A SECURITY STUDY OF TWO NON-TOMOGRAPHIC QUANTUM COMMUNICATION PROTOCOLS

SYED MUHAMAD ASSAD

NATIONAL UNIVERSITY OF SINGAPORE

2010

A SECURITY STUDY OF TWO NON-TOMOGRAPHIC QUANTUM COMMUNICATION PROTOCOLS

SYED MUHAMAD ASSAD

(B.Sc. (Hons), NUS)

A THESIS SUBMITTED

FOR THE JOINT NUS–ANU DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF PHYSICS

NATIONAL UNIVERSITY OF SINGAPORE

2010

Acknowledgements

I would like to thank my principal supervisor Prof. Berthold-Georg Englert at NUS for his guidance and tireless support throughout my Ph.D. candidature. I would also like to thank Prof. Lam Ping Koy for his support and for giving me the opportunity to do part of my research at the ANU.

Thank you, Jun Suzuki, for working with me on the direct communication protocol. Thank you, Andreas Keil, for your endless enthusiasm in tackling the most challenging problems.

A special thank you to Nicolai Grosse for your patience in teaching me everything I know about experimental quantum optics. Your ability to find simple and quick solutions to solve what at first looks like insurmountable problems makes working with you really fun and enriching.

Thank you to Daniel Alton for the many interesting discussions that we had in ironing out the problems in the continuous variable key distribution protocol. Your discipline and drive are very admirable.

Thank you to Thomas Symul, Daniel Alton, Christian Weedbrook and Timothy Ralph for teaching me continuous variable quantum information while I was at ANU and for allowing me to work on your interesting CVQKD protocol.

Thank you to Michael Stefzky, Moritz Mehmet and Wu Ru Gway for the joint effort in battling with the experiments we did at the ANU.

Thank you to my colleagues and friends at the NUS: Gelo Tabia, Marta Wolak, Dario Poletti, Amir Kalev, Philippe Raynal, Chua Wee Kang, Looi Shiang Yong, Bess Fang, Han Rui, Lu Yin, Teo Yong Siah, Niels Lorch and Daniel Kwan. You have made my stay at NUS a memorable one.

To my students and to my fellow instructors Nidhi Sharma, Jeremy Chong, Qiu Leiju and Setiawan, I would like to say thank you for renewing my interest in physics.

Thank you to Gleb Maslennikov, Tey Meng Khoon, Alexander Ling, Syed Abdullah and Brenda Chng for accommodating me in the lab when I needed to get away from the office once in a while.

Thank you to Ben Buchler, Vikram Sharma, Magnus Hsu, Chong Ken Li, Guy Micklethwait, Katherine Wagner, Zhou Hongxin and Roger Senior who shared the office with me at the ANU. Thank you for the stimulating discussions, thank you for the chess games and thank you for generally making my stay at the ANU a pleasant one.

Thank you Chong Ken Li for sharing with me your expertise on excess noise in fibres.

I would like to thank Nicolai Grosse and Jun Suzuki again for your many comments that helped in improving the thesis. I would also like to thank Low Han Ping for his careful reading of the thesis.

Contents

Abstract

The aim of this thesis is to study the security of two particular quantum communication protocols. We want to investigate what is the maximum amount of channel noise for which the protocols can still be secure. We do this by using well known bounds for limiting the information that an eavesdropper can obtain.

The first protocol that we study is a direct communication protocol using two-qubit states. We find the security threshold by analyzing the protocol in an entanglement based setting. The Holevo bound was used to put an upper bound on the information of an eavesdropper. To arrive at a manageable optimisation problem, we restrict the eavesdropper's attack strategy such that the noise introduced will be unbiased. Furthermore, we also impose some additional constraints on the eavesdropper that arises from the symmetry of the protocol. After doing this we then optimise the remaining parameters to arrive at the eavesdropper's optimal strategy and find out what is the maximum amount of information she can obtain. Once the eavesdropper's maximum information is known, the security threshold for secure communication was obtained by comparing that information with the information between the legitimate communicating parties.

The second protocol studied is a continuous variable quantum key distribution protocol using post-selection. For this protocol, we investigate the maximum

amount of information the eavesdropper can get under individual and collective attacks in the presence of Gaussian excess noise in the channel. By providing the eavesdropper with additional information, we can use known results on the accessible information for pure input states to bound the eavesdropper's information. For individual attacks, Levitin's result on the optimal measurement was used while for collective attacks, Holevo's bound was used to arrive at an upper bound for the eavesdropper's information. From this we can then arrive at the post-selection region where the legitimate communicating parties have more information than the eavesdropper. We can then find the maximum amount of noise that the protocol can tolerate before the eavesdropper knows too much and the protocol fails.

List of Tables

List of Figures

Chapter 1

Introduction

Quantum key distribution was one of the first real applications of quantum information in the commercial world. In fact apart from the quantum random number generator there is still no other real application of quantum information.

In 1994 Shor discovered an efficient factoring algorithm that works on a quantum machine [50]. That discovery threatens to jeopardise existing classical cryptography protocols whose security depends on the mathematical complexity of factoring large numbers. However as far as we know, there has not been much success in coherently manipulating more than a handful of qubits. In 2001, the first successful quantum factorising machine was able to factorise 15 [56]. By manipulating seven qubits, the group from Stanford and IBM reported that the prime factors of 15 are 3 and 5. In 2007, optical implementations of a compiled version of Shor's algorithm for factoring the same number were reported by two independent groups [31, 37]. This record has not been beaten. So for now at least, classical cryptography is still safe and not under much threat.

But when the day comes that our capable scientists and engineers succeed in building a quantum factorising machine of decent size, many of the current cryptography protocols will become insecure. In fact the successful labs will be able to decipher not only current secret messages, but also all old messages that were encrypted using the compromised protocols.

1.1 Quantum key distribution

It will then be time to look for a more secure cryptography protocol. One protocol that is not challenged by Shor's factoring algorithm is the *one-time pad* protocol of 1917 which Shannon proved to be unbreakable in 1945 during World War II. However the one-time pad is not a replacement for modern cryptography protocols such as the public key cryptography. This is because in the one-time pad, all the different parties that wish to communicate must a priori share a string of random keys. The amount of shared random keys required must be equal to the length of the message that each party wishes to communicate. In other words everyone must have a trusted channel with everyone else in which to distribute the keys. This is where quantum key distribution comes in. It acts as a trusted courier in the one-time pad protocol.

The first published mention of using quantum mechanics for ensuring security was in Wiesner's 1983 paper where he proposed a quantum currency that is impossible to counterfeit [59]. A year later, the first quantum cryptography protocol was proposed by Bennett and Brassard [7]. This has become known as the BB84 protocol.

For a more comprehensive review of the field, the reader can refer to review articles on the topic [21, 35, 45]. In this introduction, we shall restrict ourselves to giving a brief explanation of the BB84 protocol as well as a quantum key distribution protocol that uses continuous degrees of freedom.

1.1.1 BB84 protocol

The communicating parties are traditionally called Alice and Bob. In a quantum key distribution protocol, Alice wishes to establish a string of secret keys with Bob. In the BB84 protocol, Alice will send to Bob one of four possible qubit states chosen at random. These four states are the horizontally/vertically polarised states and the diagonal/anti-diagonal states. The horizontal and diagonal states are assigned the bit 0, while the vertical and anti-diagonal states are assigned the bit 1.

Bob will measure the qubits he received in either the horizontal–vertical basis or the diagonal–anti-diagonal basis. He chooses one of the two bases at random. After Bob's measurements are completed, Alice will announce through an authenticated public channel the basis in which she encoded her signals.

Every time that Bob measures in the same basis as Alice encodes, and this happens on average half of the time, Alice and Bob will share a perfectly correlated bit. The other half of the time when their bases do not match, Alice and Bob expect no correlation at all. In this sense, the efficiency of the protocol is half. On average, half of the encoding Alice sends will end up as the secret keys.

After authenticating themselves, Alice and Bob then use a fraction of the measurement outcomes to check that they indeed see the correlations that were expected. This check establishes that the quantum channel between them is secure.

The remaining matching-basis bits are then processed before being used as keys for the one-time pad protocol.

In this sense the protocol is not deterministic. In the perfect channel half of the data Alice sent will still be lost. This can be overcome if Bob has access to a quantum memory. He can safely store the qubits that Alice sent. Then at a later time, when Alice is sure that Bob has already received the qubits sent, Alice tells Bob the basis for each qubit. Bob then measures in the correct basis to recover the message.

The security of the original BB84 protocol stems from the fact that if someone (we call her Eve) tries to eavesdrop on the keys, she will not know a priori the basis that Alice encodes. As such, any attempt that she makes to learn something about the keys will induce noise on the signals that Bob receive. Subsequently when Alice and Bob check their correlations, they will find that it is less that what it should be. In this way, the channel can be characterised. The amount of noise they see is related to the amount of information an eavesdropper can extract. Alice and Bob can then protect their keys from the eavesdropper by using suitable error-correcting and privacy amplification schemes. If they find that the channel is too noisy, they would abandon the protocol altogether and find a different channel to use.

Since 1984, many different protocols including numerous variations of the original BB84 protocols have been proposed. Some of these protocols have been implemented in the laboratory.

1.1.2 Continuous variable key distribution

A different class of protocols uses continuous degrees of freedom instead of discrete level systems like qubits. The earliest continuous variable key distribution protocol was presented in 1999 by Ralph [40] and Hillery [26]. These protocols use squeezed states to ensure the security of the communication. One protocol that only uses coherent states was Grosshans and Grangier's coherent state protocol published in 2002 [23]. We shall explain that protocol in some detail in chapter 12. This protocol suffers from the 3 dB loss limit. For a transmission loss of greater than 50% the protocol becomes insecure.

Two different methods were introduced to overcome the 3 dB loss limit: post-selection [52] and reverse reconciliation [22]. In post-selection protocols, Alice and Bob would only select data points where they have an information advantage over Eve. In a reverse reconciliation protocol, Alice corrects her keys to have the same values as Bob's. Both protocols and their variants have been successfully implemented in laboratories.

1.2 Information theory

In this section, we define some terms and recap some useful results from information theory that will be used in this thesis. The proofs of the results can be found in standard textbooks [6, 15].

1.2.1 Classical entropy

Given a random variable A, where the outcome a_i has a probability $p(a_i)$ for $i \in \{1,2,\ldots,N\}$, the classical (Shannon) entropy of A is defined by

$$H(A) = -\sum_{i=1}^{N} p(a_i) \log p(a_i) \,. \tag{1.1}$$

The logarithm is taken in base 2. This measures the bits of information we gain, on average, when we learn about a letter of A. Equivalently, it gives the least average number of bits required to identify a letter of A. In other words, to unambiguously transmit a message of length M, say:

$$\underbrace{\{a_2, a_4, a_N, a_1, a_2, \ldots, a_4\}}_{M \text{ entries}} \,, \tag{1.2}$$

there exists (sometimes only when M tends to infinity) a suitable encoding scheme in which we can just send $M \times H(A)$ bits of information. In this sense, $H(A)/\log N$ is also the best compression limit for the random variable A. This is Shannon's noiseless coding theorem [49].

1.2.2 Von Neumann entropy

The von Neumann entropy is the quantum analogue of Shannon entropy. Given a quantum state represented by the density operator ρ, the von Neumann entropy of

ρ is defined as

$$S(\rho) = -\operatorname{Tr}\{\rho \log \rho\} \tag{1.3}$$

$$= -\sum_n \lambda_n \log \lambda_n \tag{1.4}$$

where λ_n are the non zero eigenvalues of ρ. Again, suppose Alice sends a message with M letters, say:

$$\underbrace{\{|\psi_2\rangle, |\psi_4\rangle, |\psi_N\rangle, |\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_4\rangle\}}_{M \text{ entries}}, \tag{1.5}$$

where each letter is chosen at random from the ensemble of pure states $|\psi_i\rangle$ with probability $p(\psi_i)$ for $i \in \{1, 2, \ldots, N\}$. Each letter is described by

$$\rho = \sum_{i=1}^{N} |\psi_i\rangle\, p(\psi_i)\, \langle\psi_i| \ . \tag{1.6}$$

To reliably transmit this whole quantum state, there exist an encoding scheme in which Alice can just send $M \times S(\rho)$ qubits (in the limit of large M). This is Schumacher's quantum noiseless coding theorem [47].

1.2.3 Mutual information

Consider a noisy channel in which Alice sends Bob some classical signals a_i with probabilities $p(a_i)$. When Alice sends the signal a_i, Bob obtains the measurement outcome b_j with conditional probability $p(b_j|a_i)$.

The mutual information $I(A,B)$ measures how much one random variable A can tell us about another random variable B. It gives the maximum value for the

average information transmitted to Bob per bit that Alice sends. Alice and Bob will be able to attain this if they use a suitable encoding and decoding scheme (which might be available only in the asymptotic limit of infinite signal length).

The mutual information is given by the difference between the entropy of Alice's distribution (before Bob's measurement) and the entropy of Alice's distribution conditioned on Bob's outcomes.

$$I(A,B) = H(A) - H(A|B) \; . \tag{1.7}$$

What this says is that the amount of information transmitted to Bob is equal to the amount of information initially contained in Alice's distribution minus the amount of information that is left in Alice's distribution after Bob has performed his measurement.

In terms of the probabilities, the entropy of Alice's distribution is

$$H(A) = -\sum_i p(a_i) \log p(a_i) \; . \tag{1.8}$$

Now conditioned on Bob obtaining an outcome b_j, entropy of Alice's distribution would be

$$H(A|B = b_j) = -\sum_i p(a_i|b_j) \log p(a_i|b_j) \; . \tag{1.9}$$

On average, Alice's entropy conditioned on Bob's outcomes would be

$$H(A|B) = \sum_j p(b_j) H(A|B = b_j) \tag{1.10}$$

$$= -\sum_{i,j} p(a_i, b_j) \log \frac{p(a_i, b_j)}{p(b_j)} \tag{1.11}$$

$$= H(A,B) - H(B) \tag{1.12}$$

which is the chain rule for joint entropy. $H(A,B)$ is the joint entropy of A and B. The mutual information between Alice and Bob is then

$$I(A,B) = H(A) + H(B) - H(A,B)\ , \tag{1.13}$$

symmetric between Alice and Bob. The relationship between the entropies $H(A)$, $H(B)$, $H(A,B)$, $H(A|B)$, $H(B|A)$ and the mutual information $I(A,B)$ is expressed in the Venn diagram in figure 1.1.

1.2.4 Accessible information and Holevo quantity

Now if instead of sending classical signals, Alice sends Bob signals using quantum states through a noisy quantum channel. The message that Alice sends is from the classical random variable A. Bob measures every quantum state individually using some fixed quantum measurement apparatus Π. After the measurement is completed, this apparatus gives a classical outcome for each quantum state. We now have a classical joint probability distribution (A,B) between Alice and Bob. We can then calculate how much information Bob receives per letter by the mutual information $I(A,B)$.

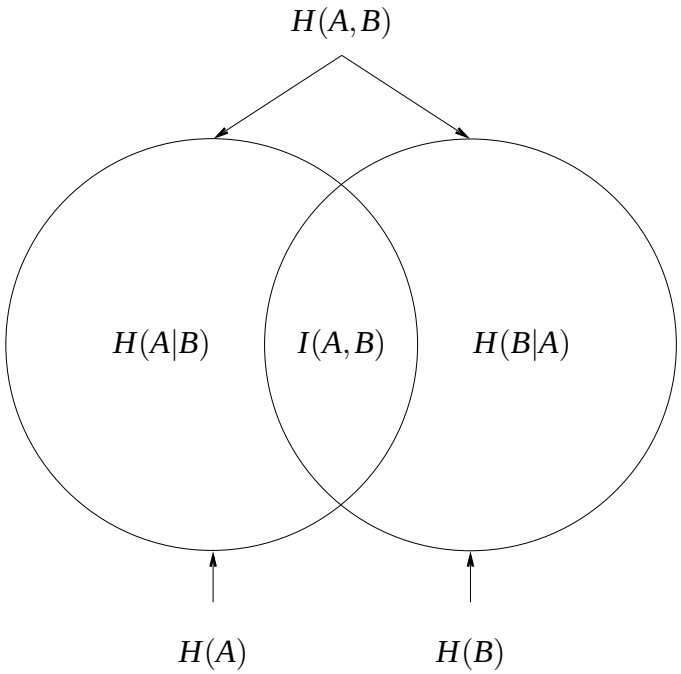


Figure 1.1: Venn diagram representing the relationship between entropy and mutual information. $H(A)$ and $H(B)$ are depicted by the whole circles. $H(A,B)$ is the union of the two circles.

If Bob uses a different measurement scheme $\tilde{\Pi}$, he may end up with a different value of mutual information. The accessible information I_{acc} is defined as the maximum of $I(A,B)$ over all possible measurement apparatus.

Given the state that Alice sends and the a priori probabilities, the task of finding the accessible information is in general not easy. An algorithm to approach this problem numerically was proposed in [57].

There are however bounds that bound the accessible information from above. One of them is the Holevo quantity. The accessible information is bounded by the Holevo quantity,

$$I_{\text{acc}} \leq S(\rho) - \sum p_i S(\rho_i) \equiv \chi(\{p_i \rho_i\}), \tag{1.14}$$

where ρ_i are Alice's quantum signals and p_i are the a priori probabilities for each ρ_i. The state $\rho = \sum_i p_i \rho_i$ is the statistical mixture that Bob receives.

1.3 Overview of the thesis

This objective of this thesis is to investigate the security of two particular quantum communication protocols when implemented in a noisy channel. It is organised as follows.

In chapter 2 we state the general security criteria for quantum cryptography. These criteria will be used in both protocols. Following this the thesis is divided into two parts.

The first part is concerned with a direct communication quantum communication protocol that utilises two qubits to transmit a single classical bit [3–5]. In

chapter 3, we present this protocol. Chapter 4 looks at a particular intercept and resend attack on the protocol. Chapter 5 considers a more general attack by considering an equivalent entanglement based protocol. Chapter 6 formulates the optimisation problem in terms of the matrix representations of Eve's ancillary states. In chapter 7 we define a basis between Alice and Bob so that the constraints on Eve can be written down explicitly. In chapter 8, we solve the optimisation problem for simple cases when there is no noise in the channel and also when there is so much noise that the state between Alice and Bob becomes separable. Chapter 9 solves the general case for arbitrary noise level. In order to make the problem more tractable, we had to make some symmetry assumptions on Eve's attack. In chapter 10, we present a conclusion and an outlook for possible future works.

In appendix A, we show how to construct an equivalent entanglement based protocol for an arbitrary channel between Alice and Bob. Appendix B lists down explicitly the 64 constraints on Eve's ancillary states for a chosen Alice–Bob basis. Appendix C gives the Schmidt decomposition of Eve's purification between Alice–Bob and Eve.

The second part of the thesis begins with a review on continuous variable Gaussian states in chapter 11. Chapter 12 provides an example of one of the earliest continuous variable quantum key distribution protocols. This protocol suffers from the 3 dB loss limit. In chapter 13, we introduce the actual protocol that will be studied. This protocol uses post-selection to overcome the 3 dB loss limit. Chapter 14 reviews and extends work that was done on the protocol in the presence of vacuum noise. In chapter 15, we study the security of the protocol when there is thermal noise in the channel. In studying this, we need to compute

the inner products between Eve's ancillary states which is obtained by performing the straightforward but lengthy Gaussian integrations. These inner products are computed in appendix E. In chapter 16 we calculate some numerical values for useful information between Alice and Bob for a specific channel with transmission loss of 0.5. Finally in chapter 17 we summarise the results of this part and present an outlook for future works.

Original work in the thesis: The contents of chapters 1 and 2 are a compilation of existing works. The protocol presented in chapter 3 is not new and was first published in 2002 [3]. However the experimental setup for the protocol in section 3.3 has never been published elsewhere. The biased intercept and resend attack in section 4.2 is a particular case of the optimal scheme presented in [4]. The analysis and results for the unbiased intercept and resend attack in section 4.3 are original. For the remainder of part one of thesis, the tools used for analysing the security are not new, but their application to this protocol is original.

In part two of the thesis, chapters 11 and 12 are a review of existing works on Gaussian states and continuous variable key distributions. Chapters 13 and 14 are elaborations of the protocol published in [52]. Except for figure 14.3, all the other figures in chapter 14 are original. The analytical formula for the post-selection region in section 14.3.2 is also new. Section 14.4 extends the work in [52] to a collective attack. The contents in chapters 15 and 16 were done in collaboration with the authors of [1, 54]. The general input state for Eve and the formulation of her state in terms of a covariance matrix in section 15.1 are original and has not been published elsewhere. The analytical formulas for Eve's inner products presented in 15.1.2 were contributed by me. All the calculations and results in sections 15.4 and 15.5 are original work. The analytical formula for

the reconciliation direction in section 15.4, the formula for the asymptotic limit of the post-selection region and the cubic equation that gives the noise threshold in section 15.5 were also my contributions. Chapter 16 elaborates on the theory calculations presented in [54] for a particular value of transmission and excess noise.

Chapter 2

Security criteria for quantum key distribution protocols

In this thesis, we will be investigating the security of two quantum communication protocols. The first protocol is a discrete variable protocol involving a two-qubit system while the second protocol is a continuous variable protocol where the signals are transmitted using single-mode coherent states. We will use the same methods to study both protocols.

In this chapter, we shall discuss in general how much information an eavesdropper would be able to get in a generic quantum key distribution protocol.

Throughout this thesis, we assume ideal situations for Alice and Bob. In particular, we assume that Alice has a perfect random number generator and that Eve does not have access to Alice and Bob's labs. We also assume that Alice and Bob have access to a public but authenticated classical channel. Eve can listen to the channel but she cannot tamper with it.

Furthermore, the bounds we provide here are for the asymptotic limit of infinite key lengths. Methods for security analysis of finite key length have been developed by Hayashi [24] and Scarani and Renner [46] but they are beyond the scope of this thesis.

This chapter is organised as follows. Section 2.1 gives the definitions of a quantum state and quantum measurement. Section 2.2 discusses the various types of eavesdropping that an adversary can do depending on how much power she has. We also discuss how her information can be bounded. In section 2.3, we look at how Alice and Bob characterise the channel. This is to determine how much information was leaked to the eavesdropper. In section 2.4, we calculate the explicit values for the accessible information and Holevo quantity for two pure input states with equal probability. Finally, section 2.5 gives a discussion on the classical post-processing steps required in order to extract secret keys from the raw data.

2.1 Quantum states and quantum measurements

Throughout this thesis, we shall deal with quantum states passing through a quantum channel and being measured using quantum measurement devices. A quantum state is a physical entity with a fixed physical property. We are usually interested in only some degrees of freedom for the entity. Mathematically, the state is represented by a positive semi-definite operator with unit trace in a complex Hilbert space. The dimension of the Hilbert space corresponds to the degrees of freedom that we are interested in.

When we speak of a quantum channel, we refer to a fixed physical interaction that brings one quantum state to another quantum state in the same Hilbert space. The channel is memoryless; it acts on each quantum state independently. We can think of the channel as an ensemble of identical channels, each of which is used only once. Mathematically, a quantum channel can be represented by a completely positive and trace preserving linear operator acting on the space of the quantum states.

A quantum measurement device is a box with certain well defined physical interactions and having a number of (possibly continuous) outcomes. Whenever a physical state is put inside this box, the physical interactions are such that one of its outcomes will click. This outcome presumably measures some physical property of the quantum state. The box then resets to its initial state; ready to measure the next incoming state. As far as this thesis is concerned, once a quantum state has been measured, it is destroyed and not available for further measurements. Mathematically, the outcomes of a measurement apparatus is associated with the set of positive semi-definite operators $\Pi = \{\pi_j\}_{j\in J}$. The outcomes are labelled by j and J denotes the set of all possible outcomes. The outcomes sum up to the identity on the Hilbert space of the quantum state on which the measurement is performed. The set Π is called a positive operator value measure (POVM). For a state ρ that is to be measured, the probability that it will trigger the j-th outcome is given by the trace $\mathrm{Tr}\{\rho\pi_j\}$.

2.2 Eve's attacks

We assume that Eve is capable of doing perfect quantum operations and that she has a perfect noiseless channel between both Alice and Bob. The noisy quantum channel between Alice and Bob is replaced by Eve's perfect channel. But Eve sends Bob a state that was corrupted by her measurements such that Alice and Bob still think that the channel is noisy.

Eve's plan of attack would be to attach probes to the signals that Alice sends to Bob. Eve lets these probes interact with the signal. But we restrict each probe to interact with a different signal. After that, Eve waits until Alice and Bob have concluded the protocol and even after they have utilised the key to transmit a message. Only then will Eve measure her probes in such a way so that she gains as much information as she can on the secret message. We assume that Eve can store her probes indefinitely.

If we restrict Eve to measure each probe independently, this attack is called an individual attack. The more general case where Eve can measure her probes together is called a collective attack.

Depending on the probes Eve chooses, and how she measures those probes, she may be able to get some information on the secret message. Our task is to quantify how much information Eve can get. By knowing this information limit on Eve, Alice and Bob can plan to use suitably strong privacy amplification techniques to eliminate Eve's information.

Fortunately, given the quantum state of Eve's probes, we can bound Eve's information in an individual as well as a collective attack. In an individual attack, the amount of information Eve can attain by using a particular measurement strat-

egy on her probes is given by the mutual information [49]. The maximum amount of mutual information Eve can get (by using the best measurement strategy on her probes) is called the accessible information.

The final key rate between Alice and Bob is given by the difference between Alice and Bob's mutual information and Eve's accessible information (Csiszar and Korner [16]).

For a collective attack, the amount of classical information Eve can extract from her probes is bounded by Holevo's bound [27]. This bound was shown to be attainable by Holevo [28] and Schumacher and Westmoreland [48]. The final key rate between Alice and Bob is given by the difference between Alice and Bob's mutual information and the Holevo quantity (Devetak and Winter [17]).

The most general class of attack is known as coherent attack (also called joint attack). This is when Eve attaches one probe in a high dimensional Hilbert space to all of Alice's incoming signals. After Alice has sent her message, Eve then measures her signal probe. However it was shown that for a finite dimensional system, a coherent attack does not perform better than a collective attack (Renner [43]). This result was later extended to an infinite dimensional system in [42].

2.3 Characterising the channel

In practice, the channel between Alice and Bob will not be perfect. There will be some loss and noise due to interactions with the environment or perhaps to the presence of an eavesdropper. To arrive at a bound on Eve's knowledge of the channel, we assume that all noise in the channel is due to Eve.

For Alice and Bob to put an upper bound on the information Eve can get, they would need to continuously characterise the channel. In most protocols, the channel characterisation is done by using the actual signals and measurement outcomes that will be used to generate the keys.

Protocols where Alice and Bob can fully characterise the channel are called tomographic protocols. The six-state protocol [10] and the Singapore protocol [19] are examples of tomographic protocols. In these tomographic protocols, there is a one-to-one correspondence between the noise that Alice and Bob see and the probes that Eve uses.

In other protocols, there will not be enough information for complete characterisation of the channel. These protocols are classified as incomplete tomographic protocols. This means that Eve can use several probing strategies, leaving Bob with different quantum states, but Alice and Bob will not know which exact strategy Eve used. The security analysis in such protocols are complicated by the fact that Alice and Bob do not know what is the quantum state of Eve's probe.

2.4 Eve's information for two pure states

In this section, we summarise two useful results: the accessible information and the Holevo quantity for two pure states with equal a priori probabilities. These give the maximum amount of classical information that can be obtained by individual measurements and collective measurements respectively.

2.4.1 Accessible information for two pure states

Two pure states can always be mapped onto a two dimensional Hilbert space. We can represent these two states in the computational basis as

$$\begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix} |\psi_1\rangle = \begin{pmatrix} \cos\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} \end{pmatrix}, \begin{pmatrix} \langle 0| \\ \langle 1| \end{pmatrix} |\psi_2\rangle = \begin{pmatrix} \sin\frac{\alpha}{2} \\ \cos\frac{\alpha}{2} \end{pmatrix}. \tag{2.1}$$

In the Bloch's sphere, the two states will have the Bloch vectors

$$\psi_1 = \begin{pmatrix} \sin\alpha \\ 0 \\ \cos\alpha \end{pmatrix}, \psi_2 = \begin{pmatrix} \sin\alpha \\ 0 \\ -\cos\alpha \end{pmatrix}. \tag{2.2}$$

The measurement that optimises the mutual information is a POVM with two outcomes (Levitin [32]):

$$|\phi_1\rangle = |0\rangle \hat{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\phi_2\rangle = |1\rangle \hat{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.3}$$

In the Bloch's sphere, the two outcomes point to the north and south poles respectively

$$\phi_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \phi_2 = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}. \tag{2.4}$$

The state and measurement vectors are depicted in figure 2.1. The probability

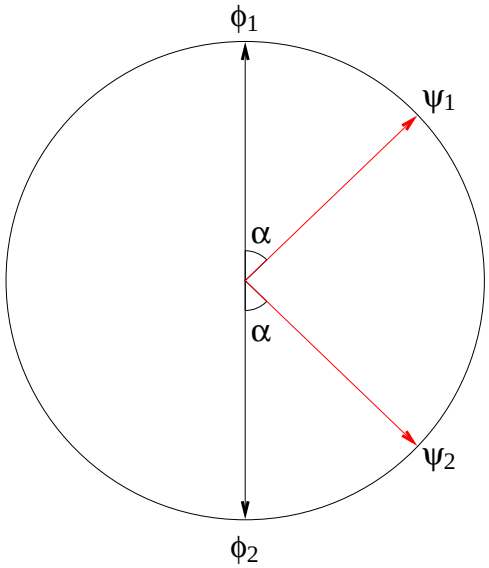


Figure 2.1: Bloch sphere representation for the POVM that maximises the mutual information for two pure input states with equal a priori probabilities. The two pure input states ψ_1 and ψ_2 are represented by the red lines while the two measurement outcomes ϕ_1 and ϕ_2 are shown in black.

table obtained using this POVM would be

Signal state	POVM outcome	
	$\langle\phi_1\|$	$\langle\phi_2\|$
$\|\psi_1\rangle$	$\frac{1}{2}\cos^2\frac{\alpha}{2}$	$\frac{1}{2}\sin^2\frac{\alpha}{2}$
$\|\psi_2\rangle$	$\frac{1}{2}\sin^2\frac{\alpha}{2}$	$\frac{1}{2}\cos^2\frac{\alpha}{2}$

for which the mutual information is

$$I = \frac{1}{2}\left[\left(2\cos^2\frac{\alpha}{2}\right)\log\left(2\cos^2\frac{\alpha}{2}\right) + \left(2\sin^2\frac{\alpha}{2}\right)\log\left(2\sin^2\frac{\alpha}{2}\right)\right] \tag{2.5}$$

$$= \frac{1}{2}\left[(1+\cos\alpha)\log(1+\cos\alpha) + (1-\cos\alpha)\log(1-\cos\alpha)\right] \tag{2.6}$$

$$= \Phi(\cos\alpha) \tag{2.7}$$

$$= \Phi\left(\sqrt{1-\left|\langle\psi_1|\psi_2\rangle\right|^2}\right), \tag{2.8}$$

where

$$\Phi(x) = \frac{1}{2}\Big[(1+x)\log(1+x) + (1-x)\log(1-x)\Big] \tag{2.9}$$

is a monotonically increasing function.

This is the maximum amount of information that can be obtained by individual measurements on the input states.

2.4.2 Holevo quantity for two pure states

The Holevo quantity for two pure states in section 2.4.1 is given by the entropy of the statistical mixture

$$\rho_T = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2| \tag{2.10}$$

$$\hat{=} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\sin\alpha \\ \frac{1}{2}\sin\alpha & \frac{1}{2} \end{pmatrix} \tag{2.11}$$

which has eigenvalues $\frac{1}{2}(1 \pm \sin\alpha)$. The Holevo quantity is

$$\chi = -\frac{(1+\sin\alpha)}{2}\log\frac{(1+\sin\alpha)}{2} - \frac{(1-\sin\alpha)}{2}\log\frac{(1-\sin\alpha)}{2} \tag{2.12}$$

$$= 1 - \frac{1}{2}[(1+\sin\alpha)\log(1+\sin\alpha) + (1-\sin\alpha)\log(1-\sin\alpha)] \tag{2.13}$$

$$= 1 - \Phi(\sin\alpha) \tag{2.14}$$

$$= 1 - \Phi\left(\left|\langle\psi_1|\psi_2\rangle\right|\right) \ . \tag{2.15}$$

This gives the maximum amount of information that can be obtained by collective measurements on the input states.

2.5 Classical post-processing

After having a bound on Eve's information about the raw keys, Alice and Bob would like to eliminate Eve's information so that they can share an absolutely secret key. This is done by doing some post-processing on the raw bits.

The raw bits are established via the quantum key distribution protocol. Alice first generates a string of N' random bits. She transmits this string to Bob through a noisy channel. If the channel noise is unbiased, then the string as seen by Bob will also be completely random. In other words, Bob's string will still have an entropy of N' bits. Next Alice and Bob performs basis reconciliation depending on the protocol. For example in the BB84 protocol, basis reconciliation would involve Alice and Bob discarding data points from mismatch bases. After this step, Alice and Bob would have a string of N bits.

The mutual information between Alice and Bob can be calculated after doing a parameter estimation on the channel. We denote this by NI_{AB}. Eve's information on Alice's bits can also be estimated, and we denote her maximum information as NI_E. We assume that I_{AB} is greater than I_E. Otherwise the protocol fails and no secret key can be generated. The post-processing begins after this point. The post-processing can be divided into two parts, information reconciliation and privacy amplification.

Information reconciliation involves Alice sending classical bits to Bob so that Bob can correct his errors [9]. At the end of this process, Alice and Bob will share a perfectly correlated random string of length N. Their mutual information will be N bits. In a perfect reconciliation protocol, Alice will need to send just

	Mutual information between Alice and Bob	Mutual information between Eve and Alice
Raw key	NI_{AB}	NI_E
I.R.	N	$N(1-I_{AB}+I_E)$
P.A.	$N(I_{AB}-I_E)$	0

Table 2.1: Table showing the mutual information between the Alice and Bob and between Eve and Alice at the various stages of the post-processing procedure. In the information reconciliation (I.R.) step, Alice announces $N(1-I_{AB})$ bits of information for Bob to correct his errors. In the privacy amplification (P.A.) step, the length of the string is reduced by $N(1-I_{AB}+I_E)$ bits so that the final mutual information between Eve and Alice is zero.

$N(1-I_{AB})$ classical bits to do the reconciliation. Listening to these bits, Eve's mutual information with Alice is now $N(I_E+1-I_{AB})$ bits.

The next step is privacy amplification [8]. In this step, Alice will choose a random universal hashing function and apply that function on her string. As a result, her string will reduce in length from N to

$$M = N - N(I_E+1-I_{AB}) \tag{2.16}$$

$$= N(I_{AB}-I_E)\,. \tag{2.17}$$

Bob will apply the same function to distill an identical string of length M. The ratio of the new string to the old string is $M/N = I_{AB}-I_E$. Because Eve's N bits string differs from Alice's, when Eve applies the hashing function, her resulting M bits string will be completely uncorrelated to Alice's string. Eve has zero information on Alice's bits, while Alice and Bob share a string of $M = N(I_{AB}-I_E)$ secret bits. The mutual information between the Alice and Bob and between Alice and Eve at the various stages of the post-processing procedure are summarised in table 2.1.

Part I

Security analysis of a quantum direct communication protocol in the presence of unbiased noise

Chapter 3

Introduction to the protocol

The first protocol that we shall investigate is a discrete variable direct communication protocol. This direct communication protocol enables Alice to send messages to Bob without the need to first establish a shared secret key.

In section 3.1, we will give the origins of the protocol that we want to study. We also recap some preliminary work that was done to analyse the security of the protocol. In section 3.2, we shall formally introduce the protocol with an example to demonstrate its workings. In section 3.3, a possible experimental setup for of the protocol will be presented. Finally section 3.4 gives a discussion on the direct communication protocol. It also provides a comparison between a direct communication protocol and a key distribution protocol.

3.1 Introduction

The protocol that we shall study uses two-qubit states for transmitting a classical bit. The idea of using two qubits to deterministically send a classical bit was pub-

lished by Beige, Englert, Kurtsiefer and Weinfurter in a book chapter in 2002 [3]. The protocol can also be found in [5] with slight generalisations.

Deterministic here means that for every two-qubit state that Alice sends, Bob will get one bit of key. Both publications briefly mention a two-qubit protocol in which Alice can transmit the message securely without having to first establish a key. This *direct communication* protocol was published as a separate publication on its own in [4].

In all those publications, the security analysis was restricted to minimising the error rate in a general intercept and resend attack. The intercept and resend strategy was not required to be unbiased.

In [4], the intercept resend attack where Eve measures Alice's qubit using an orthogonal measurement basis and then forwards the outcome state to Bob was analysed. It was found that for any orthogonal measurement used, the error rate Alice and Bob see will be at least $1/6$. Furthermore, numerical simulations in which Eve forwards a different state from her outcome state were done but the error rate was still never less than $1/6$.

3.2 The protocol

The protocol involves states of two qubits. The next paragraph will introduce the states.

Let $\{|1-\rangle, |2-\rangle, |3-\rangle, |4-\rangle\}$ be a set of orthonormal states that forms a basis in Alice's four dimensional Hilbert space. We call these states the *minus states*. We define a second set of orthonormal states which we call the *plus states*,

$\{|1+\rangle, |2+\rangle, |3+\rangle, |4+\rangle\}$, by

$$\begin{pmatrix} |1+\rangle \\ |2+\rangle \\ |3+\rangle \\ |4+\rangle \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} |1-\rangle \\ |2-\rangle \\ |3-\rangle \\ |4-\rangle \end{pmatrix} . \tag{3.1}$$

For example the state

$$|2+\rangle = \frac{1}{\sqrt{3}} \left(-|1-\rangle + |3-\rangle - |4-\rangle \right) . \tag{3.2}$$

By construction

$$\langle n+ | m- \rangle = 0 \text{ if } n = m \tag{3.3}$$

and

$$\left| \langle n+ | m- \rangle \right| = \frac{1}{\sqrt{3}} \text{ if } n \neq m \, . \tag{3.4}$$

These eight states $\{|n+\rangle, |n-\rangle\}$ for $n \in 1,2,3,4$ are the ingredients of the protocol.

In the first step of the protocol, Alice will send to Bob one of the eight states $\{|n+\rangle, |n-\rangle\}$. The parity type ($+$ or $-$) of the state Alice sends will correspond to the bit of the message that she intends to convey. The numeral type (1, 2, 3 or 4) is chosen at random.

When Bob receives Alice's two-qubit state, he picks one of two measurement boxes to measure the two-qubit state. Each box has four outcomes. The first box, we call the *plus box,* has outcomes such that the state $|n+\rangle$ will cause the

Alice's numeral type	Bob uses plus box				Bob uses minus box			
	1	2	3	4	1	2	3	4
1	+	−	−	−	−	+	+	+
2	−	+	−	−	+	−	+	+
3	−	−	+	−	+	+	−	+
4	−	−	−	+	+	+	+	−

Table 3.1: Table that Bob uses to determine the parity of Alice's bit based on Alice's numeral type and the parity type of Bob's measuring box. For example, if Alice sends a type 2, and Bob measured the state using the plus box and obtains outcome 3, Bob concludes that Alice had send a minus parity.

n-th outcome to click. Bob can construct the plus box since the plus states are mutually orthogonal. Analogously, the *minus box* distinguishes the minus states. Bob chooses his measurement box at random.

In the final stage of the protocol, after Bob has done his measurement, Alice reveals the numeral type of the state that she sends. Bob will then know what is the bit type by looking up the table 3.1.

3.2.1 Example of the protocol

The protocol is perhaps easiest understood through an example. As an example, say that Alice wants to send Bob the ten bits string

$$\{-,-,-,+,-,-,+,-,+,-\}\,.$$

She generates a string of ten random numbers from one to four

$$\{2,1,1,2,4,2,3,1,4,4\}\,.$$

She pairs each bit to a random number and sends the state corresponding to the pairing. In our example, Alice sends the states

$$\{|2-\rangle, |1-\rangle, |1-\rangle, |2+\rangle, |4-\rangle, |2-\rangle, |3+\rangle, |1-\rangle, |4+\rangle, |4-\rangle\} \ .$$

Bob will generate a string of ten random bits to use to decide which box (plus or minus) to use to measure the incoming qubit pairs. Bob generates the random string

$$\{+,-,+,-,-,+,+,+,+,-\} \, .$$

In the first qubit pair, Alice sends a minus state $|2-\rangle$ and Bob measures using the plus box. Due to the relation $\langle 2+|2-\rangle = 0$, Bob will never get the outcome 2. In fact he would get the outcomes 1, 3 or 4 with equal probability. In this case, let us say outcome 3 happens to click.

In the second qubit pair, Alice sends the minus state $|1-\rangle$ and Bob measures using the minus box. In this case, Bob will get outcome 1 for certain. The outcomes for Bob are given in following table.

Alice send	Bob's measurement box	Bob's outcome	Bob's decoded bit
$\|2-\rangle$	$+$	3	$-$
$\|1-\rangle$	$-$	1	$-$
$\|1-\rangle$	$+$	2	$-$
$\|2+\rangle$	$-$	1	$+$
$\|4-\rangle$	$-$	4	$-$
$\|2-\rangle$	$+$	4	$-$
$\|3+\rangle$	$+$	3	$+$
$\|1-\rangle$	$+$	2	$-$
$\|4+\rangle$	$+$	4	$+$
$\|4-\rangle$	$-$	4	$-$

When Alice sends the same parity type as Bob's measurement box, Bob's outcome would be the same as Alice's numeral state (as in cases 2, 5, 7, 9 and 10). If Alice's parity differs from the parity of Bob's measurement box, then Bob's outcome will not be the same as Alice's numeral state.

For the first qubit pair, after Alice announces that she sends a type 2 state, Bob can find out from table 3.1 that Alice sends the minus bit. Bob can also decode all the remaining incoming qubit pairs correctly to unravel Alice's message.

3.3 Experimental setup

To our knowledge, no experiments were conducted with regards to this protocol. In this section, we outline a possible realisation of the protocol's two separate degrees of freedoms using a photon. We use the polarisation of the photon as one qubit $\{|v\rangle, |h\rangle\}$ and its path through an interferometer as the second $\{|L\rangle, |R\rangle\}$.

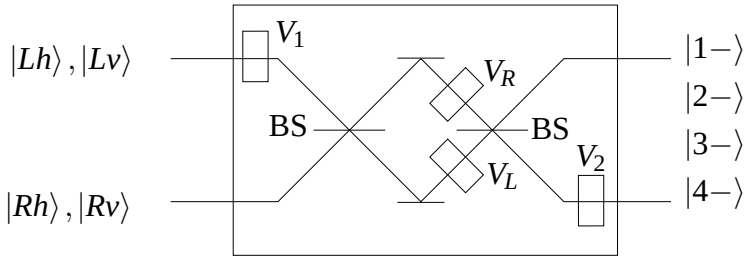


Figure 3.1: An experimental setup for converting the plus states to the minus states. It consists of an interferometer with two sets of polarisers V_R and V_L to convert the plus states to the minus states. The polarisers V_R and V_L consist of a half waveplate sandwiched between two quarter waveplates. The angle settings for the waveplates are stated in the text. The polarisers V_1 and V_2 are set to do nothing. BS denotes beam splitter.

The labels v and h denote vertical and horizontal polarisations while the labels L and R denote the upper and lower arms of the interferometer respectively.

In [20], it was shown that an arbitrary two-qubit operation can be realised by a combination of wave plates and phase shifter. In particular, the setup in figure 3.1 can realise any two-qubit gate by suitable choices of phase shifters and wave plate V_1, V_2, V_L and V_R. Each of these V consists of a half wave plate sandwiched between a quarter wave plate plus a phase shifter. The unitary action of the beam splitters are given by:

$$U_{BS} = \frac{1}{\sqrt{2}}\Big(|R\rangle\langle R| + |L\rangle\langle L| + \mathrm{i}\,|R\rangle\langle L| + \mathrm{i}\,|L\rangle\langle R| \Big) \tag{3.5}$$

and the mirrors by:

$$U_M = -\mathrm{i}\Big(|L\rangle\langle R| + |R\rangle\langle L| \Big)\,. \tag{3.6}$$

The quarter wave plates acts like

$$V_{\frac{\lambda}{4}}(\theta) = \frac{1}{\sqrt{2}}\Big(1 - \mathrm{i}\sigma_1 \sin(2\theta) - \mathrm{i}\sigma_3 \cos(2\theta)\Big) \tag{3.7}$$

and the half wave plate acts like

$$V_{\frac{\lambda}{2}}(\theta) = -\mathrm{i}\Big(\sigma_1 \sin(2\theta) + \sigma_3 \cos(2\theta)\Big) \tag{3.8}$$

where

$$\sigma_1 = |h\rangle\langle v| + |v\rangle\langle h| \tag{3.9}$$

and

$$\sigma_3 = |v\rangle\langle v| - |h\rangle\langle h| \ . \tag{3.10}$$

The complete V is made up of

$$V(\alpha,\beta,\gamma,\phi) = \exp(\mathrm{i}\phi) V_{\frac{\lambda}{4}}(\gamma) V_{\frac{\lambda}{2}}(\beta) V_{\frac{\lambda}{4}}(\alpha) \ . \tag{3.11}$$

If we define the plus basis as

$$\{|1+\rangle, |2+\rangle, |3+\rangle, |4+\rangle\} = \{|Lv\rangle, |Lh\rangle, |Rv\rangle, |Rh\rangle\} \ , \tag{3.12}$$

then the choice

$$V_1 = 1\,, \tag{3.13}$$

$$V_2 = 1\,, \tag{3.14}$$

$$V_L = V(\alpha, \beta_L, \gamma, \phi)\,, \tag{3.15}$$

$$V_R = V(\alpha, \beta_R, \gamma, \phi) \tag{3.16}$$

would convert the plus basis into the minus basis where the angles are

$$\gamma = \frac{\pi}{8}\,, \tag{3.17}$$

$$\beta_{R/L} = \pm\cos^{-1}\left(\frac{1}{2}\sqrt{2 \pm \sqrt{2 \pm \frac{4\sqrt{2}}{3}}}\right)\,, \tag{3.18}$$

$$\alpha = -\frac{3\pi}{8}\,, \tag{3.19}$$

$$\phi = 0\,. \tag{3.20}$$

With this choice,

$$V_L = \frac{1}{\sqrt{3}}\Big[|v\rangle\langle v|\,\mathrm{i} + |v\rangle\langle h|\,(1+\mathrm{i}) + |h\rangle\langle v|\,(-1+\mathrm{i}) + |h\rangle\langle h|\,(-\mathrm{i})\Big]\,, \tag{3.21}$$

$$V_R = \frac{1}{\sqrt{3}}\Big[|v\rangle\langle v|\,(-\mathrm{i}) + |v\rangle\langle h|\,(1-\mathrm{i}) + |h\rangle\langle v|\,(-1-\mathrm{i}) + |h\rangle\langle h|\,(\mathrm{i})\Big] \tag{3.22}$$

and with the combined action of the wave plates as

$$V_{WP} = |L\rangle\langle L| \otimes V_L + |R\rangle\langle R| \otimes V_R\,, \tag{3.23}$$

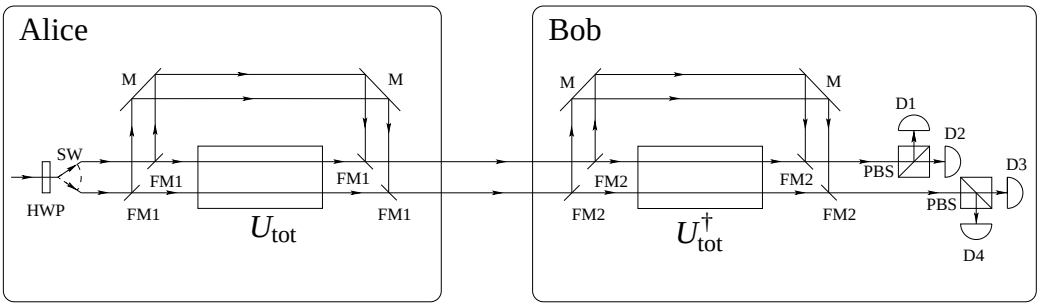


Figure 3.2: Experimental setup for the two-qubit direct communication protocol. Alice uses a half wave plate (HWP) to send either horizontal or vertical polarised light. The switch (SW) is used to select either the upper or lower arm of the interferometer. When her set of flipper mirrors (FM1) is activated, the light will be reflected off the mirrors (M) and bypass the conversion box (U_{tot}). This will send a state with positive parity to Bob. Deactivating the flipper mirrors will cause the light to go through the conversion box which brings a positive parity state to a negative parity state. This will send a state with negative parity to Bob. When Bob activates his set of flipper mirrors (FM2), the light only goes through a polarising beam splitter (PBS) before being detected at the detectors (D1–D4). This will act to distinguish the plus parity states. To implement the negative parity measurement, Bob deactivates his flipper mirrors causing the light to pass first through the reverse conversion box ($U_{\text{tot}}^{\dagger}$) before the detection.

the setup in figure 3.1 is described by the unitary

$$U_{\text{tot}} = U_{BS} V_{WP} U_M U_{BS} \tag{3.24}$$

$$= |1-\rangle\langle 1+| + |2-\rangle\langle 2+| + |3-\rangle\langle 3+| + |4-\rangle\langle 4+| \tag{3.25}$$

which converts the plus basis to the minus basis as promised. We call this setup the *conversion box*. It turns out that the conversion box will convert the minus states to the plus states.

The final setup between Alice and Bob is depicted in figure 3.2. Alice always starts by creating one of the four plus states. To send a minus state, Alice will put

her plus state through the conversion box U_{tot}. This two-qubit state is then sent to Bob via the quantum channel. At Bob's laboratory, he has a set of four detectors used to perform a measurement in the plus basis. To measure in the minus basis, Bob will pass the two-qubit state through a conversion box operated in reverse $U_{\text{tot}}^{\dagger}$ before measuring them.

3.4 Discussions on direct communication

In this section, we discuss the distinctive features of a direct communication protocol. We will then point out the main differences between a direct communication and a key distribution protocol.

