\ p(\tilde{\omega}_{10}|f^z_{11}) &= \left(\sqrt{1-\eta}\cos\theta - \sqrt{\eta}\sin\theta\right)^2 \\ p(\tilde{\omega}_{11}|f^z_{11}) &= \left(\sqrt{1-\eta}\sin\theta + \sqrt{\eta}\cos\theta\right)^2, \end{aligned} \tag{5.17}$$

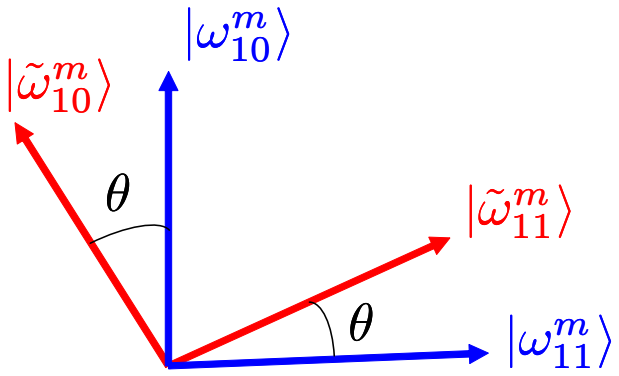


Figure 5.2: Rotated square-root measurement.

where, for instance, $p(\tilde{\omega}_{10}|f_{11}^z)$ denotes the probability of getting the result of measurement $|\tilde{\omega}_{10}\rangle\langle\tilde{\omega}_{10}|$ provided the state $|f_{11}^z\rangle$ was sent.

Using the probabilities in Eq. (5.17), we can compute the mutual information between Alice and Eve as a function of θ. The optimal measurement for Eve then corresponds to the θ that maximizes the mutual information between her and Alice. Due to the symmetric nature of the protocol, the mutual information between Eve and Bob is the same as that between Eve and Alice.

5.3.2 x/y Basis

Because the ancilla structure in the x and y bases are identical, we shall only consider what happens when Eve receives ancillas from the x basis.

If Alice measured bit '0' ($k = 0$, with probability $\frac{1}{2}$), Eve will obtain the mixed state

$$\rho_{k=0}^x = (\alpha+\beta_1)|f_{00}^x\rangle\langle f_{00}^x| + (\alpha+\beta_2)|f_{10}^x\rangle\langle f_{10}^x|, \tag{5.18}$$

and if Alice measured '1' ($k = 1$, with probability $\frac{1}{2}$), Eve will obtain the state

$$\rho_{k=1}^x = (\alpha+\beta_1)|f_{01}^x\rangle\langle f_{01}^x| + (\alpha+\beta_2)|f_{11}^x\rangle\langle f_{11}^x|. \tag{5.19}$$

The structure of the ancillas is given by Eq. (5.9):

$$\begin{aligned}
\langle f^x_{00}|f^x_{01}\rangle &= \frac{\alpha-\beta_1}{\alpha+\beta_1}\equiv\lambda_0\\
\langle f^x_{10}|f^x_{11}\rangle &= \frac{\alpha-\beta_2}{\alpha+\beta_2}\equiv\lambda_1\\
\langle f^x_{0k'}|f^x_{1k}\rangle &= -\frac{\gamma}{\sqrt{(\alpha+\beta_1)(\alpha+\beta_2)}}\omega^{k+k'}\equiv\mu\omega^{k+k'}.
\end{aligned} \tag{5.20}$$

Consider the *total state* describing Eve's ancillas:

$$\varrho^x_E = \frac{\alpha+\beta_1}{2}|f^x_{00}\rangle\langle f^x_{00}| + \frac{\alpha+\beta_1}{2}|f^x_{01}\rangle\langle f^x_{01}| + \frac{\alpha+\beta_2}{2}|f^x_{10}\rangle\langle f^x_{10}| + \frac{\alpha+\beta_2}{2}|f^x_{11}\rangle\langle f^x_{11}|. \tag{5.21}$$

ϱ^x_E has the following eigenkets

$$\begin{aligned}
|g_0\rangle &= \frac{1}{\sqrt{N_0}}\left(|f^x_{00}\rangle + |f^x_{01}\rangle\right)\\
|g_1\rangle &= \frac{1}{\sqrt{N_1}}\left(|f^x_{10}\rangle + |f^x_{11}\rangle\right)\\
|g_2\rangle &= \frac{1}{\sqrt{N_2}}\left[\kappa_+\left(|f^x_{00}\rangle - |f^x_{01}\rangle\right) + \epsilon\left(|f^x_{10}\rangle - |f^x_{11}\rangle\right)\right]\\
|g_3\rangle &= \frac{1}{\sqrt{N_3}}\left[\kappa_-\left(|f^x_{00}\rangle - |f^x_{01}\rangle\right) + \epsilon\left(|f^x_{10}\rangle - |f^x_{11}\rangle\right)\right],
\end{aligned} \tag{5.22}$$

where

$$\begin{aligned}
\kappa_\pm &= \beta_2-\beta_1 \pm \sqrt{(\beta_2-\beta_1)^2+4\gamma^2}\\
\epsilon &= 2\gamma\sqrt{\frac{\alpha+\beta_2}{\alpha+\beta_1}}.
\end{aligned} \tag{5.23}$$

The normalization constants N_k ($k=0,1,2,3$) read

$$\begin{aligned}
N_0 &= 2(1+\lambda_0)\\
N_1 &= 2(1+\lambda_1)\\
N_2 &= \frac{4}{\alpha+\beta_1}\left[\beta_1\kappa_+^2 + 4\gamma^2\left(\beta_1 - \sqrt{(\beta_2-\beta_1)^2+4\gamma^2}\right)\right]\\
N_3 &= \frac{4}{\alpha+\beta_1}\left[\beta_1\kappa_-^2 + 4\gamma^2\left(\beta_1 + \sqrt{(\beta_2-\beta_1)^2+4\gamma^2}\right)\right].
\end{aligned} \tag{5.24}$$