The novel feature of a direct communication protocol is that the message itself is being transmitted through the quantum channel. To ensure secrecy of the message, the message must remain undecipherable until the channel security during transmission has been checked. This is a unique situation where a secret message has to go through a channel whose security can only be checked after its use. To ensure the message remains undecipherable two different sets of basis are used in this protocol. The basis announcements that enable the decoding of the message are only released after the channel security has been established.

For direct communication to take place, Bob must be able to decode each bit deterministically. For him to do this without having a quantum storage device, the protocol uses a two-qubit state to transmit a single bit.

To date, most quantum communication implementations have favoured key distribution rather than direct communication. There are several practical reasons for the former's popularity.

One reason is that a key distribution protocol is less affected by losses than a direct communication protocol. In a key distribution protocol, a lost signal merely means that Alice and Bob have to transmit more signals to generate sufficient raw bits. Since the lost signals do not contain any message yet, they do not compromise security. A direct communication protocol however is not as robust against loss. Loss translates to missing bits in the message and hence noise in the transmitted message.

Another advantage of key distribution over direct communication is that once generated, the secret keys can be accumulated and stored for future use. The quantum channel can be consistently utilised to establish a reserve of keys. In a direct communication protocol, the message can only be transmitted when Alice has something to communicate to Bob. The channel will be utilised during these periods. However there will be lull periods when Alice does not have anything to say to Bob where the quantum channel would stay idle. Hence we can foresee that the capacity of the quantum channel would be better utilised in a key distribution protocol rather than a direct communication protocol.

In a key distribution protocol, secret two way communication between Alice and Bob is possible once the secret keys have been established. However in a direct communication protocol, to achieve the same thing, a two way quantum channel would be needed.

A major flaw of a direct communication protocol is that since the message is being transmitted, then in the presence of noise, the eavesdropper can gain information on the message itself. For example, Eve could use the same procedure that Bob uses to decode the two-qubit states that she intercepts. Doing this, the message is no longer secret. Eve would gain partial knowledge of the message.

It is possible for Alice to perform a ‘privacy amplification’ procedure prior to using the channel. This would result in Alice and Bob sharing a completely secret message but at the expense that the message will be completely random. This procedure is discussed briefly in chapter 10.

For these reasons, we do not expect a direct communication protocol to be favoured over a key distribution protocol in the near future. For the situation to change, we would need to have a quantum channel with a high transmission rate. We would also need to develop the ability to easily manipulate two-qubit states. And at a more fundamental level, we would need to find a way such that Bob can deterministically decode Alice’s message but not Eve.

Even if we concede that performing direct communication is not feasible, the protocol can still be used as a key distribution protocol. The results in this thesis can be used to generate secret keys in a conventional key distribution protocol.

Chapter 4

Noise 1: Intercept and resend strategies

In this chapter, we shall look at a particular class of intercept and resend attacks. This class involves Eve measuring Alice's two-qubit states using the plus or minus measurement box with equal probability. Eve then forwards a plus or minus state with certain probabilities depending on the outcomes of her measurements.

In general, Eve could use a different set of POVM to measure Alice's two-qubit state. But in this chapter, we let her measure only the plus or minus POVM. If Eve measures this on all of Alice's two-qubit states, she will be able to gain full information on Alice's message after Alice announces her numeral type.

Section 4.1 gives some intuition on how the presence of an eavesdropper in the channel can be noticed. In section 4.2, we present a simple eavesdropping strategy for Eve that happens to be biased. Finally, section 4.3 introduces the concept of unbiased noise and gives an example of an unbiased eavesdropping strategy.

State Alice sends	Outcome of Bob's measurement							
	$\langle 1+\|$	$\langle 2+\|$	$\langle 3+\|$	$\langle 4+\|$	$\langle 1-\|$	$\langle 2-\|$	$\langle 3-\|$	$\langle 4-\|$
$\|1+\rangle$	$\frac{1}{16}$	0	0	0	0	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$
$\|2+\rangle$	0	$\frac{1}{16}$	0	0	$\frac{1}{48}$	0	$\frac{1}{48}$	$\frac{1}{48}$
$\|3+\rangle$	0	0	$\frac{1}{16}$	0	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{48}$
$\|4+\rangle$	0	0	0	$\frac{1}{16}$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	0
$\|1-\rangle$	0	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{16}$	0	0	0
$\|2-\rangle$	$\frac{1}{48}$	0	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{16}$	0	0
$\|3-\rangle$	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{48}$	0	0	$\frac{1}{16}$	0
$\|4-\rangle$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	0	0	0	0	$\frac{1}{16}$

Table 4.1: Joint probability table for the raw data between Alice and Bob for the direct communication protocol in a noiseless channel.

4.1 Introduction

The security of the protocol hinges on the fact that if an eavesdropper tries to learn about the message that Alice sends, she will leave behind some traces that Alice and Bob can detect.

Alice puts some control bits in her message string. These bits are randomly chosen and randomly interspersed between the message. They will be used to check the integrity of the channel. Alice will announce the positions of the control bits. For each control bit, Bob then tells Alice the measurement box he used as well as its outcome. If the channel is perfectly noiseless, then Alice and Bob would expect to get a joint probability that looks like table 4.1. If Alice and Bob obtains anything different, that would indicate the possible presence of an eavesdropper in the channel.

4.2 A simple but biased intercept and resend attack

Let us look at a particular strategy for the eavesdropper Eve. Suppose she does an intercept and resend attack. Eve intercepts all the incoming qubits and measures each of them using her own plus or minus box. She then forwards the resulting states to Bob. If Eve was lucky and her chosen basis happens to match the parity type that Alice encoded, then Eve would not be detected. However if Eve were to measure in the opposite basis, then Bob might get a measurement outcome that he should otherwise never get.

For example if Alice sends the state $|1+\rangle$ as a control bit. When Eve measures the qubit pair using the plus basis (she does this half of the time) she will get the outcome $|1+\rangle$. She forwards this to Bob and in this case Alice and Bob do not suspect that anything is amiss. However when Eve measures using the minus basis (which she does with probability half), she gets one of the three possible outcomes: $\{|2-\rangle, |3-\rangle, |4-\rangle\}$, each with equal probability. When she forwards any of this state to Bob, there is a chance that if Bob were to measure using the plus basis, his 2, 3 or 4 outcomes would trigger. These outcomes are impossible in the secure channel. Hence Alice and Bob suspect that their channel has been compromised.

The probability matters are summarised in the following table. It gives the probabilities of Bob's outcomes for each of Eve's possible outcomes.

State Eve forwards	Outcome of Bob's measurement								Eve's M.P.
	$\langle 1+\|$	$\langle 2+\|$	$\langle 3+\|$	$\langle 4+\|$	$\langle 1-\|$	$\langle 2-\|$	$\langle 3-\|$	$\langle 4-\|$	
$\|1+\rangle$	$\frac{1}{4}$	0	0	0	0	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{2}$
$\|2-\rangle$	$\frac{1}{36}$	0	$\frac{1}{36}$	$\frac{1}{36}$	0	$\frac{1}{12}$	0	0	$\frac{1}{6}$
$\|3-\rangle$	$\frac{1}{36}$	$\frac{1}{36}$	0	$\frac{1}{36}$	0	0	$\frac{1}{12}$	0	$\frac{1}{6}$
$\|4-\rangle$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	0	0	0	0	$\frac{1}{12}$	$\frac{1}{6}$
Bob's M.P.	$\frac{1}{3}$	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{18}$	0	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	1
Bob's E.P.	$\frac{1}{2}$	0	0	0	0	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	1

The abbreviations M.P. and E.P. stand for *marginal probabilities* and *expected probabilities*. We see that Bob gets the states $|2+\rangle$, $|3+\rangle$ and $|4+\rangle$ each with a probability of $1/18$. In the secure channel, these states are never expected.

Repeating this for all the other states that Alice sends, we get the joint probability table between Alice and Bob as given by the following table.

State Alice sends	Outcome of Bob's measurement							
	$\langle 1+\|$	$\langle 2+\|$	$\langle 3+\|$	$\langle 4+\|$	$\langle 1-\|$	$\langle 2-\|$	$\langle 3-\|$	$\langle 4-\|$
$\|1+\rangle$	$\frac{1}{24}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{144}$	0	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$
$\|2+\rangle$	$\frac{1}{144}$	$\frac{1}{24}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{48}$	0	$\frac{1}{48}$	$\frac{1}{48}$
$\|3+\rangle$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{24}$	$\frac{1}{144}$	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{48}$
$\|4+\rangle$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{24}$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	0
$\|1-\rangle$	0	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{144}$
$\|2-\rangle$	$\frac{1}{48}$	0	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{144}$	$\frac{1}{24}$	$\frac{1}{144}$	$\frac{1}{144}$
$\|3-\rangle$	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{48}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{24}$	$\frac{1}{144}$
$\|4-\rangle$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{24}$

This joint probability table is biased in the sense that the mismatched basis results are free of noise but the matching basis results suffer from noise.

Eve will get be able to decode with full certainty Alice's bits once Alice announces her numeral type. Summing up the entries of the joint probability table,

Alice and Bob ends up with the following binary symmetric channel for every numeral type.

Alice's bit	Bob's bit	
	$+$	$-$
$+$	$\frac{5}{12}$	$\frac{1}{12}$
$-$	$\frac{1}{12}$	$\frac{5}{12}$

The error rate corresponding to this attack is $Q = 1/6$.

We do not allow Eve to do any attacks that result in biased joint probability outcomes. The next section will define more precisely what we mean by unbiased attacks which result in unbiased noise as seen by Alice and Bob.

4.3 Unbiased noise

In an ideal world, Alice and Bob would have a perfect noiseless channel. They would abort the protocol whenever they find that their channel is contaminated. However living in a universe that is not so ideal, Alice and Bob compromise by allowing some noise in the channel. Still they insist that the noise is *unbiased*. By this, we mean that all the entries of Alice and Bob's joint probability table are modified in the same way. The new noisy probabilities are related to the noiseless probabilities by

$$p_{\text{new}} = (1-\varepsilon)p_{\text{old}} + \varepsilon\frac{1}{64}\,, \tag{4.1}$$

where $0 \leq \varepsilon \leq 1$ quantifies the amount of noise in the channel. With this unbiased noise the new joint probability table between Alice and Bob is given by table 4.2.

State Alice sends	Outcome of Bob's measurement							
	$\langle 1+\|$	$\langle 2+\|$	$\langle 3+\|$	$\langle 4+\|$	$\langle 1-\|$	$\langle 2-\|$	$\langle 3-\|$	$\langle 4-\|$
$\|1+\rangle$	$\frac{4-3\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$
$\|2+\rangle$	$\frac{\varepsilon}{64}$	$\frac{4-3\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$
$\|3+\rangle$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-3\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$
$\|4+\rangle$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-3\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$
$\|1-\rangle$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{4-3\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$
$\|2-\rangle$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{4-3\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$
$\|3-\rangle$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-3\varepsilon}{64}$	$\frac{\varepsilon}{64}$
$\|4-\rangle$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{4-\varepsilon}{192}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{\varepsilon}{64}$	$\frac{4-3\varepsilon}{64}$

Table 4.2: Joint probability table for the raw data between Alice and Bob for the direct communication protocol in a channel with unbiased noise ε.

The intercept and resend attack strategy in section 4.2 clearly does not mimic an unbiased noise channel. In fact for that attack, the joint probability table between Alice and Bob shows no noise in the event where Alice's state parity does not match Bob's measurement parity. However when their parities match, they see a noise value corresponding to $\varepsilon = 4/9$.

After Alice and Bob find out their actual joint probability table for the strategy in section 4.2, they can make their joint probability table unbiased by adding some controlled noise on their raw keys. This will reduce their correlations, but it will allow Alice and Bob to obtain an upper bound on Eve's information based only on unbiased attacks. For this particular attack, the strategy involves Bob randomly flipping $1/4$ of his outcomes to the opposite parity type.

When Bob does this, the new unbiased probabilities $\tilde{p}$ are related to the old biased probabilities p by

$$\tilde{p}(a\pm, b\pm) = \frac{3}{4}p(a\pm, b\pm) + \frac{1}{4}p(a\pm, b\mp)\,, \tag{4.2}$$

$$\tilde{p}(a\pm, b\mp) = \frac{3}{4}p(a\pm, b\mp) + \frac{1}{4}p(a\pm, b\pm)\,. \tag{4.3}$$

We work out four of the probabilities below

$$\tilde{p}(1+, 1+) = \frac{3}{4} \times \frac{1}{24} + \frac{1}{4} \times 0 = \frac{1}{32}\,, \tag{4.4}$$

$$\tilde{p}(1+, 2+) = \frac{3}{4} \times \frac{1}{144} + \frac{1}{4} \times \frac{1}{48} = \frac{1}{96}\,, \tag{4.5}$$

$$\tilde{p}(1+, 1-) = \frac{3}{4} \times 0 + \frac{1}{4} \times \frac{1}{24} = \frac{1}{96}\,, \tag{4.6}$$

$$\tilde{p}(1+, 2-) = \frac{3}{4} \times \frac{1}{48} + \frac{1}{4} \times \frac{1}{144} = \frac{5}{288}\,. \tag{4.7}$$

Comparing with the unbiased probability table 4.2, we can check that this corresponds to a noise level of $\varepsilon = 2/3$.

This flipping of parity does not change Eve's input states when she attacks Alice. It also does not reveal any additional information to Eve. If Alice and Bob introduce controlled noise to remove any bias in their joint probabilities, then Eve will not have any advantage in doing a biased attack. She loses the opportunity to add her own noise into the channel by doing a biased attack. Hence for the same unbiased error rate, there is an unbiased strategy that is at least as good as a biased strategy. In the next section, we shall give an unbiased intercept and resend attack that has a noise level of $\varepsilon = 2/3$.

4.3.1 Unbiased attack with noise level of $\varepsilon = 2/3$

To mimic an unbiased noise, let us consider a different intercept and resend strategy for Eve. She needs to introduce some artificial noise such that Alice and Bob see something unbiased.

Consider this strategy for Eve. Once again Eve measures the incoming two-qubit state using either the plus or minus box. But she sends whatever state she measures with a probability of only $3/4$. She sends the states with the opposite parity with probability $1/4$. We shall see that this attack results in unbiased noise between Alice and Bob.

For example, say Alice sends the state $|1+\rangle$. Again, Eve will get the state $|1+\rangle$ with probability $1/2$ or the states $\{|2-\rangle, |3-\rangle, |4-\rangle\}$, each with probability $1/6$. When Eve gets the state $|1+\rangle$, she will send out $|1+\rangle$ with probability $3/4$ and the opposite parity state $|1-\rangle$ with probability $1/4$. She does the same if she gets the minus states.

The following table summarises the total probabilities for Eve to send out each state when Alice sends the state $|1+\rangle$.

Eve's outcome	Eve's forwarded state								Eve's M.P.
	$\|1+\rangle$	$\|2+\rangle$	$\|3+\rangle$	$\|4+\rangle$	$\|1-\rangle$	$\|2-\rangle$	$\|3-\rangle$	$\|4-\rangle$	
$\|1+\rangle$	$\frac{3}{8}$	0	0	0	$\frac{1}{8}$	0	0	0	$\frac{1}{2}$
$\|2-\rangle$	0	$\frac{1}{24}$	0	0	0	$\frac{1}{8}$	0	0	$\frac{1}{6}$
$\|3-\rangle$	0	0	$\frac{1}{24}$	0	0	0	$\frac{1}{8}$	0	$\frac{1}{6}$
$\|4-\rangle$	0	0	0	$\frac{1}{24}$	0	0	0	$\frac{1}{8}$	$\frac{1}{6}$
Total M.P.	$\frac{3}{8}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	1

The last entry of the table gives the state that Bob will receive from Eve, given that Alice sends the state $|1+\rangle$. When Bob performs his measurements, he will get the outcomes as given in the next table.

State Eve	Outcome of Bob's measurement								Eve's
forwards	$\langle 1+\|$	$\langle 2+\|$	$\langle 3+\|$	$\langle 4+\|$	$\langle 1-\|$	$\langle 2-\|$	$\langle 3-\|$	$\langle 4-\|$	M.P.
$\|1+\rangle$	$\frac{3}{16}$	0	0	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{3}{8}$
$\|2+\rangle$	0	$\frac{1}{48}$	0	0	$\frac{1}{144}$	0	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{24}$
$\|3+\rangle$	0	0	$\frac{1}{48}$	0	$\frac{1}{144}$	$\frac{1}{144}$	0	$\frac{1}{144}$	$\frac{1}{24}$
$\|4+\rangle$	0	0	0	$\frac{1}{48}$	$\frac{1}{144}$	$\frac{1}{144}$	$\frac{1}{144}$	0	$\frac{1}{24}$
$\|1-\rangle$	0	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{16}$	0	0	0	$\frac{1}{8}$
$\|2-\rangle$	$\frac{1}{48}$	0	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{16}$	0	0	$\frac{1}{8}$
$\|3-\rangle$	$\frac{1}{48}$	$\frac{1}{48}$	0	$\frac{1}{48}$	0	0	$\frac{1}{16}$	0	$\frac{1}{8}$
$\|4-\rangle$	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{48}$	0	0	0	0	$\frac{1}{16}$	$\frac{1}{8}$
Bob's M.P.	$\frac{1}{4}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{5}{36}$	$\frac{5}{36}$	$\frac{5}{36}$	1

The last entry in the table gives the actual outcomes of Bob's detectors when Alice sends the state $|1+\rangle$. Comparing with Alice and Bob's joint probability table with unbiased noise when Alice sends $|1+\rangle$, Alice and Bob would not be able to differentiate between Eve's presence and a channel with unbiased noise at $\varepsilon = 2/3$.

Of course, Bob will get similar unbiased marginal probabilities when Alice sends other states as well.

We note that since the channel between Alice and Eve was perfect, by doing this intercept and resend attack, Eve knows everything about the bits that Alice sends. So we can conclude that when Alice and Bob see an unbiased noise level of $\varepsilon = 2/3$, Eve already has full information about Alice's bits.

4.3.2 A slightly more general unbiased attack with noise level of $\varepsilon \geq 2/3$

In fact the intercept and resend strategy that we just presented is just one of many intercept and resend strategies that Eve can use but that still mimics an unbiased noise. Here we present a slightly more general strategy.

The strategy is as follows. When Eve measures the outcome 1 in the plus box, she forwards to Bob the states in the following table with the shown probabilities.

State Eve forwards	Probability
$\|1+\rangle$	p_0
$\|2+\rangle$	p_1
$\|3+\rangle$	p_1
$\|4+\rangle$	p_1
$\|1-\rangle$	p_2
$\|2-\rangle$	p_3
$\|3-\rangle$	p_3
$\|4-\rangle$	p_3

Putting this into words, she forwards the state she receives with probability p_0, the states having a different numeral but the same parity with probability p_1, the state with the same numeral but a different parity with probability p_2 and the states having a different numeral and a different parity with probability p_3.

Using this strategy, given that Alice sends the state $|1+\rangle$, the probabilities of Bob obtaining a particular outcome after summing over all of Eve's possible outcomes are given in the following table.

Bob's outcome	Probability
$\langle 1+\vert$	$\frac{1}{6}(2p_0+p_1+3p_3)$
$\langle 2+\vert$	$\frac{1}{18}(p_0+8p_1+3p_2+6p_3)$
$\langle 3+\vert$	$\frac{1}{18}(p_0+8p_1+3p_2+6p_3)$
$\langle 4+\vert$	$\frac{1}{18}(p_0+8p_1+3p_2+6p_3)$
$\langle 1-\vert$	$\frac{1}{6}(3p_1+p_2+p_3)$
$\langle 2-\vert$	$\frac{1}{18}(3p_0+6p_1+p_2+8p_3)$
$\langle 3-\vert$	$\frac{1}{18}(3p_0+6p_1+p_2+8p_3)$
$\langle 4-\vert$	$\frac{1}{18}(3p_0+6p_1+p_2+8p_3)$

For the noise to be consistent with the unbiased noise, Eve needs to choose her probabilities p_0, p_1, p_2 and p_3 such that Bob's outcomes match the entries of the unbiased joint probability table 4.2. This gives four equations for the four probabilities:

$$\frac{1}{6}(2p_0+p_1+3p_3) = \frac{4-3\varepsilon}{8}\,, \tag{4.8}$$

$$\frac{1}{18}(p_0+8p_1+3p_2+6p_3) = \frac{\varepsilon}{8}\,, \tag{4.9}$$

$$\frac{1}{6}(3p_1+p_2+p_3) = \frac{\varepsilon}{8}\,, \tag{4.10}$$

$$\frac{1}{18}(3p_0+6p_1+p_2+8p_3) = \frac{4-\varepsilon}{24}\,. \tag{4.11}$$

These four equations are not all independent. They can be reduced to the following three equations

$$\begin{aligned} p_0+p_3 &= \frac{7-6\varepsilon}{4}\,,\\ p_1+p_3 &= \frac{3\varepsilon-2}{4}\,,\\ p_2-p_3 &= \frac{3-3\varepsilon}{4}\,, \end{aligned} \tag{4.12}$$

where we have one free parameter remaining. The least value of ε consistent with this unbiased intercept resend strategy can be obtained from the second equation. Because probabilities have to be positive,

$$p_1 + p_3 = \frac{3\varepsilon - 2}{4} \geq 0 \tag{4.13}$$

$$\implies \varepsilon \geq \frac{2}{3}. \tag{4.14}$$

The unique choice of $p_0 = 3/4$, $p_1 = 0$, $p_2 = 1/4$ and $p_3 = 0$ corresponds to our earlier unbiased intercept resend strategy for $\varepsilon = 2/3$. For $\varepsilon > 2/3$, there is more than one eavesdropping strategy for Eve in this class.

4.4 Alice and Bob's mutual information for unbiased noise

For an unbiased attack, we can find the mutual information between Alice and Bob in terms of the noise parameter. Summing up the entries in table 4.2, the channel between Alice and Bob is the following binary symmetric channel.

Alice's bit	Bob's bit	
	$+$	$-$
$+$	$\frac{2-\varepsilon}{4}$	$\frac{\varepsilon}{4}$
$-$	$\frac{\varepsilon}{4}$	$\frac{2-\varepsilon}{4}$

For this channel, the mutual information between Alice and Bob will be

$$I_{AB} = \frac{2-\varepsilon}{2}\log(2-\varepsilon) + \frac{\varepsilon}{2}\log\varepsilon\,. \tag{4.15}$$

We note that for the unbiased channel, the error rate Q equals to $\varepsilon/2$.

Chapter 5

Noise 2: General eavesdropping strategies

The intercept and resend strategy that we presented in the last chapter is just one class of attacks that Eve can perform. The more general thing for her to do would be to entangle some ancilla states to Alice's qubit pairs via a unitary evolution. Eve keeps her ancillas and sends Alice's sub-system to Bob. To extract the most information out of her ancillas, Eve will only measure her ancillas once Alice and Bob have finished the whole protocol and used the resulting keys.

Eve's entangling scheme is constrained by the probabilities that Alice and Bob check in table 4.1. The security analysis boils down to finding the best entangling scheme for Eve (subject to the probability constraints) for a given noise level ε.

In this chapter, we shall recast the problem in a different setting. We look at an equivalent protocol so that the security analysis becomes slightly neater. Instead of Alice sending qubit pairs to Bob, we will consider the modified protocol where Eve sends Alice a qubit pair and she sends Bob another qubit pair. Where Alice

prepares a state to send to Bob in the original protocol, in this setting Alice will do a measurement on the state that Eve sends. Her measurement will collapse Bob's state to the state that Alice intends Bob to receive.

Section 5.1 presents the protocol in its original setting where Alice sends a pure state to Bob through a noisy channel. Section 5.2 looks at the equivalent protocol where Eve controls the source. Finally, section 5.3 introduces the eavesdropper and the records that she has access to when Alice and Bob see noise in their channel.

5.1 Alice–Bob channel

In the original protocol, there is a quantum channel between Alice and Bob. When Alice sends a pure state to Bob, by the time the state gets to Bob, this channel would have turned it to something else (unless the channel is perfectly isolated).

There are several equivalent ways to parametrise the channel. We can regard a channel $\mathcal{E}$ as a unitary transformation U_{BE} being done on the input state ρ_A and an ancillary state $|0\rangle_E$. The output state ρ_B is obtained by tracing out the ancillary subsystem at the end of the unitary evolution

$$\rho_A \rightarrow \rho_B = \mathcal{E}(\rho_A) = \mathrm{Tr}_E \left\{ U_{BE} \left(\rho_A \otimes |0\rangle_E \langle 0|_E \right) U_{BE}^{\dagger} \right\} \tag{5.1}$$

where $\mathcal{E}(\rho)$ denotes the action of the channel on a state ρ. The maximum dimension of the ancillary state $|0\rangle$ needed to specify an arbitrary channel is d^2, where d is the dimension of Hilbert space of the input states (see for example [39]).

The channel can also be described by a pure state in d^4 dimensions between Alice–Bob and Eve. When Alice obtains a POVM outcome corresponding to an arbitrary state ρ_A that she sends, the resulting state at Bob's end would be the outcome of the channel $\rho_B = S(\rho_A)$. In appendix A, we provide an explicit construction for the pure state between Alice–Bob and Eve for an arbitrary channel between Alice and Bob.

5.2 Alice measures protocol

We now introduce the equivalent protocol where Alice and Bob share an entangled state emitting from a source. Alice will measure her state using a POVM and the state Bob receives at this end will depend on the outcome of Alice's measurement.

In this scheme, we consider a source which emits two qubit-pairs, the first pair to Alice and the second to Bob. The qubit pair is in the state

$$|\Psi\rangle_{AB} = (|1+,1+\rangle + |2+,2+\rangle + |3+,3+\rangle + |4+,4+\rangle)\,\frac{1}{2} \tag{5.2}$$

where the notation $|a,b\rangle$ means $|a\rangle\,|b\rangle$. The state $|a\rangle$ goes to Alice and the state $|b\rangle$ goes to Bob. We choose this state as the source because we must have the statistical operator for Bob to be the completely mixed state. Using relation (3.1)

$$|n+\rangle = U\,|n-\rangle = \sum_{m=1}^{4} |m-\rangle\, u_{m,n}\,, \tag{5.3}$$

where

$$u_{m,n} = \langle m- | U | n- \rangle = \langle m- | n+ \rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & -1 & -1 & -1 \\ 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \end{pmatrix}_{m,n} , \quad (5.4)$$

we can write the source state $|\Psi\rangle_{AB}$ in terms of the minus states. The source state becomes

$$|\Psi\rangle_{AB} = \frac{1}{2} \sum_{n=1}^{4} |n+, n+\rangle \quad (5.5)$$

$$= \frac{1}{2} \sum_{n=1}^{4} \sum_{m=1}^{4} \sum_{m'=1}^{4} u_{m,n} u_{m',n} |m-, m'-\rangle \quad (5.6)$$

$$= \frac{1}{2} \sum_{n=1}^{4} \sum_{m=1}^{4} \sum_{m'=1}^{4} u^*_{m,n} u_{m',n} |m-, m'-\rangle \quad (5.7)$$

$$= \frac{1}{2} \sum_{m=1}^{4} \sum_{m'=1}^{4} \delta_{m',m} |m-, m'-\rangle \quad (5.8)$$

$$= \frac{1}{2} \sum_{m=1}^{4} |m-, m-\rangle \ . \quad (5.9)$$

The third equality follows because $u_{m,n}$ is real.

In this setting, Alice also has two measuring apparatus, the plus box and the minus box. To prepare a plus state, Alice puts the qubit-pair she receives into her plus box. If she gets the n-th outcome she would collapse Bob's qubit pair to the $|n+\rangle$ state. In the original protocol, Alice randomly chooses a numeral type, but now this random selection is made by her measuring box. To prepare a minus

state, Alice would measure her qubit pair using the minus box. From this point onwards, the protocol remains the same as the original one.

5.3 When there is noise

If Alice and Bob get the source state in the state $|\Psi\rangle_{AB}$, then they will obtain a joint probability table like table 4.1. We shall see in section 8.1 that with this pure state, Alice and Bob can be certain that their communication is completely private. An eavesdropper would not be able to gain any information about their communication. That is if Alice and Bob see a probability table like table 4.1, they can be sure that the source state was the pure state $|\Psi\rangle_{AB}$.

But when noise is present, the probability table that Alice and Bob get will no longer be the perfect table. Alice and Bob insist on the noise being unbiased and not too large. They only continue with the protocol if they have a joint probability table like table 4.2 and the noise level ε is less than a certain threshold ε_0. Otherwise they conclude that someone is eavesdropping and abort the protocol, they refuse to communicate. This threshold will be the maximum amount of noise that Alice and Bob can protect themselves against (by using error correcting codes and privacy amplification techniques) and yet still maintain a completely private communication.

On insisting for an unbiased noise, Alice and Bob hope to get a source state

$$\rho_{AB}^{(h)} = (1-\varepsilon)\,|\Psi\rangle_{AB}\langle\Psi|_{AB} + \varepsilon\frac{1}{16}\,, \tag{5.10}$$

a mixture of the perfect source state with an unbiased noise state. But with only the joint probability table accessible to them, they cannot be sure. For any non zero amount of noise, there will be many different states that will give rise to the same joint probability table for Alice and Bob. Thus Alice and Bob must be content with the following 64 restrictions on the source state they actually get:

$$\mathrm{Tr}\left\{\rho_{AB}\left|a+,b+\right\rangle\left\langle a+,b+\right|\right\} = \frac{1-\varepsilon}{4}\delta_{a,b} + \frac{\varepsilon}{16}\,, \tag{5.11}$$

$$\mathrm{Tr}\left\{\rho_{AB}\left|a-,b-\right\rangle\left\langle a-,b-\right|\right\} = \frac{1-\varepsilon}{4}\delta_{a,b} + \frac{\varepsilon}{16}\,, \tag{5.12}$$

$$\mathrm{Tr}\left\{\rho_{AB}\left|a+,b-\right\rangle\left\langle a+,b-\right|\right\} = \frac{1-\varepsilon}{12}(1-\delta_{a,b}) + \frac{\varepsilon}{16}\,, \tag{5.13}$$

$$\mathrm{Tr}\left\{\rho_{AB}\left|a-,b+\right\rangle\left\langle a-,b+\right|\right\} = \frac{1-\varepsilon}{12}(1-\delta_{a,b}) + \frac{\varepsilon}{16} \tag{5.14}$$

for $\{a,b\} \in \{1,2,3,4\}$, where ρ_{AB} is the state from the source.

5.3.1 The eavesdropper

When Alice and Bob see noise in their communication, they attribute that noise to a malicious eavesdropper Eve that controls their source. They want to know how much information Eve can learn so that they can protect the communication by building in redundancies in the message. If Alice and Bob receive the state ρ_{AB} from the source we can always assume that this (possibly mixed) state is part of a higher dimensional pure state $|\Psi\rangle_{ABE}$, where tracing over Eve's subsystem gives Alice and Bob's state ρ_{AB},

$$\rho_{AB} = \mathrm{Tr}_E\left\{\left|\Psi\right\rangle_{ABE}\left\langle\Psi\right|_{ABE}\right\}\,. \tag{5.15}$$

In this language, for every state that the source provides Alice and Bob, Eve has a record in the from of

$$\rho_E = \mathrm{Tr}_{AB}\left\{|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} . \tag{5.16}$$

Eve will keep all her records, until Alice and Bob have performed all their measurements and Alice has revealed her numeral types. At this point the communication is over and Bob knows the message that Alice wanted to communicate to him. Now Eve is ready to extract some information about the message by performing a collective measurement on all her records.

Suppose Alice announces that her measurement outcome was a type 1. Eve's input state would depend on whether it was a type $1+$ or $1-$. If Alice's outcome was $1+$, Eve's record state becomes $\rho^E_{A=1+}$ and if Alice's outcome was $1-$, Eve's record collapses to $\rho^E_{A=1-}$, where

$$\rho^E_{A=1+} = 4\,\mathrm{Tr}_{AB}\left\{(|1+\rangle\langle 1+|\otimes 1_B)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} , \tag{5.17}$$

$$\rho^E_{A=1-} = 4\,\mathrm{Tr}_{AB}\left\{(|1-\rangle\langle 1-|\otimes 1_B)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} . \tag{5.18}$$

The two states are normalised so that the trace of both $\rho^E_{A=1+}$ and $\rho^E_{A=1-}$ are equal to one. On average, the message Alice sends has the same number of plus and minus bits. The probability of Eve to get either state is $1/2$.

The maximum amount of information that Eve can learn from the type 1 states is given by the Holevo quantity of her records

$$I^E_{A=1} = \chi\left(\frac{1}{2}\rho^E_{A=1+}, \frac{1}{2}\rho^E_{A=1-}\right) \tag{5.19}$$

$$= S\left(\frac{1}{2}\rho^E_{A=1+} + \frac{1}{2}\rho^E_{A=1-}\right) - \frac{1}{2}S\left(\rho^E_{A=1+}\right) - \frac{1}{2}S\left(\rho^E_{A=1-}\right) \ . \tag{5.20}$$

The total information Eve learns about the message is then the average of the information that she learns from each numeral type

$$I^E_A = \frac{1}{4}\left(I^E_{A=1} + I^E_{A=2} + I^E_{A=3} + I^E_{A=4}\right) \ . \tag{5.21}$$

Eve could also choose to learn about Bob's measurement outcomes instead of Alice's. In this case, she will get an analogous quantity I^E_B. Our task is to find out what is the maximum value that the quantity I^E_A (or I^E_B) can attain for a given noise ε. We want to maximise I^E_A (or I^E_B) over all possible purifications $|\Psi\rangle_{ABE}$ subject to the 64 conditions (5.11)–(5.14).

5.3.2 Eve's purification

To perform the maximisation of Eve's information, we write the pure joint Alice–Bob–Eve state as

$$|\Psi\rangle_{ABE} = \sum_{a=1}^{4}\sum_{b=1}^{4} |e_a\rangle\,|e_b\rangle\,\left|E_{a,b}\right\rangle \ , \tag{5.22}$$

where $|e_a\rangle$ and $|e_b\rangle$ are some arbitrary orthonormal basis for Alice and Bob. The 16 kets $|E_{ab}\rangle$ are Eve's records which is the purification of Alice and Bob's state.

The choice of this purification determines the information Eve will get. The remaining task would be to find the optimal purification that would give Eve the maximum information.

In writing the purified state $|\Psi\rangle_{ABE}$, the choice of basis for Alice and Bob is irrelevant to Eve. Suppose we write instead

$$|\Psi\rangle_{ABE} = \sum_{n=1}^{4}\sum_{m=1}^{4} |\phi_{n,m}\rangle\,|F_{n,m}\rangle \ , \tag{5.23}$$

where $|\phi_{n,m}\rangle$ is some (possibly entangled) orthonormal basis for Alice and Bob. In terms of Alice and Bob's old basis, the state $|\Psi\rangle_{ABE}$ is

$$|\Psi\rangle_{ABE} = \sum_{a,b=1}^{4}\sum_{n,m=1}^{4} |e_a,e_b\rangle\,\langle e_a,e_b|\phi_{n,m}\rangle\,|F_{n,m}\rangle \tag{5.24}$$

$$= \sum_{a,b=1}^{4} |e_a,e_b\rangle \left(\sum_{n,m=1}^{4} \langle e_a,e_b|\phi_{n,m}\rangle\,|F_{n,m}\rangle\right) \tag{5.25}$$

Comparing this with equation (5.22) we see that the $|F_{ab}\rangle$ kets are related to the $|E_{ab}\rangle$ kets by the unitary transformation

$$|E_{ab}\rangle = \sum_{n=1}^{4}\sum_{m=1}^{4} |F_{nm}\rangle\,\langle e_a,e_b|\phi_{n,m}\rangle \ . \tag{5.26}$$

5.3.3 Eve's input states

From equations (5.17) and (5.18), we can write Eve's reduced states when Alice announces that she obtained an outcome of type 1. For the $1+$ outcome, we have

$$\rho^E_{A=1+} = 4\,\mathrm{Tr}_{AB}\left\{\left(|1+\rangle\langle 1+|\otimes 1_B\right)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} \tag{5.27}$$

$$= 4\sum_{a,b=1}^{4}\sum_{a',b'=1}^{4}\mathrm{Tr}_{AB}\left\{\left(|1+\rangle\langle 1+|\otimes 1_B\right)\left|e_a,e_b,E_{a,b}\right\rangle\left\langle e'_a,e'_b,E_{a',b'}\right|\right\} \tag{5.28}$$

$$= 4\sum_{b=1}^{4}\left(\sum_{a=1}^{4}\left|E_{a,b}\right\rangle\left\langle 1+\left|e_a\right\rangle\right.\right)\left(\sum_{a=1}^{4}\left\langle e_a\right|1+\rangle\left\langle E_{a,b}\right|\right) \tag{5.29}$$

while for the $1-$ outcome, we have

$$\rho^E_{A=1-} = 4\,\mathrm{Tr}_{AB}\left\{\left(|1-\rangle\langle 1-|\otimes 1_B\right)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} \tag{5.30}$$

$$= 4\sum_{a,b=1}^{4}\sum_{a',b'=1}^{4}\mathrm{Tr}_{AB}\left\{\left(|1-\rangle\langle 1-|\otimes 1_B\right)\left|e_a,e_b,E_{a,b}\right\rangle\left\langle e'_a,e'_b,E_{a',b'}\right|\right\} \tag{5.31}$$

$$= 4\sum_{b=1}^{4}\left(\sum_{a=1}^{4}\left|E_{a,b}\right\rangle\left\langle 1-\left|e_a\right\rangle\right.\right)\left(\sum_{a=1}^{4}\left\langle e_a\right|1-\rangle\left\langle E_{a,b}\right|\right)\ . \tag{5.32}$$

Each state is written as the sum of four projectors and would have a maximum of rank four. The total state $\rho^E_{A=1} = \frac{1}{2}\rho^E_{A=1+} + \frac{1}{2}\rho^E_{A=1-}$ can at most have rank eight.

We can also find Eve's reduced states conditioned on the outcome of Bob's measurement. For completeness, we shall write down those states here. For exam-

ple, if Bob's outcome happens to be of type $2+$, then Eve's record state becomes

$$\rho^E_{B=2+} = 4\,\mathrm{Tr}_{AB}\left\{\left(1_A \otimes |2+\rangle\langle 2+|\right)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} \tag{5.33}$$

$$= 4\sum_{a=1}^{4}\left(\sum_{b=1}^{4}|E_{a,b}\rangle\langle 2+|e_b\rangle\right)\left(\sum_{b=1}^{4}\langle e_b|2+\rangle\langle E_{a,b}|\right). \tag{5.34}$$

If Bob announces the numeral type of her outcome, then Eve would try and distinguish if her record state is in the state $\rho^E_{B=2+}$ or $\rho^E_{B=2-}$. But since Bob does not reveal his numeral type, for Eve to guess Bob's parity, she has to distinguish whether her record is in the state

$$\begin{aligned}\rho^E_{A=1,B=+} =& \frac{1}{8}\left(\frac{4-3\varepsilon}{64}\rho^E_{\substack{A=1+\\B=1+}} + \frac{4-\varepsilon}{192}\left(\rho^E_{\substack{A=1+\\B=2-}} + \rho^E_{\substack{A=1+\\B=3-}} + \rho^E_{\substack{A=1+\\B=4-}}\right)\right)\\ &+ \frac{1}{8}\left(\frac{\varepsilon}{64}\rho^E_{\substack{A=1-\\B=1+}} + \frac{\varepsilon}{64}\left(\rho^E_{\substack{A=1-\\B=2-}} + \rho^E_{\substack{A=1-\\B=3-}} + \rho^E_{\substack{A=1-\\B=4-}}\right)\right)\end{aligned} \tag{5.35}$$

or

$$\begin{aligned}\rho^E_{A=1,B=-} =& \frac{1}{8}\left(\frac{\varepsilon}{64}\rho^E_{\substack{A=1+\\B=1-}} + \frac{\varepsilon}{64}\left(\rho^E_{\substack{A=1+\\B=2+}} + \rho^E_{\substack{A=1+\\B=3+}} + \rho^E_{\substack{A=1+\\B=4+}}\right)\right)\\ &+ \frac{1}{8}\left(\frac{4-3\varepsilon}{64}\rho^E_{\substack{A=1-\\B=1-}} + \frac{4-\varepsilon}{192}\left(\rho^E_{\substack{A=1-\\B=2+}} + \rho^E_{\substack{A=1-\\B=3+}} + \rho^E_{\substack{A=1-\\B=4+}}\right)\right)\end{aligned} \tag{5.36}$$

where the state for example $\rho^E_{\substack{A=1-\\B=3+}}$ is Eve's reduced state when Alice obtains outcome $1-$ and Bob obtains the outcome $3+$,

$$\rho^E_{\substack{A=1-\\B=3+}} = \frac{\mathrm{Tr}_{AB}\left\{\left(|1-\rangle\langle -1|\otimes|3+\rangle\langle 3+|\right)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\}}{\mathrm{Tr}\left\{\left(|1-\rangle\langle -1|\otimes|3+\rangle\langle 3+|\right)|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\}}. \tag{5.37}$$

However, in this thesis, we shall only be concerned with Eve trying to distinguish Alice's states. Eve's reduced states conditioned on the outcome of Bob's measure-

ment would only be relevant if Alice and Bob were to do a reverse reconciliation which is not what is done.

Chapter 6

The optimisation problem

In this chapter, we formalise the problem of optimising Eve's information in a matrix formulation. There are two sections. In the section 6.1, we write down the constraints on the reduced state between Alice and Bob. In section 6.2, we find how these constraints set a restriction on Eve's reduced state.

6.1 The constraints

We write the Alice–Bob–Eve pure state as

$$|\Psi\rangle_{ABE} = \sum_{I=1}^{16} |AB_I\rangle\,|E_I\rangle \ , \tag{6.1}$$

where the kets $|AB_I\rangle$ are 16 arbitrary (but not necessarily separable) orthonormal basis for Alice and Bob. Eve's records $|E_I\rangle$ are not necessarily normalised or orthogonal.

The 64 constraints are

$$\mathrm{Tr}_{AB}\left\{(P_{a\pm}\otimes Q_{b\pm})\,\rho_{AB}\right\} = p(a\pm,b\pm) \tag{6.2}$$

for all four combinations of pluses and minuses and for $\{a,b\}\in\{1,2,3,4\}$. The state $\rho_{AB}=\mathrm{Tr}_E\left\{|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\}$ is Alice and Bob's reduced state and $P_{a\pm}$ and $Q_{b\pm}$ are the measurement outcomes for Alice and Bob

$$P_{a\pm} = \frac{1}{2}|a\pm\rangle\langle a\pm|\ , \tag{6.3}$$

$$Q_{b\pm} = \frac{1}{2}|b\pm\rangle\langle b\pm| \tag{6.4}$$

with the sums

$$\sum_{a=1}^{4}(P_{a+}+P_{a-}) = 1_A\ , \tag{6.5}$$

$$\sum_{b=1}^{4}(Q_{b+}+Q_{b-}) = 1_B\ . \tag{6.6}$$

The right hand side of equation (6.2) are the probabilities for Alice and Bob to get the outcome $a\pm,b\pm$ as given in table 4.2. The sum of the 16 probabilities in each sector is a quarter

$$\sum_{a,b=1}^{4}p(a+,b+) = \sum_{a,b=1}^{4}p(a+,b-) = \sum_{a,b=1}^{4}p(a-,b+) = \sum_{a,b=1}^{4}p(a-,b-) = \frac{1}{4} \tag{6.7}$$

and the sum of all 64 probabilities adds up to one.

6.2 Eve's records

Eve's statistical operator would be

$$\rho^E = \mathrm{Tr}_{AB}\left\{|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} \tag{6.8}$$

$$= \sum_{I=1}^{16} |E_I\rangle\langle E_I| \ . \tag{6.9}$$

Conditioned on Alice and Bob getting the outcome of $a\pm$ and $b\pm$ Eve's reduced state would be

$$\rho^E_{a\pm,b\pm} = \mathrm{Tr}_{AB}\left\{(P_{a\pm}\otimes Q_{b\pm})|\Psi\rangle_{ABE}\langle\Psi|_{ABE}\right\} \tag{6.10}$$

$$= \sum_{I,I'=1}^{16} |E_I\rangle\langle AB_{I'}|P_{a\pm}\otimes Q_{b\pm}|AB_I\rangle\langle E_{I'}| \tag{6.11}$$

where the trace

$$\mathrm{Tr}\left\{\rho^E_{a\pm,b\pm}\right\} = p(a\pm,b\pm) \tag{6.12}$$

equals to the probability of Eve to get that state. Introducing an orthonormal basis $|F_J\rangle$ for Eve,

$$\langle F_J|\rho^E_{b\pm,a\pm}|F_{J'}\rangle = \sum_{I,I'=1}^{16}\langle F_J|E_I\rangle\langle AB_{I'}|P_{a\pm}\otimes Q_{b\pm}|AB_I\rangle\langle E_{I'}|F_{J'}\rangle \tag{6.13}$$

$$= \sum_{I,I'=1}^{16}\langle F_J|E_I\rangle\langle AB_I|P^\dagger_{a\pm}\otimes Q^\dagger_{b\pm}|AB_{I'}\rangle^*\langle E_{I'}|F_{J'}\rangle \tag{6.14}$$

where since

$$\langle F_J|\rho^E|F_{J'}\rangle = \sum_{I=1}^{16}\langle F_J|E_I\rangle\langle E_I|F_{J'}\rangle \tag{6.15}$$

$$= \sum_{I,K=1}^{16}\langle F_J|E_I\rangle\langle F_I|F_K\rangle\langle E_K|F_{J'}\rangle \tag{6.16}$$

$$= \langle F_J|XX^\dagger|F_{J'}\rangle \tag{6.17}$$

with

$$X = \sum_{I=1}^{16}|E_I\rangle\langle F_I| \tag{6.18}$$

so that finally,

$$\langle F_J|X|F_{J'}\rangle = \sum_{I=1}^{16}\langle F_J|E_I\rangle\langle F_I|F_{J'}\rangle \tag{6.19}$$

$$= \langle F_J|E_{J'}\rangle\,. \tag{6.20}$$

Also

$$\langle F_J|X^\dagger X|F_{J'}\rangle = \sum_{I,I'=1}^{16}\langle F_J|F_I\rangle\langle E_I|E_{I'}\rangle\langle F_{I'}|F_{J'}\rangle \tag{6.21}$$

$$\implies \sum_{k=1}^{16}\langle F_J|X^\dagger|F_k\rangle\langle F_k|X|F_{J'}\rangle = \langle E_J|E_{J'}\rangle\,. \tag{6.22}$$

So if we have all the inner products $\langle E_J|E_{J'}\rangle$, we can take the (arbitrary) square root to get $\langle F_J|X|F_{J'}\rangle = \langle F_J|E_{J'}\rangle$ which gives us a column representation for the vectors $|E_{J'}\rangle$ in the orthonormal $|F_J\rangle$ basis. The choice of the square root X fixes the orthonormal basis $|F_J\rangle$. Putting this back into Eve's record state in equa-

tion (6.14), we get the matrix elements

$$\langle F_J|\,\rho^E_{a\pm,b\pm}\,|F_{J'}\rangle = \sum_{I,I'=1}^{16} \langle F_J|E_I\rangle\,\langle AB_I|\,P^\dagger_{a\pm}\otimes Q^\dagger_{b\pm}\,|AB_{I'}\rangle^*\,\langle E_{I'}|F_{J'}\rangle \tag{6.23}$$

$$= \sum_{I,I'=1}^{16} \langle F_J|\,X\,|F_I\rangle\,\langle AB_I|\,P^\dagger_{a\pm}\otimes Q^\dagger_{b\pm}\,|AB_{I'}\rangle^*\,\langle F_{I'}|\,X^\dagger\,|F_{J'}\rangle\ . \tag{6.24}$$

Eve's measurement strategy depends on the type Alice announces. Eve's two input states when Alice announces a type 1 would be

$$\rho^E_{A=1+} = \sum_{b=1}^{4} \left(\rho^E_{1+,b+} + \rho^E_{1+,b-}\right) \tag{6.25}$$

and

$$\rho^E_{A=1-} = \sum_{b=1}^{4} \left(\rho^E_{1-,b+} + \rho^E_{1-,b-}\right)\ . \tag{6.26}$$

The constraints on Eve's records are

$$p(a\pm,b\pm) = \mathrm{Tr}_{AB}\left\{\left(P_{a\pm}\otimes Q_{b\pm}\right)\rho_{AB}\right\} \tag{6.27}$$

$$= \sum_{I,I'=1}^{16} \langle AB_{I'}|\left(P_{a\pm}\otimes Q_{b\pm}\right)|AB_I\rangle\,\langle E_{I'}|E_I\rangle \tag{6.28}$$

$$= \sum_{I,I',k=1}^{16} \langle F_K|\,X\,|F_I\rangle\,\langle AB_I|\,P^\dagger_{a\pm}\otimes Q^\dagger_{b\pm}\,|AB_{I'}\rangle^*\,\langle F_{I'}|\,X^\dagger\,|F_K\rangle \tag{6.29}$$

Eve's optimisation problem would be to find X (once she has chosen a basis $|F\rangle$) which maximises I^E_A, the information Eve can learn, subject to the constraints above. After choosing some orthonormal basis $|AB_I\rangle$ for Alice–Bob and $|F_I\rangle$ for

Eve, we write Eve's input states as a 16 by 16 matrix

$$\rho^{E}_{a\pm,b\pm} = \mathcal{X}\left(\mathcal{P}^{\mathrm{T}}_{a\pm} \otimes Q^{\mathrm{T}}_{b\pm}\right)\mathcal{X}^{\dagger} \tag{6.30}$$

where $\mathcal{X}$ is the matrix representation of X,

$$\mathcal{X}_{J,J'} = \langle F_J | X | F_{J'} \rangle \tag{6.31}$$

and $\left(\mathcal{P}^{\mathrm{T}}_{a\pm} \otimes Q^{\mathrm{T}}_{b\pm}\right)$ is a 16 by 16 matrix with entries

$$\left(\mathcal{P}^{\mathrm{T}}_{a\pm} \otimes Q^{\mathrm{T}}_{b\pm}\right)_{J,J'} = \langle AB_J | P^{\dagger}_{a\pm} \otimes Q^{\dagger}_{b\pm} | AB_{J'} \rangle^{*} \ . \tag{6.32}$$

The constraints on $\mathcal{X}$ becomes

$$\mathrm{Tr}\left\{\mathcal{X}\left(\mathcal{P}^{\mathrm{T}}_{a\pm} \otimes Q^{\mathrm{T}}_{b\pm}\right)\mathcal{X}^{\dagger}\right\} = p\left(a\pm, b\pm\right) \ . \tag{6.33}$$

The optimisation problem is now to find the 256 matrix entries of $\mathcal{X}$ subject to the 64 constraints in equation (6.33) to maximise Eve's accessible information which is obtained by finding the entropies of states involving the sum of states in equation (6.30).