If we now adopt $\{|g_0\rangle, |g_1\rangle, |g_2\rangle, |g_3\rangle\}$ as an orthonormal set of basis, the optimal measurement for Eve can be expressed as $\{|\Omega_0\rangle\langle\Omega_0|, |\Omega_1\rangle\langle\Omega_1|, |\Omega_2\rangle\langle\Omega_2|, |\Omega_3\rangle\langle\Omega_3|\}$, where

$$(|\Omega_0\rangle, |\Omega_1\rangle, |\Omega_2\rangle, |\Omega_3\rangle) = (|g_0\rangle, |g_1\rangle, |g_2\rangle, |g_3\rangle) \begin{pmatrix} -a & a & b & b \\ b & -b & a & a \\ c & c & -d & d \\ d & d & c & -c \end{pmatrix}, \tag{5.25}$$

with a, b, c and d being real. By requiring that the measurement operators to sum to unity $\sum_{k=0}^{3} |\Omega_k\rangle\langle\Omega_k| = 1$, we have the following relations between the four real parameters:

$$\begin{aligned} a^2 + b^2 &= \frac{1}{2} \\ c^2 + d^2 &= \frac{1}{2}. \end{aligned} \tag{5.26}$$

As before, we can compute the mutual information between Alice and Eve for this basis and maximize it over the two independent variables a and c to obtain the maximum information that Eve can obtain about Alice's measurement.

5.4 Discussion

By determining the experimental parameters $\frac{R}{T}$, g and V from state tomography, Alice and Bob can determine the maximal mutual information of Eve and compute the yield in the various bases to find out if the particular two-photon state they are receiving is secure against incoherent attacks. Table 5.1 shows the values of mutual information for various values of g and V. The ratio $\frac{R}{T}$ was fixed at 1.1 (the value reported in [Fattal et al., 2004]). For certain values of g and V, the CK yield (denoted as ν_m, for the mth basis) is zero in all measurement bases. For such states one cannot extract secure bits from the CK theorem. More interesting are the cases where the CK yield is zero in one measurement basis and positive in another. In such cases, Alice and Bob reject the data obtained by measurements in the basis with zero yield and process only the data from the basis for which the CK yield is positive. Finally, in the case where all the CK yields are positive, Alice and Bob use the data from all the bases. The average CK yield in every case is given by $\nu = \frac{1}{3}(\nu_x + \nu_y + \nu_z)$.

		z basis			x/y basis			
g	V	$\mathcal{I}_{AB}$	max $\mathcal{I}_{AE}$	ν_z	$\mathcal{I}_{AB}$	max $\mathcal{I}_{AE}$	$\nu_{x,y}$	ν
0.1	0.6	0.3478	0.6070	0	0.1872	0.4320	0	0
0.02	0.4	0.7598	0.7550	0.0048	0.1085	0.1088	0	0.0016
0.1	0.84	0.3478	0.3528	0	0.3869	0.3755	0.0114	0.0076
0.1	0.9	0.3478	0.2845	0.0633	0.4525	0.3321	0.1204	0.1014

Table 5.1: Table of yields in the three bases for $\frac{R}{T} = 1.1$, and different values of g and V. Due to the asymmetric nature of the state in the z and x/y bases, the yield is different for those bases. The yield is the same in the x and y bases.

5.4.1 Perfect Beamsplitters

Of particular interest is the case when we have perfect beamsplitters ($\frac{R}{T} = 1$). The state produced by the source is then in a Bell diagonal form:

$$\alpha|z_{00}\rangle\langle z_{00}| + \alpha|z_{01}\rangle\langle z_{01}| + \beta_1|z_{10}\rangle\langle z_{10}| + \beta_2|z_{11}\rangle\langle z_{11}|.$$

The security of such states was analyzed in Chapter 2 and the results can be applied to this situation.

In Fig. 5.3 the average CK yield is plotted against g and V. We observe that the protocol is always secure against incoherent attacks as long as $g = 0$ and $V > 0$, although fewer secure bits can be distilled for smaller V. In fact, the state for which $g = 0$ corresponds to one of the rank 2 Bell diagonal resistant states that was identified in Section 2.2.5:

$$\beta_1|z_{10}\rangle\langle z_{10}| + \beta_2|z_{11}\rangle\langle z_{11}|.$$

More detailed analysis reveals that for such states, the mutual information between Alice and Eve is always zero when Alice and Bob perform measurements in the x or y basis. This is due to the fact that Eve's ancillas corresponding to different outcomes of Alice's measurements in the x and y bases are the same, i.e. they do not carry any information whatsoever about Alice's and Bob's correlations. Therefore, if Alice and Bob agree on using only the data from the x and y measurements (thereby sacrificing the efficiency), the protocol becomes secure against *all* possible attacks by Eve and the protocol guarantees unconditional security. For $g, V = 0$, the state becomes separable and no secure bits can be extracted.

In realistic situations however, the value of g can be small but not exactly zero (for example, the value of g reported in [Santori et al., 2001] was 0.02). In this case, the protocol is secure over a smaller range of V. Even then, it is reasonable to conjecture that the information that Eve can extract from her ancillas in the x or y basis is negligible, and the protocol remains pretty robust against all possible attacks by her in those bases.

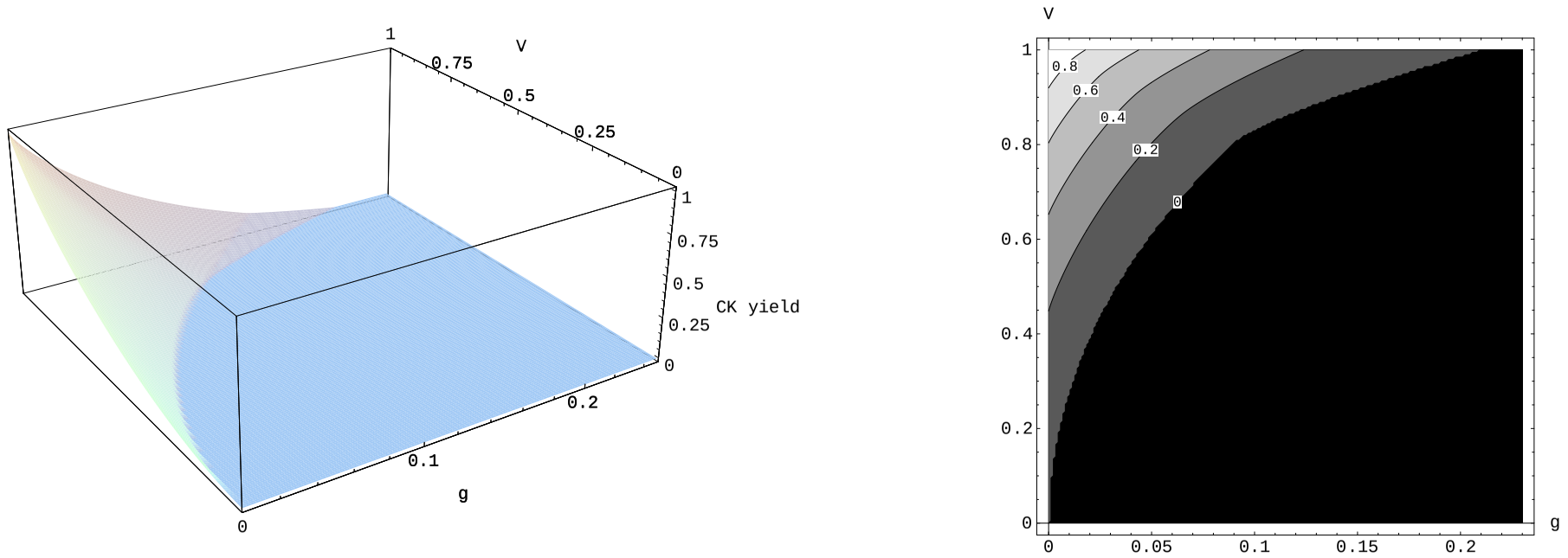


Figure 5.3: Three-dimensional plot of the CK yield for perfect beamsplitters $R = T$ (*left*), and its corresponding contour plot (*right*). The threshold for security is given by the contour for which the CK yield is zero. For $g = 0$, security is guaranteed as long as V is greater than zero, although fewer secure bits can be distilled for smaller V.

5.5 Noisy Channel

So far, we have excluded the effects of noise in the channel so that Alice and Bob expect to receive the state 'as-is' from the source. In reality however, this is not the case: Alice and Bob would expect their quantum channel to be affected by interactions with the environment so that the state they receive contains some noise. Let us consider what happens when there is *symmetric white noise* present in the channel, i.e. the state that Alice and Bob expect to receive is of the form:

$$\varrho^z = \frac{1-F}{2}\begin{pmatrix} 2\alpha & & & \\ & \beta_1+\beta_2+2\gamma & \beta_1-\beta_2 & \\ & \beta_1-\beta_2 & \beta_1+\beta_2-2\gamma & \\ & & & 2\alpha \end{pmatrix} + \frac{F}{4}1\otimes 1, \quad (5.27)$$

where the parameter F gives the amount of unbiased noise admixed to the original state from the source. We have $0 \leq F \leq 1$, where $F = 0$ corresponds to the absence of noise in the quantum channel while $F = 1$ refers to the situation of a completely noisy channel.

Detailed analysis shows that the situation is similar to that for the noiseless case, with the following substitutions made:

$$\begin{aligned} \alpha &\longrightarrow (1-F)\alpha + \frac{F}{4} \\ \beta_1 &\longrightarrow (1-F)\beta_1 + \frac{F}{4} \\ \beta_2 &\longrightarrow (1-F)\beta_2 + \frac{F}{4} \\ \gamma &\longrightarrow (1-F)\gamma. \end{aligned} \quad (5.28)$$

Thus, for example, we have the following relations for Eve's purification of the form given by Eq. (5.7):

$$\begin{aligned} \mu_{ak}^{(z)} &= \delta_{a,0}(1-F)\alpha + \delta_{a,1}(1-F)\left[(\delta_{k,0}-\delta_{k,1})\gamma + \frac{\beta_1+\beta_2}{2}\right] + \frac{F}{4} \\ \mu_{ak}^{(x)} = \mu_{ak}^{(y)} &= \delta_{a,0}(1-F)\frac{\alpha+\beta_1}{2} + \delta_{a,1}(1-F)\frac{\alpha+\beta_2}{2} + \frac{F}{4} \end{aligned} \quad (5.29)$$

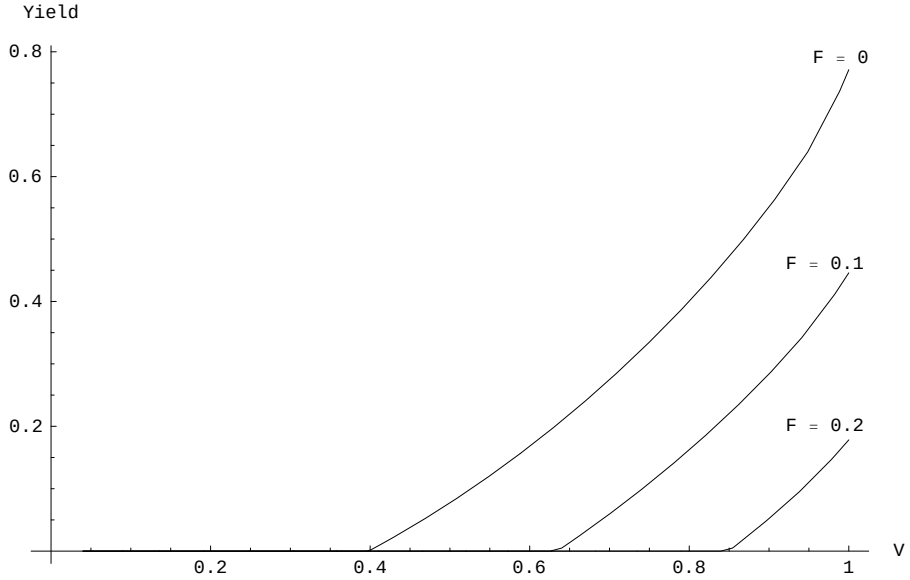


Figure 5.4: Average CK yield for $\frac{R}{T} = 1.1$ and $g = 0.02$ and different amounts of noise in the channel F. For a noiseless channel ($F = 0$), when $V \lesssim 0.394$, one can no longer extract secure bits by means of one-way communication because the CK yield is zero. As the amount of noise increases, the CK yield drops until for $F \gtrsim 0.277$, where we will not be able to distill any secure bits at all (because the CK yield is 0 for all values of V).