Chapter 7

Choosing a basis

In this chapter, we will choose a basis for Alice and Bob to write out our equations. Once a basis is chosen, the constraints for Eve can be written out explicitly.

This chapter consists of two sections. In section 7.1, we pick the plus basis as the basis we shall work in for Alice and Bob. In section 7.2, we pick a basis for Eve which corresponds to taking the Hermitian square root of her reduced state $X^\dagger X$ as the choice for X.

7.1 Alice–Bob's basis

While the basis choice does not affect Eve's strategy or the final information Eve can attain, it does however affect the number of pages needed to write down Eve's constraints and input states in full.

Eve's strategy is fully defined by her purification

$$|\Psi\rangle_{ABE} = \sum_{I=1}^{16} |AB_I\rangle\,|E_I\rangle \ . \tag{7.1}$$

Once we specify the Alice–Bob basis $|AB_I\rangle$, Eve's record states $|E_I\rangle$ is also fixed by the purification. We shall choose the plus states as a basis for Alice–Bob,

$$|AB_I\rangle = |a+, b+\rangle \tag{7.2}$$

where $I = 4(a-1)+b$. With this basis choice, the matrix elements

$$(\mathcal{P}_{a\pm} \otimes Q_{b\pm})_{J,J'} = \langle AB_J | P_{a\pm} \otimes Q_{b\pm} | AB_{J'} \rangle \tag{7.3}$$

are real. Also the 64 constraints are

$$p(n\pm, m\pm) = \sum_{a,b,a',b'=1}^{4} \langle a'+, b'+ | P_{n\pm} \otimes Q_{m\pm} | a+, b+ \rangle \langle E_{a',b'} | E_{a,b} \rangle \tag{7.4}$$

$$= \sum_{a,b,a',b'=1}^{4} \langle a'+ | P_{n\pm} | a+ \rangle \langle b'+ | Q_{m\pm} | b+ \rangle \langle E_{a',b'} | E_{a,b} \rangle \tag{7.5}$$

for $n, m \in \{1,2,3,4\}$.

We divide these 64 constraints into three groups. The first group with 16 constraints is when both Alice and Bob measure in the plus basis. We call these the short constraints. The second group is when Alice and Bob measure in a different basis. The 32 constraints in this group are called the medium constraints. The final group is when both Alice and Bob measure in the minus basis. This gives the final 16 constraints which we call the long constraints.

7.1.1 Short constraints

An example of the short constraint would be when Alice gets the outcome $n\pm = 1+$ and Bob obtains $m\pm = 1+$. The probability for this outcome is $p(1+,1+) =$

$(4-3\varepsilon)/64$, and so this constraint reads

$$\langle E_{1,1}|E_{1,1}\rangle = \frac{4-3\varepsilon}{16}\,. \tag{7.6}$$

A second example is when $n\pm = 1+$ and $m\pm = 2+$. The probability for this outcome is $p(1+,2+) = \varepsilon/64$, which gives the constraint

$$\langle E_{1,2}|E_{1,2}\rangle = \frac{\varepsilon}{16}\,. \tag{7.7}$$

The 16 probabilities when Alice and Bob both measure in the plus basis determine the norm of all of Eve's 16 record states

$$\langle E_{a,b}|E_{a,b}\rangle = \frac{4-3\varepsilon}{16} \quad \text{for} \quad a = b\,, \tag{7.8}$$

$$\langle E_{a,b}|E_{a,b}\rangle = \frac{\varepsilon}{16} \quad \text{for} \quad a \neq b\,. \tag{7.9}$$

We call these 16 equations the short constraints. The double indices on $|E_{a,b}\rangle$ correspond to the single index on $|E_I\rangle$ by the relation $I = 4(a-1)+b$.

7.1.2 Medium constraints

As an example of the medium constraint, consider the case when Alice gets the outcome $1+$ and Bob measures in the minus basis and get the outcome $1-$. The constraint that this must happen with probability $p(1+,1-) = \varepsilon/64$ gives the con-

dition

$$\begin{aligned} p(1+,1-) =& \frac{1}{12}\big(\langle E_{1,2}|E_{1,2}\rangle + \langle E_{1,2}|E_{1,3}\rangle + \langle E_{1,2}|E_{1,4}\rangle \\ &+ \langle E_{1,3}|E_{1,2}\rangle + \langle E_{1,3}|E_{1,3}\rangle + \langle E_{1,3}|E_{1,4}\rangle \\ &+ \langle E_{1,4}|E_{1,2}\rangle + \langle E_{1,4}|E_{1,3}\rangle + \langle E_{1,4}|E_{1,4}\rangle\big) \\ =& \frac{\varepsilon}{64}\,. \end{aligned} \tag{7.10}$$

Substituting the norms from the short constraints, we get

$$\begin{aligned} &\langle E_{1,2}|E_{1,3}\rangle + \langle E_{1,2}|E_{1,4}\rangle + \langle E_{1,3}|E_{1,2}\rangle \\ &+ \langle E_{1,3}|E_{1,4}\rangle + \langle E_{1,4}|E_{1,2}\rangle + \langle E_{1,4}|E_{1,3}\rangle = 0\,, \end{aligned} \tag{7.11}$$

which is a constraint on the sum of the real parts

$$\mathrm{Re}\langle E_{1,2}|E_{1,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{1,4}\rangle + \mathrm{Re}\langle E_{1,3}|E_{1,4}\rangle = 0\,. \tag{7.12}$$

A second example is for Alice to get the outcome $1+$ and Bob gets the outcome $2-$. This occurs with probability $p(1+,2-) = (4-\varepsilon)/192$, from which we get the constraint

$$\begin{aligned} p(1+,2-) =& \frac{1}{12}\big(\langle E_{1,1}|E_{1,1}\rangle - \langle E_{1,1}|E_{1,3}\rangle + \langle E_{1,1}|E_{1,4}\rangle \\ &- \langle E_{1,3}|E_{1,1}\rangle + \langle E_{1,3}|E_{1,3}\rangle - \langle E_{1,3}|E_{1,4}\rangle \\ &+ \langle E_{1,4}|E_{1,1}\rangle - \langle E_{1,4}|E_{1,3}\rangle + \langle E_{1,4}|E_{1,4}\rangle\big) \\ =& \frac{4-\varepsilon}{192}\,. \end{aligned} \tag{7.13}$$

Substituting the short constraints, this simplifies to

$$-\mathrm{Re}\langle E_{1,1}|E_{1,3}\rangle + \mathrm{Re}\langle E_{1,1}|E_{1,4}\rangle - \mathrm{Re}\langle E_{1,3}|E_{1,4}\rangle = 0\,. \tag{7.14}$$

In total there are 32 of such constraints on the real parts that we get when Alice and Bob measure in different bases. We call these the *medium constraints*. These constraints are written out in full in appendix B.

7.1.3 Long constraints

The long constraints arise when Alice and Bob both measure in the minus basis. For example, the probability for Alice to get the outcome $1-$ and Bob to get the same outcome $1-$ gives the constraint

$$\sum_{a,b,a',b'=1}^{4} \langle a'+|1-\rangle\langle 1-|a+\rangle\langle b'+|1-\rangle\langle 1-|b+\rangle\langle E_{a',b'}|E_{a,b}\rangle = \frac{4-3\varepsilon}{64}\,. \tag{7.15}$$

This constraint would have 81 different inner products when written in full. However, substituting the results of the short and medium constraints, this simplifies

to

$$\begin{aligned}
&\mathrm{Re}\langle E_{2,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,3}\rangle \\
&+ \mathrm{Re}\langle E_{2,2}|E_{4,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,4}\rangle \\
&+ \mathrm{Re}\langle E_{2,3}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,4}\rangle + \mathrm{Re}\langle E_{2,4}|E_{3,2}\rangle \\
&+ \mathrm{Re}\langle E_{2,4}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,3}\rangle \\
&+ \mathrm{Re}\langle E_{3,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,2}\rangle \\
&+ \mathrm{Re}\langle E_{3,3}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,3}\rangle \\
&= \frac{3-3\varepsilon}{4}\,.
\end{aligned} \tag{7.16}$$

We call these the *long constraints*. The 16 long constraints are given in appendix B.

7.2 Eve's basis

Once Eve decides on an eavesdropping strategy, the inner products of her records, that is all the terms in $\langle E_I|E_J\rangle$, are fixed. This determines the inner product $\langle F_I|X^\dagger X|F_J\rangle = \langle E_I|E_J\rangle$ where we recall that the square root $X = \sum_{I=1}^{16}|E_I\rangle\langle F_I|$. We are still free to choose an arbitrary basis $|F_I\rangle$ which will determine the choice of the square root X. We shall choose such that X is Hermitian. A different choice of X would amount to a unitary transformation on the basis $|F_I\rangle$.

We choose a basis for Eve so that $X^\dagger = X$. This is obtained by first diagonalising $\rho^E = XX^\dagger$,

$$XX^\dagger = \sum_{I=1}^{16}|\phi_I\rangle\lambda_I^2\langle\phi_I| \tag{7.17}$$

with $\lambda_I \geq 0$ and $\langle \phi_I | \phi_{I'} \rangle = \delta_{I,I'}$, and then choosing the square root to be

$$X = X^\dagger = \sum_{I=1}^{16} |\phi_I\rangle \lambda_I \langle \phi_I| \ . \tag{7.18}$$

In these basis (for Alice–Bob and Eve), Eve's input states would have the matrix representation

$$\rho^E_{a\pm,b\pm} = \mathcal{X} \left(\mathcal{P}_{a\pm} \otimes \mathcal{Q}_{b\pm} \right) \mathcal{X} \ . \tag{7.19}$$

We will work with these matrices in the remaining chapters of this part of the thesis to find out the maximum information that Eve can gain.

Chapter 8

Solving the equations for easy cases

Before going to the general case, we shall look at three easy cases that can be solved analytically. In section 8.1, we look at the case when there is no noise in the channel. In section 8.2, we look at the case where there is a lot noise for which we already know from the intercept and resend attack that Eve will be able to get full information. Section 8.3 looks into the special case when Alice and Bob do a complete tomography on the state that they receive.

8.1 No noise: $\varepsilon = 0$

We want to find all possible solutions to Eve's record states when there is no noise. When there is no noise, the short constraints becomes

$$\langle E_{1,1}|E_{1,1}\rangle = \langle E_{2,2}|E_{2,2}\rangle = \langle E_{3,3}|E_{3,3}\rangle = \langle E_{4,4}|E_{4,4}\rangle = \frac{1}{4} \tag{8.1}$$

and $\langle E_{i,j}|E_{i,j}\rangle = 0$ when $i \neq j$. And from Cauchy–Schwarz inequality, the inner products

$$\left|\langle E_{i,j}|E_{i',j'}\rangle\right|^2 \leq \langle E_{i,j}|E_{i,j}\rangle\langle E_{i',j'}|E_{i',j'}\rangle \tag{8.2}$$

$$= 0 \tag{8.3}$$

when $i \neq j$ or when $i' \neq j'$. With this all of the medium constraints are automatically satisfied. The long constraints reduce to six equations

$$\begin{aligned} &\mathrm{Re}\langle E_{1,1}|E_{2,2}\rangle = \mathrm{Re}\langle E_{1,1}|E_{3,3}\rangle = \mathrm{Re}\langle E_{1,1}|E_{4,4}\rangle \\ &= \mathrm{Re}\langle E_{2,2}|E_{3,3}\rangle = \mathrm{Re}\langle E_{2,2}|E_{4,4}\rangle = \mathrm{Re}\langle E_{3,3}|E_{4,4}\rangle = \frac{1}{4} \end{aligned} \tag{8.4}$$

which means that all four non-zero record states are equal

$$|E_{1,1}\rangle = |E_{2,2}\rangle = |E_{3,3}\rangle = |E_{4,4}\rangle \ . \tag{8.5}$$

The joint Alice–Bob–Eve pure state is then

$$|\Psi\rangle_{ABE} = \sum_{n=1}^{4} |n+, n+\rangle\,|E_{1,1}\rangle \tag{8.6}$$

which is a separable state between Alice–Bob and Eve. In this case even before doing error correction, the raw keys between Alice and Bob are already perfectly correlated and Eve has no information about it.

8.2 A lot of noise: $\varepsilon \geq 2/3$

In this section we shall examine what are Eve's possible strategies when she is allowed to add a large amount of noise. In section 4.3.1 we had an intercept and resend strategy where Eve gains full information at a noise level $\varepsilon = 2/3$. Here, we find what is the equivalent entanglement based attack corresponding to that prepare and send attack.

In the prepare and send scenario, there is a noisy channel between Alice and Bob. We recall that in this channel, for the particular value of $\varepsilon = 2/3$, Eve measures the incoming two-qubit state in either the plus or minus basis. She then forwards the outcome of her measurement with probability $3/4$ and with probability $1/4$ she forwards the state with the opposite parity. We can describe this channel $\mathcal{E}$ by its action on a positive operator ρ

$$\begin{aligned}
\rho \to \mathcal{E}(\rho) = &\frac{1}{2}\sum_{n=1}^{4} \mathrm{Tr}\left\{\rho \left|n+\right\rangle\left\langle n+\right|\right\}\left(\frac{3}{4}\left|n+\right\rangle\left\langle n+\right| + \frac{1}{4}\left|n-\right\rangle\left\langle n-\right|\right) \\
&+ \frac{1}{2}\sum_{n=1}^{4} \mathrm{Tr}\left\{\rho \left|n-\right\rangle\left\langle n-\right|\right\}\left(\frac{3}{4}\left|n-\right\rangle\left\langle n-\right| + \frac{1}{4}\left|n+\right\rangle\left\langle n+\right|\right) \qquad (8.7) \\
= &\sum_{n=1}^{4}\left(\frac{3}{8}\left|n+\right\rangle\left\langle n+\right|\rho\left|n+\right\rangle\left\langle n+\right| + \frac{1}{8}\left|n-\right\rangle\left\langle n+\right|\rho\left|n+\right\rangle\left\langle n-\right|\right) \\
&+ \sum_{n=1}^{4}\left(\frac{3}{8}\left|n-\right\rangle\left\langle n-\right|\rho\left|n-\right\rangle\left\langle n-\right| + \frac{1}{8}\left|n+\right\rangle\left\langle n-\right|\rho\left|n-\right\rangle\left\langle n+\right|\right) \qquad (8.8) \\
= &\sum_{n=1}^{4}\left(A_n^{(1)}\rho A_n^{(1)\dagger} + A_n^{(2)}\rho A_n^{(2)\dagger} + A_n^{(3)}\rho A_n^{(3)\dagger} + A_n^{(4)}\rho A_n^{(4)\dagger}\right) \qquad (8.9)
\end{aligned}$$

where

$$\begin{aligned} A_n^{(1)} &= |n+\rangle\langle n+| \sqrt{\frac{3}{8}}\,, \\ A_n^{(2)} &= |n-\rangle\langle n-| \sqrt{\frac{3}{8}}\,, \\ A_n^{(3)} &= |n+\rangle\langle n-| \sqrt{\frac{1}{8}}\,, \\ A_n^{(4)} &= |n-\rangle\langle n+| \sqrt{\frac{1}{8}} \end{aligned} \tag{8.10}$$

for $n \in \{1,2,3,4\}$.

The more general channel corresponding to the intercept and resend schemes in section 4.3.2 for noise values of $\varepsilon > 2/3$ can be found in a similarly straightforward manner. For that intercept and resend scheme, a particular state ρ would transform to the state

$$\begin{aligned} \rho \rightarrow \mathcal{E}(\rho) = &\frac{1}{2}\sum_{n=1}^{4} \mathrm{Tr}\{\rho\,|n+\rangle\langle n+|\} \\ &\times \left[p_0\,|n+\rangle\langle n+| + p_2\,|n-\rangle\langle n-| + \sum_{m\neq n} \left(p_1\,|m+\rangle\langle m+| + p_3\,|m-\rangle\langle m-|\right)\right] \\ &+ \frac{1}{2}\sum_{n=1}^{4} \mathrm{Tr}\{\rho\,|n-\rangle\langle n-|\} \\ &\times \left[p_0\,|n-\rangle\langle n-| + p_2\,|n+\rangle\langle n+| + \sum_{m\neq n} \left(p_1\,|m-\rangle\langle m-| + p_3\,|m+\rangle\langle m+|\right)\right], \end{aligned} \tag{8.11}$$

where p_0, p_1, p_2 and p_3 are the probabilities introduced in section 4.3.2 of which only one is a free parameter. The channel can be written as

$$\mathcal{E}(\rho) = \sum_{n=1}^{4} \left(A_n^{(1)} \rho A_n^{(1)\dagger} + A_n^{(2)} \rho A_n^{(2)\dagger} + \sum_{n \neq m} \left(A_{n,m}^{(3)} \rho A_{n,m}^{(3)\dagger} + A_{n,m}^{(4)} \rho A_{n,m}^{(4)\dagger} \right) \right) + \sum_{n=1}^{4} \left(B_n^{(1)} \rho B_n^{(1)\dagger} + B_n^{(2)} \rho B_n^{(2)\dagger} + \sum_{n \neq m} \left(B_{n,m}^{(3)} \rho B_{n,m}^{(3)\dagger} + B_{n,m}^{(4)} \rho B_{n,m}^{(4)\dagger} \right) \right) \tag{8.12}$$

where the Kraus operators for this channel are

$$\begin{aligned}
A_n^{(1)} &= |n+\rangle \langle n+| \sqrt{\frac{p_0}{2}} \quad , & B_n^{(1)} &= |n-\rangle \langle n-| \sqrt{\frac{p_0}{2}} \, , \\
A_n^{(2)} &= |n-\rangle \langle n+| \sqrt{\frac{p_2}{2}} \quad , & B_n^{(2)} &= |n+\rangle \langle n-| \sqrt{\frac{p_2}{2}} \, , \\
A_{n,m}^{(3)} &= |m+\rangle \langle n+| \sqrt{\frac{p_1}{2}} \quad , & B_{n,m}^{(3)} &= |m-\rangle \langle n-| \sqrt{\frac{p_1}{2}} \, , \\
A_{n,m}^{(4)} &= |m-\rangle \langle n+| \sqrt{\frac{p_3}{2}} \quad , & B_{n,m}^{(4)} &= |m+\rangle \langle n-| \sqrt{\frac{p_3}{2}}
\end{aligned}$$

for $n, m \in \{1,2,3,4\}$. Through straightforward but tedious computations, it turns out that the channel does not depend on the probabilities p_i.

We now want to obtain the pure state $|\Psi\rangle_{ABE}$ which corresponds to this channel. The intercept and resend attack is equivalent to Eve sending Alice and Bob a

separable state such that the joint state between Alice and Bob is

$$\begin{aligned}
&\rho_{AB} = \\
&\frac{1}{8}\sum_{n=1}^{4} |n+\rangle\langle n+| \otimes \\
&\quad \left[p_0 |n+\rangle\langle n+| + p_2 |n-\rangle\langle n-| + \sum_{m\neq n} \left(p_1 |m+\rangle\langle m+| + p_3 |m-\rangle\langle m-| \right) \right] \\
&+ \frac{1}{8}\sum_{n=1}^{4} |n-\rangle\langle n-| \otimes \\
&\quad \left[p_0 |n-\rangle\langle n-| + p_2 |n+\rangle\langle n+| + \sum_{m\neq n} \left(p_1 |m-\rangle\langle m-| + p_3 |m+\rangle\langle m+| \right) \right] .
\end{aligned} \tag{8.13}$$

In the plus basis between Alice–Bob, this state has matrix entries

$$\langle AB_M|\,\rho_{AB}\,|AB_N\rangle = \big\langle E_N\big|E_M\big\rangle =$$

$$\begin{pmatrix}
a & \cdot & \cdot & \cdot & \cdot & x_1 & \bar{x}_3 & \bar{x}_3 & \cdot & \bar{x}_3 & x_1 & \bar{x}_3 & \cdot & \bar{x}_3 & \bar{x}_3 & x_1 \\
. & b & \cdot & \cdot & x_2 & \cdot & x_4 & \bar{x}_4 & \bar{x}_4 & \cdot & \bar{x}_3 & x_5 & \bar{x}_4 & \cdot & \bar{x}_5 & x_3 \\
. & \cdot & b & \cdot & \bar{x}_4 & x_3 & \cdot & \bar{x}_5 & x_2 & \bar{x}_4 & \cdot & x_4 & \bar{x}_4 & x_5 & \cdot & \bar{x}_3 \\
. & \cdot & \cdot & b & \bar{x}_4 & \bar{x}_3 & x_5 & \cdot & \bar{x}_4 & \bar{x}_5 & x_3 & \cdot & x_2 & x_4 & \bar{x}_4 & . \\
. & x_2 & \bar{x}_4 & \bar{x}_4 & b & \cdot & \cdot & \cdot & \cdot & x_4 & \bar{x}_3 & \bar{x}_5 & \cdot & \bar{x}_4 & x_5 & x_3 \\
x_1 & \cdot & x_3 & \bar{x}_3 & \cdot & a & \cdot & \cdot & x_3 & \cdot & x_1 & x_3 & \bar{x}_3 & \cdot & x_3 & x_1 \\
\bar{x}_3 & x_4 & \cdot & x_5 & . & \cdot & b & \cdot & \bar{x}_4 & x_2 & \cdot & x_4 & \bar{x}_5 & x_4 & \cdot & x_3 \\
\bar{x}_3 & \bar{x}_4 & \bar{x}_5 & \cdot & \cdot & \cdot & \cdot & b & x_5 & x_4 & x_3 & \cdot & x_4 & x_2 & x_4 & . \\
. & \bar{x}_4 & x_2 & \bar{x}_4 & \cdot & x_3 & \bar{x}_4 & x_5 & b & \cdot & \cdot & \cdot & \cdot & \bar{x}_5 & x_4 & \bar{x}_3 \\
\bar{x}_3 & \cdot & \bar{x}_4 & \bar{x}_5 & x_4 & \cdot & x_2 & x_4 & \cdot & b & \cdot & \cdot & x_5 & \cdot & x_4 & x_3 \\
x_1 & \bar{x}_3 & \cdot & x_3 & \bar{x}_3 & x_1 & \cdot & x_3 & \cdot & \cdot & a & \cdot & x_3 & x_3 & \cdot & x_1 \\
\bar{x}_3 & x_5 & x_4 & \cdot & \bar{x}_5 & x_3 & x_4 & \cdot & \cdot & \cdot & \cdot & b & \bar{x}_4 & x_4 & x_2 & . \\
. & \bar{x}_4 & \bar{x}_4 & x_2 & \cdot & \bar{x}_3 & \bar{x}_5 & x_4 & \cdot & x_5 & x_3 & \bar{x}_4 & b & \cdot & \cdot & . \\
\bar{x}_3 & \cdot & x_5 & x_4 & \bar{x}_4 & \cdot & x_4 & x_2 & \bar{x}_5 & \cdot & x_3 & x_4 & \cdot & b & \cdot & . \\
\bar{x}_3 & \bar{x}_5 & \cdot & \bar{x}_4 & x_5 & x_3 & \cdot & x_4 & x_4 & x_4 & \cdot & x_2 & \cdot & \cdot & b & . \\
x_1 & x_3 & \bar{x}_3 & \cdot & x_3 & x_1 & x_3 & \cdot & \bar{x}_3 & x_3 & x_1 & \cdot & \cdot & \cdot & \cdot & a
\end{pmatrix}_{M,N}$$

where $\bar{x}$ denotes the negative of x and the dots are zeros. The magnitudes $a = (4-3\varepsilon)/16$ and $b = \varepsilon/16$ while the inner products x_i are

$$\begin{aligned} x_1 = x_2 &= \frac{1-\varepsilon}{16}\,, \\ x_3 = x_4 &= \frac{1-\varepsilon}{32}\,, \\ x_5 &= 0 \end{aligned} \tag{8.14}$$

all of which does not depend on the probability p_i. The reason for distinguishing between x_1 and x_2 for example will be clear when we generalise Eve's attack in the next chapter. These inner products define the attack that Eve does.

This matrix is diagonalised in appendix C and using the formulation in chapter 6, we can check that Eve gets full information about Alice and Bob's bits when she uses this attack.

8.3 Full tomography solution

For completeness, we note that if Alice and Bob were allowed to do full tomography on their states, then Eve's attack would be restricted to $\langle E_N | E_M \rangle = \langle AB_M | \rho_{AB}^{(t)} | AB_N \rangle$ where

$$\rho_{AB}^{(t)} = (1-\varepsilon) |\Psi\rangle_{AB} \langle\Psi|_{AB} + \varepsilon \frac{1}{16} \tag{8.15}$$

$$= \frac{1-\varepsilon}{16} \sum_{m,n} |n+, n+\rangle \langle m+, m+| + \frac{\varepsilon}{16} \tag{8.16}$$

is the true unbiased noise state as in equation (5.10). This state would correspond to the values

$$\begin{aligned} x_1 &= \frac{1-\varepsilon}{4} \,, \\ x_2 = x_3 = x_4 = x_5 &= 0 \,. \end{aligned} \tag{8.17}$$

For this attack, $|\Psi\rangle_{AB}$ is an eigenvector of the state ρ_{AB} with an eigenvalue of $(16-15\varepsilon)/16$. The remaining 15 eigenvectors are degenerate and have eigenvalues of $\varepsilon/16$. Eve's sub-normalised input state when Alice obtains an outcome $n+$ and Bob obtains an outcome $m+$ will be unitarily equivalent to the state

$\sqrt{\rho_{AB}}\,|n+,m+\rangle\,\langle n+,m+|\,\sqrt{\rho_{AB}}^{\dagger}$:

$$\rho^{E}_{n+,m+} \sim \sqrt{\rho_{AB}}\,|n+,m+\rangle\,\langle n+,m+|\,\sqrt{\rho_{AB}}^{\dagger}\,. \tag{8.18}$$

We use the symbol '$\sim$' to denote unitary equivalence. To compute Eve's information, we need to find the eigenvalues for Eve's input states when say Alice announces the type 1

$$\rho^{E}_{A=1+} = 4\sum_{m}\rho^{E}_{1+,m+} \sim 4\sum_{m}\sqrt{\rho_{AB}}\,|1+,m+\rangle\,\langle 1+,m+|\,\sqrt{\rho_{AB}}^{\dagger}\,, \tag{8.19}$$

$$\rho^{E}_{A=1-} = 4\sum_{m}\rho^{E}_{1-,m-} \sim 4\sum_{m}\sqrt{\rho_{AB}}\,|1-,m-\rangle\,\langle 1-,m-|\,\sqrt{\rho_{AB}}^{\dagger} \tag{8.20}$$

and also the eigenvalues for her total state

$$\rho^{E}_{A=1} = \frac{1}{2}\left(\rho^{E}_{A=1+} + \rho^{E}_{A=1-}\right)\,. \tag{8.21}$$

For $n \neq m$

$$\sqrt{\rho_{AB}}\,|n\pm,m\pm\rangle = |n\pm,m\pm\rangle\,\sqrt{\frac{\varepsilon}{16}} \tag{8.22}$$

while for $n = m$,

$$\begin{aligned}
\sqrt{\rho_{AB}}\,|n\pm,n\pm\rangle &= |\Psi\rangle_{AB}\langle\Psi|_{AB}\sqrt{\frac{16-15\varepsilon}{16}}\,|n\pm,n\pm\rangle \\
&\quad + (1-|\Psi\rangle_{AB}\langle\Psi|_{AB})\sqrt{\frac{\varepsilon}{16}}\,|n\pm,n\pm\rangle \\
&= |\Psi\rangle_{AB}\frac{1}{2}\sqrt{\frac{16-15\varepsilon}{16}} + \left(|n\pm,n\pm\rangle - |\Psi\rangle_{AB}\frac{1}{2}\right)\sqrt{\frac{\varepsilon}{16}} \\
&= |n\pm,n\pm\rangle\left(\frac{\sqrt{16-15\varepsilon}}{16} + \frac{3\sqrt{\varepsilon}}{16}\right) \\
&\quad + \sum_{m\neq n}|m\pm,m\pm\rangle\left(\frac{\sqrt{16-15\varepsilon}}{16} - \frac{\sqrt{\varepsilon}}{16}\right) \\
&\equiv |\phi_n\pm\rangle\sqrt{\frac{4-3\varepsilon}{16}} \qquad (8.23)
\end{aligned}$$

where $|\phi_n\pm\rangle$ are properly normalised. We can also see that the four vectors $\sqrt{\rho_{AB}}|1\pm,m\pm\rangle$ for $m \in \{1,2,3,4\}$ are orthogonal. From this it follows that Eve's input states $\rho^E_{A=1+}$ and $\rho^E_{A=1-}$ have eigenvalues

$$\left\{\frac{4-3\varepsilon}{4}\,,\ \frac{\varepsilon}{4}\quad(\text{deg }3)\right\}\,. \qquad (8.24)$$

The abbreviation 'deg' denotes degeneracy. The entropies of Eve's input states are then

$$S\left(\rho^E_{A=1+}\right) = S\left(\rho^E_{A=1-}\right) = -\frac{4-3\varepsilon}{4}\log\frac{4-3\varepsilon}{4} - \frac{3\varepsilon}{4}\log\frac{\varepsilon}{4}\,. \qquad (8.25)$$

We now proceed to find the eigenvalues for Eve's total state. Eve's total state when Alice announces a type 1 is unitarily equivalent to

$$\rho^E_{A=1} \sim 2\sum_m \sqrt{\rho_{AB}}\left(|1+,m+\rangle\langle 1+,m+| + |1-,m-\rangle\langle 1-,m-|\right)\sqrt{\rho_{AB}}^\dagger \tag{8.26}$$

$$\begin{aligned} &= |\phi_1+\rangle\langle\phi_1+|\,\frac{4-3\varepsilon}{8} + \frac{\varepsilon}{8}\sum_{m=2,3,4}|1+,m+\rangle\langle 1+,m+| \\ &\quad + |\phi_1-\rangle\langle\phi_1-|\,\frac{4-3\varepsilon}{8} + \frac{\varepsilon}{8}\sum_{m=2,3,4}|1-,m-\rangle\langle 1-,m-|\ . \end{aligned} \tag{8.27}$$

The first six eigenvectors for this state are

$$\{|1+,2+\rangle, |1+,3+\rangle, |1+,4+\rangle, |1-,2-\rangle, |1-,3-\rangle, |1-,4-\rangle\} \tag{8.28}$$

which have eigenvalues $\varepsilon/8$ and the final two eigenvectors are proportional to

$$\{|\phi_1+\rangle + |\phi_1-\rangle\ ,\ |\phi_1+\rangle - |\phi_1-\rangle\} \tag{8.29}$$

whose corresponding eigenvalues are

$$\frac{4-3\varepsilon}{8}\left(1 \pm \langle\phi_1+|\phi_1-\rangle\right) \tag{8.30}$$

$$= \frac{4-3\varepsilon}{8}\left(1 \pm \frac{4-4\varepsilon}{4-3\varepsilon}\right) \tag{8.31}$$

$$= \begin{cases} \frac{8-7\varepsilon}{8} \\ \frac{\varepsilon}{8} \end{cases} \tag{8.32}$$

respectively. With this we find that the entropy of Eve's total state is

$$S\left(\rho^E_{A=1}\right) = -\frac{8-7\varepsilon}{8}\log\frac{8-7\varepsilon}{8} - \frac{7\varepsilon}{8}\log\frac{\varepsilon}{8}\ . \tag{8.33}$$

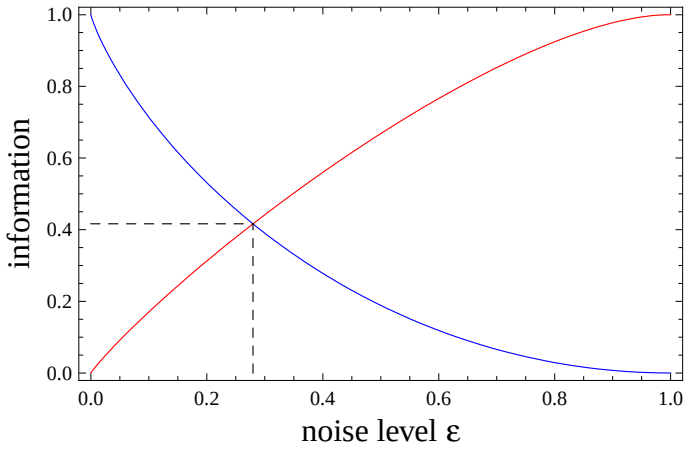


Figure 8.1: Plot of Eve's information (in red) and the mutual information between Alice and Bob (in blue) as a function of the unbiased noise level ε when Alice and Bob can do a complete tomography of their state for the direct communication protocol. The two curves intersect at $\varepsilon = 0.279621$.

Putting this together with the entropies of Eve's input states (8.25), the maximum amount of information Eve can extract can be computed using the Holevo bound

$$\chi = S\left(\rho^E_{A=1}\right) - \frac{1}{2}S\left(\rho^E_{A=1+}\right) - \frac{1}{2}S\left(\rho^E_{A=1-}\right) \geq I_E \ . \tag{8.34}$$

This is plotted in figure 8.1 together with the mutual information between Alice and Bob that we had in section 4.4. Eve's information intersects Alice and Bob's information at $\varepsilon = 0.279621$. This corresponds to a bit error rate of $Q = 0.13981$.

The maximum information transferred per signal is obtained from the difference of Alice and Bob's mutual information and Eve's information

$$r_k = I_{AB} - I_E \ . \tag{8.35}$$

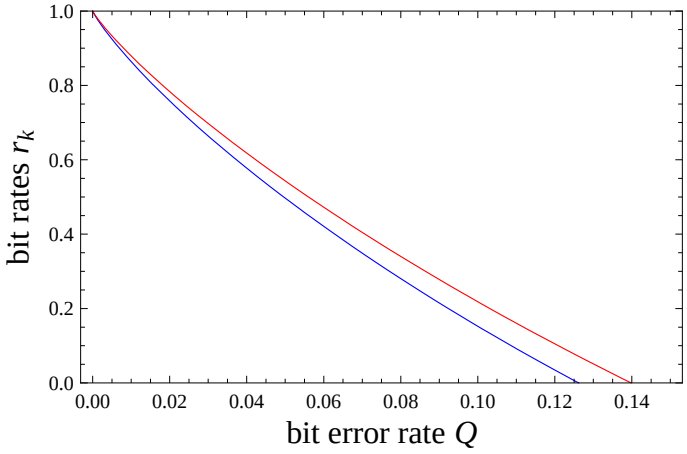


Figure 8.2: Plot of the bit rates for the direct communication protocol when Eve is restricted to a tomographic attack (in red) and the tomographic six-states protocol (in blue) as a function of the bit error rate.

This quantity would be called the key rate if we used the protocol to distribute random keys instead of sending a message. We compare this with the key rate for the fully tomographic six-state protocol in figure 8.2. The key rate for the six-state protocol becomes zero when the error rate is greater than $Q = 0.126193$ [13, 34]. The tomographic version of the direct communication protocol has a higher key rate for all values of bit error below the security threshold.

Chapter 9

Imposing symmetry constraints

The optimisation problem as stated at the end of chapter 6 as it stands is quite intractable analytically. There are 256 variables with 64 constraints, of which only 49 are independent. The function to be optimised, the Holevo quantity, is nonlinear and we have to optimise this subject to the positivity constraints on Eve's reduced state. With the 49 constraints, we have 207 free parameters to optimise.

To make the problem tractable, we impose some additional constraints on Eve's records. These constraints were partly motivated by a numerical search on the optimisation problem. For example, we shall insist that Eve uses the same strategy to discriminate against the plus parity states as she does against the minus parity states.

After imposing these additional constraints, we can reduce Eve's free parameters to just four. At this point we can use standard variational methods to optimise the remaining parameters to obtain Eve's maximum information.

In sections 9.1 and 9.2 of this chapter we impose a parity symmetry and numeral symmetry on Eve's attacks. After imposing these symmetry constraints, we diagonalise Eve's reduced state in section 9.3. The optimisation for Eve's information will be carried out in section 9.4. Finally in section 9.5, we calculate Eve's information and from there find the efficiency of the protocol.

9.1 Parity symmetry

We want Eve's different inputs to be unitarily equivalent if we swap the parity and that the unitary operator does not depend on the numeral type. That is we insist that

$$\rho^E_{a+,b+} = U_P^\dagger \rho^E_{a-,b-} U_P \tag{9.1}$$

for some unitary operator U_P that does not depend on a and b. This constraint is motivated by the fact that the plus and minus basis play equal roles. They are on equal footing and we do not expect Eve to gain by treating one basis differently from the second. From equation (6.30), this constraint requires that the elements for Eve's square root matrix $\mathcal{X}$ must satisfy the relation

$$\mathcal{X}\left(\mathcal{P}^T_{a+} \otimes Q^T_{b+}\right)\mathcal{X}^\dagger = \mathcal{U}_P^\dagger \mathcal{X}\left(\mathcal{P}^T_{a-} \otimes Q^T_{b-}\right)\mathcal{X}^\dagger \mathcal{U}_P \tag{9.2}$$

where $\mathcal{U}_P$ is the matrix representation for U_P with matrix elements

$$\left(\mathcal{U}_P\right)_{J,J'} = \langle F_J | U_P | F_{J'} \rangle . \tag{9.3}$$

The plus and the minus parity states are related by the unitary transformation

$$V_P = \sum_{a,b=1}^{4} |a-\rangle \langle a+| \otimes |b-\rangle \langle b+| \tag{9.4}$$

with matrix elements

$$(\mathcal{V}_P)_{J,J'} = \langle AB_J | V_P | AB_{J'} \rangle \ . \tag{9.5}$$

By construction

$$V_P \, (P_{a+} \otimes Q_{b+}) \, V_P^\dagger = P_{a-} \otimes Q_{b-} \tag{9.6}$$

and its equivalent matrix relation

$$\mathcal{V}_P \, (\mathcal{P}_{a+} \otimes \mathcal{Q}_{b+}) \, \mathcal{V}_P^\dagger = \mathcal{P}_{a-} \otimes \mathcal{Q}_{b-} \ . \tag{9.7}$$

Finally, substituting

$$\mathcal{P}_{a-}^T \otimes \mathcal{Q}_{b-}^T = \mathcal{V}^* \left(\mathcal{P}_{a+}^T \otimes \mathcal{Q}_{b+}^T \right) \mathcal{V}^T \tag{9.8}$$

into equation (9.2), we arrive at the relation

$$\mathcal{X} \left(\mathcal{P}_{a+}^T \otimes \mathcal{Q}_{b+}^T \right) \mathcal{X}^\dagger = \left(\mathcal{U}_P^\dagger \mathcal{X} \mathcal{V}_P^* \right) \left(\mathcal{P}_{a+}^T \otimes \mathcal{Q}_{b+}^T \right) \left(\mathcal{V}_P^T \mathcal{X}^\dagger \mathcal{U}_P \right) \tag{9.9}$$

which will be satisfied if we impose the condition that $\mathcal{X}$ commutes with $\mathcal{V}_P^*$ and set $\mathcal{U}_P = \mathcal{V}_P^*$:

$$\mathcal{X} = \mathcal{V}_P^T \mathcal{X} \mathcal{V}_P^* \,. \tag{9.10}$$

This imposes an additional 104 independent constraints to our equations. This reduces the number of free parameters from 207 down to 103.

9.2 Numeral symmetry

To further reduce the number of free parameters we impose another symmetry requirement on Eve's input. We require that if Alice and Bob re-label their numeral labels cyclically, Eve's record states should remain unitarily equivalent. In fact we insist on a stronger condition that when we permute one index to the next in the cyclic permutation, the unitary transformation for Eve's record states does not depend on the index.

Repeating the analysis done for the parity symmetry, we impose the condition that

$$\mathcal{X} = \mathcal{V}_{N1}^T \mathcal{X} \mathcal{V}_{N1}^* \tag{9.11}$$

where

$$(\mathcal{V}_{N1})_{J,J'} = \langle AB_J | V_{N1} | AB_{J'} \rangle \tag{9.12}$$

and

$$\begin{aligned} V_{N1} = &(|1+\rangle\langle 2+| - |2+\rangle\langle 3+| + |3+\rangle\langle 4+| + |4+\rangle\langle 1+|)_A \\ &\otimes (|1+\rangle\langle 2+| - |2+\rangle\langle 3+| + |3+\rangle\langle 4+| + |4+\rangle\langle 1+|)_B \end{aligned} \tag{9.13}$$

which permutes the numeral indices from $1 \to 2 \to 3 \to 4 \to 1$. This gives another 78 more independent equations, bringing the number of free parameters to 25.

We impose a last symmetry for Eve's records

$$\begin{aligned} V_{N2} = &(|1+\rangle\langle 3+| + |3+\rangle\langle 2+| - |2+\rangle\langle 4+| + |4+\rangle\langle 1+|)_A \\ &\otimes (|1+\rangle\langle 3+| + |3+\rangle\langle 2+| - |2+\rangle\langle 4+| + |4+\rangle\langle 1+|)_B \end{aligned} \tag{9.14}$$

which permutes the numeral indices from $1 \to 3 \to 2 \to 4 \to 1$. This gives another 21 more independent equations, bringing the number of free parameters to four.

Labelling the remaining parameters as x_1, x_2, x_3, x_4, x_5 we have five parameters to optimise with one constraint on the sum

$$x_1 + x_2 + 2x_3 + 2x_4 = \frac{1-\varepsilon}{4} \,. \tag{9.15}$$

These parameters correspond to the entries in the matrix $\mathcal{X}^\dagger\mathcal{X}$. With these constraints, the matrix $\mathcal{X}^\dagger\mathcal{X}$ takes the form

$$\langle E_I | E_J \rangle = (\mathcal{X}^\dagger\mathcal{X})_{I,J} =$$

$$\begin{pmatrix}
a & \cdot & \cdot & \cdot & \cdot & x_1 & \bar{x}_3 & \bar{x}_3 & \cdot & \bar{x}_3 & x_1 & \bar{x}_3 & \cdot & \bar{x}_3 & \bar{x}_3 & x_1 \\
\cdot & b & \cdot & \cdot & x_2 & \cdot & x_4 & \bar{x}_4 & \bar{x}_4 & \cdot & \bar{x}_3 & x_5 & \bar{x}_4 & \cdot & \bar{x}_5 & x_3 \\
\cdot & \cdot & b & \cdot & \bar{x}_4 & x_3 & \cdot & \bar{x}_5 & x_2 & \bar{x}_4 & \cdot & x_4 & \bar{x}_4 & x_5 & \cdot & \bar{x}_3 \\
\cdot & \cdot & \cdot & b & \bar{x}_4 & \bar{x}_3 & x_5 & \cdot & \bar{x}_4 & \bar{x}_5 & x_3 & \cdot & x_2 & x_4 & \bar{x}_4 & \cdot \\
\cdot & x_2 & \bar{x}_4 & \bar{x}_4 & b & \cdot & \cdot & \cdot & \cdot & x_4 & \bar{x}_3 & \bar{x}_5 & \cdot & \bar{x}_4 & x_5 & x_3 \\
x_1 & \cdot & x_3 & \bar{x}_3 & \cdot & a & \cdot & \cdot & x_3 & \cdot & x_1 & x_3 & \bar{x}_3 & \cdot & x_3 & x_1 \\
\bar{x}_3 & x_4 & \cdot & x_5 & \cdot & \cdot & b & \cdot & \bar{x}_4 & x_2 & \cdot & x_4 & \bar{x}_5 & x_4 & \cdot & x_3 \\
\bar{x}_3 & \bar{x}_4 & \bar{x}_5 & \cdot & \cdot & \cdot & \cdot & b & x_5 & x_4 & x_3 & \cdot & x_4 & x_2 & x_4 & \cdot \\
\cdot & \bar{x}_4 & x_2 & \bar{x}_4 & \cdot & x_3 & \bar{x}_4 & x_5 & b & \cdot & \cdot & \cdot & \cdot & \bar{x}_5 & x_4 & \bar{x}_3 \\
\bar{x}_3 & \cdot & \bar{x}_4 & \bar{x}_5 & x_4 & \cdot & x_2 & x_4 & \cdot & b & \cdot & \cdot & x_5 & \cdot & x_4 & x_3 \\
x_1 & \bar{x}_3 & \cdot & x_3 & \bar{x}_3 & x_1 & \cdot & x_3 & \cdot & \cdot & a & \cdot & x_3 & x_3 & \cdot & x_1 \\
\bar{x}_3 & x_5 & x_4 & \cdot & \bar{x}_5 & x_3 & x_4 & \cdot & \cdot & \cdot & \cdot & b & \bar{x}_4 & x_4 & x_2 & \cdot \\
\cdot & \bar{x}_4 & \bar{x}_4 & x_2 & \cdot & \bar{x}_3 & \bar{x}_5 & x_4 & \cdot & x_5 & x_3 & \bar{x}_4 & b & \cdot & \cdot & \cdot \\
\bar{x}_3 & \cdot & x_5 & x_4 & \bar{x}_4 & \cdot & x_4 & x_2 & \bar{x}_5 & \cdot & x_3 & x_4 & \cdot & b & \cdot & \cdot \\
\bar{x}_3 & \bar{x}_5 & \cdot & \bar{x}_4 & x_5 & x_3 & \cdot & x_4 & x_4 & x_4 & \cdot & x_2 & \cdot & \cdot & b & \cdot \\
x_1 & x_3 & \bar{x}_3 & \cdot & x_3 & x_1 & x_3 & \cdot & \bar{x}_3 & x_3 & x_1 & \cdot & \cdot & \cdot & \cdot & a
\end{pmatrix}_{I,J}$$

where $\bar{x}$ denotes the negative of x and the dots are zeros. The magnitudes $a = (4 - 3\varepsilon)/16$ and $b = \varepsilon/16$. The negative signs in one of the terms in equations (9.13) and (9.14) were inserted so that this matrix is similar to the one we obtained in section 8.2 for the intercept and resend attack.

9.3 Diagonalising Eve's attack

After imposing the symmetry constraints, we are left with a manageable problem. The 16 by 16 matrix $\mathcal{X}^\dagger\mathcal{X}$ can be diagonalised which will also give the Schmidt decomposition of Eve's pure state between Alice–Bob and Eve. These eigenvectors are given in appendix C.

From this we can also get the eigenvalues of the matrix representing Eve's total state $\mathcal{X}\mathcal{X}^\dagger$. The eigenvalues are

$$\begin{aligned}
\mu_1 &= \frac{1}{16}\left(16-15\varepsilon-48x_2-96x_3-96x_4\right)\ ,\\
\mu_{2,3,4} &= \frac{1}{16}\left(\varepsilon+16x_2-32x_4\right)\ ,\\
\mu_{5,6,7} &= \frac{1}{16}\left(\varepsilon+16x_2-32x_3+32x_4\right)\ ,\\
\mu_{8,9,10} &= \frac{1}{16}\left(\varepsilon+16x_2+64x_3+32x_4\right)\ ,\\
\mu_{11,12,13} &= \frac{1}{16}\left(\varepsilon-16x_2-32x_5\right)\ ,\\
\mu_{14} &= \frac{1}{16}\left(\varepsilon-16x_2+64x_4+32x_5\right)\ ,\\
\mu_{15,16} &= \frac{1}{16}\left(\varepsilon-16x_2-32x_4+32x_5\right)\ .
\end{aligned} \tag{9.16}$$

The parameters x_2, x_3, x_4 and x_5 must be chosen such that these eigenvalues are positive.

9.4 Optimisation problem

To compute the Holevo quantity, we need to find the eigenvalues of $\rho^E_{a\pm}$ and $\rho^E_a = \frac{1}{2}\rho^E_{a+} + \frac{1}{2}\rho^E_{a-}$. Our assumptions on Eve's records ensure that her reduced states $\rho^E_{a\pm}$ have the same set of eigenvalues for all $a \in \{1,2,3,4\}$. The eigenvalues turn

out to be

$$\left\{ \frac{4-3\varepsilon}{4} \, , \, \frac{\varepsilon}{4} \quad (\deg 3) \right\} \tag{9.17}$$

which depends on ε only. Also the combined state ρ_a^E has eigenvalues

$$\begin{aligned}
\lambda_1 &= \frac{1}{8}\left(\varepsilon - 16x_2 + 32x_4\right) \, , \\
\lambda_2 &= \frac{1}{8}\left(\varepsilon + 16x_2 - 32x_4\right) \, , \\
\lambda_{3,4} &= \frac{1}{8}\left(\varepsilon - 16x_3 + 16x_4 - 16x_5\right) \, , \\
\lambda_{5,6} &= \frac{1}{8}\left(\varepsilon + 16x_3 - 16x_4 + 16x_5\right) \, , \\
\lambda_7 &= \frac{1}{8}\left(\varepsilon + 16x_2 + 64x_3 + 32x_4\right) \, , \\
\lambda_8 &= \frac{1}{8}\left(8 - 7\varepsilon - 16x_2 - 64x_3 - 32x_4\right)
\end{aligned} \tag{9.18}$$

for all $a \in \{1,2,3,4\}$. Hence to maximise the Holevo quantity, we need to maximise the entropy of ρ_a^E,

$$S\left(\rho_a^E\right) = -\sum_i \lambda_i \log \lambda_i \, , \tag{9.19}$$

where λ_i are the non zero eigenvalues of ρ_a^E. There are four parameters to optimise: x_2, x_3, x_4 and x_5. The entropy will be extremised when

$$\frac{\partial S}{\partial x_j} = 0 \,, \tag{9.20}$$

$$-\sum_{i=1}^{8}\left(\lambda_i \frac{1}{\lambda_i}\frac{\partial \lambda_i}{\partial x_j} + \frac{\partial \lambda_i}{\partial x_j}\log\lambda_i\right) = 0 \,, \tag{9.21}$$

$$-\sum_{i=1}^{8}\left(\frac{\partial \lambda_i}{\partial x_j} + \log \lambda_i^{\frac{\partial \lambda_i}{\partial x_j}}\right) = 0 \,, \tag{9.22}$$

$$\prod_{i=1}^{8}\left(\lambda_i^{\frac{\partial \lambda_i}{\partial x_j}}\right) = 1 \tag{9.23}$$

where the first term in the third equality above vanishes because the sum of the eigenvalues $\sum \lambda_i = 1$.