$$
\begin{aligned}
\langle f^z_{a'k'} | f^z_{ak} \rangle &= \begin{cases} \delta_{k,k'}, & \text{if } a = a' = 0, \\ \delta_{k,k'} + (1 - \delta_{k,k'}) \frac{\beta_1 - \beta_2}{\sqrt{\left[\beta_1 + \beta_2 + \frac{F}{2(1-F)}\right]^2 - 4\gamma^2}}, & \\ & \text{if } a = a' = 1, \\ 0, & \text{if } a \neq a'. \end{cases} \\
\langle f^x_{a'k'} | f^x_{ak} \rangle &= \langle f^y_{a'k'} | f^y_{ak} \rangle \\
&= \begin{cases} \delta_{k,k'} + (1 - \delta_{k,k'}) \frac{\alpha - \beta_1}{\alpha + \beta_1 + \frac{F}{2(1-F)}}, & \text{if } a = a' = 0; \\ \delta_{k,k'} + (1 - \delta_{k,k'}) \frac{\alpha - \beta_2}{\alpha + \beta_2 + \frac{F}{2(1-F)}}, & \text{if } a = a' = 1; \\ -\frac{\gamma}{\sqrt{\left[\alpha + \beta_1 + \frac{F}{2(1-F)}\right]\left[\alpha + \beta_2 + \frac{F}{2(1-F)}\right]}} \omega^{k+k'}, & \text{if } a \neq a'. \end{cases}
\end{aligned}
\tag{5.30}
$$

The optimal POVM for Eve is thus of the same form as before, and we can obtain the condition for security and the CK yield for various proportions of noise. This is shown in Fig. 5.4, for fixed values of $\frac{R}{T} = 1.1$ and $g = 0.02$ (values reported in [Fattal et al., 2004; Santori et al., 2001]). We can distill less secure bits as the amount of noise increases.

Chapter 6

Conclusion

In this thesis, a generalized tomographic QKD scheme applicable to Bell diagonal states was presented and its resistance to various eavesdropping attacks was analyzed, both in the CK regime and when Alice and Bob perform distillation. The inequivalence of advantage distillation and entanglement distillation in the situation of a coherent attack by an eavesdropper was also shown. Furthermore, certain states that offer unconditional security were identified. These are the rank 2 Bell diagonal states.

The security of the tomographic protocol using a source of entangled photons produced in the experimental scheme proposed by Fattal *et al.* [Fattal et al., 2004] was also analyzed against the most general incoherent attack. From the analysis, the number of secure bits that can be distilled by means of one-way communication between Alice and Bob can be given as a function of the experimentally accessible parameters R, T, g and V , and for different degrees of unbiased noise in the channel F. A number of useful observations from the analysis, such as the unconditional security of rank 2 Bell diagonal states and the security of states with small values of g, could also be applied to other QKD schemes based on such a photon source.

The tomographic protocol that was considered here admits noise of a few specific form, ie. we have considered states of the form Eqs. (2.10) and (5.27). Experimentally, noise may be of a more general nature, so that a more detailed analysis than the one presented is required. Characterization of these actual states in QKD may change the noise bounds for secure communication in many cases.

Appendix A

State Tomography

Here, it will be shown that Alice and Bob can determine the exact state of their two-qubit source by comparing their respective data for the tomographically complete set of measurements $\{\sigma_x, \sigma_y, \sigma_z\}$.

The most general two-qubit state ϱ is completely characterized by 15 real parameters, and can be written in the following form:

$$\varrho \;=\; \frac{1}{4}\left[1\otimes 1+\sum_{k=1}^{3} a_k\sigma_k^A\otimes 1+1\otimes\sum_{k=1}^{3} b_k\sigma_k^B+\sum_{k,l=1}^{3} T_{kl}\sigma_k^A\otimes\sigma_l^B\right], \quad \text{(A.1)}$$

where the parameters a_k, b_k, and T_{kl} ($k, l = 1, 2, 3$) are all real, and we have denoted σ_x, σ_y and σ_z by σ_1, σ_2 and σ_3 respectively. By noting that $\sigma_i\sigma_j = \delta_{ij} + \mathrm{i}\epsilon_{ijk}\sigma_k$, we have the following expressions for the various expectation values*:

$$\begin{aligned}
\left\langle\sigma_i^A\right\rangle &= \mathrm{Tr}\left[\sigma_i^A\otimes 1\;\varrho\right] = a_i \\
\left\langle\sigma_i^B\right\rangle &= \mathrm{Tr}\left[1\otimes\sigma_i^B\;\varrho\right] = b_i \\
\left\langle\sigma_i^A\otimes\sigma_j^B\right\rangle &= \mathrm{Tr}\left[\sigma_i^A\otimes\sigma_j^B\;\varrho\right] = T_{ij}. \qquad \text{(A.2)}
\end{aligned}$$

Alice and Bob can thus deduce all the 15 values of the parameters characterizing their state from the average values of their basis measurements.

*Here the *Levi-Cevita symbol* ϵ_{ijk} takes values 1 if the indices i, j, k are an even permutation of $1, 2, 3$, -1 if the indices are an odd permutation, and 0 otherwise.

Appendix B

State Measurements

Here, a few properties about state measurements on quantum systems will be mentioned.

B.1 Generalized Measurements

Consider a quantum system initially prepared in the state whose density operator is ρ. A measurement operation $\rho \rightarrow \mathcal{L}(\rho)$ is carried out on the system. This measurement has n distinguishable outcomes, labeled as ω_k, $k = 0, 1, 2, \ldots, n-1$, with corresponding final density operators ρ'_k. The *quantum detection operators* Π_k corresponding to each result ω_k is such that the probability of obtaining ω_k given the initial state ρ is

$$p(\omega_k|\rho) = \mathrm{Tr}\left[\rho\Pi_k\right]. \tag{B.1}$$

For a pure state, $\rho = |\psi\rangle\langle\psi|$, so that this probability is simply

$$p(\omega_k|\psi) = \langle\psi|\Pi_k|\psi\rangle. \tag{B.2}$$

We demand a few properties of Π_k:

1. Since the probabilities (B.1) must be non-negative for all states ρ, this implies

$$\langle\psi|\Pi_k|\psi\rangle \geq 0, \tag{B.3}$$

for all pure states $|\psi\rangle$. Hence, all the Π_k's must be *positive* (semi-definite):

$$\Pi_k \geq 0, \tag{B.4}$$

for $k = 0, 1, \ldots, n-1$.

A few consequences follow from this property:

(a) Since $\langle\psi|\Pi_k|\psi\rangle$ must be real for all states $|\psi\rangle$, i.e.

$$\langle\psi|\Pi_k|\psi\rangle = \langle\psi|\Pi_k|\psi\rangle^* = \langle\psi|\Pi_k^\dagger|\psi\rangle, \tag{B.5}$$

each Π_k must be *Hermitian*.

(b) Since $\langle\psi|\Pi_k|\psi\rangle \geq 0$ for all $|\psi\rangle$, we can take $|\psi\rangle$ to be one of the (orthonormal) eigenkets of Π_k, so that the eigenvalues of each Π_k must be non-negative.

2. The probabilities (B.1) must sum to 1 for all states ρ. It follows that the Π_k form a *resolution of the identity*:

$$\sum_{k=0}^{n-1} \Pi_k = 1. \tag{B.6}$$

The conditions above are the necessary and sufficient conditions for the realisability of an experiment whose outcomes have the probability distribution $p(\omega_k|\rho)$ [Kraus, 1983]. Such a set of detection operator is commonly known as a *Positive Operator Valued Measure* (POVM).

Construct the following *measuring operator*

$$M_k = \Pi_k^{1/2}, \tag{B.7}$$

so that $\Pi_k = M_k^\dagger M_k$. This is always possible from the positivity of Π_k. Then the density operator immediately after a measurement with result ω_k can be written as

$$\rho'_k = \frac{M_k \rho M_k^\dagger}{\mathrm{Tr}\left[M_k^\dagger M_k \rho\right]} = \frac{M_k \rho M_k^\dagger}{p(\omega_k|\rho)}. \tag{B.8}$$

The presence of the probability in the denominator serves to normalize the state, so that $\mathrm{Tr}\left[\rho'_k\right] = 1$. If we do not record the result of the measurement, then the final density operator ρ' is given by a distribution of the density operators ρ_k corresponding to the possible

outcomes of the operation, weighted by their respective probabilities $p(\omega_k|\rho)$:

$$\rho' = \sum_{k=0}^{n-1} p(\omega_k|\rho)\rho'_k = \sum_{k=0}^{n-1} M_k \rho M_k^\dagger. \tag{B.9}$$

B.2 Non-Orthogonal States

We show that it is not possible to reliably distinguish between two non-orthogonal states.

Suppose we wish to distinguish with certainty the non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$. To do this, we make use of a set of measuring operators $\{M_m\}_{m=1}^2$, and require that

$$p(1||\psi_1\rangle) = \langle\psi_1|M_1^\dagger M_1|\psi_1\rangle = 1 \tag{B.10}$$

$$p(2||\psi_2\rangle) = \langle\psi_2|M_2^\dagger M_2|\psi_2\rangle = 1 \tag{B.11}$$

$$p(1||\psi_2\rangle) = \langle\psi_2|M_1^\dagger M_1|\psi_2\rangle = 0 \tag{B.12}$$

$$p(2||\psi_1\rangle) = \langle\psi_1|M_2^\dagger M_2|\psi_1\rangle = 0. \tag{B.13}$$

(B.12) and (B.13) imply that

$$M_2|\psi_1\rangle = 0 \tag{B.14}$$

$$M_1|\psi_2\rangle = 0 \tag{B.15}$$

Since the M_m's form a valid set of measuring operators, they resolve the identity:

$$M_1^\dagger M_1 + M_2^\dagger M_2 = 1, \tag{B.16}$$

so that

$$\langle\psi_1|M_1^\dagger M_1|\psi_2\rangle + \langle\psi_1|M_2^\dagger M_2|\psi_2\rangle = \langle\psi_1|\psi_2\rangle. \tag{B.17}$$

Invoking (B.14) and (B.15), we have

$$\langle\psi_1|\psi_2\rangle = 0, \tag{B.18}$$

a contradiction, since $|\psi_1\rangle$ and $|\psi_2\rangle$ are non-orthogonal. We have thus proven that it is not

possible to distinguish between non-orthogonal states reliably.

On the other hand, if $|\psi_1\rangle$ and $|\psi_2\rangle$ were orthogonal states, we can distinguish among them unambiguously; the measuring operators are simply the orthogonal projectors, $|\psi_1\rangle\langle\psi_1|$ and $|\psi_2\rangle\langle\psi_2|$. Such a measurement is also known as a *von Neumann measurement*.

Note that if we allow the possibility of inconclusive results, we can in fact have error-free discrimination amongst non-orthogonal states [Ivanovic, 1987; Helstrom, 1976].

B.3 Square-Root Measurement

Consider a set of n pure states $\{|\psi_j\rangle\}_{j=0,1,\ldots,n-1}$ occurring with equal a priori probabilities, $\eta_j = \frac{1}{n}$. These states are also *symmetric*, in the sense that it satisfies the following conditions:

$$\begin{aligned} |\psi_j\rangle &= U|\psi_{j-1}\rangle = U^j|\psi_0\rangle \\ U|\psi_{n-1}\rangle &= |\psi_0\rangle, \end{aligned} \tag{B.19}$$

for some unitary operator U. U transforms each state into its successor, and the final state back to the original state. The optimum measurement which distinguishes these states with minimum probability of error can be derived analytically and is known as the *square-root measurement* [Chefles, 2000b; Helstrom, 1976].

Define the operator

$$\Phi = \sum_{j=0}^{n-1} |\psi_j\rangle\langle\psi_j|. \tag{B.20}$$

The optimum detection operators are then of the form

$$\Pi_j = |\omega_j\rangle\langle\omega_j|, \tag{B.21}$$

where

$$|\omega_j\rangle = \Phi^{-\frac{1}{2}}|\psi_j\rangle. \tag{B.22}$$

The $|\omega_j\rangle$'s are in general unnormalized and non-orthogonal. The Π_j's defined in this way form a valid set of POVM's:

1. $$\langle\psi|\Pi_j|\psi\rangle = |\langle\omega_j|\psi\rangle|^2 \geq 0$$

   for any pure state $|\psi\rangle$, i.e. the Π_j's are positive operators;

2. $$\sum_{j=0}^{n-1}\Pi_j = \sum_{j=0}^{n-1}\Phi^{-\frac{1}{2}}|\psi_j\rangle\langle\psi_j|\Phi^{-\frac{1}{2}} = \Phi^{-\frac{1}{2}}\Phi\Phi^{-\frac{1}{2}} = 1,$$

   i.e. the Π_j's form a resolution of the identity.