At this point, we want to find solutions to these equations for which Eve's total state remains positive. It turns out that there are two families of solutions. The first is when the noise level ε is greater than or equal to $2/3$ and as we shall see in the next sub-section, these solutions will give Eve full information. The second family is when ε is less than $2/3$. For these solutions, Eve will no longer be able to gain full information.

9.4.1 A lot of noise: $\varepsilon \geq 2/3$

We start with the case when the noise level ε is greater than or equal to $2/3$. Taking the derivative of the entropy with respect to x_2, the first condition for extremising the entropy is

$$\frac{\partial S}{\partial x_2} = 0 \tag{9.24}$$

which gives

$$\left[\frac{1}{8}(\varepsilon+16x_2-32x_4)\right]^{16}\times\left[\frac{1}{8}(\varepsilon+16x_2+64x_3+32x_4)\right]^{16}$$
$$\times\left[\frac{1}{8}(\varepsilon-16x_2+32x_4)\right]^{-16}\times\left[\frac{1}{8}(8-7\varepsilon-16x_2-64x_3-32x_4)\right]^{-16}=1 \tag{9.25}$$

provided that non of the eigenvalues are zero. This simplifies to

$$(\varepsilon+16x_2-32x_4)\times(\varepsilon+16x_2+64x_3+32x_4)$$
$$\times\ (\varepsilon-16x_2+32x_4)^{-1}\times(8-7\varepsilon-16x_2-64x_3-32x_4)^{-1}=1\,. \tag{9.26}$$

The other three conditions are

$$\frac{\partial S}{\partial x_3}=0 \tag{9.27}$$

which gives

$$(\varepsilon+16x_3-16x_4+16x_5)\times(\varepsilon+16x_2+64x_3+32x_4)^2$$
$$\times(\varepsilon-16x_3+16x_4-16x_5)^{-1}\times(8-7\varepsilon-16x_2-64x_3-32x_4)^{-2}=1 \tag{9.28}$$

and

$$\frac{\partial S}{\partial x_4}=0 \tag{9.29}$$

which gives

$$\begin{aligned}&(\varepsilon-16x_2+32x_4)\times(\varepsilon-16x_3+16x_4-16x_5)\\&\times(\varepsilon+16x_2+64x_3+32x_4)\times(\varepsilon+16x_2-32x_4)^{-1}\\&\times(\varepsilon+16x_3-16x_4+16x_5)^{-1}\times(8-7\varepsilon-16x_2-64x_3-32x_4)^{-1}=1\end{aligned}\tag{9.30}$$

and

$$\frac{\partial S}{\partial x_5}=0\tag{9.31}$$

$$\implies x_5\times(x_4-x_3)^{-1}=1\,.\tag{9.32}$$

The solutions to these four equations, parametrised by a parameter α are

$$\begin{aligned}x_2&=2\alpha\,,\\x_3&=\frac{1}{16}(1-\varepsilon-16\alpha)\,,\\x_4&=\alpha\,,\\x_5&=\frac{1}{16}[32\alpha-(1-\varepsilon)]\,.\end{aligned}\tag{9.33}$$

The choice of α must satisfy the requirement that Eve's total state $\mathcal{X}\mathcal{X}^\dagger$ has positive eigenvalues. Substituting this solution into the eigenvalues, the eigenvalues

as a function of ε and α are

$$\begin{aligned}
\mu_1 &= \frac{1}{16}(10-9\varepsilon-96\alpha)\ , \\
\mu_{2,3,4} &= \frac{1}{16}\varepsilon\ , \\
\mu_{5,6,7} &= \frac{1}{16}(3\varepsilon-2+96\alpha)\ , \\
\mu_{8,9,10} &= \frac{1}{16}(4-3\varepsilon)\ , \\
\mu_{11,12,13} &= \frac{1}{16}(2-\varepsilon-96\alpha)\ , \\
\mu_{14} &= \mu_5\ , \\
\mu_{15,16} &= \frac{1}{16}(3\varepsilon-2)\ .
\end{aligned} \tag{9.34}$$

These eigenvalues are always positive provided

$$\varepsilon > \frac{2}{3} \quad \text{and} \quad \frac{3\varepsilon-2}{96} \leq \alpha \leq \frac{2-\varepsilon}{96}\ . \tag{9.35}$$

For every one of the solution, Eve's total state ρ_a^E has eigenvalues

$$\left\{\lambda_{1,2,3,4,5,6} = \frac{\varepsilon}{8} \quad \text{and} \quad \lambda_{7,8} = \frac{4-3\varepsilon}{8}\right\} \tag{9.36}$$

that does not depend on α and gives Eve full information. The class of intercept and resend attacks in section 8.2 is a special case of the solution when $\alpha = (1-\varepsilon)/32$.

9.4.2 Not so much noise: $\varepsilon < 2/3$

When $\varepsilon < 2/3$, the solutions in the previous sub-section are no longer admissible as they will make Eve's total state negative. The first two eigenvalues of $\mathcal{X}\mathcal{X}^\dagger$ to

become negative are the eigenvalues

$$\mu_{15,16} = \frac{1}{16}\left(\varepsilon - 16x_2 - 32x_4 + 32x_5\right) . \tag{9.37}$$

Setting these to zero, we can write x_5 in terms of the remaining parameters

$$x_5 = x_4 + \frac{1}{2}x_2 - \frac{1}{32}\varepsilon . \tag{9.38}$$

The combined state ρ_a^E now has eigenvalues

$$\begin{aligned}
\lambda_1 &= \frac{1}{8}\left(\varepsilon - 16x_2 + 32x_4\right) , \\
\lambda_2 &= \frac{1}{8}\left(\varepsilon + 16x_2 - 32x_4\right) , \\
\lambda_{3,4} &= \frac{1}{16}\left(3\varepsilon - 16x_2 - 32x_3\right) , \\
\lambda_{5,6} &= \frac{1}{16}\left(\varepsilon + 16x_2 + 32x_3\right) , \\
\lambda_7 &= \frac{1}{8}\left(\varepsilon + 16x_2 + 64x_3 + 32x_4\right) , \\
\lambda_8 &= \frac{1}{8}\left(8 - 7\varepsilon - 16x_2 - 64x_3 - 32x_4\right) .
\end{aligned} \tag{9.39}$$

Doing as we did before, the three conditions $\frac{\partial S}{\partial x_2} = \frac{\partial S}{\partial x_3} = \frac{\partial S}{\partial x_4} = 0$ give three equations. The first equation

$$\frac{\partial S}{\partial x_2} = 0 \tag{9.40}$$

leads to

$$\begin{aligned}&(\varepsilon+16x_2-32x_4)\times(\varepsilon+16x_2+32x_3)\\&\quad\times(\varepsilon+16x_2+64x_3+32x_4)\times(\varepsilon-16x_2+32x_4)^{-1}\\&\quad\times(3\varepsilon-16x_2-32x_3)^{-1}\times(8-7\varepsilon-16x_2-64x_3-32x_4)^{-1}=1\,.\end{aligned}\tag{9.41}$$

The second equation

$$\frac{\partial S}{\partial x_3}=0\tag{9.42}$$

gives

$$\begin{aligned}&(\varepsilon+16x_2+32x_3)\times(\varepsilon+16x_2+64x_3+32x_4)^2\\&\quad\times(3\varepsilon-16x_2-32x_3)^{-1}\times(8-7\varepsilon-16x_2-64x_3-32x_4)^{-2}=1\,.\end{aligned}\tag{9.43}$$

From the final equation

$$\frac{\partial S}{\partial x_4}=0\,,\tag{9.44}$$

we get

$$\begin{aligned}&(\varepsilon-16x_2+32x_4)\times(\varepsilon+16x_2+64x_3+32x_4)\\&\quad\times(\varepsilon+16x_2-32x_4)^{-1}\times(8-7\varepsilon-16x_2-64x_3-32x_4)^{-1}=1\,.\end{aligned}\tag{9.45}$$

Equation (9.45) follows from equations (9.41) and (9.43). The solutions to these equations can be found by solving a cubic equation. From equation (9.45), we can

write x_3 as

$$x_3 = \frac{1}{16\varepsilon}\Big[\varepsilon(1-\varepsilon) + 16x_2(1-\varepsilon) - 16x_4(2-\varepsilon)\Big] \,. \tag{9.46}$$

Substituting this into equation (9.43), we obtain a cubic equation in x_2 with coefficients involving x_4 and ε

$$\begin{aligned}
&\Big[4096(2-\varepsilon)\Big] + x_2\Big[-256\Big(\varepsilon(-2+3\varepsilon) - 96(-2+\varepsilon)x_4\Big)\Big] \\
&\quad + 16x_2^2\Big[(\varepsilon^2(2+3\varepsilon) + 64\varepsilon(-2+3\varepsilon)x_4 - 3072(-2+\varepsilon)x_4^2\Big] \\
&\quad + x_2^3\Big[(2-3\varepsilon)\varepsilon^3 - 32\varepsilon^2(2+3\varepsilon)x_4 \\
&\qquad - 1024\varepsilon(-2+3\varepsilon)x_4^2 + 32768(-2+\varepsilon)x_4^3\Big] = 0 \,.
\end{aligned} \tag{9.47}$$

The solution to this equation can be written as

$$\begin{aligned}
x_2 &= g_2(\varepsilon) + 2\alpha \,, \\
x_3 &= g_3(\varepsilon) - \alpha \,, \\
x_4 &= \alpha
\end{aligned} \tag{9.48}$$

which is parametrised by α and where g_2 and g_3 are functions of ε only. The function g_2 is obtained by solving for the roots the cubic equation above. Explicitly,

$$\begin{aligned}
g_2 &= \frac{8\varepsilon^2 + 24\varepsilon^3 - 18\varepsilon^4 - 2\varepsilon w + 3\varepsilon^2 w - w^2}{48(2-\varepsilon)w} \,, \\
g_3 &= \frac{1}{16}(1-\varepsilon) + g_2\frac{(1-\varepsilon)}{\varepsilon}
\end{aligned} \tag{9.49}$$

and

$$w = 2^{\frac{1}{3}}\Big[2\varepsilon^3(2-3\varepsilon)^2(5-3\varepsilon) + 3\varepsilon^3(2-\varepsilon)\sqrt{6(2-\varepsilon)\left(4-18\varepsilon+54\varepsilon^2-27\varepsilon^3\right)}\Big]^{\frac{1}{3}} . \tag{9.50}$$

From these solutions we obtain the eigenvalues of Eve's total state ρ_a^E, all of which do not depend on α:

$$\begin{aligned}
\lambda_1 &= \frac{1}{8}\left(\varepsilon - 16g_2\right) , \\
\lambda_2 &= \frac{1}{8}\left(\varepsilon + 16g_2\right) , \\
\lambda_{3,4} &= \frac{1}{16}\left(3\varepsilon - 16g_2 - 32g_3\right) , \\
\lambda_{5,6} &= \frac{1}{16}\left(\varepsilon + 16g_2 + 32g_3\right) , \\
\lambda_7 &= \frac{1}{8}\left(\varepsilon + 16g_2 + 64g_3\right) , \\
\lambda_8 &= \frac{1}{8}\left(8 - 7\varepsilon - 16g_2 - 64g_3\right) .
\end{aligned} \tag{9.51}$$

We plot the eigenvalues as a function of ε in figure 9.1.

From the eigenvalues we can calculate the bound on the mutual information between Eve and Alice. Any value of α for which $\mathcal{X}\mathcal{X}^\dagger$ is positive is admissible

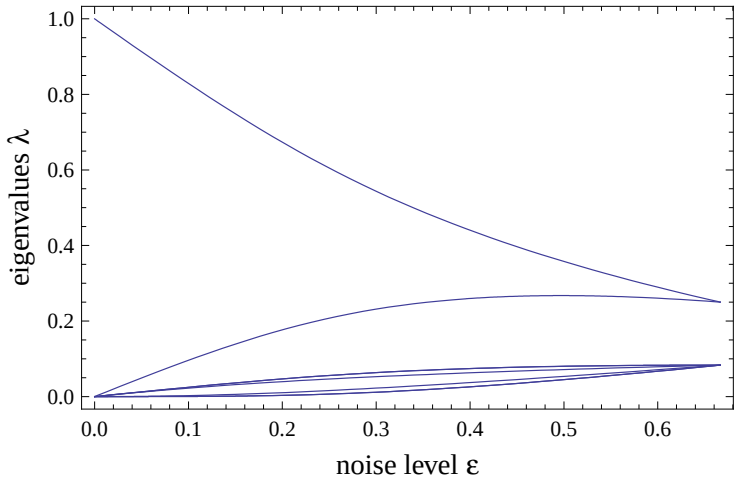


Figure 9.1: Plot of the eigenvalues of Eve's conditional state ρ_a^E as a function of the noise level.

and gives the same information. The eigenvalues of $\mathcal{X}\mathcal{X}^\dagger$ are

$$\begin{aligned}
\mu_1 &= \frac{1}{16}\left(16-15\varepsilon-48g_2-96g_3-96\alpha\right)\,,\\
\mu_{2,3,4} &= \frac{1}{16}\left(\varepsilon+16g_2\right)\,,\\
\mu_{5,6,7} &= \frac{1}{16}\left(\varepsilon+16g_2-32g_3+96\alpha\right)\,,\\
\mu_{8,9,10} &= \frac{1}{16}\left(\varepsilon+16g_2+64g_3\right)\,,\\
\mu_{11,12,13} &= \frac{1}{16}\left(2\varepsilon-32g_2-96\alpha\right)\,,\\
\mu_{14} &= 6\alpha\,,\\
\mu_{15,16} &= 0\,.
\end{aligned} \tag{9.52}$$

The eigenvalues $\mu_{2,3,4}$, $\mu_{8,9,10}$ and $\mu_{15,16}$ do not depend on α and they are non-negative for all values of $0 \leq \varepsilon \leq 2/3$. The remaining eigenvalues are positive as

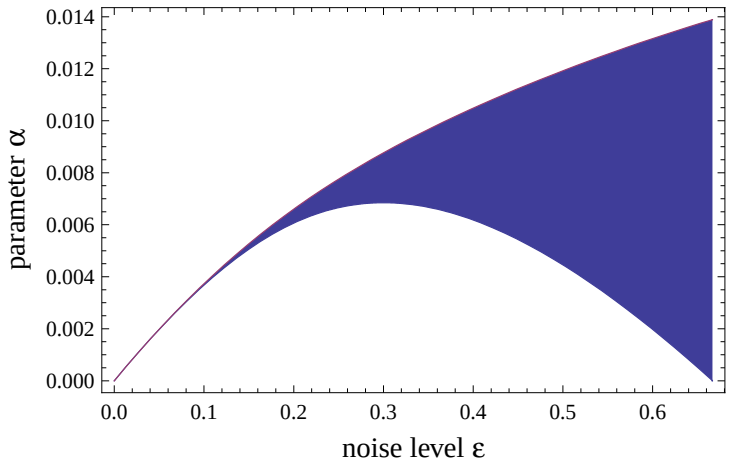


Figure 9.2: Plot showing the admissible region of the parameter α for which the eigenvalues of Eve's total state $\mathcal{X}\mathcal{X}^\dagger$ is positive.

long as

$$\frac{32g_3 - 16g_2 - \varepsilon}{96} \leq \alpha \leq \frac{2\varepsilon - 32g_2}{96} \tag{9.53}$$

for which a solution always exists. This range is plotted in figure 9.2.

9.5 Eve's information and protocol efficiency

At this point we have all the ingredients needed to calculate the Holevo quantity

$$\chi = S\left(\rho_a^E\right) - \frac{1}{2}S\left(\rho_{a+}^E\right) - \frac{1}{2}S\left(\rho_{a-}^E\right) \tag{9.54}$$

which is an achievable bound on Eve's information. This is plotted in figure 9.3 together with the mutual information between Alice and Bob that we had in section 4.4. From the intersection of the two curves, we find that the noise threshold

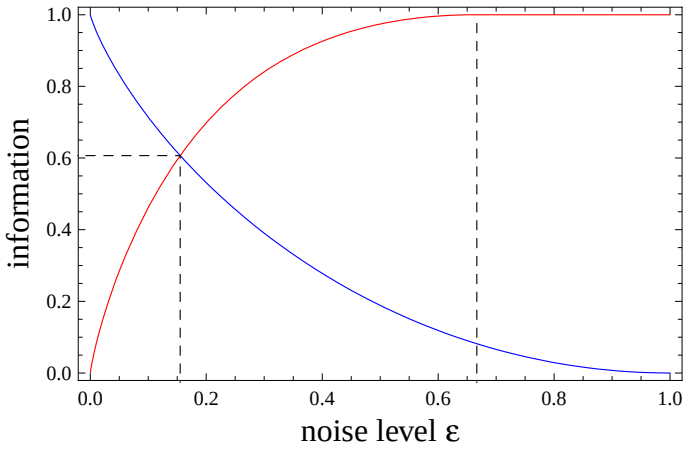


Figure 9.3: Plot of Eve's information (in red) and the mutual information between Alice and Bob (in blue) as a function of the unbiased noise level ε for Eve's optimal attack. The two curves intersect at $\varepsilon_0 = 0.154969$.

for secure communication is $\varepsilon_0 = 0.154969$ which corresponds to an error rate of $Q = 0.0774845$.

The maximum information transferred per signal is obtained from the difference of Alice and Bob's mutual information and Eve's information

$$r_k = I_{AB} - I_E \ . \tag{9.55}$$

We compare this quantity with the key rate from the BB84 protocol in figure 9.4. The key rate for the BB84 protocol becomes zero when the error rate is greater than $Q = 0.110028$ [13,51]. The BB84 protocol has a higher key rate compared to the direct communication protocol for all values of error rate below its threshold.

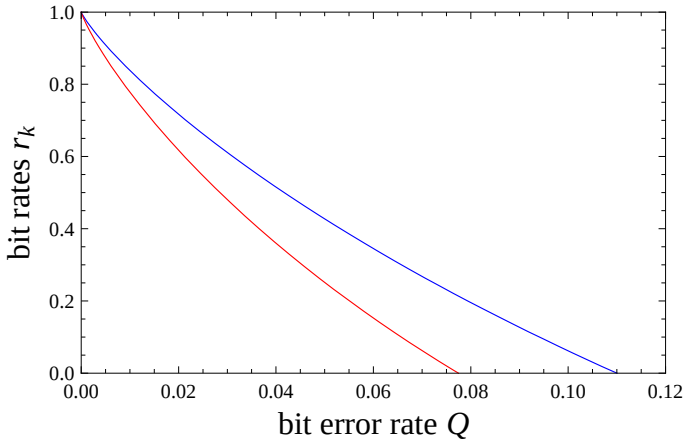


Figure 9.4: Plot of the bit rates for the direct communication protocol (in red) and the BB84 protocol (in blue) as a function of the bit error rate.

Chapter 10

Conclusion and outlook

In the first part of the thesis, we found some plausible upper bounds on Eve's information. To derive these bounds, we had to impose some symmetry constraints to reduce the number of free parameters for Eve's attack.

Without imposing the symmetry constraints, a numerical search was carried out to determine the optimal solution using Monte-Carlo methods. The only constraints imposed on Eve's attack was that the joint probability table between Alice and Bob should be consistent with an unbiased noise channel. No solutions were found that were better than the known solution. But this does not say much since the dimension of the search space is exceedingly large.

At this point, we can ask the following question: Is it possible to restrict Eve's attack if we allow Alice and Bob to perform some random processing on their qubits before measuring them? The method of introducing random processing on the data to achieve an upper bound on Eve's information was first presented by Kraus, Gisin and Renner in [29]. In appendix D, we show that if we allow Alice and Bob were to perform some random operations on their qubits, to get an upper

bound on Eve's information, the state of Eve's ancilla can be parametrised by only nine parameters. The checks that Alice and Bob do on their measurement statistics would put further constraints on this state. By doing this random processing, the number of parameters for Eve in her attack can be naturally reduced.

In this thesis we have not discussed the error correction and privacy amplification parts of the protocol. These would come after knowing how much information Eve can obtain. If we use this protocol for key distribution, these procedures are well known and can be easily adapted to the needs of this protocol.

However to use the protocol for direct communication, things are not so simple. If the message itself is being transmitted, then Eve could possibly intercept the message and gain partial knowledge of its contents. It is too late to perform an analogue of a 'privacy amplification' procedure as in a key distribution protocol.

It would be interesting to see if Alice can still transmit a deterministic and secret message to Bob. One way to achieve this is to have Alice suitably encrypt her message such that Bob would be able to decipher perfectly but Eve would not be able to obtain any information. How much encryption Alice needs to perform would depend on the amount of information Eve has on the raw data. By encrypt, we mean that Alice pre-processes her message using a publicly known error correcting and privacy amplification scheme prior to sending it to Bob.

The complete details for such pre-processing would need more study. But roughly speaking, Alice will encode the raw bits that she sends with redundancies by reversing Bob's decoding process. For example, to send the message $\mathbf{x}$, Alice will first need to find a longer message $\mathbf{y}$ such that $h_m(\mathbf{y}) = \mathbf{x}$, where h_m is a randomly chosen hashing function from a suitable universal class of hashing functions. This encoding is the analogue of the privacy amplification step in quantum

key distribution. It is to ensure that even if Eve has some partial knowledge on $\mathbf{y}$, she cannot learn anything about the actual message $\mathbf{x}$. Of course the problem with this is that by definition a universal hashing function does not have an inverse. It is hard to find $\mathbf{y}$ given $\mathbf{x}$.

Instead, say Alice creates the string $\mathbf{y}$. With this, she can deterministically and securely send the message $\mathbf{x} = h_m(\mathbf{y})$ to Bob. In other words, Alice will know what the message will be before she decides to transmit it. But she cannot deterministically choose her message.

Before Bob can apply h_m to learn about the actual message $\mathbf{x}$, he needs to have the error-free string $\mathbf{y}$. To ensure Bob can get the error-free string, Alice has to do one more step of encoding using error correcting codes. She would need to find the message $\mathbf{z}$ such that $g(\mathbf{z}) = g(\mathbf{z}') = \mathbf{y}$, where $\mathbf{z}'$ is the message that Bob receives which is corrupted by the expected amount of error in the transmission and g is the error correcting protocol. Alice will then perform one way communication. She sends some classical bits to Bob so that Bob can correct all his errors. How much classical information Alice needs to send will depend on the mutual information between Alice and Bob. After Bob has an error-free string $\mathbf{y}$, Alice will then reveal the actual function h_m so that Bob can get the actual message $\mathbf{x}$.

The reason that the encrypting process can be done prior to Alice sending her signal is because of the fact that the protocol is deterministic. Hence Alice knows that the final result of Bob's successful decoding is just her original message. In a conventional quantum key distribution protocol, it would not be possible (nor would it be necessary) for Alice to do such encryption prior to sending her signals because of the random nature of Bob's raw bits and also the final key.

We remark that since some amount of post-processing needs to be performed between Alice and Bob, the protocol is not really a direct communication protocol in the strictest sense. Alice still needs to send classical bits to Bob in order for Bob to recover her message. It can then be said that since Alice still needs to send classical bits to Bob anyway, then there is not much advantage of this protocol over a key distribution protocol.

A major concern for the protocol that we have briefly mentioned in the introduction is its performance in the presence of channel loss. In most discrete variable quantum key distribution protocols, lost qubits (or qudits) do not contribute to the error rate because such events are simply rejected. But in a direct communication protocol, a lost signal means that some information on the message itself is lost. Therefore the lost signals have to be accounted as errors when characterising the channel. For such events, Bob would randomly choose a bit '0' or '1' to fill in his empty slots. If the error rate is not too large, then the post-processing procedures will be able to correct for these errors. To minimise Eve's information, Alice should not reveal her numeral type for lost events. However if the channel loss is too high, this will lead to a high noise level. If the noise level is beyond what the protocol can tolerate, then it will have to be aborted and Alice and Bob have to restart. Each time they restart the protocol, Alice will have to start from the beginning. She cannot make use of the signals that Bob had received in their previous attempts. That is, she has to make new basis choices and a new choice of hashing function to encrypt her entire message. This is to ensure that any information that Eve had gained from the failed communication attempts cannot be used to eavesdrop on the current attempt.

Including the effects of loss, the joint state between Alice and Bob would be

$$\rho_{AB} = [|\Psi\rangle_{AB}\langle\Psi|_{AB}(1-\varepsilon)+\varepsilon]\,\eta + (1-\eta) \tag{10.1}$$

$$= |\Psi\rangle_{AB}\langle\Psi|_{AB}(1-\varepsilon)\eta + \varepsilon\eta + (1-\eta)\,, \tag{10.2}$$

where η is the channel transmission. The effective noise parameter would be $\varepsilon' = \varepsilon\eta + (1-\eta)$. We need this quantity to be less than the noise threshold of 0.155.

In the thesis, we investigated how much information Eve could potentially gain if she were to attack Alice. We can also repeat the analysis to see how much information she can gain if she attacks Bob instead. When Eve chooses to attack Bob, her input states are given at the end of section 5.3.3. But we do not expect Eve to learn more information from Bob then she can from Alice. This is because Alice publicly reveals her numeral type whilst Bob does not have to reveal anything. If this expectation is true, then the protocol will be more efficient if Alice and Bob were to do a direct communication version of reverse reconciliation.

Extension of the protocol to finite bit lengths also remains to be done. Typically the message that Alice wants to send would be of a relatively short length. The amount of data that is needed to characterise the channel up to some confidence may end up to be longer than the actual message itself. This question still needs to be addressed.

An experimental setup for the protocol was proposed in section 3.3. This uses two degrees of freedom of a single photon to encode a qubit-pair and the setup is relatively simple to implement. However the sensitivity of the protocol to losses

means that the detector efficiency is a critical factor for experiments. Detector efficiency refers to the fraction of photons registered to the number of photons impinging on the detector. To establish a secure key, the detection efficiency has to be at least $\eta = 0.845$. Avalanche photo diodes are the most commonly used detectors in quantum key distribution protocols. Good thick junction silicon single photon avalanche photo diodes have peak efficiency of around 0.7 near 800 nm, falling to 0.03 at 1064 nm [11,14]. Using superconducting transition edge sensors, better detection efficiencies of up to 0.95 at 1556 nm was achieved by Lita in 2008 [33, 44]. However, these detectors have slower count rates and need to be cooled to temperatures less than 100 mK.

Based on the above discussions, we can conclude that the direct communication protocol can already be implemented as a proof-of-principle type of experiment. However to be seriously considered as an alternative to key distribution protocols, we would need to wait for technological developments that lead to faster and more efficient photon detectors.

Appendices

Appendix A

Equivalence of Alice-prepares and Alice-measures protocols

In the original protocol, Alice prepares a state ρ_B and forwards this through a quantum channel $\mathcal{E}$ to Bob. The resulting state that Bob gets will be $\tilde{\rho}_B = \mathcal{E}(\rho_B)$.

In this appendix, we provide an explicit construction of this channel in terms of a pure state shared between Alice–Bob and Eve. Every input state to the channel would correspond to a POVM outcome for Alice. The output of the channel corresponds to the reduced state for Bob.

We describe the channel $\mathcal{E}$ as a unitary transformation U_{BE} acting on the input state ρ_B and an ancillary state $|e_1\rangle$. The output state $\mathcal{E}(\rho_B)$ is obtained by tracing out the ancillary subsystem at the end of the unitary evolution

$$\rho_B \to \tilde{\rho}_B \equiv \mathcal{E}(\rho_B) = \mathrm{Tr}_E \left\{ U_{BE} \left(\rho_B \otimes |e_1\rangle \langle e_1| \right) U_{BE}^{\dagger} \right\} . \tag{A.1}$$

The maximum dimension of the ancillary state $|e_1\rangle$ needed to specify an arbitrary channel is d^2, where d is the dimension of Hilbert space of the input states [39].

We can also write this in the Kraus representation

$$\rho_B \to \tilde{\rho}_B = \sum_k \underbrace{\langle e_k| U_{BE} |e_1\rangle}_{F_k^{(B)}} \rho_B \underbrace{\langle e_1| U_{BE}^\dagger |e_k\rangle}_{F_k^{(B)\dagger}} \tag{A.2}$$

$$= \sum_k F_k^{(B)} \rho_B F_k^{(B)\dagger} \tag{A.3}$$

where the vectors $|e_k\rangle$ extends $|e_1\rangle$ to an orthonormal basis. The operators $F_k^{(B)}$ are the Kraus operators satisfying

$$\sum_k F_k^{(B)\dagger} F_k^{(B)} = 1^{(B)} \tag{A.4}$$

which is a condition on the preservation of the trace of the output states. This representation is equivalent to specifying the action of the channel on a set of d^2 linearly independent state vectors (for example the SIC-POVM [41]).

The choice of basis vectors for Eve $|e_k\rangle$ for $k \in \{1,2,\ldots,d^2\}$ are arbitrary. We also specify an arbitrary set of d orthonormal basis vectors for Alice $|a_n\rangle$ and an arbitrary set for Bob $|b_m\rangle$ for $\{n,m\} \in \{1,2,\ldots,d\}$. In this basis, the Kraus operators have matrix elements

$$\langle b_n| F_k^{(B)} |b_m\rangle = \langle b_n, e_k| U_{BE} |b_m, e_1\rangle \ . \tag{A.5}$$

The matrix elements for the output state become

$$\langle b_n|\tilde{\rho}_B|b_m\rangle = \sum_k \sum_{m',n'} \langle b_n, e_k|U_{BE}|b_{m'}, e_1\rangle \langle b_{m'}|\rho_B|b_{n'}\rangle \langle b_{n'}, e_1|U_{BE}^\dagger|b_m, e_k\rangle \ . \tag{A.6}$$

The correspondence between the state that Alice prepares in the original protocol and the POVM outcome she projects onto is obtained via the pure maximally entangled state between Alice and Bob

$$|\Psi_{\text{true}}\rangle = \sum_n |a_n, b_n\rangle \frac{1}{\sqrt{d}} \ . \tag{A.7}$$

To prepare a state ρ_B, Alice projects onto the POVM outcome π_A such that

$$\rho_B = \text{Tr}_A\{(\pi_A \otimes 1_B)|\Psi_{\text{true}}\rangle\langle\Psi_{\text{true}}|\} \tag{A.8}$$

$$= \frac{1}{d}\sum_{n,m} \langle a_m|\pi_A|a_n\rangle |b_n\rangle\langle b_m| \tag{A.9}$$

or in terms of the matrix elements

$$\langle b_n|\rho_B|b_m\rangle = \frac{1}{d}\langle a_m|\pi_A|a_n\rangle \ . \tag{A.10}$$

At this point, we want to find the states $|E_{i,j}\rangle$ that correspond to a channel $\mathcal{E}$, such that for every ρ_B, the output δ_B

$$\delta_B \equiv \text{Tr}_A\{(\pi_A \otimes 1_{BE})|\Psi\rangle\langle\Psi|\} = \mathcal{E}(\rho_B) \tag{A.11}$$

is the same as the output of $\mathcal{E}$, where

$$|\Psi\rangle = \sum_{n,m} |a_n, b_m\rangle \, |E_{n,m}\rangle \tag{A.12}$$

and

$$\pi_a = d \sum_{n,m} |a_m\rangle \langle b_n| \, \rho_B \, |b_m\rangle \langle a_n| \ . \tag{A.13}$$

The output state δ_B is

$$\begin{aligned}
\delta_B &= \mathrm{Tr}_A \left\{ (\pi_A \otimes 1_{BE}) \, |\Psi\rangle \langle\Psi| \right\} && \text{(A.14)} \\
&= \sum_{\substack{n,n' \\ m,m'}} \langle a_{n'}| \, \pi_A \, |a_n\rangle \left\langle E_{n',m'} \middle| E_{n,m} \right\rangle |b_m\rangle \langle b_{m'}| && \text{(A.15)} \\
&= d \sum_{\substack{n,n' \\ m,m'}} \langle b_n| \, \rho_B \, |a_{n'}\rangle \left\langle E_{n',m'} \middle| E_{n,m} \right\rangle |b_m\rangle \langle b_{m'}| && \text{(A.16)}
\end{aligned}$$

which have matrix elements

$$\begin{aligned}
\langle b_m| \, \delta_B \, |b_{m'}\rangle &= d \sum_{n,n'} \langle b_n| \, \rho_B \, |a_{n'}\rangle \left\langle E_{n',m'} \middle| E_{n,m} \right\rangle && \text{(A.17)} \\
&= d \sum_k \sum_{n,n'} \langle b_n| \, \rho_B \, |a_{n'}\rangle \left\langle E_{n',m'} \middle| e_k \right\rangle \left\langle e_k \middle| E_{n,m} \right\rangle && \text{(A.18)} \\
&= \sum_k \sum_{n,n'} \sqrt{d} \left\langle e_k \middle| E_{n,m} \right\rangle \langle b_n| \, \rho_B \, |a_{n'}\rangle \left\langle E_{n',m'} \middle| e_k \right\rangle \sqrt{d} \ . && \text{(A.19)}
\end{aligned}$$

Comparing this with the matrix elements of the output of the channel described by U_{BE} in (A.6), we see that by choosing

$$\sqrt{d}\langle e_k|E_{n,m}\rangle = \langle b_m, e_k| U_{BE} |b_n, e_1\rangle \tag{A.20}$$

$$\implies |E_{n,m}\rangle = \frac{1}{\sqrt{d}} \sum_k |e_k\rangle \langle b_m, e_k| U_{BE} |b_n, e_1\rangle \tag{A.21}$$

we get the two outputs to be the same: $\delta_B = \tilde{\rho}_B$.

Appendix B

The constraints

This appendix lists out the 64 constraints on the inner products between Eve's probe states after choosing the basis as in chapter 7. Of these 64 constraints, only 49 of them are independent.

B.1 Short constraints

The 16 short constraints are obtained when both Alice and Bob measure in the plus basis. They are

$$\begin{aligned}
\langle E_{1,1}|E_{1,1}\rangle &= \frac{4-3\varepsilon}{16}\,,\\
\langle E_{1,2}|E_{1,2}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{1,3}|E_{1,3}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{1,4}|E_{1,4}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{2,1}|E_{2,1}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{2,2}|E_{2,2}\rangle &= \frac{4-3\varepsilon}{16}\,,\\
\langle E_{2,3}|E_{2,3}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{2,4}|E_{2,4}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{3,1}|E_{3,1}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{3,2}|E_{3,2}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{3,3}|E_{3,3}\rangle &= \frac{4-3\varepsilon}{16}\,,\\
\langle E_{3,4}|E_{3,4}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{4,1}|E_{4,1}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{4,2}|E_{4,2}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{4,3}|E_{4,3}\rangle &= \frac{\varepsilon}{16}\,,\\
\langle E_{4,4}|E_{4,4}\rangle &= \frac{4-3\varepsilon}{16}\,.
\end{aligned}$$

B.2 Medium constraints

There are 32 medium constraints. Sixteen of them are from the cases when Alice measures in the plus basis while Bob measures in the minus basis. These are

$$
\begin{aligned}
&\mathrm{Re}\langle E_{1,2}|E_{1,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{1,4}\rangle + \mathrm{Re}\langle E_{1,3}|E_{1,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,1}|E_{1,3}\rangle - \mathrm{Re}\langle E_{1,1}|E_{1,4}\rangle + \mathrm{Re}\langle E_{1,3}|E_{1,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,1}|E_{1,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{1,4}\rangle - \mathrm{Re}\langle E_{1,2}|E_{1,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,1}|E_{1,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{1,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{1,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,2}|E_{2,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{2,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{2,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,1}|E_{2,3}\rangle - \mathrm{Re}\langle E_{2,1}|E_{2,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{2,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,1}|E_{2,2}\rangle - \mathrm{Re}\langle E_{2,1}|E_{2,4}\rangle - \mathrm{Re}\langle E_{2,2}|E_{2,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,1}|E_{2,2}\rangle - \mathrm{Re}\langle E_{2,1}|E_{2,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{2,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{3,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{3,2}|E_{3,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{3,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{3,1}|E_{3,3}\rangle - \mathrm{Re}\langle E_{3,1}|E_{3,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{3,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{3,1}|E_{3,2}\rangle - \mathrm{Re}\langle E_{3,1}|E_{3,4}\rangle - \mathrm{Re}\langle E_{3,2}|E_{3,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{3,1}|E_{3,2}\rangle - \mathrm{Re}\langle E_{3,1}|E_{3,3}\rangle + \mathrm{Re}\langle E_{3,2}|E_{3,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{4,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{4,2}|E_{4,4}\rangle + \mathrm{Re}\langle E_{4,3}|E_{4,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{4,1}|E_{4,3}\rangle - \mathrm{Re}\langle E_{4,1}|E_{4,4}\rangle + \mathrm{Re}\langle E_{4,3}|E_{4,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{4,1}|E_{4,2}\rangle - \mathrm{Re}\langle E_{4,1}|E_{4,4}\rangle - \mathrm{Re}\langle E_{4,2}|E_{4,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{4,1}|E_{4,2}\rangle - \mathrm{Re}\langle E_{4,1}|E_{4,3}\rangle + \mathrm{Re}\langle E_{4,2}|E_{4,3}\rangle = 0\,.
\end{aligned}
$$

Note that not all of the above equations are independent. For example, every fourth equation can be obtained from the previous three.

The remaining 16 medium constraints are obtained from the cases when Alice measures in the minus basis and Bob measures in the plus basis. These are

$$\begin{aligned}
&\mathrm{Re}\langle E_{2,1}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,1}|E_{4,1}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,2}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,2}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,3}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,3}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{2,4}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,1}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,1}|E_{4,1}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,2}|E_{3,2}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,2}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,3}|E_{3,3}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,3}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,4}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,4}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,1}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,1}\rangle - \mathrm{Re}\langle E_{2,1}|E_{4,1}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,2}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,2}\rangle - \mathrm{Re}\langle E_{2,2}|E_{4,2}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,3}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,3}\rangle - \mathrm{Re}\langle E_{2,3}|E_{4,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,4}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,4}|E_{4,4}\rangle - \mathrm{Re}\langle E_{2,4}|E_{4,4}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,1}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,1}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,1}|E_{3,1}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,2}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,2}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,3}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,3}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,3}\rangle = 0\,,\\
&\mathrm{Re}\langle E_{1,4}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,4}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,4}|E_{3,4}\rangle = 0\,.
\end{aligned}$$

The last four equations can be obtained from the first twelve. There are altogether 24 independent equations from the medium constraints.

B.3 Long constraints

Finally the 16 long constraints are obtained when both Alice and Bob measure in the minus basis. These are

$$\begin{aligned}
&\mathrm{Re}\langle E_{2,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,3}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,4}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{3,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{3,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,3}\rangle = \frac{3-3\varepsilon}{4}\,, \\
&\mathrm{Re}\langle E_{2,1}|E_{3,3}\rangle - \mathrm{Re}\langle E_{2,1}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,3}\rangle - \mathrm{Re}\langle E_{2,1}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,3}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{2,4}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,4}|E_{3,3}\rangle - \mathrm{Re}\langle E_{2,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{3,1}|E_{4,3}\rangle - \mathrm{Re}\langle E_{3,1}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{3,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,3}\rangle = \frac{1-\varepsilon}{4}\,, \\
&-\mathrm{Re}\langle E_{2,1}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,1}|E_{3,4}\rangle - \mathrm{Re}\langle E_{2,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{2,2}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,4}\rangle - \mathrm{Re}\langle E_{2,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,4}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,2}\rangle \\
&-\mathrm{Re}\langle E_{3,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,1}|E_{4,4}\rangle - \mathrm{Re}\langle E_{3,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{3,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,2}\rangle = \frac{1-\varepsilon}{4}\,, \\
&\mathrm{Re}\langle E_{2,1}|E_{3,2}\rangle - \mathrm{Re}\langle E_{2,1}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,2}\rangle - \mathrm{Re}\langle E_{2,1}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{2,2}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,3}\rangle \\
&-\mathrm{Re}\langle E_{2,3}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,2}\rangle - \mathrm{Re}\langle E_{2,3}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,2}\rangle \\
&+\mathrm{Re}\langle E_{3,1}|E_{4,2}\rangle - \mathrm{Re}\langle E_{3,1}|E_{4,3}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,3}\rangle \\
&-\mathrm{Re}\langle E_{3,3}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,2}\rangle = \frac{1-\varepsilon}{4}\,,
\end{aligned}$$

$$
\begin{aligned}
&\mathrm{Re}\langle E_{1,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,3}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{1,3}|E_{3,2}\rangle + \mathrm{Re}\langle E_{1,3}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,2}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{1,4}|E_{3,2}\rangle + \mathrm{Re}\langle E_{1,4}|E_{3,3}\rangle - \mathrm{Re}\langle E_{1,4}|E_{4,2}\rangle - \mathrm{Re}\langle E_{1,4}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{3,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{3,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,3}\rangle = \frac{1-\varepsilon}{4}\,, \\
&\mathrm{Re}\langle E_{1,1}|E_{3,3}\rangle - \mathrm{Re}\langle E_{1,1}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,3}\rangle + \mathrm{Re}\langle E_{1,1}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{1,3}|E_{3,1}\rangle + \mathrm{Re}\langle E_{1,3}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,1}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{1,4}|E_{3,1}\rangle + \mathrm{Re}\langle E_{1,4}|E_{3,3}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,1}\rangle - \mathrm{Re}\langle E_{1,4}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{3,1}|E_{4,3}\rangle - \mathrm{Re}\langle E_{3,1}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,3}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{3,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{3,4}|E_{4,3}\rangle = \frac{3-3\varepsilon}{4}\,, \\
&\mathrm{Re}\langle E_{1,1}|E_{3,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{1,1}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{1,2}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,4}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{1,2}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{1,4}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,4}|E_{3,2}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,2}\rangle \\
&+\mathrm{Re}\langle E_{3,1}|E_{4,2}\rangle - \mathrm{Re}\langle E_{3,1}|E_{4,4}\rangle + \mathrm{Re}\langle E_{3,2}|E_{4,1}\rangle - \mathrm{Re}\langle E_{3,2}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{3,4}|E_{4,1}\rangle - \mathrm{Re}\langle E_{3,4}|E_{4,2}\rangle = \frac{1-\varepsilon}{4}\,, \\
&-\mathrm{Re}\langle E_{1,1}|E_{3,2}\rangle + \mathrm{Re}\langle E_{1,1}|E_{3,3}\rangle + \mathrm{Re}\langle E_{1,1}|E_{4,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,3}\rangle \\
&-\mathrm{Re}\langle E_{1,2}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{1,2}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{1,3}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,3}|E_{3,2}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,1}\rangle + \mathrm{Re}\langle E_{1,3}|E_{4,2}\rangle \\
&-\mathrm{Re}\langle E_{3,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{3,1}|E_{4,3}\rangle - \mathrm{Re}\langle E_{3,2}|E_{4,1}\rangle - \mathrm{Re}\langle E_{3,2}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{3,3}|E_{4,1}\rangle - \mathrm{Re}\langle E_{3,3}|E_{4,2}\rangle = \frac{1-\varepsilon}{4}\,,
\end{aligned}
$$

$$
\begin{aligned}
&-\mathrm{Re}\langle E_{1,2}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,2}|E_{2,4}\rangle + \mathrm{Re}\langle E_{1,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{1,3}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,3}|E_{2,4}\rangle + \mathrm{Re}\langle E_{1,3}|E_{4,2}\rangle + \mathrm{Re}\langle E_{1,3}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{1,4}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,4}|E_{2,3}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{2,2}|E_{4,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,3}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,3}\rangle = \frac{1-\varepsilon}{4}\,,
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Re}\langle E_{1,1}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,1}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,3}\rangle + \mathrm{Re}\langle E_{1,1}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{1,3}|E_{2,1}\rangle + \mathrm{Re}\langle E_{1,3}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,1}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{1,4}|E_{2,1}\rangle + \mathrm{Re}\langle E_{1,4}|E_{2,3}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,1}\rangle - \mathrm{Re}\langle E_{1,4}|E_{4,3}\rangle \\
&-\mathrm{Re}\langle E_{2,1}|E_{4,3}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,4}\rangle - \mathrm{Re}\langle E_{2,3}|E_{4,1}\rangle - \mathrm{Re}\langle E_{2,3}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{4,1}\rangle - \mathrm{Re}\langle E_{2,4}|E_{4,3}\rangle = \frac{1-\varepsilon}{4}\,,
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Re}\langle E_{1,1}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{1,1}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{1,2}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,2}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{1,2}|E_{4,4}\rangle \\
&-\mathrm{Re}\langle E_{1,4}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,4}|E_{2,2}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{1,4}|E_{4,2}\rangle \\
&-\mathrm{Re}\langle E_{2,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,4}\rangle - \mathrm{Re}\langle E_{2,2}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,2}|E_{4,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{4,1}\rangle + \mathrm{Re}\langle E_{2,4}|E_{4,2}\rangle = \frac{3-3\varepsilon}{4}\,,
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Re}\langle E_{1,1}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{1,1}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{1,2}|E_{2,1}\rangle + \mathrm{Re}\langle E_{1,2}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,1}\rangle - \mathrm{Re}\langle E_{1,2}|E_{4,3}\rangle \\
&-\mathrm{Re}\langle E_{1,3}|E_{2,1}\rangle + \mathrm{Re}\langle E_{1,3}|E_{2,2}\rangle + \mathrm{Re}\langle E_{1,3}|E_{4,1}\rangle - \mathrm{Re}\langle E_{1,3}|E_{4,2}\rangle \\
&-\mathrm{Re}\langle E_{2,1}|E_{4,2}\rangle + \mathrm{Re}\langle E_{2,1}|E_{4,3}\rangle - \mathrm{Re}\langle E_{2,2}|E_{4,1}\rangle - \mathrm{Re}\langle E_{2,2}|E_{4,3}\rangle \\
&+\mathrm{Re}\langle E_{2,3}|E_{4,1}\rangle - \mathrm{Re}\langle E_{2,3}|E_{4,2}\rangle = \frac{1-\varepsilon}{4}\,,
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Re}\langle E_{1,2}|E_{2,3}\rangle + \mathrm{Re}\langle E_{1,2}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,3}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,4}\rangle \\
&+\mathrm{Re}\langle E_{1,3}|E_{2,2}\rangle + \mathrm{Re}\langle E_{1,3}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,3}|E_{3,2}\rangle - \mathrm{Re}\langle E_{1,3}|E_{3,4}\rangle \\
&+\mathrm{Re}\langle E_{1,4}|E_{2,2}\rangle + \mathrm{Re}\langle E_{1,4}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,4}|E_{3,2}\rangle - \mathrm{Re}\langle E_{1,4}|E_{3,3}\rangle \\
&+\mathrm{Re}\langle E_{2,2}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{3,2}\rangle + \mathrm{Re}\langle E_{2,4}|E_{3,3}\rangle = \frac{1-\varepsilon}{4}\,, \\
&-\mathrm{Re}\langle E_{1,1}|E_{2,3}\rangle + \mathrm{Re}\langle E_{1,1}|E_{2,4}\rangle + \mathrm{Re}\langle E_{1,1}|E_{3,3}\rangle - \mathrm{Re}\langle E_{1,1}|E_{3,4}\rangle \\
&-\mathrm{Re}\langle E_{1,3}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,3}|E_{2,4}\rangle + \mathrm{Re}\langle E_{1,3}|E_{3,1}\rangle + \mathrm{Re}\langle E_{1,3}|E_{3,4}\rangle \\
&+\mathrm{Re}\langle E_{1,4}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,4}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,4}|E_{3,1}\rangle + \mathrm{Re}\langle E_{1,4}|E_{3,3}\rangle \\
&-\mathrm{Re}\langle E_{2,1}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,1}|E_{3,4}\rangle - \mathrm{Re}\langle E_{2,3}|E_{3,1}\rangle - \mathrm{Re}\langle E_{2,3}|E_{3,4}\rangle \\
&+\mathrm{Re}\langle E_{2,4}|E_{3,1}\rangle - \mathrm{Re}\langle E_{2,4}|E_{3,3}\rangle = \frac{1-\varepsilon}{4}\,, \\
&\mathrm{Re}\langle E_{1,1}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,1}|E_{3,2}\rangle + \mathrm{Re}\langle E_{1,1}|E_{3,4}\rangle \\
&+\mathrm{Re}\langle E_{1,2}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,2}|E_{2,4}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,1}\rangle + \mathrm{Re}\langle E_{1,2}|E_{3,4}\rangle \\
&-\mathrm{Re}\langle E_{1,4}|E_{2,1}\rangle - \mathrm{Re}\langle E_{1,4}|E_{2,2}\rangle + \mathrm{Re}\langle E_{1,4}|E_{3,1}\rangle + \mathrm{Re}\langle E_{1,4}|E_{3,2}\rangle \\
&+\mathrm{Re}\langle E_{2,1}|E_{3,2}\rangle - \mathrm{Re}\langle E_{2,1}|E_{3,4}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,1}\rangle - \mathrm{Re}\langle E_{2,2}|E_{3,4}\rangle \\
&-\mathrm{Re}\langle E_{2,4}|E_{3,1}\rangle - \mathrm{Re}\langle E_{2,4}|E_{3,2}\rangle = \frac{1-\varepsilon}{4}\,, \\
&\mathrm{Re}\langle E_{1,1}|E_{2,2}\rangle - \mathrm{Re}\langle E_{1,1}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,1}|E_{3,2}\rangle + \mathrm{Re}\langle E_{1,1}|E_{3,3}\rangle \\
&+\mathrm{Re}\langle E_{1,2}|E_{2,1}\rangle + \mathrm{Re}\langle E_{1,2}|E_{2,3}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,2}|E_{3,3}\rangle \\
&-\mathrm{Re}\langle E_{1,3}|E_{2,1}\rangle + \mathrm{Re}\langle E_{1,3}|E_{2,2}\rangle + \mathrm{Re}\langle E_{1,3}|E_{3,1}\rangle - \mathrm{Re}\langle E_{1,3}|E_{3,2}\rangle \\
&+\mathrm{Re}\langle E_{2,1}|E_{3,2}\rangle - \mathrm{Re}\langle E_{2,1}|E_{3,3}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,2}|E_{3,3}\rangle \\
&-\mathrm{Re}\langle E_{2,3}|E_{3,1}\rangle + \mathrm{Re}\langle E_{2,3}|E_{3,2}\rangle = \frac{3-3\varepsilon}{4}\,.
\end{aligned}
$$

Out of these 16 equations, seven are redundant and only nine are independent.