For equally-probable symmetric states, this measurement then attains the minimum error probability

$$\begin{aligned} p_{error} &= 1 - p_{success} \\ &= 1 - \frac{1}{n}\sum_{j=0}^{n-1}\left|\langle\psi_j|\Phi^{-\frac{1}{2}}|\psi_j\rangle\right|^2. \end{aligned} \tag{B.23}$$

It is because of the presence of the $\Phi^{-\frac{1}{2}}$ in Π_j that this measurement is known as the *square-root measurement*.

Finally, we note that for orthogonal states, the square root measurement reduces to the orthogonal projectors $|\psi_j\rangle\langle\psi_j|$, so that square root measurement is indeed the most optimal measurement in this case.

Appendix C

Proof of Optimality

Here, we show the optimality of the measurement given in Section 2.2.3. Consider the following quantum communication scenario: Alice sends N quantum states ρ_j to Eve with *a priori* probabilities p_j, $j = 1, \ldots, N$. The state which Eve receives from Alice is therefore given by

$$\rho = \sum_{j=1}^{N} p_j \rho_j. \tag{C.1}$$

Eve performs a positive-operator valued measurement (POVM) composed of K operators $\{\Pi_k\}_{k=1}^{K}$ such that

$$\Pi_k \geq 0 \tag{C.2}$$

$$\sum_{k=1}^{K} \Pi_k = 1. \tag{C.3}$$

The POVM she chooses is such that the measurement gives her the maximum information that can be extracted from ρ. The amount of information is quantified by the mutual information

$$\mathcal{I}_{AE} = \sum_{j,k} p_{jk}^{(\mathrm{EA})} \log \frac{p_{jk}^{(\mathrm{EA})}}{p_j^{(\mathrm{E})} p_k^{(\mathrm{A})}}, \tag{C.4}$$

where

$$p_{jk}^{(\mathrm{EA})} = p_k \mathrm{Tr}\left[\Pi_j \rho_k\right] \tag{C.5}$$

is the probability of Alice sending the kth state and Eve getting the jth outcome;

$$p_j^{(\mathrm{E})} = \sum_k p_{jk}^{(\mathrm{EA})} = \mathrm{Tr}\left[\Pi_j \rho\right] \tag{C.6}$$

is the probability of Eve getting the jth outcome, and

$$p_k^{(\mathrm{A})} = \sum_j p_{jk}^{(\mathrm{EA})} = p_k \tag{C.7}$$

is the probability of Alice sending state ρ_k. We observe that Eq. (C.4) can also be expressed as

$$\mathcal{I}_{AE} = \sum_j \mathrm{Tr}\left[\Pi_j R_j\right], \tag{C.8}$$

where

$$R_j = \sum_k \rho_k \log \frac{p_{jk}^{(\mathrm{EA})}}{p_j^{(\mathrm{E})} p_k^{(\mathrm{A})}}. \tag{C.9}$$

Eve's choice of POVM is such that it maximizes the mutual information of Eq. (C.9). Consider a variation of the POVM $\delta\Pi_k$. This variation is subject to the constraint of Eq. (C.3), so that

$$\sum_k \delta\Pi_k = 0. \tag{C.10}$$

The response of Eq. (C.9) to a variation of the POVM is given by

$$\delta\mathcal{I}_{AE} = \sum_j \mathrm{Tr}\left[R_j \delta\Pi_j\right] + \sum_j \mathrm{Tr}\left[\Pi_j \delta R_j\right]. \tag{C.11}$$

The second term vanishes, since

$$\begin{aligned}
\sum_j \mathrm{Tr}\left[\Pi_j \delta R_j\right] &= \sum_{j,k} \mathrm{Tr}\left[\Pi_j \rho_k \frac{p_j^{(\mathrm{E})} p_k^{(\mathrm{A})}}{p_{jk}^{(\mathrm{EA})}} \delta\left(\frac{p_{jk}^{(\mathrm{EA})}}{p_j^{(\mathrm{E})} p_k^{(\mathrm{A})}}\right)\right] \\
&= \sum_{j,k} \mathrm{Tr}\left[\Pi_j \rho_k\right] \frac{p_j^{(\mathrm{E})}}{p_{jk}^{(\mathrm{EA})}} \delta\left(\frac{p_{jk}^{(\mathrm{EA})}}{p_j^{(\mathrm{E})}}\right) \\
&= \sum_{j,k} p_j^{(\mathrm{E})} \delta\left(\frac{p_{jk}^{(\mathrm{EA})}}{p_j^{(\mathrm{E})}}\right), \quad \text{since } \mathrm{Tr}\left[\Pi_j \rho_k\right] = p_{jk}^{(\mathrm{EA})} \\
&= \sum_j p_j^{(\mathrm{E})} \delta\left(\frac{p_j^{(\mathrm{E})}}{p_j^{(\mathrm{E})}}\right) \\
&= 0. \qquad \text{(C.12)}
\end{aligned}$$

We thus have

$$\delta \mathcal{I}_{AE} = \sum_j \mathrm{Tr}\left[R_j \delta \Pi_j\right]. \qquad \text{(C.13)}$$

Now, the positive operator Π_j can also be expressed in the form

$$\Pi_j = A_j^\dagger A_j, \qquad \text{(C.14)}$$

for some invertible operator A_j. We can then write Eq. (C.13) as

$$\delta \mathcal{I}_{AE} = \sum_j \mathrm{Tr}\left[R_j \left(\delta A_j^\dagger A_j + A_j^\dagger \delta A_j\right)\right], \qquad \text{(C.15)}$$

with the variations in A_j subject to the constraint of Eq. (C.3):

$$\sum_j \delta A_j^\dagger A_j + \sum_j A_j^\dagger \delta A_j = 0. \qquad \text{(C.16)}$$