Appendix C

Schmidt decomposition of Eve's attack

In this appendix we will find the Schmidt decomposition of the pure state between Alice–Bob and Eve after imposing the constraints in chapter 9. With those constraints, the matrix representation for Eve's total state $\mathcal{X}\mathcal{X}^\dagger$ can be fully diagonalised. In fact, we find the reduced state between Alice and Bob is fixed up to its eigenvalues.

We recap that Eve's attack is defined by her purification

$$|\Psi\rangle_{ABE} = \sum_{I=1}^{16} |AB_I\rangle\,|E_I\rangle \tag{C.1}$$

where we chose $|AB_I\rangle$ to be the tensor products of the plus basis between Alice and Bob

$$\begin{aligned} |AB_1\rangle &= |1+\rangle_A \otimes |1+\rangle_B \ , \\ |AB_2\rangle &= |1+\rangle_A \otimes |2+\rangle_B \ , \\ |AB_3\rangle &= |1+\rangle_A \otimes |3+\rangle_B \ , \\ &\vdots \\ |AB_{16}\rangle &= |4+\rangle_A \otimes |4+\rangle_B \ . \end{aligned} \tag{C.2}$$

The kets $|E_I\rangle$ are fixed, up to a unitary transformation, by Eve's strategy. However the inner products between the kets are uniquely fixed by her strategy. After imposing the symmetry constraints, we find that the inner products are parametrised by five parameters which we call x_1, x_2, x_3, x_4 and x_5. The entries for the matrix

which we called $\mathcal{X}^\dagger\mathcal{X}$ are given by the 16 by 16 inner products

$$\langle E_I | E_J \rangle =$$

$$\begin{pmatrix}
a & \cdot & \cdot & \cdot & \cdot & x_1 & \bar{x}_3 & \bar{x}_3 & \cdot & \bar{x}_3 & x_1 & \bar{x}_3 & \cdot & \bar{x}_3 & \bar{x}_3 & x_1 \\
\cdot & b & \cdot & \cdot & x_2 & \cdot & x_4 & \bar{x}_4 & \bar{x}_4 & \cdot & \bar{x}_3 & x_5 & \bar{x}_4 & \cdot & \bar{x}_5 & x_3 \\
\cdot & \cdot & b & \cdot & \bar{x}_4 & x_3 & \cdot & \bar{x}_5 & x_2 & \bar{x}_4 & \cdot & x_4 & \bar{x}_4 & x_5 & \cdot & \bar{x}_3 \\
\cdot & \cdot & \cdot & b & \bar{x}_4 & \bar{x}_3 & x_5 & \cdot & \bar{x}_4 & \bar{x}_5 & x_3 & \cdot & x_2 & x_4 & \bar{x}_4 & \cdot \\
\cdot & x_2 & \bar{x}_4 & \bar{x}_4 & b & \cdot & \cdot & \cdot & \cdot & x_4 & \bar{x}_3 & \bar{x}_5 & \cdot & \bar{x}_4 & x_5 & x_3 \\
x_1 & \cdot & x_3 & \bar{x}_3 & \cdot & a & \cdot & \cdot & x_3 & \cdot & x_1 & x_3 & \bar{x}_3 & \cdot & x_3 & x_1 \\
\bar{x}_3 & x_4 & \cdot & x_5 & \cdot & \cdot & b & \cdot & \bar{x}_4 & x_2 & \cdot & x_4 & \bar{x}_5 & x_4 & \cdot & x_3 \\
\bar{x}_3 & \bar{x}_4 & \bar{x}_5 & \cdot & \cdot & \cdot & \cdot & b & x_5 & x_4 & x_3 & \cdot & x_4 & x_2 & x_4 & \cdot \\
\cdot & \bar{x}_4 & x_2 & \bar{x}_4 & \cdot & x_3 & \bar{x}_4 & x_5 & b & \cdot & \cdot & \cdot & \cdot & \bar{x}_5 & x_4 & \bar{x}_3 \\
\bar{x}_3 & \cdot & \bar{x}_4 & \bar{x}_5 & x_4 & \cdot & x_2 & x_4 & \cdot & b & \cdot & \cdot & x_5 & \cdot & x_4 & x_3 \\
x_1 & \bar{x}_3 & \cdot & x_3 & \bar{x}_3 & x_1 & \cdot & x_3 & \cdot & \cdot & a & \cdot & x_3 & x_3 & \cdot & x_1 \\
\bar{x}_3 & x_5 & x_4 & \cdot & \bar{x}_5 & x_3 & x_4 & \cdot & \cdot & \cdot & \cdot & b & \bar{x}_4 & x_4 & x_2 & \cdot \\
\cdot & \bar{x}_4 & \bar{x}_4 & x_2 & \cdot & \bar{x}_3 & \bar{x}_5 & x_4 & \cdot & x_5 & x_3 & \bar{x}_4 & b & \cdot & \cdot & \cdot \\
\bar{x}_3 & \cdot & x_5 & x_4 & \bar{x}_4 & \cdot & x_4 & x_2 & \bar{x}_5 & \cdot & x_3 & x_4 & \cdot & b & \cdot & \cdot \\
\bar{x}_3 & \bar{x}_5 & \cdot & \bar{x}_4 & x_5 & x_3 & \cdot & x_4 & x_4 & x_4 & \cdot & x_2 & \cdot & \cdot & b & \cdot \\
x_1 & x_3 & \bar{x}_3 & \cdot & x_3 & x_1 & x_3 & \cdot & \bar{x}_3 & x_3 & x_1 & \cdot & \cdot & \cdot & \cdot & a
\end{pmatrix}_{I,J}$$

where $\bar{x}$ denotes the negative of x and the dots are zeros. The magnitudes $a = (4-3\varepsilon)/16$ and $b = \varepsilon/16$. Not all five parameters are independent. They are related by the sum

$$x_1 + x_2 + 2x_3 + 2x_4 = \frac{1-\varepsilon}{4}. \tag{C.3}$$

The eigenvectors of this simplified matrix does not depend on any of the parameters or on the noise level ε. The 16 eigenvectors (up to a normalisation constant)

are given by the columns of the following matrix

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & \bar{1} & 0 & \bar{1} & 1 & 0 & 0 & 0 & 1 & 1 & 2 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & \bar{1} & 0 & \bar{1} & 1 & 1 & 0 & 0 & 1 & \bar{1} & 1 \\
0 & 1 & 0 & 1 & \bar{1} & 0 & 1 & 1 & 0 & \bar{1} & 0 & 1 & 0 & 1 & \bar{1} & \bar{1} \\
0 & 1 & 1 & 0 & 1 & \bar{1} & 0 & \bar{1} & 1 & 0 & 0 & 0 & \bar{1} & \bar{1} & \bar{2} & 0 \\
1 & 0 & 0 & 0 & \bar{1} & \bar{1} & 1 & \bar{2} & \bar{2} & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \bar{1} & 0 & 1 & 1 & 0 & 1 & \bar{1} & 0 & \bar{1} & 0 & \bar{1} & 0 & 1 & \bar{1} & \bar{1} \\
0 & 0 & 1 & \bar{1} & 0 & 1 & 1 & 0 & \bar{1} & \bar{1} & 1 & 0 & 0 & \bar{1} & 1 & \bar{1} \\
0 & 0 & 1 & 1 & 0 & 1 & \bar{1} & 0 & \bar{1} & 1 & \bar{1} & 0 & 0 & \bar{1} & 1 & \bar{1} \\
0 & \bar{1} & 0 & 1 & 1 & 0 & 1 & \bar{1} & 0 & \bar{1} & 0 & 1 & 0 & \bar{1} & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & \bar{1} & \bar{1} & 2 & \bar{2} & \bar{2} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & \bar{1} & 0 & 1 & 1 & 0 & \bar{1} & \bar{1} & 0 & 0 & 0 & \bar{1} & 1 & 2 & 0 \\
0 & 1 & 0 & 1 & \bar{1} & 0 & 1 & 1 & 0 & \bar{1} & 0 & \bar{1} & 0 & \bar{1} & 1 & 1 \\
0 & 0 & 1 & \bar{1} & 0 & 1 & 1 & 0 & \bar{1} & \bar{1} & \bar{1} & 0 & 0 & 1 & \bar{1} & 1 \\
0 & 1 & \bar{1} & 0 & 1 & 1 & 0 & \bar{1} & \bar{1} & 0 & 0 & 0 & 1 & \bar{1} & \bar{2} & 0 \\
1 & 0 & 0 & 0 & \bar{1} & 1 & \bar{1} & \bar{2} & 2 & \bar{2} & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

The corresponding eigenvalues are

$$\begin{aligned}
\mu_1 &= \frac{1}{16}\left(16-15\varepsilon-48x_2-96x_3-96x_4\right)\ , \\
\mu_{2,3,4} &= \frac{1}{16}\left(\varepsilon+16x_2-32x_4\right)\ , \\
\mu_{5,6,7} &= \frac{1}{16}\left(\varepsilon+16x_2-32x_3+32x_4\right)\ , \\
\mu_{8,9,10} &= \frac{1}{16}\left(\varepsilon+16x_2+64x_3+32x_4\right)\ , \\
\mu_{11,12,13} &= \frac{1}{16}\left(\varepsilon-16x_2-32x_5\right)\ , \\
\mu_{14} &= \frac{1}{16}\left(\varepsilon-16x_2+64x_4+32x_5\right)\ , \\
\mu_{15,16} &= \frac{1}{16}\left(\varepsilon-16x_2-32x_4+32x_5\right)\ .
\end{aligned} \tag{C.4}$$

Having diagonalised $\mathcal{X}^\dagger\mathcal{X}$, it is now easy to write the Schmidt decomposition of $|\Psi\rangle_{ABE}$ between Alice–Bob and Eve.

C.1 Schmidt basis of Alice–Bob

We begin by the singular value decomposition of $\mathcal{X}^\dagger\mathcal{X}$ as

$$\left\langle E_J\middle|E_K\right\rangle = \left(\mathcal{X}^\dagger\mathcal{X}\right)_{J,K} = \sum_{N=1}^{16}\phi^*_{N,J}\mu_N\phi_{N,K} \tag{C.5}$$

where ϕ are the orthonormal eigenvectors of $\mathcal{X}^\dagger\mathcal{X}$

$$\sum_{J=1}^{16}\phi_{N,J}\phi^*_{M,J} = \delta_{N,M} \tag{C.6}$$

and

$$\sum_{K=1}^{16}\left(\mathcal{X}^{\dagger}\mathcal{X}\right)_{J,K}\phi^{*}_{M,K} = \sum_{N,K=1}^{16}\phi^{*}_{N,J}\mu_N\phi_{N,K}\phi^{*}_{M,K} \tag{C.7}$$

$$= \sum_{N=1}^{16}\phi^{*}_{N,J}\mu_N\delta_{N,M} \tag{C.8}$$

$$= \phi^{*}_{M,J}\mu_M\,. \tag{C.9}$$

Next, we introduce an orthonormal basis $|F_N\rangle$ so that

$$\langle F_N|E_K\rangle = \mathcal{X}_{N,K} = \sqrt{\mu_N}\phi_{N,K} \tag{C.10}$$

or equivalently

$$|F_N\rangle = \sum_{K=1}^{16}|E_K\rangle\,\frac{\phi^{*}_{N,K}}{\sqrt{\mu_N}}\,. \tag{C.11}$$

With this, we can write $|E_K\rangle$ in the $|F_N\rangle$ basis as

$$|E_K\rangle = \sum_{N=1}^{16}|F_N\rangle\,\phi_{N,K}\sqrt{\mu_N}\,, \tag{C.12}$$

so that the pure state between Alice–Bob and Eve becomes

$$|\Psi\rangle_{ABE} = \sum_{K=1}^{16}|AB_K\rangle\,|E_K\rangle \tag{C.13}$$

$$= \sum_{K,N=1}^{16}|AB_K\rangle\,|F_N\rangle\,\sqrt{\mu_N}\phi_{N,K} \tag{C.14}$$

$$= \sum_{N=1}^{16}|\alpha_N\rangle\,|F_N\rangle\,\sqrt{\mu_N}\,, \tag{C.15}$$

where we define the Schmidt basis $|\alpha_N\rangle$ as

$$|\alpha_N\rangle = \sum_{K=1}^{16} |AB_K\rangle \, \phi_{N,K} \, . \tag{C.16}$$

They form an orthonormal basis for Alice–Bob

$$\langle \alpha_N | \alpha_M \rangle = \sum_{K,K'=1}^{16} \langle AB_{K'} | AB_K \rangle \phi^*_{N,K'} \phi_{M,K} \tag{C.17}$$

$$= \sum_{K=1}^{16} \phi^*_{N,K} \phi_{M,K} \tag{C.18}$$

$$= \delta_{N,M} \, . \tag{C.19}$$

Equation (C.15) provides the Schmidt decomposition of Eve's pure state between Alice–Bob and Eve. The Schmidt vectors $|\alpha_N\rangle$ can be obtained from the eigenvectors of $\mathcal{X}^\dagger \mathcal{X}$ in equation (C.4). For example $|\alpha_1\rangle$ corresponding to the eigenvalue μ_1 would be

$$|\alpha_1\rangle = |1+,1+\rangle + |2+,2+\rangle + |3+,3+\rangle + |4+,4+\rangle \, . \tag{C.20}$$

We can also write this state in the Bell basis: $|\psi_i\rangle_{AB1} \otimes |\psi_j\rangle_{AB2}$. Here $|\psi_i\rangle_{AB1}$ are the Bell basis for Alice's first qubit and Bob's first qubit and the Bell basis are

defined as

$$\begin{aligned}
|\psi_1\rangle &= (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)\,\frac{1}{\sqrt{2}}\,, \\
|\psi_2\rangle &= (|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle)\,\frac{1}{\sqrt{2}}\,, \\
|\psi_3\rangle &= (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)\,\frac{1}{\sqrt{2}}\,, \\
|\psi_4\rangle &= (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)\,\frac{1}{\sqrt{2}}\,,
\end{aligned} \tag{C.21}$$

where the kets $|\uparrow\rangle$ and $|\downarrow\rangle$ are the computational basis.

If we identify the plus basis as a two-qubit state in the computational basis with

$$\begin{aligned}
|1+\rangle &= |\uparrow\uparrow\rangle\,, \\
|2+\rangle &= |\uparrow\downarrow\rangle\,, \\
|3+\rangle &= |\downarrow\uparrow\rangle\,, \\
|4+\rangle &= |\downarrow\downarrow\rangle
\end{aligned} \tag{C.22}$$

then the Schmidt basis for Alice–Bob becomes

$$
\begin{aligned}
|\alpha_1\rangle &= |\psi_1,\psi_1\rangle \ , \\
|\alpha_2\rangle &= |\psi_1,\psi_3\rangle \frac{1}{\sqrt{2}} + |\psi_4,\psi_4\rangle \frac{1}{\sqrt{2}} \ , \\
|\alpha_3\rangle &= |\psi_2,\psi_3\rangle \frac{1}{\sqrt{2}} + |\psi_3,\psi_1\rangle \frac{1}{\sqrt{2}} \ , \\
|\alpha_4\rangle &= |\psi_3,\psi_2\rangle \frac{1}{\sqrt{2}} + |\psi_3,\psi_3\rangle \frac{1}{\sqrt{2}} \ , \\
|\alpha_5\rangle &= |\psi_1,\psi_2\rangle \frac{1}{\sqrt{3}} + |\psi_1,\psi_3\rangle \frac{1}{\sqrt{3}} - |\psi_4,\psi_4\rangle \frac{1}{\sqrt{3}} \ , \\
|\alpha_6\rangle &= |\psi_2,\psi_2\rangle \frac{1}{\sqrt{3}} - |\psi_2,\psi_3\rangle \frac{1}{\sqrt{3}} + |\psi_3,\psi_1\rangle \frac{1}{\sqrt{3}} \ , \\
|\alpha_7\rangle &= |\psi_2,\psi_1\rangle \frac{1}{\sqrt{3}} - |\psi_3,\psi_2\rangle \frac{1}{\sqrt{3}} + |\psi_3,\psi_3\rangle \frac{1}{\sqrt{3}} \ , \\
|\alpha_8\rangle &= |\psi_1,\psi_2\rangle \sqrt{\frac{2}{3}} - |\psi_1,\psi_3\rangle \frac{1}{\sqrt{6}} + |\psi_4,\psi_4\rangle \frac{1}{\sqrt{6}} \\
|\alpha_9\rangle &= |\psi_2,\psi_2\rangle \sqrt{\frac{2}{3}} + |\psi_2,\psi_3\rangle \frac{1}{\sqrt{6}} - |\psi_3,\psi_1\rangle \frac{1}{\sqrt{6}} \ , \\
|\alpha_{10}\rangle &= |\psi_2,\psi_1\rangle \sqrt{\frac{2}{3}} + |\psi_3,\psi_2\rangle \frac{1}{\sqrt{6}} - |\psi_3,\psi_3\rangle \frac{1}{\sqrt{6}} \ , \\
|\alpha_{11}\rangle &= |\psi_4,\psi_1\rangle \ , \\
|\alpha_{12}\rangle &= |\psi_3,\psi_4\rangle \ , \\
|\alpha_{13}\rangle &= |\psi_2,\psi_4\rangle \ , \\
|\alpha_{14}\rangle &= |\psi_1,\psi_4\rangle \frac{1}{\sqrt{3}} + |\psi_4,\psi_2\rangle \frac{1}{\sqrt{3}} + |\psi_4,\psi_3\rangle \frac{1}{\sqrt{3}} \ , \\
|\alpha_{15}\rangle &= \sqrt{\frac{2}{3}}\,|\psi_1,\psi_4\rangle - |\psi_4,\psi_2\rangle \frac{1}{\sqrt{6}} - |\psi_4,\psi_3\rangle \frac{1}{\sqrt{6}} \ , \\
|\alpha_{16}\rangle &= |\psi_4,\psi_2\rangle \frac{1}{\sqrt{2}} - |\psi_4,\psi_3\rangle \frac{1}{\sqrt{2}} \ .
\end{aligned}
\tag{C.23}
$$

Appendix D

Random processing before measurement

In this appendix, we show how the optimisation problem for Eve's information can be simplified if we let Alice and Bob perform some random processing on their two-qubits before measurement.

Following [29], for every qubit pair that Alice and Bob receive, Alice decides with probability half to swap qubits one and two. When Alice swaps her qubits, she will then tell Bob to do the same.

From equation (5.2), the true state that Alice and Bob expect from the source is

$$|\Psi\rangle_{AB} = \frac{1}{2}\Big(|1+,1+\rangle + |2+,2+\rangle + |3+,3+\rangle + |4+,4+\rangle\Big) . \qquad \text{(D.1)}$$

If Alice and Bob identify the plus states with two qubits in the computational basis as follows

$$\begin{aligned} |1+\rangle &= |\uparrow\uparrow\rangle \ , \\ |2+\rangle &= |\uparrow\downarrow\rangle \ , \\ |3+\rangle &= |\downarrow\uparrow\rangle \ , \\ |4+\rangle &= |\downarrow\downarrow\rangle \ , \end{aligned} \tag{D.2}$$

then the true state can be written as

$$|\Psi\rangle_{AB} = \frac{1}{2}\left(|\uparrow\uparrow\rangle_A|\uparrow\uparrow\rangle_B + |\uparrow\downarrow\rangle_A|\uparrow\downarrow\rangle_B + |\downarrow\uparrow\rangle_A|\downarrow\uparrow\rangle_B + |\downarrow\downarrow\rangle_A|\downarrow\downarrow\rangle_B\right) \tag{D.3}$$

$$= \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle\right)_{AB1} \otimes \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle\right)_{AB2} \ . \tag{D.4}$$

In this form, it is clear that if the state between Alice and Bob was the true state (plus unbiased noise), then swapping the first and second qubits should leave the state unchanged. We also see that for the true state, Alice's first qubit is only entangled with Bob's first qubit.

Suppose the state between Alice and Bob has the purification $\left|\Phi^{12}\right\rangle_{ABE}$ such that $\rho_{AB}^{12} = \mathrm{Tr}_E\left\{\left|\Phi^{12}\right\rangle_{ABE}\left\langle\Phi^{12}\right|_{ABE}\right\}$. When Alice decides to swap or not to swap based on a random number R_1, the effective state between Alice and Bob would be $\rho_{AB} = \frac{1}{2}\left(\rho_{AB}^{12} + \rho_{AB}^{21}\right)$ where ρ_{AB}^{21} is obtained by swapping qubits one and two.

The state describing the combined system would be

$$|\chi\rangle_{ABER_1} = \frac{1}{\sqrt{2}}\left(\left|\Phi^{12}\right\rangle_{ABE}|12\rangle_{R1} + \left|\Phi^{21}\right\rangle_{ABE}|21\rangle_{R1}\right) \ , \tag{D.5}$$

where the R_1 kets are orthonormal.

We now provide Eve with the R_1 system which she can measure after sending Alice and Bob their qubits. This provides Eve at least as much power as she had before. Hence it is sufficient to consider the reduced state between Alice and Bob as obtained by tracing out E and R_1. In other words it is sufficient to only consider ρ_{AB} having the form $\rho_{AB} = \frac{1}{2}\left(\rho_{AB}^{12} + \rho_{AB}^{21}\right)$.

We can write an arbitrary state between Alice and Bob as

$$\rho_{AB}^{12} = \frac{1}{16} \sum_{a_1=0}^{4} \sum_{a_2=0}^{4} \sum_{b_1=0}^{4} \sum_{b_2=0}^{4} c_{a_1,a_2,b_1,b_2}^{12} \sigma_{a_1}^{(1)} \sigma_{a_2}^{(2)} \tau_{b_1}^{(1)} \tau_{b_2}^{(2)} , \tag{D.6}$$

where $\sigma_0 = 1$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$ and $\sigma_3 = \sigma_z$ are the Pauli operators for Alice. The superscripts 1 and 2 refer to qubits one and two. The τ operators are Bob's Pauli operators following the same convention. The coefficients c_{a_1,a_2,b_1,b_2} make up 256 real numbers constrained by the positivity of ρ and the normalisation condition: $c_{0000} = 1$.

Swapping qubits one and two, the state ρ_{AB}^{21} will have the Pauli coefficients $c_{a_1,a_2,b_1,b_2}^{21} = c_{a_2,a_1,b_2,b_1}^{12}$. The state $\rho_{AB} = \frac{1}{2}\left(\rho_{AB}^{12} + \rho_{AB}^{21}\right)$ will then have the Pauli coefficients

$$c_{a_1,a_2,b_1,b_2} = \frac{1}{2}\left(c_{a_1,a_2,b_1,b_2}^{12} + c_{a_1,a_2,b_1,b_2}^{21}\right) \tag{D.7}$$

$$= \frac{1}{2}\left(c_{a_2,a_1,b_2,b_1}^{21} + c_{a_2,a_1,b_2,b_1}^{12}\right) \tag{D.8}$$

$$= c_{a_2,a_1,b_2,b_1} \tag{D.9}$$

which set the restrictions $c_{a_1,a_2,b_1,b_2} = c_{a_2,a_1,b_2,b_1}$.

Another set of (local) operations that will leave the true state unchanged is for Alice and Bob to perform $\sigma_x \otimes \tau_x$, $\sigma_y \otimes \tau_y$ or $\sigma_z \otimes \tau_z$ on each qubit. For each qubit,

Alice will randomly decide with equal probability to apply 1, σ_x, σ_y or σ_z. She then tells Bob to do the same operation on his qubits.

We introduce a second random system R_2 which Alice uses to decide which operation to perform on her qubit pair. By placing this random system in Eve's control, we can repeat the argument done for swapping the qubits to show that it is sufficient to consider the state between Alice and Bob with the form

$$\begin{aligned}
\rho_{AB}^{0} &= \frac{1}{16}\sum_{n=0}^{4}\sum_{m=0}^{4}\left(\sigma_n^{(1)}\sigma_m^{(2)}\tau_n^{(1)}\tau_m^{(2)}\right)\rho_{AB}\left(\sigma_n^{(1)}\sigma_m^{(2)}\tau_n^{(1)}\tau_m^{(2)}\right) \\
&= \frac{1}{256}\sum_{\substack{n,m \\ a_1,a_2 \\ b_1,b_2}} c_{a_1,a_2,b_1,b_2}\left(\sigma_n^{(1)}\sigma_m^{(2)}\tau_n^{(1)}\tau_m^{(2)}\right)\left(\sigma_{a_1}^{(1)}\sigma_{a_2}^{(2)}\tau_{b_1}^{(1)}\tau_{b_2}^{(2)}\right)\left(\sigma_n^{(1)}\sigma_m^{(2)}\tau_n^{(1)}\tau_m^{(2)}\right) \\
&= \frac{1}{256}\sum_{\substack{a_1,a_2 \\ b_1,b_2}} \begin{array}{l} c_{a_1,a_2,b_1,b_2}\left(\sum_n \sigma_n^{(1)}\tau_n^{(1)}\sigma_{a_1}^{(1)}\tau_{b_1}^{(1)}\sigma_n^{(1)}\tau_n^{(1)}\right) \\ \quad\times\left(\sum_m \sigma_m^{(2)}\tau_m^{(2)}\sigma_{a_2}^{(2)}\tau_{b_2}^{(2)}\sigma_m^{(2)}\tau_m^{(2)}\right) \end{array} \\
&= \frac{1}{16}\sum_{\substack{a_1,a_2 \\ b_1,b_2}} c_{a_1,a_2,b_1,b_2}\left(\sigma_{a_1}^{(1)}\tau_{b_1}^{(1)}\delta_{a_1,b_1}\right)\left(\sigma_{a_2}^{(2)}\tau_{b_2}^{(2)}\delta_{a_2,b_2}\right) \\
&= \frac{1}{16}\sum_{a_1,a_2} c_{a_1,a_2,a_1,a_2}\sigma_{a_1}^{(1)}\sigma_{a_2}^{(2)}\tau_{a_1}^{(1)}\tau_{a_2}^{(2)} \ .
\end{aligned} \tag{D.10}$$

This state is diagonal in the bell basis $|\phi_i\rangle_{A1,B1}\left|\phi_j\right\rangle_{A2,B2}$ where $|\phi_i\rangle_{A1,B1}$ is one of the four bell states on the first qubits of Alice and Bob. The state has only sixteen parameters which can be taken to be the eigenvalues corresponding to each pair of bell-states. If we include the swapping constraint, this leaves ten undetermined coefficients (minus one from the normalisation requirement).

At this point, we can further constrain Eve's state by requiring that Alice and Bob's measurement statistics must be consistent with an unbiased noise state. The

problem now is to optimise the remaining free parameters to maximise Eve's information subject to these constraints. We expect this optimisation problem to be more tractable than the optimisation for the original protocol since the number of variables has been naturally reduced.

Part II

Security analysis of a continuous variable quantum key distribution protocol in the presence of thermal noise

Chapter 11

Review of continuous variable Gaussian states

In this chapter, we collect some well known facts that will be used in analysing the security of the continuous variable key distribution protocol. We shall restrict our analysis to Gaussian states and how they transform under Gaussian operations.

Section 11.1 provides some basic definitions concerning coherent states. Next, section 11.2 introduces the Wigner function which is all that we shall use in the analysis of the Gaussian eavesdropping attacks. The final two sections give two examples on the transformations of the Wigner function. Section 11.3 gives an example for the transformations of a single-mode Gaussian state and section 11.4 gives an example for the transformations a two-mode Gaussian state.

11.1 The ingredients

We start with the Hamiltonian for the single-mode electromagnetic field

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right) , \tag{11.1}$$

where a is the annihilation operator while $a^\dagger$ is the creation operator. They obey the bosonic commutation relation

$$\left[a, a^\dagger\right] = 1 . \tag{11.2}$$

For our purposes, $\hbar\omega$ are just constants. The eigenstates of the Hermitian operator $a^\dagger a$ are called the Fock states and denoted as $|n\rangle$ with corresponding eigenvalues n.

From the commutation relation, the action of the annihilation and creation operators on the Fock states can be shown to be

$$a\,|n\rangle = |n-1\rangle\,\sqrt{n}\,, \tag{11.3}$$

$$a^\dagger\,|n\rangle = |n+1\rangle\,\sqrt{n+1}\,. \tag{11.4}$$

For the norms of all the states $a\,|n\rangle$ to be non-negative, the eigenvalues n can only take non-negative integer values $n \in \{0, 1, 2, \ldots \infty\}$. The state $|0\rangle$ corresponding to the eigenvalue $n = 0$ is given the special name as the vacuum state. It is the ground state of H, with the eigenenergy $\hbar\omega/2$.

We are now almost ready to introduce the coherent states. These states shall serve as the signal states that Alice would send to Bob in our key distribution

protocol. We just need one more final ingredient and that is the displacement operator

$$D(\alpha) = \exp\left(\alpha a^{\dagger} - \alpha^{*} a\right) , \tag{11.5}$$

where α is an arbitrary complex number. The coherent state $|\alpha\rangle$ is generated by operating the displacement operator $D(\alpha/k)$ on the vacuum state

$$|\alpha\rangle = D\left(\frac{\alpha}{k}\right)|0\rangle , \tag{11.6}$$

where k is some proportionality constant. From this definition for the coherent state, it also follows that the coherent states are eigenstates of the annihilation operator

$$a|\alpha\rangle = |\alpha\rangle \frac{\alpha}{k} . \tag{11.7}$$

The inner product between two coherent states $|\alpha_1\rangle$ and $|\alpha_2\rangle$ is

$$\langle\alpha_1|\alpha_2\rangle = \exp\left[\frac{|\alpha_1|^2 + |\alpha_2|^2 + 2\alpha_1^{*}\alpha_2}{2k^2}\right] , \tag{11.8}$$

so that the absolute value squared is

$$\left|\langle\alpha_1|\alpha_2\rangle\right|^2 = \exp\left[-\frac{|\alpha_1 - \alpha_2|^2}{k^2}\right] . \tag{11.9}$$

The missing steps are worked out in textbooks on quantum mechanics [2, 18, 58].

Having described operators representing the generation of coherent states which Alice sends, we now proceed to the operators which represent the measurement process for Bob. The two measurement operators at Bob's end are the amplitude quadrature operator X and phase quadrature operator Y defined as

$$X = \frac{v}{2}\left(a + a^{\dagger}\right) , \tag{11.10}$$

$$Y = \frac{v}{2\mathrm{i}}\left(a - a^{\dagger}\right) , \tag{11.11}$$

with v being a proportionality constant for Bob to choose at his convenience. Note that X and Y do not commute which means that Bob cannot measure both X and Y simultaneously on the same state. In fact the commutator between X and Y turns out to be

$$[X,Y] = \frac{i}{2}v^2 . \tag{11.12}$$

With this definition, we find that when Alice sends the coherent state $|\alpha\rangle$, Bob will get an expected value of

$$\langle\alpha|X|\alpha\rangle = \frac{v}{2}\left\langle\alpha|a + a^{\dagger}|\alpha\right\rangle \tag{11.13}$$

$$= \frac{v}{k}\mathrm{Re}(\alpha) \tag{11.14}$$

and

$$\langle\alpha|Y|\alpha\rangle = \frac{v}{2\mathrm{i}}\left\langle\alpha|a - a^{\dagger}|\alpha\right\rangle \tag{11.15}$$

$$= \frac{v}{k}\mathrm{Im}(\alpha) . \tag{11.16}$$

The variance of an operator O for the state ρ is defined as

$$\mathrm{var}(O)_\rho = \mathrm{Tr}\left\{\rho O^2\right\} - \mathrm{Tr}\left\{\rho O\right\}^2. \tag{11.17}$$

The variances in the outcomes of X and Y for the state $|\alpha\rangle$ will be

$$\mathrm{var}(X)_\alpha = \mathrm{var}(Y)_\alpha = \frac{v^2}{4}\ . \tag{11.18}$$

Throughout the thesis, we shall set the proportionality constant $k = v = 2\sigma_V$, where we have introduced another constant σ_V. With these definitions, the coherent state $|\alpha\rangle$ will give the following outcomes

$$\langle\alpha|X|\alpha\rangle = \mathrm{Re}(\alpha)\ , \tag{11.19}$$

$$\langle\alpha|Y|\alpha\rangle = \mathrm{Im}(\alpha)\ , \tag{11.20}$$

$$\mathrm{var}(X)_\alpha = \mathrm{var}(Y)_\alpha = \sigma_V^2\ , \tag{11.21}$$

where σ_V^2 is by definition the variance of a quadrature measurement on a coherent state. In this thesis, unless otherwise specified, we set $k = v = 1$ so that $\sigma_V^2 = 1/4$.

11.1.1 Beam splitter matrix

Eve's basic tool to eavesdrop on Alice's signal would be the beam splitter. For the purpose of studying that, we recap how the beam splitter affects the coherent states.

The beam splitter is represented schematically in figure 11.1 where the two input ports are labelled as A and V. The output ports are labelled with B and E.

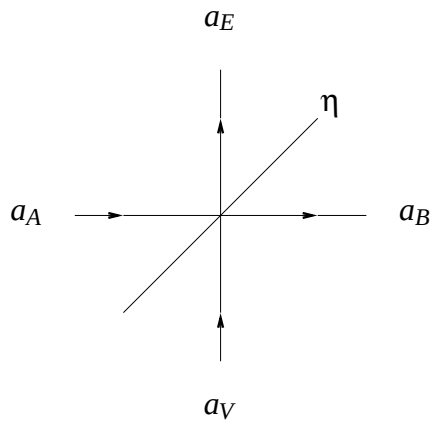


Figure 11.1: Schematic diagram of a beam splitter with two input ports A and V and two output ports B and E. The transmittivity of the beam splitter is η.

The output ports of the beam splitter are related to the input ports by the following relations on the annihilation operators

$$a_B = \sqrt{\eta}a_A - \sqrt{1-\eta}a_V \ , \tag{11.22}$$

$$a_E = \sqrt{1-\eta}a_A + \sqrt{\eta}a_V \ , \tag{11.23}$$

where η is the beam splitter transmission coefficient. When we have a coherent state $|\alpha_A\rangle$ going through the first input A and a second coherent state $|\alpha_V\rangle$ through

the second input V, the output state can be obtained from the input states as follows

$$
\begin{aligned}
&|\alpha_A\rangle_A |\alpha_V\rangle_V && (11.24)\\
&= D_A\left(\frac{\alpha_A}{k}\right) D_V\left(\frac{\alpha_V}{k}\right)|0\rangle && (11.25)\\
&= \exp\left(\alpha_A a_A^\dagger - \alpha_A^* a_A\right)\exp\left(\alpha_V a_V^\dagger - \alpha_V^* a_V\right)|0\rangle && (11.26)\\
&= \exp\left(\alpha_A\sqrt{\eta}a_B^\dagger + \alpha_A\sqrt{1-\eta}a_E^\dagger - \alpha_A^*\sqrt{\eta}a_B - \alpha_A^*\sqrt{1-\eta}a_E\right)\\
&\quad\times\exp\left(\alpha_V\sqrt{\eta}a_E^\dagger - \alpha_V\sqrt{1-\eta}a_B^\dagger - \alpha_V^*\sqrt{\eta}a_E + \alpha_V^*\sqrt{1-\eta}a_B\right)|0\rangle && (11.27)\\
&= D_B\left(\frac{\sqrt{\eta}\alpha_A - \sqrt{1-\eta}\alpha_V}{k}\right) D_E\left(\frac{\sqrt{1-\eta}\alpha_A + \sqrt{\eta}\alpha_V}{k}\right)|0\rangle && (11.28)\\
&= \left|\sqrt{\eta}\alpha_A - \sqrt{1-\eta}\alpha_V\right\rangle_B \left|\sqrt{1-\eta}\alpha_A + \sqrt{\eta}\alpha_V\right\rangle_E . && (11.29)
\end{aligned}
$$

The beam splitter affects a rotation of the input quadratures. The output quadratures in terms of the input would be

$$
\begin{pmatrix} X_B \\ Y_B \\ X_E \\ Y_E \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & 0 & -\sqrt{1-\eta} & 0 \\ 0 & \sqrt{\eta} & 0 & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & 0 & \sqrt{\eta} & 0 \\ 0 & \sqrt{1-\eta} & 0 & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} X_A \\ Y_A \\ X_V \\ Y_V \end{pmatrix} . \quad (11.30)
$$

For the Gaussian states that we shall be considering here, the beam splitter will displace the coherent amplitude by $\vec{x_0'} = M\vec{x_0}$ and rotate the covariance matrix

according to $C' = MCM^T$ where

$$\vec{x_0} = \begin{pmatrix} \langle X_A \rangle \\ \langle Y_A \rangle \\ \langle X_V \rangle \\ \langle Y_V \rangle \end{pmatrix}, \vec{x_0'} = \begin{pmatrix} \langle X_B \rangle \\ \langle Y_B \rangle \\ \langle X_E \rangle \\ \langle Y_E \rangle \end{pmatrix} \tag{11.31}$$

are the coherent amplitudes of the input and output states respectively and C is the covariance matrix for the input state

$$C = \begin{pmatrix} \langle \bar{X}_A \bar{X}_A \rangle & \langle \bar{X}_A \bar{Y}_A \rangle & \langle \bar{X}_A \bar{X}_V \rangle & \langle \bar{X}_A \bar{Y}_V \rangle \\ \langle \bar{Y}_A \bar{X}_A \rangle & \langle \bar{Y}_A \bar{Y}_A \rangle & \langle \bar{Y}_A \bar{X}_V \rangle & \langle \bar{Y}_A \bar{Y}_V \rangle \\ \langle \bar{X}_V \bar{X}_A \rangle & \langle \bar{X}_V \bar{Y}_A \rangle & \langle \bar{X}_V \bar{X}_V \rangle & \langle \bar{X}_A \bar{Y}_V \rangle \\ \langle \bar{Y}_V \bar{X}_A \rangle & \langle \bar{Y}_V \bar{Y}_A \rangle & \langle \bar{Y}_V \bar{X}_V \rangle & \langle \bar{Y}_A \bar{Y}_V \rangle \end{pmatrix} \tag{11.32}$$

while C' is the covariance matrix for the output state

$$C' = \begin{pmatrix} \langle \bar{X}_B \bar{X}_B \rangle & \langle \bar{X}_B \bar{Y}_B \rangle & \langle \bar{X}_B \bar{X}_E \rangle & \langle \bar{X}_B \bar{Y}_E \rangle \\ \langle \bar{Y}_B \bar{X}_B \rangle & \langle \bar{Y}_B \bar{Y}_B \rangle & \langle \bar{Y}_B \bar{X}_E \rangle & \langle \bar{Y}_B \bar{Y}_E \rangle \\ \langle \bar{X}_E \bar{X}_B \rangle & \langle \bar{X}_E \bar{Y}_B \rangle & \langle \bar{X}_E \bar{X}_E \rangle & \langle \bar{X}_B \bar{Y}_E \rangle \\ \langle \bar{Y}_E \bar{X}_B \rangle & \langle \bar{Y}_E \bar{Y}_B \rangle & \langle \bar{Y}_E \bar{X}_E \rangle & \langle \bar{Y}_B \bar{Y}_E \rangle \end{pmatrix}. \tag{11.33}$$

An operator with an over-line denotes the fluctuations of the operator from its mean value, $\bar{O} = O - \langle O \rangle$. M is the beam splitter matrix

$$M = \begin{pmatrix} \sqrt{\eta} & 0 & -\sqrt{1-\eta} & 0 \\ 0 & \sqrt{\eta} & 0 & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & 0 & \sqrt{\eta} & 0 \\ 0 & \sqrt{1-\eta} & 0 & \sqrt{\eta} \end{pmatrix} . \tag{11.34}$$

11.2 Wigner function and general Gaussian states

We introduce another two bases for the single-mode infinite dimensional Hilbert space. The first basis is comprised of the kets $|x\rangle$, the eigenstates of the amplitude quadrature operator X corresponding to the eigenvalues $x \in \mathbb{R}$. The second basis is comprised of the kets $|y\rangle$, the eigenstates of the phase quadrature operators with eigenvalues $y \in \mathbb{R}$.

We define the Wigner function of a single-mode state $\hat{\rho}$ though these bases by

$$\rho(x,y) = \int \frac{d\tilde{x}}{2\pi\hbar} \left\langle x - \frac{\tilde{x}}{2} \middle| \hat{\rho} \middle| x + \frac{\tilde{x}}{2} \right\rangle \exp(\mathrm{i}y\tilde{x}) \tag{11.35}$$

$$= \int \frac{d\tilde{y}}{2\pi\hbar} \left\langle y - \frac{\tilde{y}}{2} \middle| \hat{\rho} \middle| y + \frac{\tilde{y}}{2} \right\rangle \exp(\mathrm{i}x\tilde{y}) \ . \tag{11.36}$$

The second equality follows by using the inner product

$$\langle x | y \rangle = \frac{1}{\sqrt{2\pi\hbar}} \exp(\mathrm{i}xy) \ . \tag{11.37}$$

The symbol $\hbar = 2\sigma_v^2$ so that the commutation relation between X and Y reads

$$[X,Y] = \mathrm{i}\hbar\,. \tag{11.38}$$

The marginal distribution for $\hat{\rho}$ to be in the state $|x\rangle$ is then

$$\langle x|\,\hat{\rho}\,|x\rangle = \int \rho(x,y)dy \tag{11.39}$$

and for it to be in the state $|y\rangle$ would be

$$\langle y|\,\hat{\rho}\,|y\rangle = \int \rho(x,y)dx\,. \tag{11.40}$$

The normalisation condition on $\hat{\rho}$ translates to

$$\iint dx\,dy\,\rho(x,y) = 1\,. \tag{11.41}$$

The overlap between two states $\hat{\rho}_1$ and $\hat{\rho}_2$ is given by

$$\mathrm{Tr}\,\{\hat{\rho}_1\hat{\rho}_2\} = 2\pi\hbar \iint dx\,dy\,\rho_1(x,y)\rho_2(x,y)\,. \tag{11.42}$$

11.2.1 *n*-mode Gaussian states

For an n-mode state $\hat{\rho}$, the Wigner function is defined as

$$\begin{aligned}\rho\,(\vec{z}) = \int \frac{d\tilde{x}_1\ldots d\tilde{x}_n}{(2\pi\hbar)^n} \left\langle x_1 - \frac{\tilde{x_1}}{2},\ldots,x_n - \frac{\tilde{x_n}}{2}\right| \hat{\rho} \left| x_1 + \frac{\tilde{x_1}}{2},\ldots,x_n + \frac{\tilde{x}_n}{2}\right\rangle \\ \times \exp\left(\mathrm{i}y_1\tilde{x}_1\right)\ldots\exp\left(\mathrm{i}y_n\tilde{x}_n\right)\end{aligned} \tag{11.43}$$

where

$$\vec{z} = (x_1, y_1, \ldots, x_n, y_n)^{\mathrm{T}} \ . \tag{11.44}$$

If the state $\hat{\rho}$ is a Gaussian state, then its Wigner function can be written in terms of its mean $\vec{x}_0$ and the covariance matrix C as

$$\rho(\vec{z}) = \frac{1}{\sqrt{(2\pi)^{(2n)}\,|C|}} \exp\left\{ -\frac{1}{2} (\vec{z} - \vec{z}_0)^T C^{-1} (\vec{z} - \vec{z}_0) \right\} , \tag{11.45}$$

where

$$\vec{z}_0 = (\langle x_1 \rangle, \langle y_1 \rangle, \ldots, \langle x_n \rangle, \langle y_n \rangle)^{\mathrm{T}} \ . \tag{11.46}$$

and

$$C_{ij} = \langle z_i z_j \rangle \tag{11.47}$$

for $\{i, j\} \in \{1, 2, \ldots, 2n\}$. The overlap between two n-mode states $\hat{\rho}_1$ and $\hat{\rho}_2$ is given by

$$\mathrm{Tr}\{\hat{\rho}_1 \hat{\rho}_2\} = (2\pi\hbar)^n \int d\vec{z}\, \rho_1(\vec{z}) \rho_2(\vec{z}) \ . \tag{11.48}$$

A unitary Gaussian operator U acting on the Hilbert space $\mathcal{H}$ corresponds to a symplectic transformation S on the phase space of the Wigner function. A symplectic transformation would evolve the covariance matrix to $C \to SCS^{\mathrm{T}}$ and the mean becomes $\vec{z}_0 \to S\vec{z}_0$. A symplectic transformation is one that preserves

the commutation relations: $\left[Sz_j, Sz_k\right] = \left[z_j, z_k\right]$. In other words $S\Sigma^{\oplus n}S^{\mathrm{T}} = \Sigma^{\oplus n}$ where

$$\Sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} . \tag{11.49}$$

Any symplectic transformation can be realised by a combination of three operators. The first is the rotation operator $S_{\mathrm{rot}}(\theta)$

$$S_{\mathrm{rot}}(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{11.50}$$

which rotates the quadratures by an angle θ. The second operator is the squeezing operator $S_{\mathrm{sqz}}(g)$

$$S_{\mathrm{sqz}}(g) = \begin{pmatrix} \frac{1}{g} & 0 \\ 0 & g \end{pmatrix} . \tag{11.51}$$

This squeezes the amplitude quadrature by the factor g. The last operator $S_{\mathrm{mix}}(\eta)$ is the mixing operator between two modes

$$S_{\mathrm{mix}}(\eta) = \begin{pmatrix} \sqrt{\eta} & 0 & -\sqrt{1-\eta} & 0 \\ 0 & \sqrt{\eta} & 0 & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & 0 & \sqrt{\eta} & 0 \\ 0 & \sqrt{1-\eta} & 0 & \sqrt{\eta} \end{pmatrix} \tag{11.52}$$

where $0 \leq \eta \leq 1$ determines the mixing ratio.

These three operators can be realised in the lab by the passive components phase shifters, squeezers and beam splitters respectively. In particular, a local unitary Gaussian operation on a two-mode system $U = U_1 \otimes U_2$ maps to the local symplectic operation $S = S_1 \oplus S_2$. This locality restriction removes the beam splitter from our set of operations.

Williamson's theorem states that any covariance matrix can be brought into a diagonal form with diagonal entries $(\kappa_1, \kappa_1, \kappa_2, \kappa_2, \ldots, \kappa_n, \kappa_n)$ via a symplectic transformation. In this form, the phase space variables are not correlated to each other, meaning that there always exist a bi-partition in which an n-mode Gaussian state becomes separable. This also means that any zero mean Gaussian state can be created in the lab by our set of three passive components on initially uncorrelated thermal states. In this form the uncertainty relation becomes $\kappa_i \geq \sigma_V^2$ for all $i \in \{1, 2, \ldots, n\}$ [53].

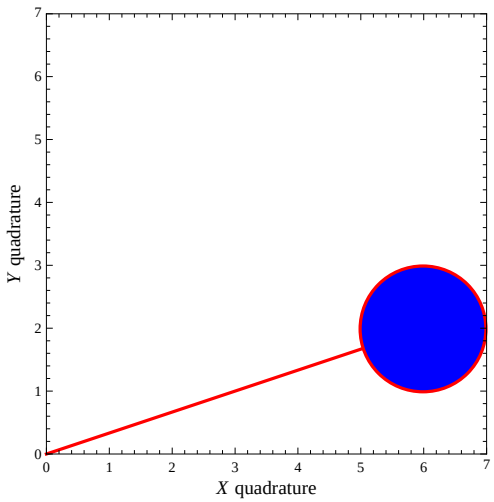
11.3 Example 1: Single-mode Gaussian states

For a single-mode Gaussian state, we can visualise its Wigner function as an ellipse in a two dimensional plane. The centre of this ellipse will correspond to the mean amplitude. The semi-major and semi-minor axis is proportional to the standard deviation of the amplitude outcome when measured along those quadratures.

The coherent state $|x_0 + \mathrm{i}y_0\rangle$ will have a mean amplitude $\mu = (x_0, y_0)$, and the covariance matrix

$$C = \begin{pmatrix} \sigma_V^2 & 0 \\ 0 & \sigma_V^2 \end{pmatrix}. \tag{11.53}$$

For example, the following ball on stick figure is used to represent the coherent state $|6+2\mathrm{i}\rangle$:



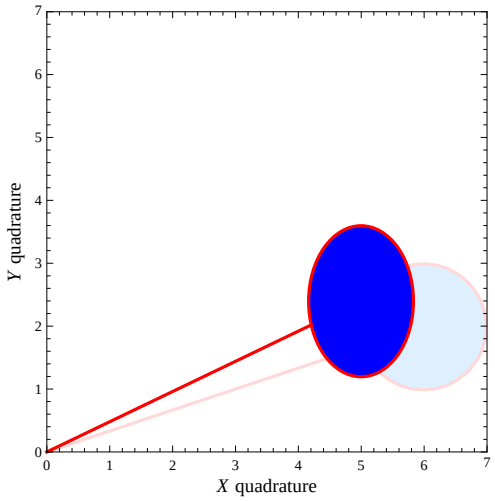
The ball is centred at $(6,2)$ and has radius 1 in units of σ_v. Applying the squeezing operator with a squeezing factor $g = 1.2$, the new state now has a mean amplitude

$$\mu = \begin{pmatrix} \frac{1}{1.2} & 0 \\ 0 & 1.2 \end{pmatrix} \begin{pmatrix} 6 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 2.4 \end{pmatrix} . \tag{11.54}$$

The covariance matrix becomes

$$\begin{aligned} C &= \begin{pmatrix} \frac{1}{1.2} & 0 \\ 0 & 1.2 \end{pmatrix} \begin{pmatrix} \sigma_V^2 & 0 \\ 0 & \sigma_V^2 \end{pmatrix} \begin{pmatrix} \frac{1}{1.2} & 0 \\ 0 & 1.2 \end{pmatrix} \\ &= \begin{pmatrix} 0.69444\sigma_V^2 & 0 \\ 0 & 1.44\sigma_V^2 \end{pmatrix} . \end{aligned} \tag{11.55}$$

The variance in the X quadrature is less than the vacuum noise. But this is at the expense of a noisier Y quadrature. The ball on stick representation of this state is shown in the following figure:



There is no correlation between the X and Y quadratures as seen by the diagonal covariance matrix and the also by the axis of the ellipse being parallel to the x and y axes.