The most general form for the variations δA_j is

$$\delta A_j = \sum_k \epsilon_{jk} A_k, \quad \text{with } \epsilon_{jk}^\dagger = -\epsilon_{kj}, \qquad \text{(C.17)}$$

where the ϵ_{jk}'s are arbitrary infinitesimal operators. Eq. (C.15) then becomes

$$\delta \mathcal{I}_{AE} = \sum_{j,k} \mathrm{Tr}\left[\left(A_k R_j A_j^\dagger - A_k R_k A_j^\dagger\right) \epsilon_{jk}\right], \qquad \text{(C.18)}$$

Now, an optimal POVM gives an extremum for Eq. (C.4) so that $\delta \mathcal{I}_{AE} = 0$. Furthermore, since the ϵ_{jk}'s are arbitrary, the optimal POVM must necessarily be such that

$$A_k R_j A_j^\dagger = A_k R_k A_j^\dagger, \tag{C.19}$$

or equivalently,

$$\Pi_k R_j \Pi_j = \Pi_k R_k \Pi_j. \tag{C.20}$$

In the case of the measurement given in Section 2.2.3, we have the following scenario: The quantum channel between Alice and Eve is such that Alice sends the following equiprobable states ($p_0^{(\mathrm{A})} = p_1^{(\mathrm{A})} = \frac{1}{2}$) to Eve

$$\begin{aligned} \rho_0 &= \sum_{a=0}^{1} p_a^{(m)} |f_{a0}^{(m)}\rangle\langle f_{a0}^{(m)}| \\ \rho_1 &= \sum_{a=0}^{1} p_a^{(m)} |f_{a1}^{(m)}\rangle\langle f_{a1}^{(m)}|, \end{aligned} \tag{C.21}$$

where ρ_k is the state that Alice sends if she obtains the kth outcome in her measurement in the mth basis. For the measurement described in Section 2.2.3, its POVM is characterized by two indices a, k:

$$\Pi_{ak} = |\omega_{ak}^m\rangle\langle\omega_{ak}^m|, \tag{C.22}$$

such that

$$\langle f_{a'k'}^m | \omega_{ak}^m \rangle = \delta_{a,a'} \left(\sqrt{\frac{1+\lambda_a^{(m)}}{2}} + \sqrt{\frac{1-\lambda_a^{(m)}}{2}} (\delta_{k,0} - \delta_{k,1})(\delta_{k',0} - \delta_{k',1}) \right). \tag{C.23}$$

For the measurement, we can obtain

$$\begin{aligned} \Pi_{a'k'} R_{ak} \Pi_{ak} &= \delta_{a,a'} \frac{p_a^{(m)}}{2} |\omega_{ak'}^m\rangle\langle\omega_{ak}^m| \times \begin{cases} 2\log\lambda_a + (1-\lambda^2)\log\frac{1+\sqrt{1-\lambda_a^2}}{1-\sqrt{1-\lambda_a^2}}, & \text{if } k = k'; \\ 2\lambda_a \log\lambda_a, & \text{otherwise} \end{cases} \\ &= \Pi_{a'k'} R_{a'k'} \Pi_{ak}, \end{aligned} \tag{C.24}$$

i.e. Eq. (C.20) is true for this POVM and so the measurement extremizes the information that Eve can extract from Alice's states.

Appendix D
Mutual Information

Here we show intuitively how the mutual information can be used to quantify the amount of correlation between two ensembles. For ease of discussion, we will be using $\log$ base 2 — the entropy and mutual information is then measured in *bits*.

We first define the Shannon entropy of an ensemble.

D.1 Shannon Entropy

Suppose we have a random variable X with n outcomes $x_1, x_2, \ldots, x_n$ that we call letters. These n letters together form an alphabet. The kth letter occurs with probability $p(k)$, so that $\sum_{k=1}^{n} p(k) = 1$. Define the *(Shannon) entropy* of the random variable X:

$$\mathrm{H}(X) \equiv -\sum_{k=1}^{n} p(k) \log_2 p(k). \tag{D.1}$$

We will now show that the entropy is the average number of bits per letter needed to describe a message drawn from this alphabet of n letters.

Suppose that we construct a message of L letters chosen from our alphabet of n letters $\{x_1, x_2, \ldots, x_n\}$, and that the letters in the message are statistically independent. For $L \gg 1$, the law of large numbers tells us that a typical string will contain $Lp(k)$ x_k's. The collection of all such typical strings form a typical sequence. The number of distinct typical

strings in this sequence is

$$N = \binom{L}{Lp(1), Lp(2), \ldots, Lp(n)} = \frac{L!}{(Lp(1))!(Lp(2))! \cdots (Lp(n))!}. \tag{D.2}$$

Using Stirling's approximation $\log x! \approx x \log x - x$ for $x \gg 1$, we obtain

$$\begin{aligned} \log_2 N &\approx L \log_2 L - L - \left[\sum_{k=1}^{n} (Lp(k) \log_2 Lp(k) - Lp(k)) \right] \\ &= -L \sum_{k=1}^{n} p(k) \log_2 p(k) \\ &= L\mathrm{H}(X). \end{aligned} \tag{D.3}$$

The number of typical strings is thus approximately

$$N \approx 2^{L\mathrm{H}(X)}. \tag{D.4}$$

The Shannon enropy $\mathrm{H}(X)$ thus quantifies how much information is conveyed, on the average, by a letter drawn from the ensemble X, for it tells us how many bits are required asymptotically as $L \to \infty$ to encode that information: The optimal code will compress each letter to $\mathrm{H}(X)$ bits asymptotically. This result is also known as *Shannon's noisless coding theorem*.

D.2 Mutual Information

The mutual information $\mathcal{I}_{XY}$ quantifies how *correlated* two messages are, that is how much do we know about a message drawn from the ensemble $X^{\otimes L} \equiv X \otimes X \cdots \otimes X$ when we have read a message drawn from $Y^{\otimes L}$.

For example, suppose Alice wishes to send Bob a message. However, the communication channel is noisy so that the message received by Bob (y) might differ from the message sent by Alice (x). The noisy channel can be characterised by the conditional probability that y is received when x is sent, $p(y|x)$. We also suppose that x is sent with *a priori* probability

$p(x)$. Given these probabilities, we can then use Bayes' rule to compute

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)}. \tag{D.5}$$

We wish to quantify how much Bob learns about x when he receives y, that is how much information does he gain about x by measuring y?