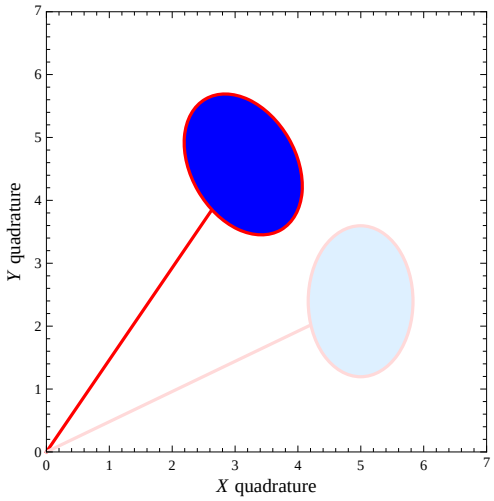
Finally if we apply the rotation operator with angle $\theta = \pi/6$ to this state, the mean amplitude would be

$$\mu = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} \begin{pmatrix} 5 \\ 2.4 \end{pmatrix} = \begin{pmatrix} 3.13013 \\ 4.57846 \end{pmatrix} . \tag{11.56}$$

The covariance matrix becomes

$$\begin{aligned} C &= \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} \begin{pmatrix} 0.69444\sigma_V^2 & 0 \\ 0 & 1.44\sigma_V^2 \end{pmatrix} \begin{pmatrix} \cos\frac{\pi}{6} & \sin\frac{\pi}{6} \\ -\sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} \\ &= \begin{pmatrix} 0.880833\sigma_V^2 & -0.322835\sigma_V^2 \\ -0.322835\sigma_V^2 & 1.25361\sigma_V^2 \end{pmatrix} . \end{aligned} \tag{11.57}$$

This state is represented by the following figure:



If we were to measure the X quadrature repeatedly, the outcomes will show a Gaussian distribution having a mean of value 3.13013 and variance $0.880833\sigma_V^2$. There would be some correlation between the X and Y quadratures as seen by the non zero off diagonal elements in the covariance matrix.

Suppose we measured X and obtained the outcome $x = 5.4$, if we were to measure the Y quadrature (not that we could actually measure both quadratures simultaneously), the conditioned outcome y will have its mean given by

$$\begin{aligned} \mu_{2|1} &= \mu_2 + C_{21}C_{11}^{-1}(x-\mu_1) \\ &= 4.57846 + \frac{-0.322835}{0.880833}(5.4-3.13013) \\ &= 3.74653\,. \end{aligned} \tag{11.58}$$

The conditional variance is given by

$$\begin{aligned} C_{2|1} &= C_{22} - C_{21}C_{11}^{-1}C_{12} \\ &= 1.25361\sigma_V^2 - \frac{0.322835^2}{0.880833}\sigma_V^2 \\ &= 1.13529\sigma_V^2 \, . \end{aligned} \tag{11.59}$$

We note that since these symplectic transformations realise unitary transformations, the purity of the transformed state remains the same. This can be quantified by the determinant of the covariance matrix which remains unchanged under a symplectic transformation.

11.4 Example 2: Two squeezed states at arbitrary angle

This example illustrates the correlations in a two-mode Einstein-Podolsky-Rosen (EPR) state. The EPR state is created by shining two squeezed states through the two inputs of a beam splitter.

We begin with an uncorrelated two-mode system. The first mode is the vacuum state which is first squeezed in the X quadrature with a squeezing factor g and then rotated by an angle θ. This state will have a mean $(0,0)$ and covariance

matrix

$$C_1 = S_{\text{rot}}(\theta) S_{\text{sqz}}(g) \begin{pmatrix} \sigma_V^2 & 0 \\ 0 & \sigma_V^2 \end{pmatrix} S_{\text{sqz}}^{\text{T}}(g) S_{\text{rot}}^{\text{T}}(\theta) \tag{11.60}$$

$$= S_{\text{rot}}(\theta) \begin{pmatrix} \sigma_{sq}^2 & 0 \\ 0 & \sigma_{asq}^2 \end{pmatrix} S_{\text{rot}}^{\text{T}}(\theta) \tag{11.61}$$

$$= \begin{pmatrix} \sigma_{sq}^2 \cos^2\theta + \sigma_{asq}^2 \sin^2\theta & \left(\sigma_{sq}^2 - \sigma_{asq}^2\right) \sin\theta\cos\theta \\ \left(\sigma_{sq}^2 - \sigma_{asq}^2\right) \sin\theta\cos\theta & \sigma_{sq}^2 \sin^2\theta + \sigma_{asq}^2 \cos^2\theta \end{pmatrix} \tag{11.62}$$

Here, $\sigma_{sq}^2 = \sigma_V^2/g$ and $\sigma_{asq}^2 = g\sigma_V^2$ where the subscripts denote squeezed and anti-squeezed respectively. They are the variances of the X and Y quadratures respectively before the rotation. This state will be the state through the first input of a $50/50$ beam splitter a_1 as shown in figure 11.2.

The second mode also starts in the vacuum state but it is first squeezed in the X quadrature with a squeezing factor $1/g$ and then rotated by an angle θ. This state will have a mean $(0,0)$ and covariance matrix

$$C_2 = S_{\text{rot}}(\theta) S_{\text{sqz}}\left(\frac{1}{g}\right) \begin{pmatrix} \sigma_V^2 & 0 \\ 0 & \sigma_V^2 \end{pmatrix} S_{\text{sqz}}^{\text{T}}\left(\frac{1}{g}\right) S_{\text{rot}}^{\text{T}}(\theta) \tag{11.63}$$

$$= S_{\text{rot}}(\theta) \begin{pmatrix} \sigma_{asq}^2 & 0 \\ 0 & \sigma_{sq}^2 \end{pmatrix} S_{\text{rot}}^{\text{T}}(\theta) \tag{11.64}$$

$$= \begin{pmatrix} \sigma_{asq}^2 \cos^2\theta + \sigma_{sq}^2 \sin^2\theta & -\left(\sigma_{sq}^2 - \sigma_{asq}^2\right) \sin\theta\cos\theta \\ -\left(\sigma_{sq}^2 - \sigma_{asq}^2\right) \sin\theta\cos\theta & \sigma_{asq}^2 \sin^2\theta + \sigma_{sq}^2 \cos^2\theta \end{pmatrix}. \tag{11.65}$$

This state is then passed through the second input of the beam splitter a_2.

The two input states are shown in the ball on stick representation in figure 11.2. As we shall see, each of the two output modes turns out to be in a thermal state when examined individually.

The covariance matrix for the output modes with $\eta = 1/2$ will be:

$$
\begin{aligned}
C_{out} &= S_{\mathrm{mix}}(\eta) C_{in} S_{\mathrm{mix}}(\eta)^{\mathrm{T}} \\
&= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} C_1 & 0_{2\times 2} \\ 0_{2\times 2} & C_2 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \frac{1}{2} \begin{pmatrix} C_1 + C_2 & C_1 - C_2 \\ C_1 - C_2 & C_1 + C_2 \end{pmatrix} \\
&= \begin{pmatrix} \sigma_{th}^2 & 0 & -\sigma_k^2 \cos(2\theta) & -\sigma_k^2 \sin(2\theta) \\ 0 & \sigma_{th}^2 & -\sigma_k^2 \sin(2\theta) & \sigma_k^2 \cos(2\theta) \\ -\sigma_k^2 \cos(2\theta) & -\sigma_k^2 \sin(2\theta) & \sigma_{th}^2 & 0 \\ -\sigma_k^2 \sin(2\theta) & \sigma_k^2 \cos(2\theta) & 0 & \sigma_{th}^2 \end{pmatrix}
\end{aligned}
\tag{11.66}
$$

where $\sigma_k^2 = \left(\sigma_{asq}^2 - \sigma_{sq}^2\right)/2$ and $\sigma_{th}^2 = \left(\sigma_{sq}^2 + \sigma_{asq}^2\right)/2$. From the diagonal blocks, we see that both of the outputs a_3 and a_4 of the beam splitter are in a thermal state with a variance of σ_{th}^2. There is no correlation between the X_3 and Y_3 quadratures or between the X_4 and Y_4 quadratures.

But the output a_3 is correlated to a_4. We want to find out what happens to the output at a_3 given that a measurement of X_4 gives the outcome x_A. The variable x_3 and y_3 will follow a Gaussian distribution and we denote its mean by $\bar{\mu}_{12}$ and

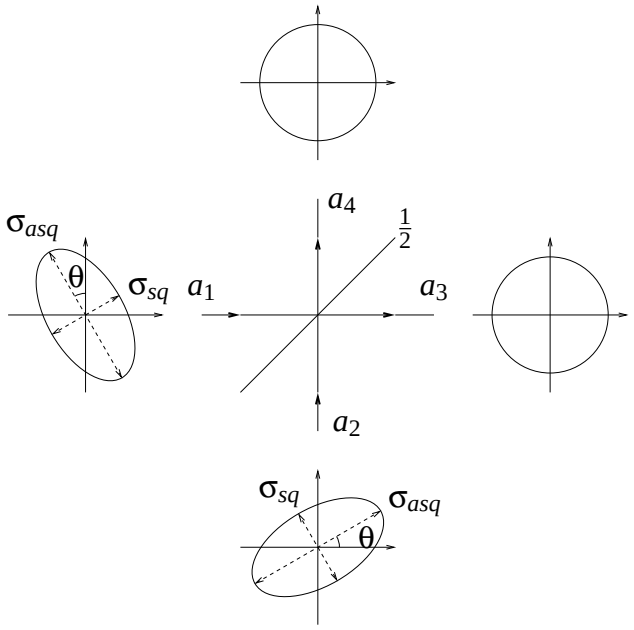


Figure 11.2: Creation of an EPR state by shining two orthogonally squeezed input states through a $50/50$ beam splitter. The output states are two thermal states which are correlated to each other.

covariance matrix by $\bar{\Sigma}_{12;12}$. The reduced state will have mean

$$\begin{aligned}\bar{\mu}_{12} &= \mu_{12} + C_{12;3}C_{3;3}^{-1}(x_A - \mu_3) \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} -\sigma_k^2\cos(2\theta) \\ -\sigma_k^2\sin(2\theta) \end{pmatrix} \frac{1}{\sigma_{th}^2}(x_A - 0) \\ &= -\frac{\sigma_k^2}{\sigma_{th}^2}\begin{pmatrix} x_A\cos(2\theta) \\ x_A\sin(2\theta) \end{pmatrix}\end{aligned} \tag{11.67}$$

and its covariance matrix is

$$\begin{aligned}\bar{\Sigma}_{12;12} &= C_{12;12} - C_{12;3}C_{3;3}^{-1}C_{3;12} \\ &= \frac{1}{2}\begin{pmatrix} \sigma_{sq}^2+\sigma_{asq}^2 & 0 \\ 0 & \sigma_{sq}^2+\sigma_{asq}^2 \end{pmatrix} - \frac{1}{2}\begin{pmatrix} \left(\sigma_{sq}^2-\sigma_{asq}^2\right)\cos^2(2\theta) \\ \left(\sigma_{sq}^2-\sigma_{asq}^2\right)\sin^2(2\theta) \end{pmatrix} \\ &\quad \times \frac{2}{\sigma_{sq}^2+\sigma_{asq}^2}\begin{pmatrix} \left(\sigma_{sq}^2-\sigma_{asq}^2\right)\cos^2(2\theta) & \left(\sigma_{sq}^2-\sigma_{asq}^2\right)\sin^2(2\theta) \end{pmatrix} \\ &= \begin{pmatrix} \frac{\sigma_V^4}{\sigma_{th}^2}\cos^2(2\theta)+\sigma_{th}^2\sin^2(2\theta) & \left(\sigma_{th}^2-\frac{\sigma_V^4}{\sigma_{th}^2}\right)\sin(2\theta)\cos(2\theta) \\ \left(\sigma_{th}^2-\frac{\sigma_V^4}{\sigma_{th}^2}\right)\sin(2\theta)\cos(2\theta) & \frac{\sigma_V^4}{\sigma_{th}^2}\sin^2(2\theta)+\sigma_{th}^2\cos^2(2\theta) \end{pmatrix}.\end{aligned} \tag{11.68}$$

Writing $\bar{\Sigma}_{12;12}$ as

$$\bar{\Sigma}_{12;12} = S_{\mathrm{rot}}(-2\theta)\begin{pmatrix} \frac{\sigma_V^4}{\sigma_{th}^2} & 0 \\ 0 & \sigma_{th}^2 \end{pmatrix} S_{\mathrm{rot}}^{\mathrm{T}}(-2\theta) \tag{11.69}$$

we see that the reduced state is a squeezed state with a minimum variance of σ_V^4/σ_{th}^2. This state is represented in the ball on stick representation in figure 11.3.

The X quadrature has a mean value of

$$-\frac{\left(\sigma_{asq}^2-\sigma_{sq}^2\right)}{\left(\sigma_{sq}^2+\sigma_{asq}^2\right)}x_A\cos(2\theta) \tag{11.70}$$

and variance

$$\frac{\sigma_V^4}{\sigma_{th}^2}\cos^2(2\theta)+\sigma_{th}^2\sin^2(2\theta)\,. \tag{11.71}$$

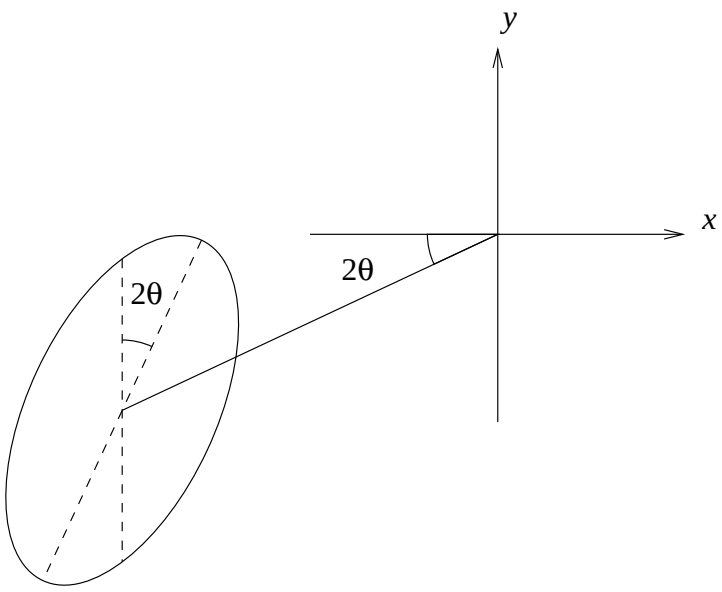


Figure 11.3: Ball on stick representation of a reduced EPR state.

For a fixed squeezing factor $g > 1$, the magnitude of the mean value is maximum whilst the variance is minimum when $\theta = 0$. For such a state, the two outputs are said to be EPR entangled.

Chapter 12

Introduction to continuous variable quantum key distribution

Continuous variable quantum key distribution uses a continuous degree of freedom to distribute secure keys between Alice and Bob. Typically, the amplitude and phase quadratures of a Gaussian beam are used to carry the signals.

In single photon implementations of quantum key distribution, when no photons arrive at Bob's detector, the signal is simply lost and does not contribute to the key generation protocol. This is a form of post-selection and the missing events do not give the eavesdropper any information.

However in continuous variable quantum key distribution with a lossy transmission line, when Alice sends a certain coherent state, Bob would still detect a coherent state, but having a smaller amplitude. The loss could be due to Eve intercepting some photons and keeping them to herself. Therefore loss would mean that Eve now has some information regarding the state that Alice sends.

In this chapter, we will look at how loss affects the security of one of the first and simplest continuous variable quantum key distribution protocols. In section 12.1, we will introduce the protocol. Section 12.2 analyses its performance in a perfect lossless channel. Finally, in section 12.3 we discuss how loss in the channel affects the protocol.

12.1 3 dB loss limit without post-selection

The early continuous variable key distribution protocols suffer from the 3 dB loss limit. When the loss in the channel is greater than 50% no secure key can be distributed. We recap one such protocol, presented by Grosshans and Grangier in 2002 [23].

In that protocol, Alice picks N pairs of real numbers $\left\{x_A^j, y_A^j\right\}$ for $j \in \{1,2,\ldots,N\}$. Both x_A^j and y_A^j are picked from a Gaussian distribution with variance σ_A^2 and zero mean:

$$p_A\left(x_A^j\right) \sim \mathcal{N}(0,\sigma_A)\ , \tag{12.1}$$

$$p_A\left(y_A^j\right) \sim \mathcal{N}(0,\sigma_A)\ . \tag{12.2}$$

Alice then prepares a sequence of N coherent states $\left|\alpha^j\right\rangle$ with the complex amplitudes $\alpha^j = x_A^j + \mathrm{i}y_A^j$.

Bob will choose to measure each coherent state with either the amplitude operator X or phase operator Y.

12.2 Perfect lossless channel

In a lossless and noiseless channel, Bob will receive the state exactly as what Alice sent without corruption. Together with a perfect measurement device, the probability of Bob's outcome x_B when he measures the amplitude quadrature given that Alice sends the coherent state with amplitude $x_A + \mathrm{i}y_A$ will be

$$p_B(x_B|x_A) \sim \mathcal{N}(x_A, \sigma_V) \ . \tag{12.3}$$

Bob's outcome given Alice's signal, will be normally distributed with mean x_A and variance σ_V^2. So when Bob measures the amplitude quadrature, he will get some information about the value of x_A, but no information about the value of y_A. In this sense there are no mismatched bases; each of Bob's measurements gives correlated data. However half of the signals that Alice encodes remains unmeasured.

The joint probability between Alice and Bob will be

$$p_{AB}(x_A, x_B) = p_B(x_B|x_A)p_A(x_A) \tag{12.4}$$

$$= \frac{1}{2\pi\sqrt{\det C}} \exp\left(-\frac{1}{2}\vec{x}C^{-1}\vec{x}\right) \tag{12.5}$$

where $\vec{x} = (x_A, x_B)$. This is a Gaussian with mean $(\bar{x_A}, \bar{x_B}) = (0,0)$ and C is the covariance matrix

$$C = \begin{pmatrix} \sigma_A^2 & \sigma_A^2 \\ \sigma_A^2 & \sigma_V^2 + \sigma_A^2 \end{pmatrix} \ . \tag{12.6}$$

This describes the raw data between Alice and Bob. The maximum amount of bits that Alice and Bob can extract from the raw data using the most efficient encoding algorithm is given by the mutual information between Alice and Bob

$$I_{AB} = \iint dx_A\, dx_B\, p_{AB}(x_A, x_B) \log \frac{p_{AB}(x_A, x_B)}{p_A(x_A)\, p_B(x_B)} \tag{12.7}$$

$$= S_A + S_B - S_{AB}\,. \tag{12.8}$$

Here $p_B(x_B)$ denotes the probability of Bob's measurement outcomes

$$p_B(x_B) = \int dx_A\, p_{AB}(x_A, x_B) \tag{12.9}$$

$$\sim \mathcal{N}\left(0, \sigma_V^2 + \sigma_A^2\right)\,, \tag{12.10}$$

and S_A is the relative entropy of Alice's data

$$S_A = -\int dx_A\, p_A(x_A) \log p_A(x_A) \tag{12.11}$$

$$= \frac{1}{2}\left[1 + \log\left(2\pi\sigma_A^2\right)\right]\,. \tag{12.12}$$

The relative entropy of Bob's data S_B is

$$S_B = -\int dx_B\, p_B(x_B) \log p_B(x_B) \tag{12.13}$$

$$= \frac{1}{2}\left[1 + \log\left(2\pi\left(\sigma_V^2 + \sigma_A^2\right)\right)\right] \tag{12.14}$$

while the joint relative entropy between Alice and Bob is

$$S_{AB} = -\iint dx_A\, dx_B\, p_{AB}(x_A, x_B) \log p_{AB}(x_A, x_B) \tag{12.15}$$

$$= \frac{1}{2}\left[2 + \log\left((2\pi)^2 \det C\right)\right] \tag{12.16}$$

$$= \frac{1}{2}\left[2 + \log\left(2\pi\sigma_A^2\right) + \log\left(2\pi\sigma_V^2\right)\right] \ . \tag{12.17}$$

Putting this together, the mutual information between Alice and Bob is

$$I_{AB} = \frac{1}{2}\log\left(\frac{\sigma_V^2 + \sigma_A^2}{\sigma_V^2}\right) \tag{12.18}$$

$$= \frac{1}{2}\log\left(1 + \frac{\sigma_A^2}{\sigma_V^2}\right) \tag{12.19}$$

$$= \frac{1}{2}\log(1 + \Sigma) \ . \tag{12.20}$$

In the last equality, we write the net mutual information in terms of the average signal to noise ratio

$$\Sigma = \int dx_A\, \frac{x_A^2}{\sigma_V^2} p_A(x_A) \tag{12.21}$$

$$= \frac{\sigma_A^2}{\sigma_V^2} \tag{12.22}$$

where x_A^2/σ_V^2 is the signal to noise ratio when Alice sends the signal x_A and Bob's measurement has a variance σ_V^2.

At this point Alice and Bob share a correlated set of continuous data and can in theory get up to $1/2 \times \log(1+\Sigma)$ bits of information for every measured data point. In fact the sliced reconciliation protocol can get arbitrarily close to the

theoretical limit [12,55]. A bigger variance of Alice's signal will result in a higher amount of shared bits between Alice and Bob.

We have analysed the case when Bob measures the amplitude quadrature X. The net information when Bob measures the phase quadrature would follow in a similar manner.

12.3 A lossy channel

We now consider the effects of transmission losses in the channel between Alice and Bob. We characterise the loss by the transmission coefficient η. The loss can be modelled by a beam splitter with transmission η. Alice's coherent state enters the first port of the beam splitter while the vacuum state enters the second port as in figure 11.1.

From section 11.1.1, the output of the beam splitter would be related to the input by

$$|\alpha\rangle_A |0\rangle_V \rightarrow |\sqrt{\eta}\alpha\rangle_B \left|\sqrt{1-\eta}\alpha\right\rangle_E . \tag{12.23}$$

That is, Bob will still receive a coherent state, but its amplitude is attenuated to $\sqrt{\eta}\alpha$. Bob's outcome is less correlated to the signal Alice sends when there is loss. The conditional probability of Bob to get the outcome x_B is now

$$p_B(x_B|x_A) \sim \mathcal{N}(\sqrt{\eta}x_A, \sigma_V) , \tag{12.24}$$

and the covariance matrix between Alice's and Bob's data C is

$$C = \begin{pmatrix} \sigma_A^2 & \sqrt{\eta}\sigma_A^2 \\ \sqrt{\eta}\sigma_A^2 & \sigma_V^2 + \eta\sigma_A^2 \end{pmatrix} . \tag{12.25}$$

The mutual information between Alice and Bob is then

$$I_{AB} = \frac{1}{2}\log\frac{\sigma_B^2}{\sigma_V^2} \tag{12.26}$$

$$= \frac{1}{2}\log\left(1+\eta\frac{\sigma_A^2}{\sigma_V^2}\right) . \tag{12.27}$$

12.3.1 Eve's information

From the other port of the beam splitter, Eve receives the coherent state $\left|\sqrt{1-\eta}\alpha\right\rangle$. The conditional probability between Alice and Eve is

$$p_E(x_B|x_A) \sim \mathcal{N}\left(\sqrt{1-\eta}x_A, \sigma_V\right) . \tag{12.28}$$

The mutual information between Alice and Eve would be

$$I_{AE} = \frac{1}{2}\log\left(1+(1-\eta)\frac{\sigma_A^2}{\sigma_V^2}\right) . \tag{12.29}$$

Figure 12.1 shows the mutual information between Alice and Bob I_{AB} and Eve's information I_E as a function of the transmission η. The information between Alice and Bob will always be greater than the information between Alice and Eve as long as $\eta > 0.5$. In this region, Alice and Bob can still extract a secure key. Provided $\eta > 0.5$, Alice and Bob can get arbitrarily large information by making

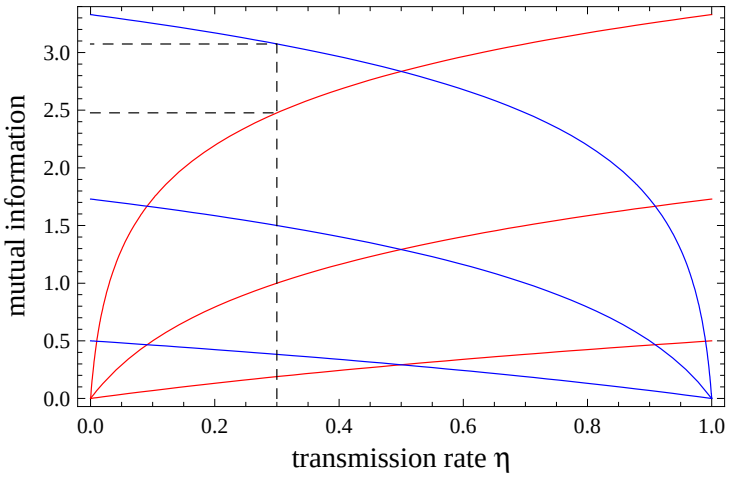


Figure 12.1: Plot of Alice–Eve's mutual information (in blue) and Alice–Bob's mutual information (in red) for a coherent state protocol without post-selection as a function of the transmission rate η. The two curves intersect at $\eta = 0.5$. For $\eta > 0.5$, Eve always has more information than Alice and Bob. The plots are reproduced for three different values of Alice's variance $\sigma_A^2 = \{\sigma_V^2, 10\sigma_V^2, 100\sigma_V^2\}$. For example at $\eta = 0.3$ and $\sigma_A^2 = 100\sigma_V^2$, the mutual information between Alice and Bob is 3.075 bits per signal while Alice and Eve has a mutual information of 2.477 bits per signal. Since Alice and Bob has more information than Alice and Eve, secure communication is still possible at this point.

the variance σ_A^2 large. However once $\eta < 0.5$, Eve will gain too much information and the protocol is no longer secure. This is the origin of the 3 dB limit.

Chapter 13

Introduction to the protocol

The protocol that we shall study was first presented by Silberhorn, Ralph, Lütkenhaus and Leuchs in 2002 [52]. In this protocol, Alice sends a coherent state $|\alpha\rangle$ to Bob. Bob measures either the real or imaginary part of α. Bob will announce the measurement basis he used as well as the absolute value of the measurement result. Alice subsequently announces the absolute value of the real or imaginary part of α depending on which measurement Bob performed. With this information, Alice and Bob will share a binary symmetric channel with some error probability that they can estimate.

Alice and Bob can also estimate the transmission and noise characteristics of the channel. From this, they can estimate how much information an eavesdropper can gain. Alice and Bob then perform post-selection. If the eavesdropper has more information than Bob, then the data point is discarded, otherwise it is kept. By doing post-selection, Alice and Bob can overcome the 3 dB limit of the Grosshans and Grangier 2002 protocol [23].

In the perfect channel with transmission $\eta = 1$, this protocol would be less efficient than the Grosshans and Grangier 2002 protocol. In this protocol, every coherent state Alice sent can give at best just one bit of information. In the Grosshans and Grangier 2002 protocol, if the transmission is greater than half, Alice can choose a large variance σ_A of the Gaussian distribution of the coherent states to send and potentially extract an arbitrarily large length of key from a single coherent state.

However if the transmission is less than half, the Grosshans and Grangier 2002 protocol would fail to yield any key whereas this protocol will still give a positive key rate up to certain noise threshold.

In section 13.1, we give a formal description of the protocol as well as how Alice and Bob estimate the channel parameters. Next, section 13.2 gives the protocol for extracting the keys from the raw data. Finally, in section 13.3, we shall calculate the mutual information between Alice and Bob as a function of the channel parameters.

13.1 The protocol

In this protocol, Alice picks N pairs of numbers $\left\{x_A^j, y_A^j\right\}$ for $j \in \{1,2,\ldots,N\}$. Both x_A^j and y_A^j are picked from a Gaussian distribution with variance σ_A^2 and mean zero

$$p_A(x_A) \sim \mathcal{N}(0,\sigma_A) \ , \tag{13.1}$$

$$p_A(y_A) \sim \mathcal{N}(0,\sigma_A) \ . \tag{13.2}$$

Alice then prepares a sequence of N coherent states $\left|\alpha^j\right\rangle$ with the complex amplitudes $\alpha^j = x_A^j + \mathrm{i}y_A^j$.

Bob will then choose to measure each coherent state with either the amplitude operator X or the phase operator Y. If the transmission channel between Alice and Bob was perfect, then when Bob measures X given that Alice sends x_A, the outcome of Bob's measurement will have a Gaussian distribution with mean x_A and variance σ_V^2.

However with a lossy and noisy transmission channel with a Gaussian noise, the outcome of Bob's measurement will have a mean of $\sqrt{\eta}x_A$ and a variance $(1+\delta)\sigma_V^2$ where η characterises the loss and δ characterises the excess noise. The conditional probabilities are drawn from the following normal distributions

$$p_B(x_B|x_A) \sim \mathcal{N}\left(\sqrt{\eta}x_A, \sqrt{1+\delta}\sigma_V\right) , \tag{13.3}$$

$$p_B(y_B|y_A) \sim \mathcal{N}\left(\sqrt{\eta}y_A, \sqrt{1+\delta}\sigma_V\right) . \tag{13.4}$$

Before proceeding with the key generation, Alice and Bob will use some measurement results to characterise the channel. They check that their data is indeed consistent with the expected probability distributions up to some confidence level. They check that for the amplitude quadrature, their joint probability $p_{AB}(x_A, x_B)$ is Gaussian with mean $(\bar{x_A}, \bar{x_B}) = (0,0)$ and covariance matrix

$$C = \begin{pmatrix} \sigma_A^2 & \sqrt{\eta}\sigma_A^2 \\ \sqrt{\eta}\sigma_A^2 & (1+\delta)\sigma_V^2 + \eta\sigma_A^2 \end{pmatrix} \tag{13.5}$$

so that

$$p_{AB}(x_A, x_B) = \frac{1}{2\pi\sqrt{\det C}} \exp\left(-\frac{1}{2}\vec{x}C^{-1}\vec{x}\right) \tag{13.6}$$

where $\vec{x} = (x_A, x_B)$. Otherwise the protocol fails and is aborted. If the probability is consistent, the three parameters of the channel—σ_A, η and δ—can be obtained from the three covariance equations

$$\left\langle x_A^2 \right\rangle = \sigma_A^2 \,, \tag{13.7}$$

$$\langle x_A x_B \rangle = \sqrt{\eta}\sigma_A^2 \,, \tag{13.8}$$

$$\left\langle x_B^2 \right\rangle = (1+\delta)\sigma_V^2 + \eta\sigma_A^2 \,. \tag{13.9}$$

Alice and Bob will repeat the same characterisation for the phase quadrature.

In the next step of the protocol, Bob announces the quadrature she measured, either X or Y as well as the absolute value of his measurement result. If Bob announces that he measured X, Alice will reveal the absolute value of x_A and if Bob announces that he measured Y, Alice will reveal the absolute value of y_A. Each pair of absolute values $(|x_A|, |x_B|)$ and $(|y_A|, |y_B|)$ constitute a binary channel between Alice and Bob.

13.2 Key extraction

When Bob measures in the X quadrature, for a given signal that Alice sends x_A and measurement outcome x_B, the raw key between Alice and Bob is given by the parity of x_A and x_B. We denote the absolute values of x_A and x_B by $s_A = |x_A|$

and $m_B = |x_B|$ respectively. If Bob measures in the phase quadrature, then it will be the imaginary parts that we shall be interested in. In this case, using the same symbols, we denote $s_A = |y_A|$ and $m_B = |y_B|$. The following table gives an example of a set of ten signals and outcomes from a hypothetical experiment with $\eta = 0.5$, $\delta = 0.2$ and $\sigma_A^2 = 4\sigma_V^2$ in units where $\sigma_V^2 = 1$.

Alice's signal, α	Bob's quadrature	Bob's outcome	m_B	s_A	Alice/Bob's bits
$0.87+0.90$i	X	1.16	1.16	0.87	$(+,+)$
$1.81+1.89$i	Y	0.16	0.16	1.89	$(+,+)$
$-1.57+4.23$i	X	-0.70	0.70	1.57	$(-,-)$
$-1.23-1.30$i	Y	-0.57	0.57	1.30	$(-,-)$
$0.80+0.60$i	X	-0.30	0.30	0.80	$(+,-)$
$-2.90+2.68$i	Y	1.03	1.03	2.68	$(+,+)$
$1.98-1.03$i	Y	0.09	0.09	1.03	$(-,+)$
$-1.37-0.21$i	Y	-1.34	1.34	0.21	$(-,-)$
$1.16+0.67$i	X	0.60	0.60	1.16	$(+,+)$
$3.77-3.11$i	X	3.60	3.60	3.77	$(+,+)$

In this example, the fifth and seventh data points contain errors.

Even in a perfect transmission channel with $\eta = 1$, this binary channel will not be perfect. There will be error when Alice sends a positive signal s_A but Bob measures a negative outcome $-m_B$ or when Alice sends a negative signal $-s_A$ but Bob measures a positive outcome m_B. The probability of error would be

$$p_{\text{error}}(s_A, m_B) \tag{13.10}$$

$$= \frac{p(m_B, -s_A) + p(-m_B, s_A)}{p(m_B, s_A) + p(-m_B, s_A) + p(m_B, -s_A) + p(-m_B, -s_A)} \tag{13.11}$$

$$= \frac{1}{1+\exp\left(\frac{2\sqrt{\eta}s_A m_B}{(1+\delta)\sigma_V^2}\right)} \tag{13.12}$$

which is $1/2$ when the product $s_A m_B = 0$ and goes to zero for large $s_A m_B$. This means that the channel is better for larger values of $s_A m_B$. The probability distribution between Alice and Bob for the channel is given by the following table.

Alice's signal	Outcome of Bob's measurement	
	m_B	$-m_B$
s_A	$\frac{1-p_{\text{error}}}{2}$	$\frac{p_{\text{error}}}{2}$
$-s_A$	$\frac{p_{\text{error}}}{2}$	$\frac{1-p_{\text{error}}}{2}$

13.3 Mutual information between Alice and Bob

From the binary symmetric probability table between Alice and Bob, we can calculate the mutual information between Alice and Bob for a particular value of s_A and m_B

$$I_{AB}(s_A, m_B) = 2\left(\frac{p_{\text{error}}}{2}\right)\log\frac{\frac{p_{\text{error}}}{2}}{\frac{1}{2}\frac{1}{2}} + 2\left(\frac{1-p_{\text{error}}}{2}\right)\log\frac{\frac{1-p_{\text{error}}}{2}}{\frac{1}{2}\frac{1}{2}} \tag{13.13}$$

$$= 1 + p_{\text{error}}\log p_{\text{error}} + (1-p_{\text{error}})\log(1-p_{\text{error}}) \tag{13.14}$$

$$= \Phi(1-2p_{\text{error}}) \tag{13.15}$$

where $\Phi(x) = [(1+x)\log(1+x) + (1-x)\log(1-x)]/2$. Depending on whether the information between Alice and Bob is greater or the information that Eve can gain is greater, the channel will be selected or not selected. Only the data from the selected channel will be used in the key generation.

The final key rate between Alice and Bob is obtained by integrating the difference between Alice and Bob's information and Eve's information $I_{AB}(s_A, m_B) - I_E(s_A, m_B)$ weighted by the probabilities $p_{AB}(s_A, m_B)$ over the post-selected re-

gion. For a given η and δ, this net information would depend on the post-selected region as well as the distribution of Alice's signal.

The regions to be post-selected are those in which Alice and Bob have a higher mutual information than Alice and Eve or Bob and Eve. To proceed we shall need to calculate Eve's information or at least put a bound on it.

Chapter 14

Eve's information without thermal noise

Before proceeding to the general case with transmission loss and noisy channel, we recap and elaborate some results for the case of transmissions in lossy channels without excess noise as presented in [52].

Section 14.1 introduces the scenario we will be analysing. In section 14.2, we calculate the mutual information between Alice and Bob after post-selection for a channel with vacuum noise. Section 14.3 analyses the security of the protocol under individual attacks. Finally, section 14.4 repeats the same analysis for collective attacks.

14.1 Post-selection without thermal noise

We are going to study the security of the protocol in a lossy quantum channel between Alice and Bob. Alice sends the coherent state $|\alpha\rangle$ with $\alpha = x_A + \mathrm{i}y_A$. In

a lossy but not noisy channel, when Bob repeatedly measures the amplitude and phase quadratures on different copies of the state that she receives, the outcome of Bob's measurement will still have variance σ_V^2 but the mean values will now be $(\langle X\rangle_\alpha, \langle Y\rangle_\alpha) = (\sqrt{\eta}x_A, \sqrt{\eta}y_A)$.

The channel between Alice and Bob is modelled by a beam splitter with transmittivity η where a vacuum state $|0\rangle$ enters through the unused port of the beam splitter. For every α, because the variance of Bob's measurement is σ_V^2, Bob is certain that he has a pure state. Bob knows that he has the coherent state $\left|\sqrt{\eta}\alpha\right\rangle$ and not something else.

However, in the noisy case, when the variances of Bob's quadrature measurements are greater than σ_V^2, Bob will not know for certain the state he received because, by only measuring the X and Y quadratures, he is not doing a complete tomography of the state. For example, he would not be able to unambiguously reconstruct the state's Wigner function. To do that he would have to measure all quadrature angles.

We attribute the loss in the channel to the actions of an adversary Eve. In the beam splitter model, the second output of the beam splitter is kept by Eve. Hence, for the input state $|\alpha\rangle$, Eve will keep state $\left|\sqrt{1-\eta}\alpha\right\rangle$ in her record.

14.2 Mutual information between Alice and Eve

As the protocol goes, Bob will then announce the quadrature that he measures and the absolute value of his measurement result. Suppose Bob chose the X quadrature as his measurement basis. Then he will announce $m_B = |x_B|$. Subsequently

Alice announces the absolute value of her signal corresponding to the measured quadrature. In this case, Alice will announce the value of $s_A = |x_A|$.

Eve would like to gain as much information as she can regarding the value of Alice's signal in the chosen quadrature, in this case the X quadrature. She would not be interested in the Y quadrature value as that value will not be used in the key generation at all.

After Alice's announcement of s_A, Eve will know that Alice encoded either s_A or $-s_A$ onto the amplitude quadrature. The parity of this encoding provides the raw key. Since Eve does not know the value of Alice's encoding in the phase quadrature y_A, her input states are then two mixed states obtained by integrating Alice's input states over y_A

$$\rho_E(\pm s_A) = \int dy_A \; p_A(y_A) \left| \sqrt{1-\eta}\,(\pm s_A + \mathrm{i}y_A) \right\rangle \left\langle \sqrt{1-\eta}\,(\pm s_A + \mathrm{i}y_A) \right| . \tag{14.1}$$

Here $p_A(y_A)$ is the probability for Alice to encode the signal y_A in the phase quadrature. To obtain an upper bound on Eve's information, we provide Eve with the actual value of y_A. Clearly, we are providing Eve with more power than she originally has. In this case, Eve's input state will be the two pure states

$$|\psi_E(\pm s_A, y_A)\rangle = \left| \sqrt{1-\eta}\,(\pm s_A + \mathrm{i}y_A) \right\rangle . \tag{14.2}$$

For this input state, we shall find the amount of information Eve can obtain by doing individual attacks (in section 14.3) and collective attacks (in section 14.4). Both values depend only on the overlap between the two input states. The overlap

between the two states is

$$f = \left|\left\langle \psi_E\left(+s_A\right)\middle|\psi_E\left(-s_A\right)\right\rangle\right| = \exp\left(-2s_A^2\left(1-\eta\right)\right) \tag{14.3}$$

which does not depend on y_A as one would expect.

14.3 Post-selection: Individual attack, without thermal noise

In this section, we consider the case where Eve carries out an individual attack.

14.3.1 Information difference

The maximum information Eve can learn when she performs an individual attack is given by the accessible information of Eve's input states. In this case Eve's input state that she can measure to attack Alice or Bob would be $|\psi_E\left(\pm s_A\right)\rangle$, which does not depend on Bob's measurement results. Using the result for accessible information for two pure input states in section 2.4.1, we find that Eve's accessible information is

$$I_E^{\text{ind}}\left(s_A\right) = \Phi\left(\sqrt{1-f^2}\right) \tag{14.4}$$

where $f = \exp\left(-2s_A^2\left(1-\eta\right)\right)$ is the absolute value of the inner product between Eve's input states. Figure 14.1 plots Eve's information against x_A for transmission $\eta = 0.5$. When Alice announces that the value of s_A is very large, Eve is very

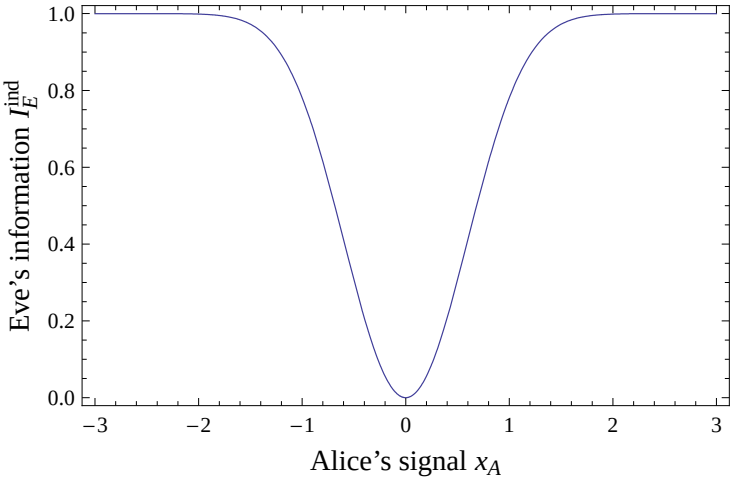


Figure 14.1: A bound for the mutual information between Alice and Eve for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ as a function of Alice's signal when Eve is limited to individual attacks. The information does not depend on Bob's measurement outcome.

confident that she can guess correctly Alice's bit. However when s_A is close to zero, Eve has very little information on Alice's bit.

From equation (13.15), we found that the mutual information between Alice and Bob was

$$I_{AB} = \Phi(1 - 2p_{\text{error}}) \tag{14.5}$$

where for noiseless transmission with $\delta = 0$, the probability of error is

$$p_{\text{error}} = \frac{1}{1 + \exp\left(\frac{2\sqrt{\eta}s_A m_B}{\sigma_V^2}\right)} \,. \tag{14.6}$$

A contour plot for the mutual information between Alice and Bob is shown in figure 14.2.

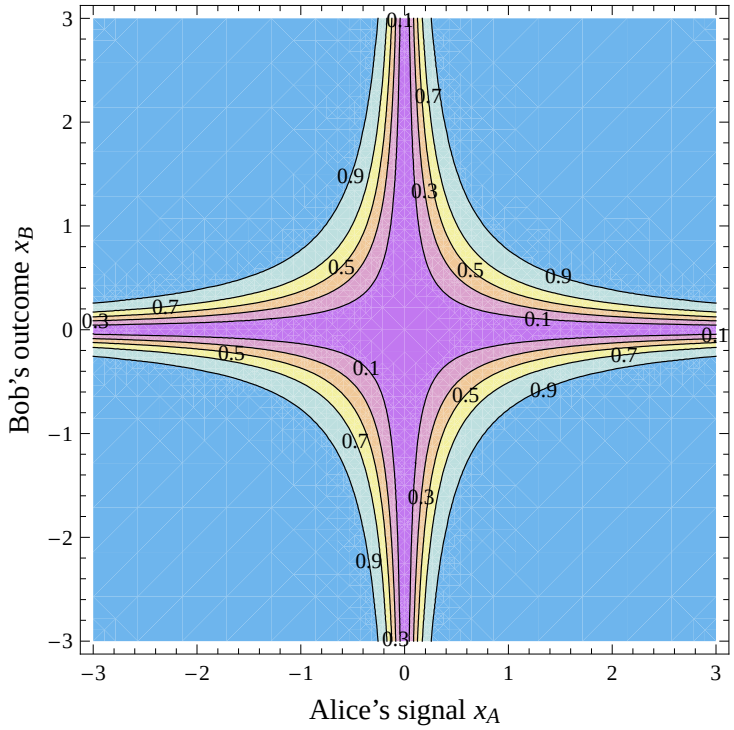


Figure 14.2: Mutual information between Alice and Bob are shown as contours for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ as a function of Alice's signal and Bob's measurement result.

14.3.2 Post-selection region

The regions to be post-selected are those in which Alice and Bob have more information than Eve. The difference between the information as a function of x_A and x_B is plotted in figure 14.3. This difference gives the theoretical limit for the key rate. Data points that fall in the post-selected region would contribute to the raw key generation. We see that the points having very large values of x_B and relatively small values of x_A give Alice and Bob a high information advantage over Eve. However, as the joint probability distribution is far from its maximum here, we don't expect that the majority of the data points to fall here.

The post-selected region is defined as the region where

$$I_{AB} > I_E^{\text{ind}} \tag{14.7}$$

$$\implies \Phi\left(1-2p_{\text{error}}\right) > \Phi\left(\sqrt{1-f^2}\right) \tag{14.8}$$

$$\implies 1-2p_{\text{error}} > \sqrt{1-f^2}\,. \tag{14.9}$$

The boundary of the post-selected region is obtained by solving

$$1-\frac{2}{1+\exp\left(\frac{2\sqrt{\eta}s_A m_B}{\sigma_V^2}\right)} = \sqrt{1-\exp\left(-4s_A^2(1-\eta)\right)} \tag{14.10}$$

which gives

$$m_B = \frac{\sigma_V^2}{2\sqrt{\eta}s_A}\log\left(\frac{2}{1-\sqrt{1-\exp\left(-4s_A^2(1-\eta)\right)}}-1\right)\,. \tag{14.11}$$

The post-selected region is shown in figure 14.3.

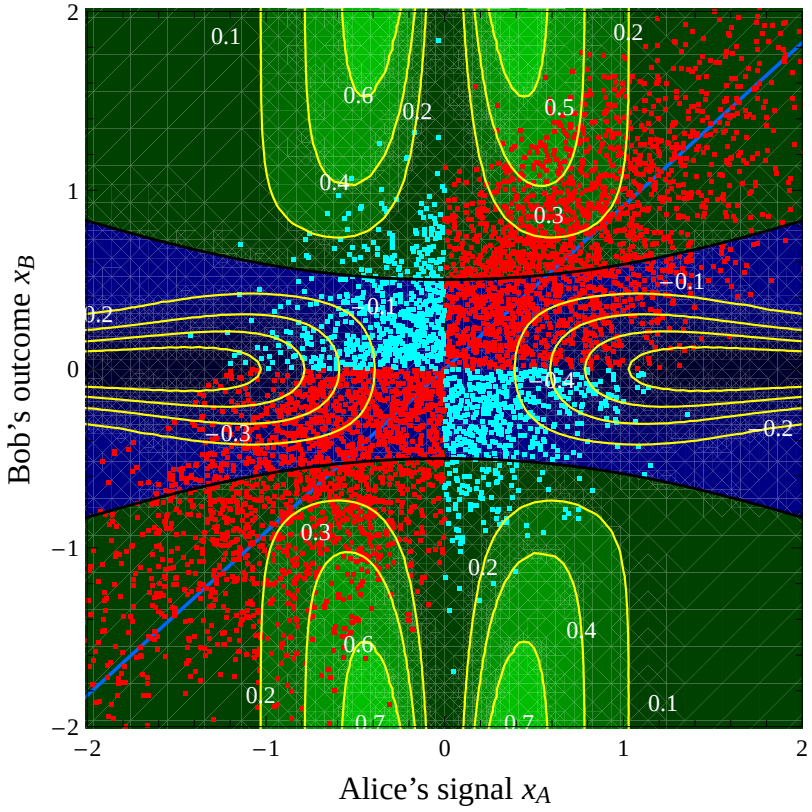


Figure 14.3: Contour plot of the difference in information between Alice–Bob and Alice–Eve for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ when Eve does individual attacks. The difference in information is plotted as a function of Alice's signal and Bob's measurement outcome. The post-selected regions, coloured in green, are those in which the difference is positive. The red and blue dots are 5000 randomly simulated data points with Alice sending randomly distributed coherent states having mean zero and variance $3\sigma_V^2$. In the protocol, those data points lying outside the post-selected region will not be included in the key-extraction scheme. The gradient of the blue line gives the ratio σ_B/σ_A.

14.3.3 Alice's distribution

Now that we know the key rate that each effective channel (s_A, m_B) provides, we want our distribution of data points to be such that it gives us the maximum key rate. We want a lot of points to fall in the high key rate region and not too many in the discarded region.

Alice can decide what states to send to Bob. For a particular value of x_A that she sends, Bob will obtain an outcome x_B with a probability $p_B(x_B|x_A)$, which is normally distributed with mean $\sqrt{\eta}x_A$ and variance $(1+\delta)\sigma_V^2$. For a given $s_A = |x_A|$, the key rate between Alice and Bob would be

$$r_k^{\text{ind}}(s_A) = \int_{\Omega_{I>0}} dm_B \left(I_{AB} - I_E^{\text{ind}}\right) p_B(m_B|s_A) \tag{14.12}$$

where $\Omega_{I>0}$ is the post-selected region. The key rate is plotted as a function of s_A in figure 14.4. From the plot, we find that the key rate is maximum when Alice's signal has the value $s_A = 0.71$.

In principle, Alice could just send the coherent states with $x_A = \pm 0.71$ and this would give a key rate rate between Alice and Bob of 0.1260 bits per signal. But in practice it would be easier for Alice to send coherent states with a Gaussian distribution rather than switching between some discrete set of coherent states.

To maximise the key rate, Alice will choose the variance of her Gaussian distribution such that

$$r_k^{\text{ind}} = \int_{\Omega_{I>0}} ds_A\, dm_B \left(I_{AB} - I_E^{\text{ind}}\right) p_{AB}(s_A, m_B) \tag{14.13}$$

$$= \int ds_A r_k^{\text{ind}}(s_A) p_A(s_A) \tag{14.14}$$

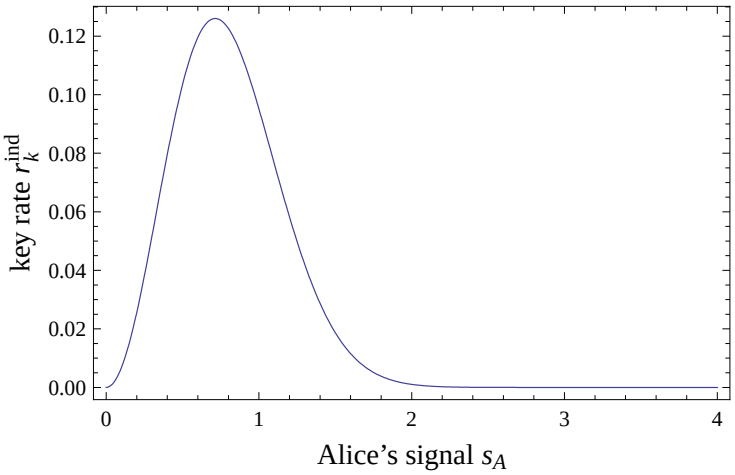


Figure 14.4: A plot of the key rate between Alice and Bob for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ after doing post-selection as a function of Alice's signal when Eve does an individual attack. The maximum key rate occurs when Alice sends $s_A = 0.71$ for which the maximum key rate extractable would be 0.1260 bits per signal.

is maximum. Here p_A is Alice's signal distribution having mean zero and variance σ_A^2. This integration can be computed numerically. Some values of r_k^{ind} corresponding to some chosen values of the variance σ_A^2 are given in the following table:

σ_A^2	Key rate r_k^{ind}
0.25	0.06080
0.50	0.06644
1.00	0.06198
4.00	0.03972

These values are plotted in figure 14.9 which shows the variation of r_k as a function of the variance σ_A^2. The maximum key rate is 0.06644 bits per signal when $\sigma_A^2 = 0.51$. This is the variance that Alice should use to maximise her key rate.

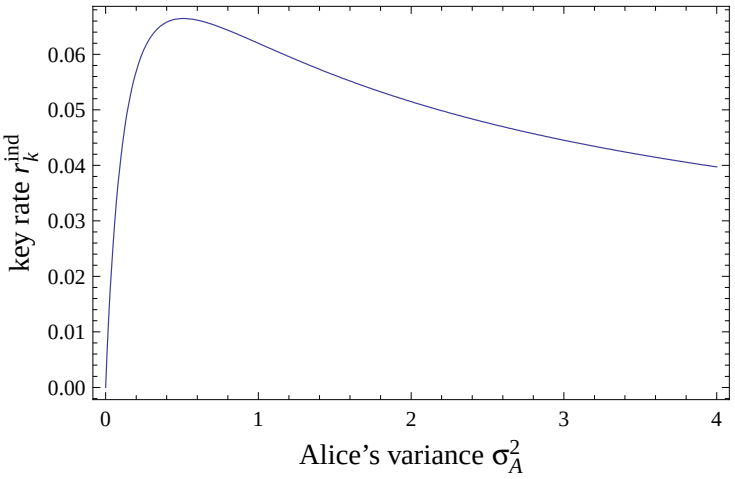


Figure 14.5: A plot of the key rate between Alice and Bob for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ after doing post-selection as a function of Alice's signal variance σ_A^2 when Alice sends a Gaussian distribution. This figure is for individual attacks by Eve. The x-axis is normalised so that the vacuum state has a variance $\sigma_V^2 = 0.25$. The maximum is when $\sigma_A^2 = 0.51$ for which the attainable key rate is 0.06644 bits per signal.

14.3.4 Optimal variance and key rate

For different values of transmission η, the optimal variances for Alice and the maximum key rates Alice and Bob can get are summarised in the following table.

η	σ_A^2	Key rate r_k^{ind}
0	–	0
0.1	0.19	0.00005
0.2	0.30	0.00268
0.3	0.38	0.01332
0.4	0.44	0.03433
0.5	0.51	0.06644
0.6	0.58	0.11077
0.7	0.68	0.17028
0.8	0.84	0.25247
0.9	1.22	0.38074
1	∞	1

The key rate goes to zero as the transmission η goes to zero. But in principle, it is always positive for all $\eta > 0$.

14.4 Post-selection: Collective attack, without thermal noise

In this section, we repeat the same analysis done in the previous section but for a collective attack.

14.4.1 Information difference

When Eve does a collective attack, the maximum information she can gain is given by the Holevo bound. After providing Eve the additional information about Alice's signal in the unmeasured quadrature, Eve's input states are just two pure states. For these two pure state inputs $|\psi_E(\pm s_A)\rangle$, we found from section 2.4.2

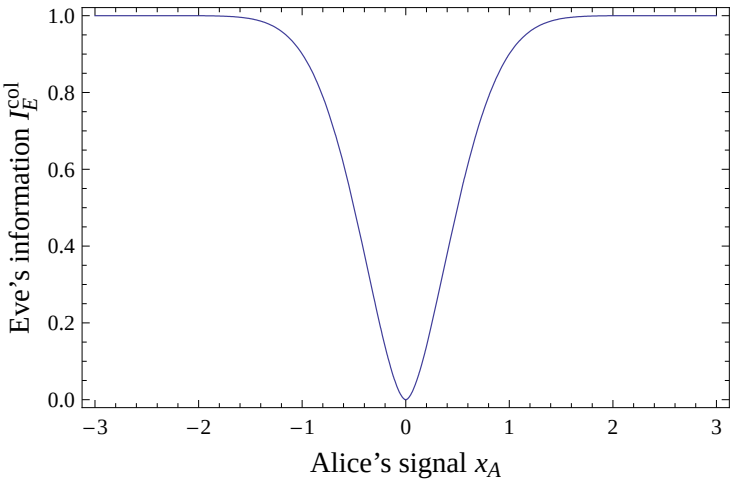


Figure 14.6: A bound for the mutual information between Alice and Eve for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ as a function of Alice's signal in a collective attack. The information does not depend on Bob's measurement outcome.

that the Holevo bound gives Eve's maximum information to be

$$I_E^{\text{col}}(s_A) = 1 - \Phi(f) \tag{14.15}$$

where $f = \exp\left(-2s_A^2(1-\eta)\right)$ is the overlap between Eve two inputs. Figure 14.6 plots Eve's information against x_A for transmission $\eta = 0.5$. When Alice announces that the value of s_A is very large, Eve is very confident that she can guess correctly Alice's bit. However when s_A is close to zero, Eve has very little information on Alice's bit.

The information between Alice and Bob depends only on the channel parameters. It does not depend on the type of attack that Eve does. As long as these parameters are the same, the mutual information between Alice and Bob is still $I_{AB} = \Phi(1 - p_{\text{error}})$, the same as in section 14.3.1 when Eve does an individual

attack. This mutual information between Alice and Bob for transmission $\eta = 0.5$ was plotted in figure 14.2.

14.4.2 Post-selection region

The difference between the mutual information between Alice and Bob and Eve's information is plotted in the contour plot in figure 14.7. Positive values of this difference gives the maximum theoretical limit for the key rate at that point. The points with positive key rate would be post-selected. Only data points that fall in the post-selected region would contribute to the raw key generation.

The post-selected region is defined by the region with

$$I_{AB} > I_E^{\text{col}} \tag{14.16}$$

$$\implies \Phi(1-2p_{\text{error}}) > 1-\Phi(f)\ . \tag{14.17}$$

14.4.3 Alice's distribution

Now that we have the key rate that each effective channel (s_A, m_B) provides, we want our distribution of points to be such that it give us the maximum net key rate. We want a lot of points to be in the high key rate region and not too many in the discarded region.

Alice can decide what states to send to Bob. For a particular value of x_A that she sends, Bob will obtain an outcome x_B with a probability $p_B(x_B|x_A)$, which is normally distributed with mean $\sqrt{\eta}x_A$ and variance $(1+\delta)\sigma_V^2$. For a given

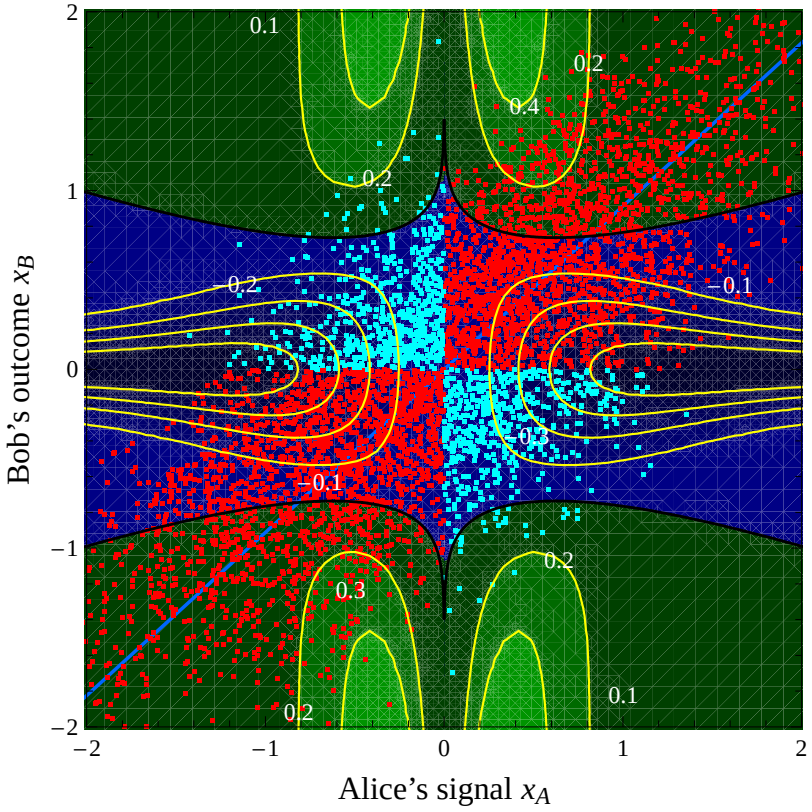


Figure 14.7: Contour plot of the difference in information between Alice–Bob and Alice–Eve for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ when Eve does collective attacks. The difference in information is plotted as a function of Alice's signal and Bob's measurement outcome. The post-selected region, coloured in green, are those in which the difference is positive. The red dots are 5000 randomly simulated data points with Alice sending randomly distributed coherent states having mean zero and variance $3\sigma_V^2$. In the protocol, those data points lying outside the post-selected region will not be included in the key-extraction scheme. The gradient of the blue line gives the ratio σ_B/σ_A.

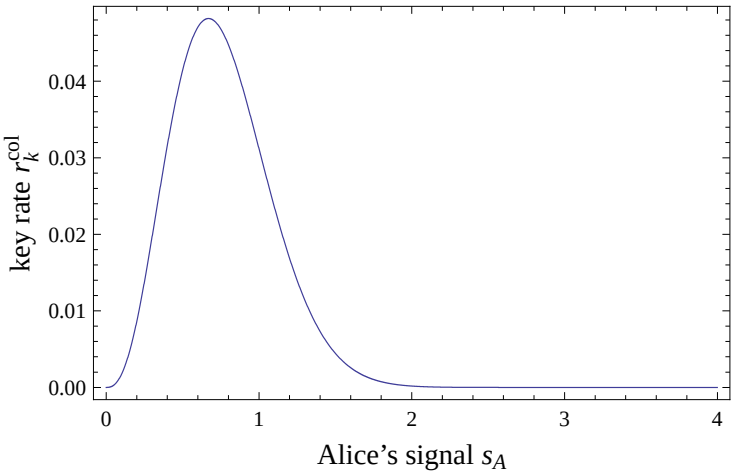


Figure 14.8: A plot of the key rate between Alice and Bob for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ after doing post-selection as a function of Alice's signal when Eve does a collective attack. The maximum key rate occurs when Alice sends $s_A = 0.67$ for which the key rate would be 0.04819 bits per signal.

$s_A = |x_A|$, the key rate between Alice and Bob would be

$$r_k^{\text{col}}(s_A) = \int_{\Omega_{I>0}} dm_B \left(I_{AB} - I_E^{\text{col}} \right) p_B(m_B|s_A) \tag{14.18}$$

where $\Omega_{I>0}$ is the post-selected region. The key rate is plotted in figure 14.8. From the graph, we see that the key rate is maximum when $s_A = 0.67$.

In principle, Alice could just use the value of $s_A = 0.67$ and send the signals having $x_A = \pm 0.67$. This would give a key rate rate of 0.04819 bits per signal. But in practice it would easier for Alice to send coherent states with a Gaussian distribution rather than switching between some discrete set of coherent states.

Alice's Gaussian distribution $p_A(s_A)$ has mean zero and the variance is chosen so that

$$r_k^{\text{col}} = \int_{\Omega_{I>0}} ds_A\, dm_B \left(I_{AB} - I_E^{\text{col}}\right) p_{AB}(s_A, m_B) \tag{14.19}$$

$$= \int ds_A r_k^{\text{col}}(s_A) p_A(s_A) \tag{14.20}$$

is maximum. This integration can be computed numerically. Some values of r_k^{col} corresponding to some chosen values of the variance σ_A^2 are given in the following table:

σ_A^2	Key rate r_k^{col}
0.25	0.02281
0.50	0.02443
1.00	0.02235
4.00	0.01401

These values are plotted in figure 14.9 which shows the variation of r_k^{col} as a function of the variance σ_A^2. The key rate attains a maximum value of 0.02445 bits per signal when $\sigma_A^2 = 0.46$. This is the variance that Alice should use to maximise the key rate.

14.4.4 Optimal variance and key rate

For different values of transmission η, the optimal variances for Alice and the maximum key rates for Alice and Bob are summarised in the following table:

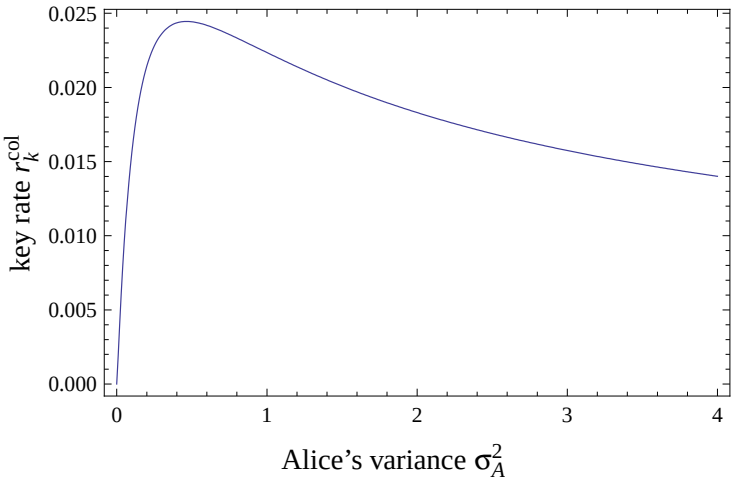


Figure 14.9: A plot of the key rate between Alice and Bob for a noiseless coherent state protocol with channel transmission $\eta = 0.5$ after doing post selection as a function of Alice's signal variance σ_A^2 when Alice sends a Gaussian distribution. This figure is for collective attacks by Eve. The vacuum state has a variance $\sigma_V^2 = 0.25$. The maximum is when $\sigma_A^2 = 0.46$ for which the attainable key rate is 0.02445 bits per signal.

η	σ_A^2	Key rate r_k^{col}
0	–	0
0.1	0.27	$< 10^{-5}$
0.2	0.33	0.00018
0.3	0.38	0.00225
0.4	0.42	0.00935
0.5	0.46	0.02445
0.6	0.52	0.05054
0.7	0.59	0.09197
0.8	0.71	0.15777
0.9	0.99	0.27469
1	∞	1

The key rate goes to zero as the transmission η goes to zero. But it remains positive for all values of $\eta > 0$.

Chapter 15

Post-selection with thermal noise

We now return to the case when the transmission channel between Alice and Bob is both lossy and noisy. In the previous chapter, we have seen that the coherent state post-selection protocol can tolerate loss in the channel when there is no excess noise. However in any practical implementations of the protocol, there will be some excess noise in the channel.

By a noisy channel with excess noise, we mean that when Alice sends the coherent state $|\alpha\rangle$ with $\alpha = x_A + iy_A$, Bob will not receive a coherent state. Instead, when Bob measures the amplitude and phase quadratures, he will find the mean values to be $(\langle X_B\rangle_\alpha, \langle Y_B\rangle_\alpha) = (\sqrt{\eta}x_A, \sqrt{\eta}y_A)$ and both measurements to have variances $\mathrm{var}(X_B)_\alpha = \mathrm{var}(Y_B)_\alpha = (1+\delta)\,\sigma_V^2$ where $\delta \geq 0$ is the excess noise and η is the channel transmission. In this analysis, we assume that the excess noise in the amplitude and phase quadratures are equal. If they are not equal up to some tolerance, Alice and Bob abort the protocol. Precisely what that tolerance should be would depend on the security level Alice and Bob desire and the uncertainties in

parameterising their channel. The details of these considerations would require further studies beyond the scope of this thesis.

In this chapter, we want to study the performance of the protocol in the presence of excess noise. Some results from this chapter have been published elsewhere [1, 54]. The effects of excess noise on the security of coherent state quantum cryptography were also discussed by Heid and Lütkenhaus [25].

Section 15.1 gives the input states that Eve receives that she will use to learn something about Alice and Bob's communication. Section 15.2 gives bounds on Eve's information for individual and collective attacks on Alice. Section 15.3 looks at the case when Eve does her attacks on Bob. Section 15.4 discusses whether it would be advantageous for Alice and Bob to do forward reconciliation or reverse reconciliation. Section 15.5 gives the noise threshold for secure key distribution in both individual and collective attacks.

15.1 Eve's input states

We want to bound Eve's information on Alice and Bob's bits when we restrict Eve to a Gaussian attack. Before doing that, we shall find out what are the restrictions on Eve's input states. Once again, we model Eve's eavesdropping via a beam splitter with a mixed state entering through one of the ports. The situation is depicted in figure 15.1.

The checks that Alice and Bob do would impose some restrictions on the Gaussian state that enters through the vacuum port $a_{V_{in}}$. Since the state that Bob receives at a_B must have the same variances in the amplitude and phase quadratures, the state entering through $a_{V_{in}}$ must also have equal variances in both quadratures

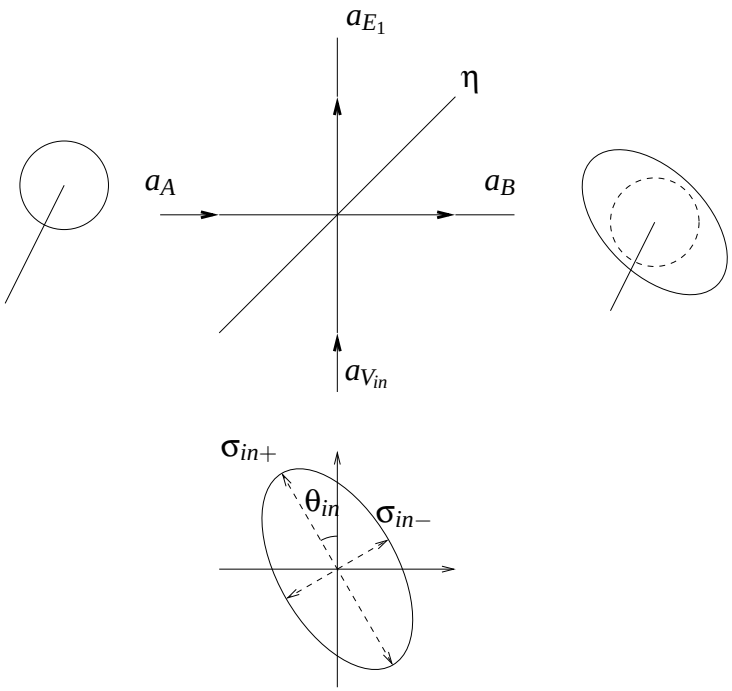


Figure 15.1: Beam splitter loss model for Eve's eavesdropping in the coherent state protocol with thermal noise. Alice sends a coherent state $|\alpha\rangle = |x_A + iy_A\rangle$ into a_A, the first port of a beam splitter with transmission η. A Gaussian state from Eve enters the second port at $a_{V_{in}}$. This state has variance σ_{th}^2 in both the X and Y quadratures. The state Bob receives at the output a_B is another Gaussian state with variances $(1+\delta)\sigma_v^2$ in the X and Y quadratures and a mean amplitude of $\sqrt{\eta}x_A + i\sqrt{\eta}y_A$.

with mean zero. We denote the variances in the X and Y quadratures of $a_{V_{in}}$ by $\mathrm{var}(X_{V_{in}}) = \mathrm{var}(Y_{V_{in}}) = \sigma_{th}^2$.

The variance of the thermal state through $a_{V_{in}}$ is related to the excess noise at Bob's output by

$$\eta\sigma_V^2 + (1-\eta)\sigma_{th}^2 = (1+\delta)\sigma_V^2, \tag{15.1}$$

from which we get

$$\sigma_{th}^2 = \left(1 + \frac{\delta}{1-\eta}\right)\sigma_V^2 \,. \tag{15.2}$$

From section 11.4, the variances along the X and Y quadratures are related to variance of the minimum-variance-quadrature σ_{in-}^2 and the variance of the maximum-variance-quadrature σ_{in+}^2 by

$$\mathrm{var}(X_{V_{in}}) = \sigma_{in-}^2 \cos^2\theta_{in} + \sigma_{in+}^2 \sin^2\theta_{in} = \sigma_{th}^2 \,, \tag{15.3}$$

$$\mathrm{var}(Y_{V_{in}}) = \sigma_{in-}^2 \sin^2\theta_{in} + \sigma_{in+}^2 \cos^2\theta_{in} = \sigma_{th}^2 \,, \tag{15.4}$$

where θ_{in} is the quadrature angle corresponding to minimum variance quadrature.

Solving these two equations, we get $\theta_{in} = \pi/4$ for which

$$\frac{1}{2}\left(\sigma_{in-}^2 + \sigma_{in+}^2\right) = \sigma_{th}^2 \,. \tag{15.5}$$

Additionally, in order to satisfy the Heisenberg uncertainty relation, we must have $\sigma_{in-}\sigma_{in+} \geq \sigma_V^2$. The acceptable range of σ_{in-}^2 and σ_{in+}^2 is shown as the black line in figure 15.2. This line can be parametrised by an eccentricity parameter ε with

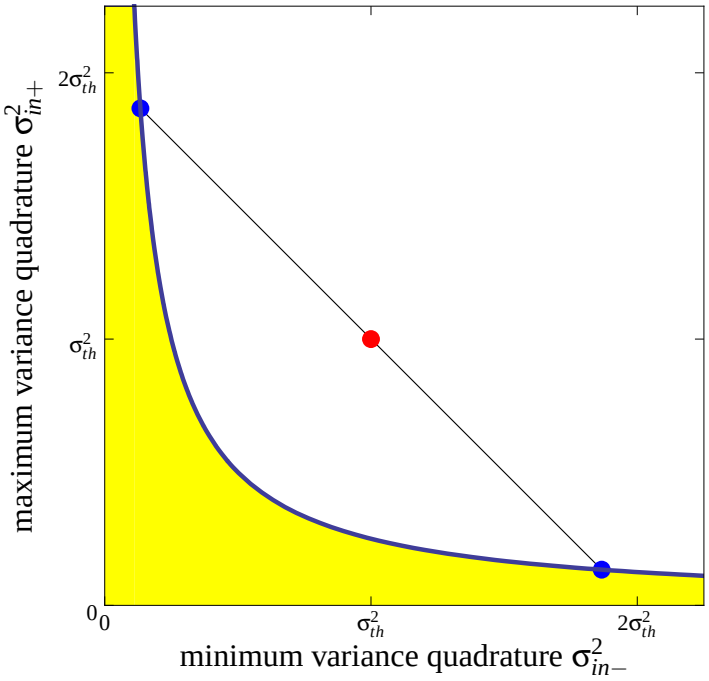


Figure 15.2: Plot showing the acceptable Gaussian states that Eve can send into the vacuum port of the beam splitter loss model in the coherent state protocol with thermal noise. The black line denotes states that are acceptable to Bob where $\frac{1}{2}\left(\sigma^2_{in-}+\sigma^2_{in+}\right)=\sigma^2_{th}$. The quadrature squeezing angles for these states must be $\theta_{in}=\pi/4$. The blue line corresponds to pure states where $\sigma_{in-}\sigma_{in+}=\sigma^2_V$. The two blue dots corresponds to Eve injecting a 45 degrees pure squeezed state through the vacuum port. At the red dot, Eve injects a thermal state, which could be entangled to a second thermal state. The area shaded yellow are states that are not physical as they would violate Heisenberg uncertainty relation.

$$\sigma_{in-}^2 = (1-\varepsilon)\sigma_{th}^2 \,, \tag{15.6}$$

$$\sigma_{in+}^2 = (1+\varepsilon)\sigma_{th}^2 \,. \tag{15.7}$$

This line intersects the Heisenberg uncertainty limit when

$$\sigma_{in-}\sigma_{in+} = \sigma_V^2 \tag{15.8}$$

$$\implies \sqrt{(1-\varepsilon^2)}\sigma_{th}^2 = \sigma_V^2 \tag{15.9}$$

$$\implies \varepsilon = \pm\sqrt{1-\frac{\sigma_V^4}{\sigma_{th}^4}} \tag{15.10}$$

giving the valid range for ε as

$$-\sqrt{1-\frac{\sigma_V^4}{\sigma_{th}^4}} \leq \varepsilon \leq \sqrt{1-\frac{\sigma_V^4}{\sigma_{th}^4}} \,. \tag{15.11}$$

The two end points of the line correspond to two pure squeezed states. At $\varepsilon = 0$, the noise corresponds to that of a true thermal state with equal noise in all quadratures. Eve would be restricted to using states at this point if Alice and Bob could do a complete characterisation of the channel.

15.1.1 The input and output states

We let Eve create the thermal state entering the quantum channel at $a_{V_{in}}$ by mixing two orthogonally squeezed states through a $50/50$ beam splitter. The thermal state created will be correlated to another thermal state which Eve is free to keep and measure later on. The whole setup with three inputs and outputs is shown in figure 15.3.

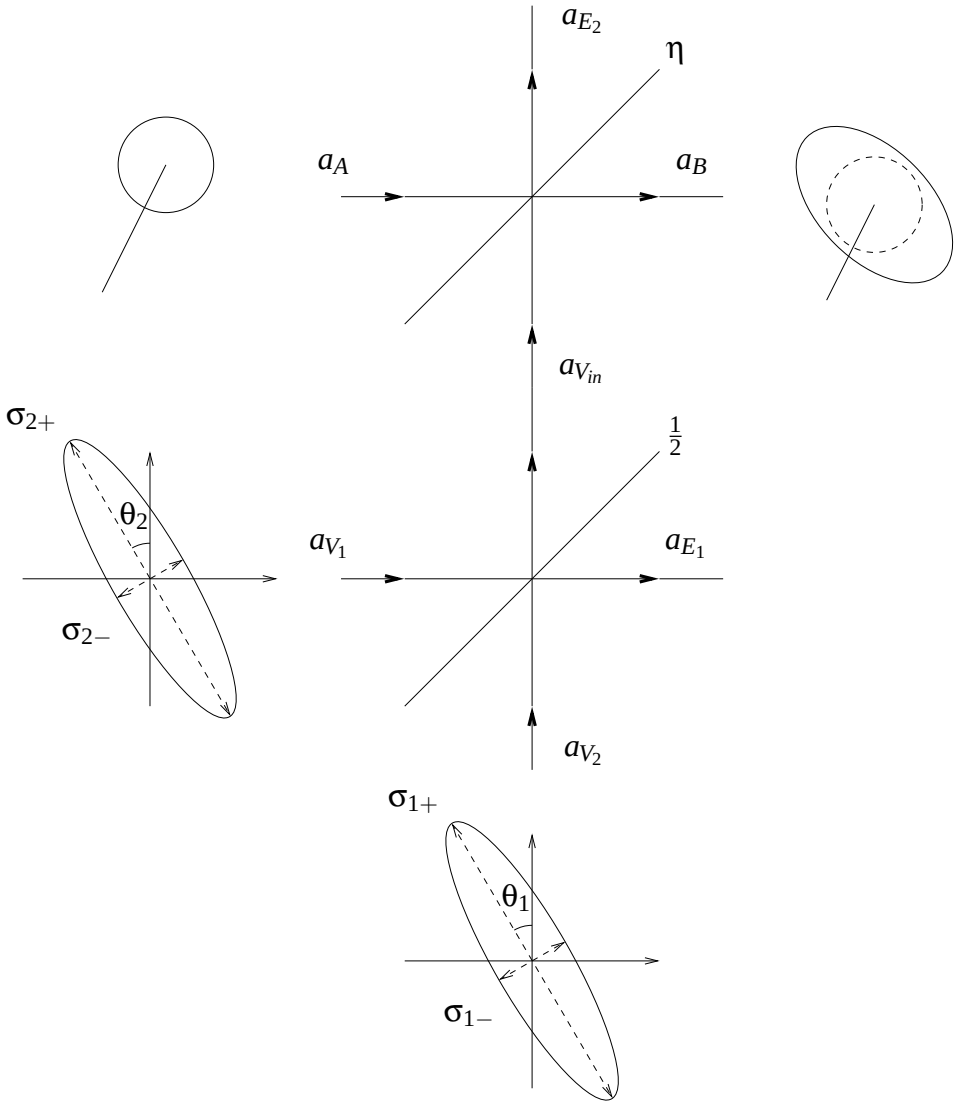


Figure 15.3: Beam splitter model for the creation of Eve's eavesdropping thermal state in the coherent state protocol with thermal noise. Eve's thermal state is created by injecting two pure squeezed state through a $50/50$ beam splitter. The rest of the model remains the same. Alice sends a coherent state into a_A, the first port of a beam splitter with transmission η. Eve's noisy Gaussian state with variance σ^2_{th} in the amplitude and phase quadratures enters the second port at $a_{V_{in}}$. The state Bob receives at the output a_B is another noisy Gaussian state.

The three inputs are Alice's coherent state at a_A and Eve's two squeezed states at a_{V_1} and a_{V_2} . The Wigner function for Alice's coherent state is centred at

$$\vec{x}_A = (x_A, y_A) \tag{15.12}$$

and has the covariance matrix

$$C_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \tag{15.13}$$

We take both of Eve's inputs to be pure squeezed states centred at $(0,0)$ and with covariance matrix

$$C_{V_1} = \begin{pmatrix} \sigma_{1-}^2 \cos^2\theta_1 + \sigma_{1+}^2 \sin^2\theta_1 & \left(\sigma_{1-}^2 - \sigma_{1+}^2\right)\sin\theta_1\cos\theta_1 \\ \left(\sigma_{1-}^2 - \sigma_{1+}^2\right)\sin\theta_1\cos\theta_1 & \sigma_{1-}^2 \sin^2\theta_1 + \sigma_{1+}^2 \cos^2\theta_1 \end{pmatrix} \tag{15.14}$$

and

$$C_{V_2} = \begin{pmatrix} \sigma_{2-}^2 \cos^2\theta_2 + \sigma_{2+}^2 \sin^2\theta_2 & \left(\sigma_{2-}^2 - \sigma_{2+}^2\right)\sin\theta_2\cos\theta_2 \\ \left(\sigma_{2-}^2 - \sigma_{2+}^2\right)\sin\theta_2\cos\theta_2 & \sigma_{2-}^2 \sin^2\theta_2 + \sigma_{2+}^2 \cos^2\theta_2 \end{pmatrix} \tag{15.15}$$

where $\sigma_{1-}\sigma_{1+} = \sigma_V^2$ and $\sigma_{2-}\sigma_{2+} = \sigma_V^2$ and the angles θ_1 and θ_2 are the squeezed quadratures. As Bob checks that the variances in both his quadratures are equal, this imposes the two constraints

$$\frac{1}{2}\left[\left(\sigma_{1-}^2 \cos^2\theta_1 + \sigma_{1+}^2 \sin^2\theta_1\right) + \left(\sigma_{2-}^2 \cos^2\theta_2 + \sigma_{2+}^2 \sin^2\theta_2\right)\right] = \sigma_{th}^2 \tag{15.16}$$

and

$$\frac{1}{2}\Big[\left(\sigma_{1-}^2\sin^2\theta_1+\sigma_{1+}^2\cos^2\theta_1\right)+\left(\sigma_{2-}^2\sin^2\theta_2+\sigma_{2+}^2\cos^2\theta_2\right)\Big]=\sigma_{th}^2\,. \quad (15.17)$$

For a fixed value of θ_1 and θ_2, these constraints determine a unique value (up to permutations) of the squeezed variances σ_{1-} and σ_{2-}.

Since x_A and y_A are not correlated, it is reasonable to choose $\theta_1=0$ and $\theta_2=\pi/2$ and treat the two quadratures independently. With this choice, we have $\sigma_{1-}=\sigma_{2-}$ and the input covariance matrix becomes

$$C=\begin{pmatrix} C_A & 0 & 0 \\ 0 & C_{V_1} & 0 \\ 0 & 0 & C_{V_2} \end{pmatrix} \quad (15.18)$$

$$=\begin{pmatrix} \sigma_V^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sigma_V^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sigma_{1-}^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma_{1+}^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sigma_{2+}^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sigma_{2-}^2 \end{pmatrix}. \quad (15.19)$$

Since the X and Y quadratures are uncorrelated throughout the protocol, we restrict the analysis to only the X quadrature. That is, we assume that Bob measured the X quadrature. The action of the two beam splitters on the X quadrature

is described by the following matrix

$$M = \begin{pmatrix} \sqrt{\eta} & -\sqrt{1-\eta} & 0 \\ \sqrt{1-\eta} & \sqrt{\eta} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \tag{15.20}$$

$$= \begin{pmatrix} \sqrt{\eta} & -\sqrt{\frac{1-\eta}{2}} & \sqrt{\frac{1-\eta}{2}} \\ \sqrt{1-\eta} & \sqrt{\frac{\eta}{2}} & -\sqrt{\frac{\eta}{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}. \tag{15.21}$$

Hence, when Alice sends the coherent state with real amplitude x_A the output state will have a mean

$$\begin{pmatrix} \mu_B \\ \mu_{E_1} \\ \mu_{E_2} \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & -\sqrt{\frac{1-\eta}{2}} & \sqrt{\frac{1-\eta}{2}} \\ \sqrt{1-\eta} & \sqrt{\frac{\eta}{2}} & -\sqrt{\frac{\eta}{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} x_A \\ 0 \\ 0 \end{pmatrix} \tag{15.22}$$

$$= \begin{pmatrix} \sqrt{\eta} x_A \\ \sqrt{1-\eta} x_A \\ 0 \end{pmatrix} \tag{15.23}$$

and covariance matrix

$$\Sigma_{B,E_1,E_2} = \begin{pmatrix} \sqrt{\eta} & -\sqrt{\frac{1-\eta}{2}} & \sqrt{\frac{1-\eta}{2}} \\ \sqrt{1-\eta} & \sqrt{\frac{\eta}{2}} & -\sqrt{\frac{\eta}{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \sigma_V^2 & 0 & 0 \\ 0 & \sigma_{1-}^2 & 0 \\ 0 & 0 & \sigma_{1+}^2 \end{pmatrix} \tag{15.24}$$

$$\times \begin{pmatrix} \sqrt{\eta} & -\sqrt{\frac{1-\eta}{2}} & \sqrt{\frac{1-\eta}{2}} \\ \sqrt{1-\eta} & \sqrt{\frac{\eta}{2}} & -\sqrt{\frac{\eta}{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}^{\mathrm{T}} \tag{15.25}$$

$$= \begin{pmatrix} \eta\sigma_V^2 + (1-\eta)\sigma_{th}^2 & \sqrt{(1-\eta)\eta}\left(\sigma_V^2 - \sigma_{th}^2\right) & \sqrt{1-\eta}\sigma_k^2 \\ \sqrt{(1-\eta)\eta}\left(\sigma_V^2 - \sigma_{th}^2\right) & (1-\eta)\sigma_V^2 - \eta\sigma_k^2 & -\sqrt{\eta}\sigma_k^2 \\ \sqrt{1-\eta}\sigma_k^2 & -\sqrt{\eta}\sigma_k^2 & \sigma_{th}^2 \end{pmatrix} \tag{15.26}$$

where

$$\sigma_{th}^2 = \frac{1}{2}\left(\sigma_{1+}^2 + \sigma_{1-}^2\right) \tag{15.27}$$

and

$$\sigma_k^2 = \frac{1}{2}\left(\sigma_{1+}^2 - \sigma_{1-}^2\right) . \tag{15.28}$$

Now in the protocol, Bob will announce the absolute value of his measurement result. At this point, we can find out what is Eve's reduced state if Bob measured the outcome x_B by taking the conditioned Gaussian state after conditioning on Bob's outcome. But it turns out the computation will be easier if we not do so yet.

We shall keep the output state as a three-mode Gaussian state between Eve and Bob.

15.1.2 Eve's reduced input

After Alice announces the absolute value of her signal $s_A = |x_A|$ and Bob announces the absolute value of his measurement outcome $m_B = |x_B|$, Eve knows that the reduced state she holds will be in one of the four possible states

$$\{|\psi_E(+s_A,+m_B)\rangle, |\psi_E(+s_A,-m_B)\rangle, |\psi_E(-s_A,+m_B)\rangle, |\psi_E(-s_A,-m_B)\rangle\}$$

with probabilities we denote by

$$\{p_E(+,+), p_E(+,-), p_E(-,+), p_E(-,-)\} \ .$$

For example, the probability that Eve has the state $|\psi_E(+s_A,-m_B)\rangle$ would be

$$p_E(+,-) = \frac{p_B(-m_B|+s_A)}{N} \tag{15.29}$$

where $p_B(x_B|x_A)$ is the probability density corresponding to Bob measuring the outcome x_B given that Alice sent the signal x_A which is given in section 13.1. N is the normalisation

$$\begin{aligned} N = {} & p_B(+m_B|+s_A) + p_B(+m_B|-s_A) \\ & + p_B(-m_B|+s_A) + p_B(-m_B|-s_A) \end{aligned} \tag{15.30}$$

so that $p_E(+,+) + p_E(+,-) + p_E(-,+) + p_E(-,-) = 1$.

We normalise the states that Eve receives with

$$\left\langle \psi_E(x_A,x_B)\middle|\psi_E(x_A,x_B)\right\rangle = p_B(x_B|x_A)\ . \tag{15.31}$$

The overlap between any two of Eve's input states can be computed by evaluating

$$\begin{aligned}&\left|\left\langle \psi_E\left(x_A,x_B\right)\middle|\psi_E\left(x_A',x_B'\right)\right\rangle\right|^2\\ &\quad=\mathrm{Tr}_E\left\{\mathrm{Tr}_B\left\{\rho_{BE}(x_A)\left|x_B\right\rangle\left\langle x_B\right|\right\}\mathrm{Tr}_B\left\{\rho_{BE}(x_A')\left|x_B'\right\rangle\left\langle x_B'\right|\right\}\right\}\ .\end{aligned} \tag{15.32}$$

The details of the integration can be found in appendix E. Here we just collect the results for the inner products. The normalisation is

$$\left\langle \psi_E\left(x_A,x_B\right)\middle|\psi_E\left(x_A,x_B\right)\right\rangle = \frac{1}{\sqrt{2\pi(1+\delta)\sigma_V^2}}\exp\left[-\frac{\left(x_B-\sqrt{\eta}x_A\right)^2}{2(1+\delta)\sigma_V^2}\right]\ . \tag{15.33}$$

The terms that differentiate Eve's inputs for attacking Alice from attacking Bob are

$$\begin{aligned}\left\langle \psi_E\left(x_A,x_B\right)\middle|\psi_E\left(x_A,-x_B\right)\right\rangle &= \frac{1}{\sqrt{2\pi(1+\delta)\sigma_V^2}}\exp\left[-\frac{(1+\delta)^2x_B^2+\eta x_A^2}{2(1+\delta)\sigma_V^2}\right]\ ,\\ \left\langle \psi_E\left(x_A,x_B\right)\middle|\psi_E\left(-x_A,x_B\right)\right\rangle &= \frac{1}{\sqrt{2\pi(1+\delta)\sigma_V^2}}\exp\left[-\frac{x_B^2+(1+\delta)x_A^2}{2(1+\delta)\sigma_V^2}\right]\ .\end{aligned} \tag{15.34}$$

Finally the inner product between the cross terms for matched and unmatched Alice's and Bob's data is

$$\begin{aligned}&\left\langle \psi_E\left(x_A,x_B\right)\middle|\psi_E\left(-x_A,-x_B\right)\right\rangle \\ &\quad=\frac{1}{\sqrt{2\pi(1+\delta)\sigma_V^2}}\exp\left[-\frac{(x_A^2-2\sqrt{\eta}x_Ax_B+(1+\delta)x_B^2}{2\sigma_V^2}\right].\end{aligned} \tag{15.35}$$

These inner products define the structure of Eve's input states which will be given in the next two sections.

15.2 Bounding Eve's information when Eve attacks Alice

To attack Alice, Eve's input states would be the two states

$$\begin{aligned}\rho_E(+s_A)=\frac{1}{N}\left(\left|\psi_E\left(+s_A,+m_B\right)\right\rangle\left\langle\psi_E\left(+s_A,+m_B\right)\right|\right. \\ \left.+\left|\psi_E\left(+s_A,-m_B\right)\right\rangle\left\langle\psi_E\left(+s_A,-m_B\right)\right|\right)\end{aligned} \tag{15.36}$$

and

$$\begin{aligned}\rho_E(-s_A)=\frac{1}{N}\left(\left|\psi_E\left(-s_A,+m_B\right)\right\rangle\left\langle(-s_A,+m_B)\right|\right. \\ \left.+\left|\psi_E\left(-s_A,-m_B\right)\right\rangle\left\langle(-s_A,-m_B)\right|\right)\end{aligned} \tag{15.37}$$

with equal probabilities and where the normalisation

$$\begin{aligned}N=p_B(+m_B|+s_A)+p_B(+m_B|-s_A) \\ +p_B(-m_B|+s_A)+p_B(-m_B|-s_A)\ .\end{aligned} \tag{15.38}$$

The two states are normalised such that

$$\mathrm{Tr}\{\rho_E(+s_A)\} = \mathrm{Tr}\{\rho_E(-s_A)\} = \frac{1}{2}\,. \tag{15.39}$$

Each of these states are of rank two and together they occupy a four dimensional space. To represent the input states in some numerical basis, we need to evaluate the inner products between the constituents $\left\langle \psi_E(x_A,x_B)\middle|\psi_E(x'_A,x'_B)\right\rangle$. Once we have a representation for the states, it is easy to calculate the Holevo quantity to get an upper bound on Eve's information for collective attacks or somewhat harder, the accessible information to get a bound on Eve's information for individual attacks.

While these quantities would give a tight bound on Eve's information, here we are interested in a bound that can be easily computed. For that purpose, we shall give Eve some additional information. We tell Eve whether Alice and Bob have matching parity or mismatched parity. With this information, with probability

$$p_1 \equiv \frac{p_B(m_B|s_A) + p_B(-m_B|-s_A)}{N} = \frac{2p_B(m_B|s_A)}{N}\,, \tag{15.40}$$

Eve would have to distinguish between the two equally likely pure states $|\psi_E(+s_A,+m_B)\rangle$ and $|\psi_E(-s_A,-m_B)\rangle$. Also, with probability

$$p_2 \equiv 1-p_1 = \frac{p_B(-m_B|s_A) + p_B(m_B|-s_A)}{N} = \frac{2p_B(-m_B|s_A)}{N}\,, \tag{15.41}$$

Eve would have to distinguish between the two equally likely pure states $|\psi_E(+s_A,-m_B)\rangle$ and $|\psi_E(-s_A,+m_B)\rangle$. Now that Eve only distinguishes between two pure states, the information she gains can be written down explicitly. From

section 2.4, we find that for individual attacks, Eve's information will be bounded by

$$I_{EA}^{\text{ind}}(s_A, m_B) \leq p_1 \Phi\left(\sqrt{1-f_1^2}\right) + p_2 \Phi\left(\sqrt{1-f_2^2}\right) , \tag{15.42}$$

while for collective attacks, Holevo's bound gives

$$I_{EA}^{\text{col}}(s_A, m_B) \leq p_1 (1-\Phi(f_1)) + p_2 (1-\Phi(f_2)) \tag{15.43}$$

where f_1 and f_2 are the normalised overlaps

$$f_1 = \frac{\left|\left\langle \psi_E(s_A, m_B) \middle| \psi_E(-s_A, -m_B) \right\rangle\right|}{\left\langle \psi_E(s_A, m_B) \middle| \psi_E(s_A, m_B) \right\rangle} , \tag{15.44}$$

$$f_2 = \frac{\left|\left\langle \psi_E(s_A, -m_B) \middle| \psi_E(-s_A, m_B) \right\rangle\right|}{\left\langle \psi_E(s_A, -m_B) \middle| \psi_E(s_A, -m_B) \right\rangle} . \tag{15.45}$$

The inner products in the numerators and denominators of f_1 and f_2 were quantities that are given in section 15.1.2. That I_{EA} is an upper bound is clear since this is the maximum amount of information Eve can obtain if she uses the parity match–mismatch announcements. Ignoring these announcements would only reduce Eve's ability to gain information.

Eve's information bound depends on the channel excess noise and transmission. For excess noise $\delta = 0.2$ and transmission $\eta = 0.5$, this bound for individual and collective attacks are plotted in figures 15.4 and 15.5 respectively. In both cases, Eve's information becomes progressively larger as s_A and m_B increases. When either s_A or m_B is larger than 2.0, Eve's information is already very close to 1 for both the individual and collective attacks.

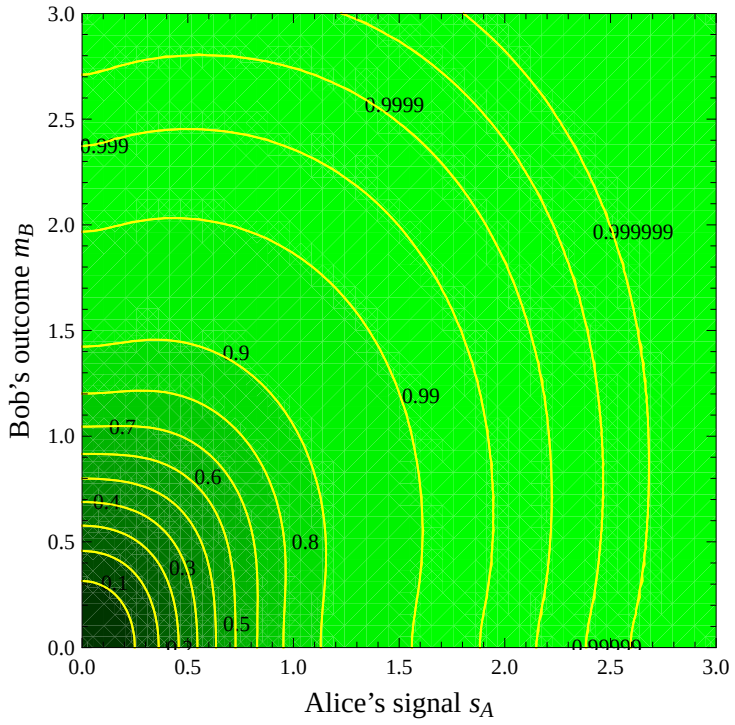


Figure 15.4: Contour plot of Eve's information bound for individual attacks in the coherent state protocol with excess noise. The amount of excess noise is $\delta = 0.2$ and the channel transmission is $\eta = 0.5$. Eve's information is plotted as a function of Alice's signal and Bob's measurement outcome.

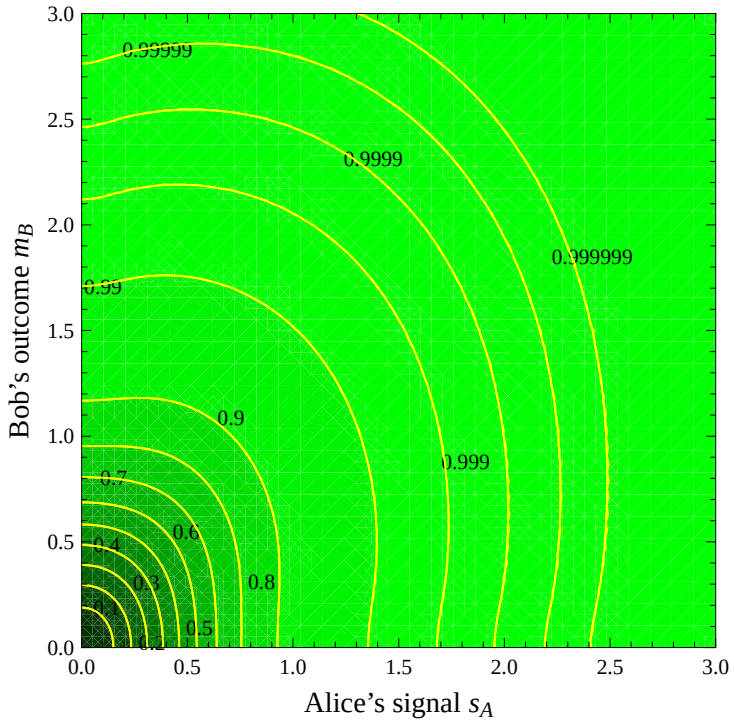


Figure 15.5: Contour plot of Eve's information bound for collective attacks in the coherent state protocol with excess noise. The amount of excess noise is $\delta = 0.2$ and the channel transmission is $\eta = 0.5$. Eve's information is plotted as a function of Alice's signal and Bob's measurement outcome.