Now, the entropy $\mathrm{H}(X)$ quantifies Bob's *a priori* ignorance per letter, before any message is received: He would require $L\mathrm{H}(X)$ bits to completely specify (asymptotically) a particular message of L letters sent by Alice.

When Bob learns about the value of y, he becomes less ignorant about x than before. Given the y's that Bob receives, Alice can then, using an optimal code, specify a particular string of L letters taken from X by sending Bob

$$\begin{aligned} H(X|Y) &= \sum_y p(y) H(X|Y=y) \\ &= -\sum_{x,y} p(y) \cdot p(x|y) \log_2 p(x|y) \\ &= -\sum_{x,y} p(x,y) \log_2 p(x,y) + \sum_y p(y) \log_2 p(y) \\ &= H(X,Y) - H(Y) \end{aligned} \tag{D.6}$$

bits per letter. $H(X|Y)$ is the conditional entropy of X given Y. We may interpret $H(X|Y)$ as the number of *additional* bits per letter needed to specify both x and y once y is known. This quantity is non-negative.

Now, the information about X that Bob gains when he learns Y is quantified by how much the number of bits per letter needed to specify X is *reduced* when Y is known. This is given by

$$\mathcal{I}_{XY} \equiv H(X) - H(X|Y) \tag{D.7}$$

$$= H(X) + H(Y) - H(X,Y) \tag{D.8}$$

$$= H(Y) - H(Y|X) \tag{D.9}$$

$$= \sum_{x,y} \log_2 p(x,y) \frac{p(x,y)}{p(x)p(y)} \tag{D.10}$$

$\mathcal{I}_{XY}$ is called the *mutual information* of X and Y. It is symmetric under interchange of X and Y, $\mathcal{I}_{XY} = \mathcal{I}_{YX}$ (we find out as much about X by learning Y as about Y by leaning X) and non-negative (learning Y can never reduce our knowledge of X).

Since $\mathcal{I}_{XY}$ quantifies the information gained about X on learning Y, we can also interpret $\mathcal{I}_{XY}$ as the amount of correlation between the two ensembles X and Y. For example, if X and Y are uncorrelated, we have $p(x, y) = p(x)p(y)$ so that using (D.10), so that

$$\mathcal{I}_{XY} = 0; \tag{D.11}$$

we find out nothing about X by learning Y if there is no correlation.

The interpretation of $\mathcal{I}_{XY}$ as the information gain about X on receiving Y is consistent with the results of *Shannon's noisy channel coding theorem*, where $\mathcal{I}_{XY}$ is also the information per letter that can be sent over a noisy channel.

Bibliography

Acín, A., Masanes, L. and Gisin, N. [2003]. *Phys. Rev. Lett., 91*, 167901.

Alber, G., Beth, T., Horodecki, M., Horodecki, P., Horodecki, R., Rötteler, M., Weinfurter, M., Werner, R. and Zeilinger, A. [2001]. *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments.* Springer Tracts in Modern Physics.

Bennett, C. H. [1992]. *Phys. Rev. Lett., 68*, 3121.

Bennett, C. H. and Brassard, G. [1984]. In *Proceedings of IEEE Conference on Computers, Systems, and Signal Processing (Bangalore, India)* (p. 175).

Bennett, C. H., Brassard, G. and Mermin, N. D. [1992]. *Phys. Rev. Lett., 68*, 557.

Bennett, C. H., DiVicenzo, D. P., Smolin, J. A. and Wootters, W. K. [1996]. *Phys. Rev. A, 54*, 3824.

Bruß, D., Christandl, M., Ekert, A., Englert, B.-G., Kaszlikowski, D. and Machiavello, C. [2003]. *Phys. Rev. Lett., 91*, 097901.

Chefles, A. [2000a]. *Contemp. Phys., 41*, 401.

Chefles, A. [2000b]. Quantum state discrimination. *Contemp. Phys., 41*, 401.

Cover, T. M. and Thomas, J. A. [1991]. *Elements of Information Theory*. Wiley-Interscience.

Csiszár, I. and Körner, J. [1978]. *IEEE-IT, 24*, 339.

Davies, E. B. [1976]. *Quantum Theory of Open Systems*. Academic Press, London.

Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. and Sanpera, A. [1996]. *Phys. Rev. Lett.*, *77*, 2818.

Ekert, A. K. [1991]. *Phys. Rev. Lett.*, *67*, 661.

Fattal, D., Inoue, K., Vuĉković, J., Santori, C., Solomon, G. S. and Yamamoto, Y. [2004]. *Phys. Rev. Lett.*, *92*, 37903.

Helstrom, C. W. [1976]. *Quantum Detection and Estimation Theory*. Academic Press, New York.

Ivanovic, I. D. [1987]. *Phys. Lett. A*, *123*, 257.

Kaszlikowski, D., Englert, B.-G. and Chua, K. T. [2004]. Coherent attack on tomographic quantum cryptography. Thesis submitted for the degree of Bachelor of Science, National University of Singapore.

Kaszlikowski, D., Lim, J. Y., Kwek, L. C. and Englert, B.-G. [2003]. *eprint arXiv/*`quant-ph`*/0312172*.

Kraus, K. [1983]. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer-Verlag, Berlin Heidelberg.

Liang, Y. C., Kaszlikowski, D., Englert, B.-G., Kwek, L. C. and Oh, C. H. [2003]. *Phys. Rev. A*, *68*, 022324.

Maurer, U. M. [1993]. *IEEE-IT*, *39*, 733.

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

Peres, A. [1996]. *Phys. Rev. Lett.*, *77*, 1413.

Rehácek, J., Englert, B.-G. and Kaszlikowski, D. [2004]. eprint arXiv/`quant-ph`/0408134.

Santori, C., Plton, M., Solomon, G., Dale, Y. and Yamamoto, Y. [2001]. *Phys. Rev. Lett.*, *86*, 1502.

Willeboordse, F. H. [2005]. Private communication.

Wootters, W. K. and Zurek, W. H. [1982]. *Nature*, *299*, 802.