15.3 Bounding Eve's information when Eve attacks Bob

Instead of attacking Alice, Eve could instead choose to attack Bob. In this case, Eve's input states would be

$$\begin{aligned}\rho_E(+m_B) = \frac{1}{N}\big(&|\psi_E(+s_A,+m_B)\rangle\langle\psi_E(+s_A,+m_B)| \\ &+|\psi_E(-s_A,+m_B)\rangle\langle\psi_E(-s_A,+m_B)|\big)\end{aligned} \tag{15.46}$$

and

$$\begin{aligned}\rho_E(-m_B) = \frac{1}{N}\big(&|\psi_E(+s_A,-m_B)\rangle\langle(+s_A,-m_B)| \\ &+|\psi_E(-s_A,-m_B)\rangle\langle(-s_A,-m_B)|\big)\end{aligned} \tag{15.47}$$

both having equal probability. By repeating a similar analysis that was done for the case when Eve attacks Alice, we can get a bound on Eve's information for attacking Bob. It turns out that for individual attack, the accessible information is bounded by

$$I_{EB}^{\text{ind}}(s_A,m_B) \leq p_1\Phi\left(\sqrt{1-f_1^2}\right) + p_2\Phi\left(\sqrt{1-f_2^2}\right), \tag{15.48}$$

while for collective attacks, Holevo's bound gives

$$I_{EB}^{\text{col}}(s_A,m_B) \leq p_1(1-\Phi(f_1)) + p_2(1-\Phi(f_2)), \tag{15.49}$$

which are the same expressions that were obtained when Eve attacks Alice. So with the additional information on whether Alice and Bob's bits match or not, it does not matter whether Eve attacks Alice or Bob.

15.4 Direct or reverse reconciliation

However in practice, Eve does not have the parity match–mismatch information and the actual accessible information or Holevo quantity when Eve attacks Alice and when Eve attacks Bob would in general be different. They would only be the same when Eve's inputs for both cases are unitarily equivalent. This happens when

$$\left\langle \psi_E\left(s_A, m_B\right) \middle| \psi_E\left(s_A, -m_B\right)\right\rangle = \left\langle \psi_E\left(s_A, m_B\right) \middle| \psi_E\left(-s_A, m_B\right)\right\rangle \tag{15.50}$$

$$\implies \exp\left[-\frac{(1+\delta)^2 m_B^2 + \eta s_A^2}{2(1+\delta)\sigma_V^2}\right] = \exp\left[-\frac{m_B^2 + (1+\delta)s_A^2}{2(1+\delta)\sigma_V^2}\right] \tag{15.51}$$

$$\implies m_B = \pm\sqrt{\frac{1+\delta-\eta}{(1+\delta)^2-1}}\, s_A\,. \tag{15.52}$$

Along this line Eve can get exactly the same information from Alice as she can from Bob. In the region

$$-\sqrt{\frac{1+\delta-\eta}{(1+\delta)^2-1}}\, s_A < m_B < \sqrt{\frac{1+\delta-\eta}{(1+\delta)^2-1}}\, s_A\,, \tag{15.53}$$

Alice would announce a relatively big value of s_A compared to Bob's announced m_B. In that case Eve shares more information with Alice than with Bob. Hence it would be more advantageous if Alice and Bob do reverse reconciliation. That is, we use Bob's raw key as a reference and Alice corrects her keys to match

Bob's. The one way post-processing is done by Bob sending classical information through the public channel.

Outside this region, Eve has more information about Bob's raw key than about Alice's raw key. So direct reconciliation, where now Alice's raw key is used as a reference, would give Alice and Bob a higher key rate.

For the bounds derived in this thesis, we recall that Eve's information with Alice is the same as her information with Bob. Hence the results on the bounds on the key rates will be valid regardless of whether Alice and Bob do a direct reconciliation or a reverse reconciliation.

15.5 Noise threshold

As long as there are some values of s_A and m_B such that Alice and Bob share more information compared to Eve's information, there will a non-empty post-selection region and in principle the key rate would be positive.

For a fixed transmission rate, as the excess noise increases, the size of the post-selection region will reduce. Beyond some noise threshold, Eve's information will become greater than Alice and Bob's information for all values of s_A and m_B. For example, when $\delta > 2\eta$, the state between Alice and Bob becomes separable. In this case, Eve can do a classical intercept and resend attack for which $I_E > I_{AB}$ for all values of s_A and m_B [38].

To find the noise threshold, we shall solve for the curve where the bound on Eve's information is equal to Alice and Bob's information

$$I_E = I_{AB} \, . \tag{15.54}$$

Since at the noise threshold, Eve's information will be greater than Alice and Bob's for all values of s_A and m_B, we can consider the case when s_A is large.

For $s_A \gg 1$, as long as $m_B \neq 0$,

$$\frac{p_1}{p_2} = \exp\left[-\frac{(m_B - \sqrt{\eta}s_A)^2}{2(1+\delta)\sigma_V^2} + \frac{(-m_B - \sqrt{\eta}s_A)^2}{2(1+\delta)\sigma_V^2}\right] \tag{15.55}$$

$$= \exp\left[\frac{2\sqrt{\eta}m_B s_A}{(1+\delta)\sigma_V^2}\right] \gg 1 \tag{15.56}$$

$$\implies p_1 \gg p_2\,. \tag{15.57}$$

This means that when $s_A \gg 1$, Alice and Bob will most likely get correlated bits. Eve practically just has to distinguish between the two pure states $|\psi_E(s_A, m_B)\rangle$ and $|\psi_E(-s_A, -m_B)\rangle$. Eve's information for individual attacks will be

$$I_E^{\text{ind}} \approx \Phi\left(\sqrt{1 - f_1^2}\right) \tag{15.58}$$

and for collective attacks, it will be

$$I_E^{\text{col}} \approx 1 - \Phi(f_1) \tag{15.59}$$

where f_1 is the properly normalised inner product between Eve's most likely input as given in equation (15.44). The approximation gets better with larger s_A.

15.5.1 Individual attacks

Equating Eve's information to Alice and Bob's information, we find that for individual attacks, the post-selection boundary for large s_A is

$$3\Phi\left(\sqrt{1-f_1^2}\right) = \Phi\left(1-2p_{\text{error}}\right) \tag{15.60}$$

$$\implies \sqrt{1-f_1^2} = 1-2p_{\text{error}}\,. \tag{15.61}$$

Since $f_1 \ll 1$, we make the approximation

$$1-\frac{1}{2}f_1^2 \approx 1-2p_{\text{error}} \tag{15.62}$$

$$\implies f_1^2 = 4p_{\text{error}}\,. \tag{15.63}$$

Substituting the expression for f_1 from equation (15.44) and for p_{error} from equation (13.12), we get

$$\frac{\exp\left[-\frac{2\left(s_A^2-2\sqrt{\eta}s_Am_B+(1+\delta)m_B^2\right)}{2\sigma_V^2}\right]}{\exp\left[-\frac{2(m_B-\sqrt{\eta}s_A)^2}{2(1+\delta)\sigma_V^2}\right]} = 4\exp\left[-\frac{2\sqrt{\eta}s_Am_B}{(1+\delta)\sigma_V^2}\right]\,. \tag{15.64}$$

Taking log on both sides and dropping constant terms, we obtain

$$-\frac{2\left(s_A^2-2\sqrt{\eta}s_Am_B+(1+\delta)m_B^2\right)}{2\sigma_V^2}+\frac{2\left(m_B-\sqrt{\eta}s_A\right)^2}{2(1+\delta)\sigma_V^2} \approx -\frac{2\sqrt{\eta}s_Am_B}{(1+\delta)\sigma_V^2} \tag{15.65}$$

$$\implies (2\delta+\delta^2)m_B^2-2\sqrt{\eta}(1+\delta)s_Am_B+(1-\eta+\delta)s_A^2=0\,. \tag{15.66}$$

Solving for m_B gives two solutions

$$m_B = \frac{\sqrt{\eta}(1+\delta) \pm \sqrt{\eta(1+\delta)^2 - \delta(2+\delta)(1-\eta+\delta)}}{(2\delta+\delta^2)} s_A \,. \tag{15.67}$$

For large s_A, the post-selection boundary would asymptote to these two lines. When the term under the radical is zero, the two lines will become one and the post-selection region becomes empty. Therefore the noise threshold δ_0 is obtained by solving for δ_0 in the cubic equation

$$\eta(1+\delta_0)^2 - \delta_0(2+\delta_0)(1-\eta+\delta_0) = 0 \tag{15.68}$$

$$\implies -\delta_0^3 + \delta_0^2(2\eta-3) + \delta_0(4\eta-2) + \eta = 0 \,. \tag{15.69}$$

Solving this equation, we find that for every value of $0 \leq \eta \leq 1$, there exist exactly one solution for δ_0 that is greater than or equal to zero. This solution is plotted in figure 15.6 as a function of η. For channels with excess noise above this line, no secure communication is possible.

15.5.2 Collective attacks

To find the noise threshold for collective attacks, we equate Eve's information to Alice and Bob's information

$$1 - \Phi(f_1) = \Phi(1 - 2p_{\text{error}}) \,. \tag{15.70}$$

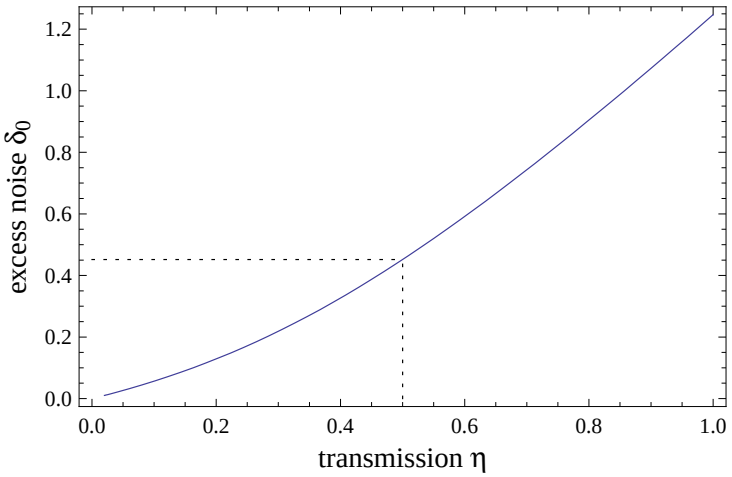


Figure 15.6: Plot of the excess noise threshold δ_0 for secure communication as a function for the channel transmission η for the coherent state protocol with thermal noise. The threshold is obtained by solving equation (15.69). At $\eta = 0.5$, the excess noise threshold is 0.4516.

Since both f_1 and p_{error} are small when s_A is large, if we keep only first order terms, we obtain the approximation

$$1 - \frac{f_1^2}{2\ln 2} \approx 1 + \frac{1 - p_{\text{error}}}{\ln 2} \ln(1 - p_{\text{error}}) + \frac{p_{\text{error}}}{\ln 2} \ln p_{\text{error}} \tag{15.71}$$

$$\implies -\frac{1}{2} f_1^2 = (1 - p_{\text{error}}) \ln(1 - p_{\text{error}}) + p_{\text{error}} \ln p_{\text{error}} \tag{15.72}$$

$$\implies -\frac{1}{2} f_1^2 \approx (1 - p_{\text{error}}) \left(-p_{\text{error}} - \frac{p_{\text{error}}^2}{2} \right) + p_{\text{error}} \ln p_{\text{error}} \tag{15.73}$$

$$\implies -\frac{1}{2} f_1^2 \approx -p_{\text{error}} \, . \tag{15.74}$$

After substituting the expressions for f_1 and p_{error}, taking log and dropping constant terms, we find that this equality gives the same asymptotic behaviour of the post-selection region as the individual attacks

$$(2\delta + \delta^2) m_B^2 - 2\sqrt{\eta}(1 + \delta) s_A m_B + (1 - \eta + \delta) s_A^2 = 0 \, . \tag{15.75}$$

Hence the noise threshold for the collective attacks is the same as the noise threshold for the individual attacks.

Chapter 16

Effects of excess noise at transmission = 0.5

In this chapter, we look in greater detail at the key rates between Alice and Bob when their channel is contaminated by various degrees of excess noise. Section 16.1 studies the case when Eve does an individual attack while section 16.2 gives the results for collective attacks. Both are done for a channel transmission rate of 50%. For a single-mode fibre with an attenuation of 0.5 dB/km at a frequency of 1550 nm, this would correspond to a fibre length of 6 km.

16.1 Individual attack

Using the bound on Eve's accessible information that we had in equation (15.42) of the previous chapter, we can now find the key rate between Alice and Bob after post-selection.

16.1.1 Excess noise = 0.2

We work out the details for a particular value of excess noise $\delta = 0.2$. This is a large excess noise compared to that typically seen in both free space and fibre based quantum key distribution experiments which is usually less than 0.01 even for large transmission losses [30, 36]. A large excess noise value was chosen in this sub-section so that its effects would be more prominent.

Figure 16.1 gives a contour plot of the key rate at each point of Alice's signal and Bob's measured result with excess noise $\delta = 0.2$. The key rate is given by the difference in Alice–Bob's mutual information, equation (13.15), and Eve's information, equation (15.42), for each value of Alice's signal s_A and Bob's measurement outcome m_B.

For each value of Alice's signal s_A, the key rate between Alice and Bob is obtained by integrating the individual key rate weighted against Bob's measurement outcome probabilities

$$r_k^{\text{ind}}(s_A) = \int_{\Omega_{I>0}} dm_B \left(I_{AB} - I_E^{\text{ind}} \right) p_B(m_B|s_A) \tag{16.1}$$

where $\Omega_{I>0}$ is the post-selection region. The key rate is plotted in figure 16.2 as a function of s_A. For values of s_A below a certain threshold $s_{A0} = 0.6613$, the key rate is exactly zero since the post-selection region is empty. For all values of $s_A > s_{A0}$, the key rate will remain positive. But it becomes very small after s_A becomes too large.

In our protocol Alice's signals follow a Gaussian distribution. The final key rate will depend on the variance of this distribution. The dependence of the key

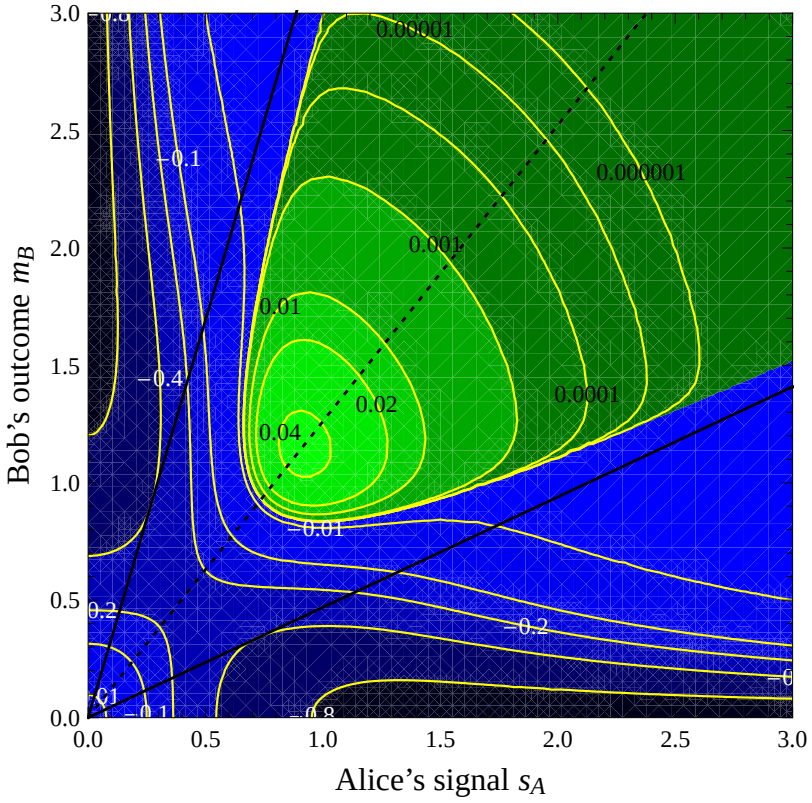


Figure 16.1: Contour plot of the key rate and post-selection region for individual attacks in the coherent state protocol with excess noise. The amount of excess noise is $\delta = 0.2$ and the channel transmission is $\eta = 0.5$. The key rate is plotted as a function of Alice's signal and Bob's measurement outcome. The post-selection regions, coloured in green, are those in which the key rate is positive. The dotted black line marks the point where Eve can gain the same amount of information from Alice as she can from Bob. For regions below (above) this line, Eve can get more information from Alice (Bob). The post-selection region asymptotes to the two solid black lines.

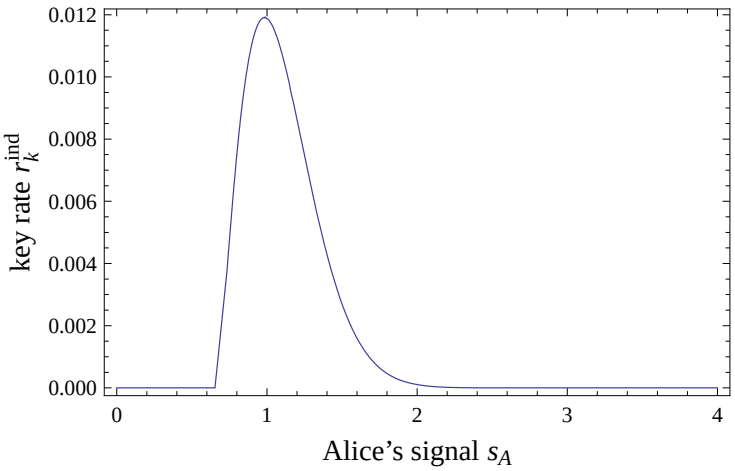


Figure 16.2: Plot of the key rate between Alice and Bob as a function of Alice's signal for the coherent state protocol with excess noise when Eve does individual attacks. The plot is for excess noise $\delta = 0.2$ and transmission $\eta = 0.5$. The maximum key rate occurs when Alice sends $s_A = 0.98$ for which the key rate would be 0.01191 bits per signal. For values of $s_A < 0.6613$, the post-selection region is empty and the key rate becomes exactly zero.

rate on Alice's variance is plotted in figure 16.3. It has a maximum value of $r_k^{\text{ind}} = 0.0029990$ bits per signal when $\sigma_A^2 = 1.15$ in units where $\sigma_V^2 = 0.25$.

16.1.2 Different values of excess noise

At $\eta = 0.5$, we find from figure 15.6 that the noise threshold for positive key rate is $\delta_0 = 0.4516$. As the amount of excess noise increases, the post-selection region becomes smaller. Only large values of s_A and m_B would yield a positive key rate. But for large values of s_A and m_B, the key rate is very low. Hence we can expect Alice's optimal variance would increase with excess noise while the final key rate would decrease.

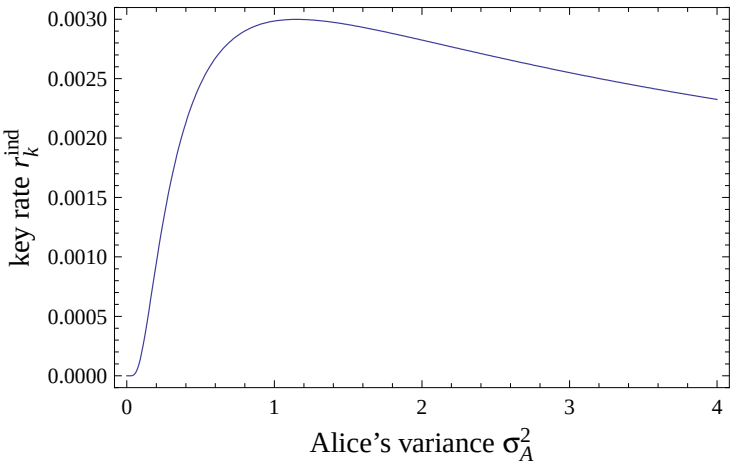


Figure 16.3: Plot of the net key rate as a function of Alice's variance σ_A^2 in the coherent state protocol with excess noise when Eve does an individual attack. The amount of excess noise is $\delta = 0.2$ and the channel transmission is $\eta = 0.5$. The vacuum state is normalised to $\sigma_V^2 = 0.25$. The maximum key rate is 0.002999 bits per signal at $\sigma_A^2 = 1.15$.

Repeating the analysis done in the previous section for different values of excess noise up to δ_0, the optimal variances and net key rates are summarised in the following table:

δ	σ_A^2	key rate r_k^{ind}
0	0.51	0.0664407
0.05	0.66	0.0345575
0.10	0.80	0.0174171
0.15	0.96	0.0079142
0.20	1.15	0.0029990
0.25	1.42	0.0008229
0.30	1.83	0.0001199
0.35	2.61	0.0000038
0.40	4.84	3.8×10^{-10}
0.45	–	$< 10^{-10}$
0.45161	–	0

In theory, the key rates are always positive when $\delta < \delta_0$. But from a practical point of view, for example when δ is 0.40, the key rate is already so small that the protocol becomes impractical.

In an actual experiment, the amount of excess noise would typically not be larger than $\delta = 0.05$. At this value of excess noise, if Alice's variance is chosen to be near its optimal value, the key rate is reduced by approximately half. This means that the protocol would still be practical despite the excess noise.

16.2 Collective attack

We repeat the analysis of the previous section for collective attacks. Everything is similar except that we now use the Holevo bound (15.43) to bound Eve's information. With this, we can once again find the key rate between Alice and Bob after post-selection.

16.2.1 Excess noise = 0.2

Again, we work out in greater detail for the case when $\delta = 0.2$. Figure 16.4 gives a contour plot of the key rate at each point of Alice's signal and Bob's measured result when the excess noise $\delta = 0.2$ for a collective attack.

For each value of Alice's signal s_A, the key rate between Alice and Bob is obtained by integrating the individual key rate weighted against Bob's measurement outcome probabilities:

$$r_k^{\text{col}}(s_A) = \int_{\Omega_{I>0}} dm \left(I_{AB} - I_E^{\text{col}} \right) p_B(m_B|s_A) \tag{16.2}$$

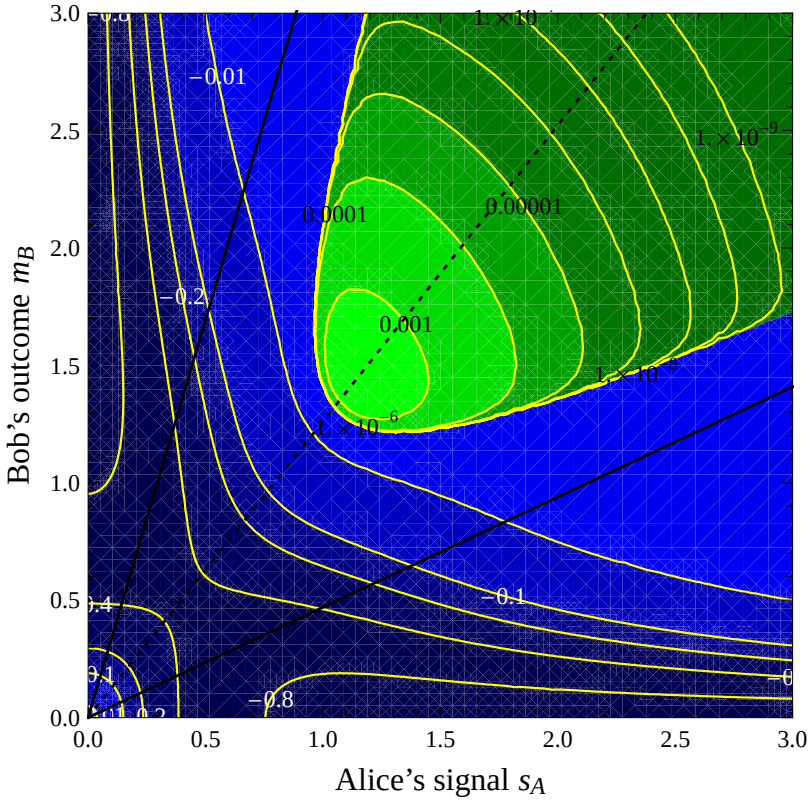


Figure 16.4: Contour plot of the key rate and post-selection region for collective attacks in the coherent state protocol with excess noise. The amount of excess noise is $\delta = 0.2$ and the channel transmission is $\eta = 0.5$. The key rate is plotted as a function of Alice's signal and Bob's measurement outcome. The post-selection regions, coloured in green, are those in which the key rate is positive. The dotted black line marks the point where Eve can gain the same amount of information from Alice as she can from Bob. For regions below (above) this line, Eve can get more information from Alice (Bob). The post-selection region asymptotes to the two solid black lines.

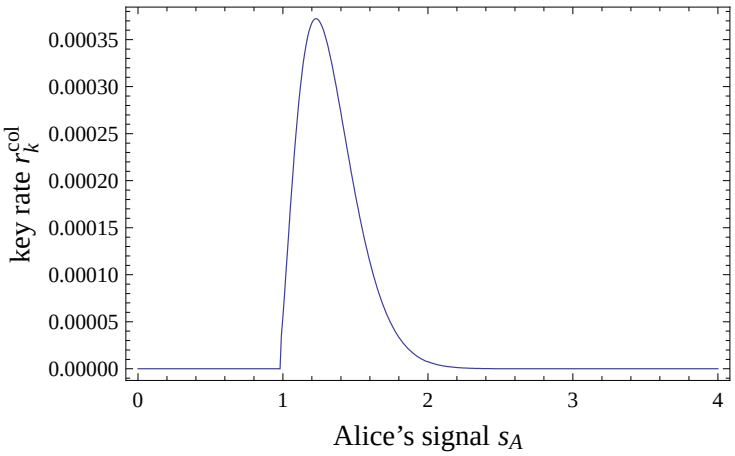


Figure 16.5: Plot of the key rate between Alice and Bob as a function of Alice's signal for the coherent state protocol with excess noise when Eve does individual attacks. The plot is for excess noise $\delta = 0.2$ and transmission $\eta = 0.5$. The maximum key rate occurs when Alice sends $s_A = 1.23$ for which the key rate would be 0.000372 bits per signal. For values of $s_A < 0.9625$, the post-selection region is empty and the key rate becomes exactly zero.

where $\Omega_{I>0}$ is the post-selection region. The key rate is plotted in figure 16.5. We see in this plot that for all values of s_A below the threshold $s_{A0} = 0.9625$, the key rate is exactly zero since the post-selection region is empty. For all values of $s_A > s_{A0}$, the key rate remains positive but the actual value becomes very small as s_A becomes very large.

In our protocol Alice's signals follow a Gaussian distribution. The final key rate will depend on the variance of this distribution. This dependence is plotted in figure 16.6 and it has a maximum value of $r_k^{\text{col}} = 0.0000632$ bits per signal at $\sigma_A^2 = 1.73$ in units where $\sigma_V^2 = 0.25$.

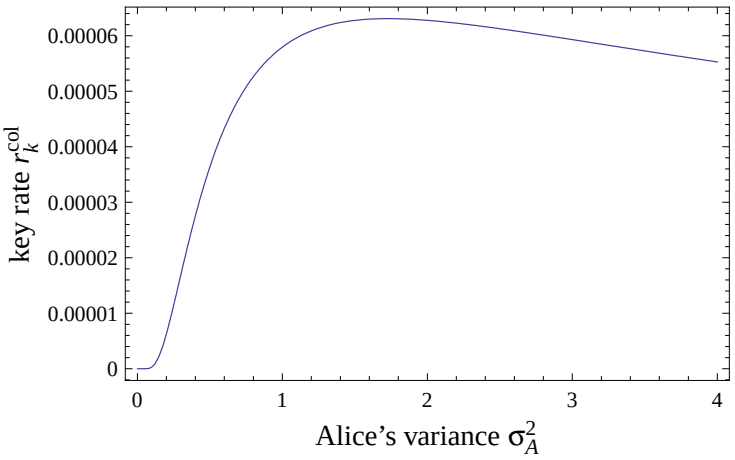


Figure 16.6: Plot of the net key rate as a function of Alice's variance σ_A^2 in the coherent state protocol with excess noise when Eve does a collective attack. The amount of excess noise is $\delta = 0.2$ and the channel transmission is $\eta = 0.5$. The vacuum state is normalised to $\sigma_V^2 = 0.25$. The maximum key rate is 0.0000632 bits per signal at $\sigma_A^2 = 1.73$.

16.2.2 Different values of excess noise

At $\eta = 0.5$, we find from figure 15.6 that the noise threshold for positive key rate is $\delta_0 = 0.4516$. Repeating the analysis done in the previous section for different values of excess noise up to δ_0, the optimal variances and net key rates are summarised in the following table:

δ	σ_A^2	key rate r_k^{col}
0	0.46	0.0244538
0.05	0.75	0.0072922
0.10	0.99	0.0021343
0.15	1.30	0.0004753
0.20	1.73	0.0000632
0.25	2.39	0.0000032
0.30	3.57	2.0×10^{-8}
0.35	6.38	6.5×10^{-13}
0.40	8.19	1.3×10^{-15}
0.45	–	$< 10^{-15}$
0.45161	–	0

In theory, the key rates would always be positive as long as $\delta < \delta_0$. However in practice, when the key rates becomes too small the protocol would be impractical. When $\delta = 0.30$, the key rate is already of the order 10^{-8}.

In an actual experiment, the amount of excess noise would typically not be larger than $\delta = 0.05$. At this value of excess noise, if Alice's variance is chosen to be near its optimal value, the key rate is reduced by a factor of 3.4. This means that the protocol would still remain practical despite the excess noise.

Chapter 17

Conclusion and outlook for part two

In the second part of the thesis, we studied the security thresholds as well as the key rates for the coherent state continuous variable quantum key distribution protocol in the presence of Gaussian excess noise. By providing Eve with the additional information on Alice's unmeasured quadrature and whether Alice and Bob's raw bits match or not, we derived an upper bound on Eve's information. We found that the protocol can remain secure even in the presence of excess noise in the channel.

The upper bound for collective attacks can be made tighter without giving Eve the match–mismatch bits information. Applying Holevo's bound directly on Eve's input states given in sections 15.2 and 15.3 would give us a tighter upper bound on Eve's information. It is worth investigating how the key rate will improve if we use this tighter bound.

This thesis proves the security in the limit of an infinite key length where the parameters of the channel can be found with arbitrary precision. In practice, to do the post-processing from the raw data to the final secret keys on a very large

string of raw bits is computationally intensive. This sets a practical limit on the key length. Within this statistical limit, the distribution that Alice and Bob see when they characterise their channel will never be perfectly Gaussian. The final key rates after accounting for the finite key length would need to be investigated.

The Gaussian attack that was considered in this thesis is just one special attack that Eve can perform while still ensuring a Gaussian joint distribution between Alice and Bob in the measured quadratures. More generally, Eve can perform a Gaussian attack by inserting a 45 degrees squeezed state instead of a thermal state through the empty port of the beam splitter in figure 15.1. It remains to be seen if this will provide Eve with more information.

Eve need not be restricted to doing a Gaussian attack. Despite doing a non-Gaussian attack, she may still simulate a thermal noise in the channel between Alice and Bob as long as she can engineer her attack such that the amplitude and phase quadratures of Bob's state remains Gaussian. To study this attack, it is not enough just to keep track on the means and covariances of the input states as we have done in the thesis. A more general approach would have to be used. One way to do this would be to express the input and output states in some continuous quadrature basis.

The effects of practical imperfections when conducting the experiment would also reduce the actual secure key rate. For example if the quantum source from Alice to Bob was not a single propagating spatial mode, and some of the Alice's signal is found in other modes of the channel, then Eve might be able to tap those channels to gain additional information about Alice and Bob's communications.

In the current protocol, we say that Alice and Bob will abort the protocol if the joint distribution that they check for is not Gaussian. However we can ask if

the protocol remains secure if the noise that Alice and Bob see is not Gaussian. In which direction and by how much will the key rate change if Alice and Bob get a skewed joint distribution? This would correspond to Eve doing an asymmetric attack.

Appendices

Appendix E

Inner products between the constituents of Eve's input states

In this appendix, we shall evaluate the inner products between Eve's reduced states given Alice's signal and Bob's outcome. These states are defined in section 15.1.2 and make up Eve's input states. The situation is depicted in figure E.1. Eve's four reduced sub-normalised states when Alice sends x_A and Bob measures the outcome x_B are

$$\left\{\left|\psi_E\left(+x_A,+x_B\right)\right\rangle,\left|\psi_E\left(+x_A,-x_B\right)\right\rangle,\left|\psi_E\left(-x_A,+x_B\right)\right\rangle,\left|\psi_E\left(-x_A,-x_B\right)\right\rangle\right\}\ .$$

We normalise the states according to

$$\left\langle\psi_E(x_A,x_B)\middle|\psi_E(x_A,x_B)\right\rangle = p_B\left(x_B|x_A\right) \tag{E.1}$$

where $p_B\left(x_B|x_A\right)$ is the probability for Bob to obtain the outcome x_B when Alice encodes the signal x_A onto the amplitude quadrature. To attack Alice, Eve's two

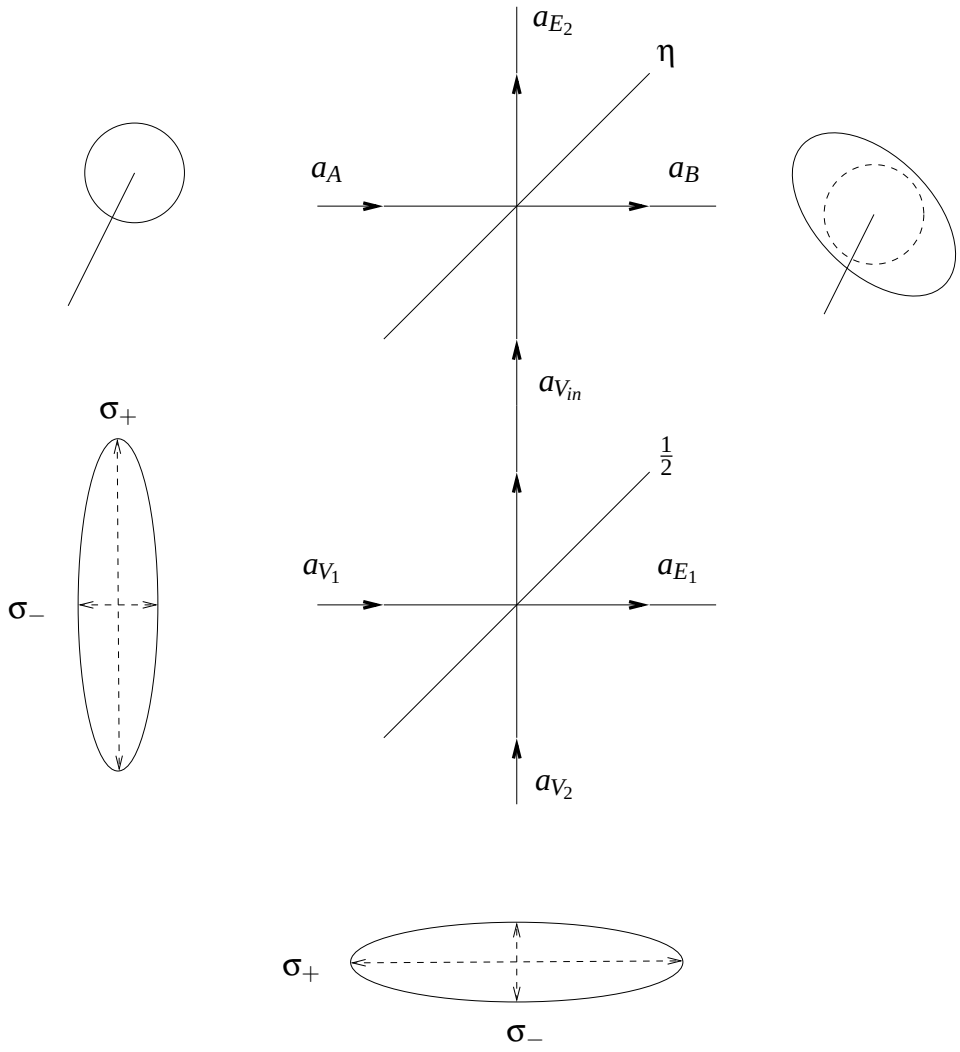


Figure E.1: The beam splitter model for the output and input states in the coherent state protocol with thermal noise when Alice inputs a coherent state and Eve creates an EPR state.

sub-normalised inputs are

$$\begin{aligned}\hat{\rho}_E(+x_A) = \frac{1}{N}\big(&|\psi_E(+x_A,+x_B)\rangle\langle\psi_E(+x_A,+x_B)| \\ &+|\psi_E(+x_A,-x_B)\rangle\langle\psi_E(+x_A,-x_B)|\big)\end{aligned} \tag{E.2}$$

and

$$\begin{aligned}\hat{\rho}_E(-x_A) = \frac{1}{N}\big(&|\psi_E(-x_A,+x_B)\rangle\langle(-x_A,+x_B)| \\ &+|\psi_E(-x_A,-x_B)\rangle\langle(-x_A,-x_B)|\big)\end{aligned} \tag{E.3}$$

where the normalisation

$$\begin{aligned}N = &\, p_B(+x_B|+x_A) + p_B(+x_B|-x_A) \\ &+ p_B(-x_B|+x_A) + p_B(-x_B|-x_A)\end{aligned} \tag{E.4}$$

and $\mathrm{Tr}\{\hat{\rho}_E(\pm x_A)\} = 1/2$ is the probability for Eve to get either state after Alice announces $|x_A|$ and Bob announces $|x_B|$. All other states will be properly normalised. In this appendix, we shall evaluate the inner products between the four pure reduced states for Eve. Consider

$$\begin{aligned}&\left|\langle\psi_E(x_A,x_B)\left|\psi_E\left(x'_A,x'_B\right)\right\rangle\right|^2 \\ &\quad = p_B(x_B|x_A)\, p_B\left(x'_B|x'_A\right)\mathrm{Tr}\left\{\hat{\rho}_E(x_A,x_B)\,\hat{\rho}_E\left(x'_A,x'_B\right)\right\},\end{aligned} \tag{E.5}$$

where $\hat{\rho}_E(x_A,x_B)$ is Eve's reduced state when Alice sends x_A and Bob obtains the outcome x_B. The state is properly normalised with

$$\mathrm{Tr}\{\hat{\rho}_E(x_A,x_B)\} = 1\,. \tag{E.6}$$

Now since the partial trace can be expressed as

$$\mathrm{Tr}_B\left\{\hat{\rho}_{BE}\left(x_A\right)\left|x_B\right\rangle\left\langle x_B\right|\right\} = p_B\left(x_B|x_A\right)\hat{\rho}_E\left(x_A,x_B\right)\ , \tag{E.7}$$

the inner product can be written as the trace

$$\begin{aligned}&\left|\left\langle\psi_E\left(x_A,x_B\right)\left|\psi_E\left(x'_A,x'_B\right)\right\rangle\right|^2\\ &\quad = \mathrm{Tr}_E\left\{\mathrm{Tr}_B\left\{\hat{\rho}_{BE}\left(x_A\right)\left|x_B\right\rangle\left\langle x_B\right|\right\}\mathrm{Tr}_B\left\{\hat{\rho}_{BE}\left(x'_A\right)\left|x'_B\right\rangle\left\langle x'_B\right|\right\}\right\}\ .\end{aligned} \tag{E.8}$$

Here $\hat{\rho}_{BE}\left(x_A\right)$ is the joint state between Bob and Eve which is the output state of the beam splitters in figure E.1. We can evaluate this inner product using the Wigner function

$$\begin{aligned}&\mathrm{Tr}_E\left\{\mathrm{Tr}_B\left\{\hat{\rho}_{BE}\left(x_A\right)\left|x_B\right\rangle\left\langle x_B\right|\right\}\mathrm{Tr}_B\left\{\hat{\rho}_{BE}\left(x'_A\right)\left|x'_B\right\rangle\left\langle x'_B\right|\right\}\right\}\\ &= (2\pi\hbar)^2\int d\vec{\mathbf{x}}_E\, d\vec{\mathbf{y}}_E\left(\int d\mathbf{x}_B\, d\mathbf{y}_B\,\rho_{BE}\left(x_A;\mathbf{x}_B,\mathbf{y}_B,\vec{\mathbf{x}}_E,\vec{\mathbf{y}}_E\right)\delta\left(\mathbf{x}_B-x_B\right)\right.\\ &\quad\left.\times\int d\mathbf{x}_B\, d\mathbf{y}_B\,\rho_{BE}\left(x'_A;\mathbf{x}_B,\mathbf{y}_B,\vec{\mathbf{x}}_E,\vec{\mathbf{y}}_E\right)\delta\left(\mathbf{x}_B-x'_B\right)\right)\end{aligned} \tag{E.9}$$

with $\vec{\mathbf{x}}_E = \left(\mathbf{x}_{E_1},\mathbf{x}_{E_2}\right)^{\mathrm{T}}$ and $\vec{\mathbf{y}}_E = \left(\mathbf{y}_{E_1},\mathbf{y}_{E_2}\right)^{\mathrm{T}}$. We write the phase space variables in bold in order to distinguish them from the parameters x_A and x_B. Also $\rho_{BE}\left(x_A;\mathbf{x}_B,\mathbf{y}_B,\vec{\mathbf{x}}_E,\vec{\mathbf{y}}_E\right)$ without the hat is the Wigner function corresponding to

state $\hat{\rho}_{BE}(x_A)$. It is given by

$$\begin{aligned}
&\rho_{BE}(x_A;\mathbf{x}_B,\mathbf{y}_B,\vec{\mathbf{x}}_E,\vec{\mathbf{y}}_E) \\
&= \frac{1}{\sqrt{(2\pi\sigma_v^2)^3}} \exp\left[-\frac{1}{2}\begin{pmatrix} \mathbf{x}_B-\sqrt{\eta}x_A \\ \mathbf{x}_{E_1}-\sqrt{1-\eta}x_A \\ \mathbf{x}_{E_2}\end{pmatrix}^{\mathrm{T}} C_x^{-1} \begin{pmatrix} \mathbf{x}_B-\sqrt{\eta}x_A \\ \mathbf{x}_{E_1}-\sqrt{1-\eta}x_A \\ \mathbf{x}_{E_2}\end{pmatrix}\right] \\
&\quad \times \frac{1}{\sqrt{(2\pi\sigma_v^2)^3}} \exp\left[-\frac{1}{2}\begin{pmatrix} \mathbf{y}_B \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2}\end{pmatrix}^{\mathrm{T}} C_p^{-1} \begin{pmatrix} \mathbf{y}_B \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2}\end{pmatrix}\right].
\end{aligned} \tag{E.10}$$

Here C_x^{-1} and C_y^{-1} are the inverse covariance matrices given by

$$C_x^{-1} = M \begin{pmatrix} \frac{1}{\sigma_v^2} & 0 & 0 \\ 0 & \frac{1}{\sigma_-^2} & 0 \\ 0 & 0 & \frac{1}{\sigma_+^2}\end{pmatrix} M^{-1} \tag{E.11}$$

and

$$C_p^{-1} = M \begin{pmatrix} \frac{1}{\sigma_v^2} & 0 & 0 \\ 0 & \frac{1}{\sigma_+^2} & 0 \\ 0 & 0 & \frac{1}{\sigma_-^2}\end{pmatrix} M^{-1} \tag{E.12}$$

with

$$M^{-1} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} & 0 \\ -\sqrt{\frac{1-\eta}{2}} & \sqrt{\frac{\eta}{2}} & \frac{1}{\sqrt{2}} \\ \sqrt{\frac{1-\eta}{2}} & -\sqrt{\frac{\eta}{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}. \tag{E.13}$$

M is the beam splitter matrix (15.20). σ_-^2 is the squeezed variance for Eve's squeezed state that makes up her EPR state. σ_+^2 is the variance in the orthogonal quadrature where $\sigma_+\sigma_- = \sigma_v^2$ (see figure E.1). Putting this together and integrat-

ing over $\mathbf{x}_B$, we arrive at

$$
\begin{aligned}
&\left|\left\langle \psi_E\left(x_A, x_B\right)\left|\psi_E\left(x_A', x_B'\right)\right\rangle\right|^2 \\
&= 2\pi\hbar \int d\mathbf{x}_{E_1}\, d\mathbf{x}_{E_2} \\
&\quad \frac{1}{\left(2\pi\sigma_v^2\right)^3} \exp\left[-\frac{1}{2}\begin{pmatrix} x_B - \sqrt{\eta}x_A \\ \mathbf{x}_{E_1} - \sqrt{1-\eta}x_A \\ \mathbf{x}_{E_2} \end{pmatrix}^{\mathrm{T}} C_x^{-1} \begin{pmatrix} x_B - \sqrt{\eta}x_A \\ \mathbf{x}_{E_1} - \sqrt{1-\eta}x_A \\ \mathbf{x}_{E_2} \end{pmatrix}\right] \\
&\quad \times \exp\left[-\frac{1}{2}\begin{pmatrix} x_B' - \sqrt{\eta}x_A' \\ \mathbf{x}_{E_1} - \sqrt{1-\eta}x_A' \\ \mathbf{x}_{E_2} \end{pmatrix}^{\mathrm{T}} C_x^{-1} \begin{pmatrix} x_B' - \sqrt{\eta}x_A' \\ \mathbf{x}_{E_1} - \sqrt{1-\eta}x_A' \\ \mathbf{x}_{E_2} \end{pmatrix}\right] \\
&\quad \times 2\pi\hbar \int d\mathbf{y}_{E_1}\, d\mathbf{y}_{E_2}\, d\mathbf{y}_B\, d\mathbf{y}_B' \frac{1}{\left(2\pi\sigma_v^2\right)^3} \exp\left[-\frac{1}{2}\begin{pmatrix} \mathbf{y}_B \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2} \end{pmatrix}^{\mathrm{T}} C_p^{-1} \begin{pmatrix} \mathbf{y}_B \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2} \end{pmatrix}\right] \\
&\quad \times \exp\left[-\frac{1}{2}\begin{pmatrix} \mathbf{y}_B' \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2} \end{pmatrix}^{\mathrm{T}} C_p^{-1} \begin{pmatrix} \mathbf{y}_B' \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2} \end{pmatrix}\right] .
\end{aligned}
\tag{E.14}
$$

The integration is broken up into a product of two independent integrations and we shall perform the x integration and the y integration separately. The y integration is a constant that does not depend on x_A or x_B. The integrations are straight forward but tedious.

E.1 y integration

We start with the y integration for which we have

$$M^{-1}\begin{pmatrix} \mathbf{y}_B \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2} \end{pmatrix} = \begin{pmatrix} \sqrt{\eta}\mathbf{y}_B + \sqrt{1-\eta}\mathbf{y}_{E_1} \\ -\sqrt{\frac{1-\eta}{2}}\mathbf{y}_B + \sqrt{\frac{\eta}{2}}\mathbf{y}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{y}_{E_2} \\ \sqrt{\frac{1-\eta}{2}}\mathbf{y}_B - \sqrt{\frac{\eta}{2}}\mathbf{y}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{y}_{E_2} \end{pmatrix} \tag{E.15}$$

and hence the y integration can be written as

$$
\begin{aligned}
&2\pi\hbar \int d\mathbf{y}_{E_1}\, d\mathbf{y}_{E_2}\, d\mathbf{y}_B\, d\mathbf{y}'_B \frac{1}{(2\pi\sigma_v^2)^3} \exp\left[-\frac{1}{2}\begin{pmatrix}\mathbf{y}_B\\ \mathbf{y}_{E_1}\\ \mathbf{y}_{E_2}\end{pmatrix}^{\mathrm{T}} C_p^{-1} \begin{pmatrix}\mathbf{y}_B\\ \mathbf{y}_{E_1}\\ \mathbf{y}_{E_2}\end{pmatrix}\right] \\
&\quad\times \exp\left[-\frac{1}{2}\begin{pmatrix}\mathbf{y}'_B\\ \mathbf{y}_{E_1}\\ \mathbf{y}_{E_2}\end{pmatrix}^{\mathrm{T}} C_p^{-1} \begin{pmatrix}\mathbf{y}'_B\\ \mathbf{y}_{E_1}\\ \mathbf{y}_{E_2}\end{pmatrix}\right] \\
&= \frac{2\pi\hbar}{(2\pi\sigma_v^2)^3} \int d\vec{\mathbf{y}} \exp\left[-\frac{\left(\sqrt{\eta}\mathbf{y}_B + \sqrt{1-\eta}\mathbf{y}_{E_1}\right)^2}{2\sigma_v^2} - \frac{\left(\sqrt{\eta}\mathbf{y}'_B + \sqrt{1-\eta}\mathbf{y}_{E_1}\right)^2}{2\sigma_v^2}\right] \\
&\quad\times \exp\left[-\frac{\left(-\sqrt{\frac{1-\eta}{2}}\mathbf{y}_B + \sqrt{\frac{\eta}{2}}\mathbf{y}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{y}_{E_2}\right)^2}{2\sigma_+^2}\right] \\
&\quad\times \exp\left[-\frac{\left(-\sqrt{\frac{1-\eta}{2}}\mathbf{y}'_B + \sqrt{\frac{\eta}{2}}\mathbf{y}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{y}_{E_2}\right)^2}{2\sigma_+^2}\right] \\
&\quad\times \exp\left[-\frac{\left(\sqrt{\frac{1-\eta}{2}}\mathbf{y}_B - \sqrt{\frac{\eta}{2}}\mathbf{y}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{y}_{E_2}\right)^2}{2\sigma_-^2}\right] \\
&\quad\times \exp\left[-\frac{\left(\sqrt{\frac{1-\eta}{2}}\mathbf{y}'_B - \sqrt{\frac{\eta}{2}}\mathbf{y}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{y}_{E_2}\right)^2}{2\sigma_-^2}\right] \\
&= \frac{2\pi\hbar}{(2\pi\sigma_v^2)^3} \int d\vec{\mathbf{y}} \exp\left[-\vec{\mathbf{y}}^{\mathrm{T}} M_y \vec{\mathbf{y}}\right]
\end{aligned}
\tag{E.16}
$$

where

$$\vec{\mathbf{y}} = \begin{pmatrix} \mathbf{y}_B \\ \mathbf{y}'_B \\ \mathbf{y}_{E_1} \\ \mathbf{y}_{E_2} \end{pmatrix} . \tag{E.17}$$

The covariance matrix M_y is

$$M_y = \begin{pmatrix} \frac{\eta}{2\sigma_v^2} + \frac{\bar{\eta}}{2}\frac{\sigma_{th}^2}{\sigma_v^4} & 0 & \frac{\sqrt{\eta\bar{\eta}}}{2\sigma_v^2} - \frac{\sqrt{\eta\bar{\eta}}}{2}\frac{\sigma_{th}^2}{\sigma_v^4} & \frac{\sqrt{\eta}}{2}\frac{\sigma_k^2}{\sigma_v^4} \\ 0 & \frac{\eta}{2\sigma_v^2} + \frac{\bar{\eta}}{2}\frac{\sigma_{th}^2}{\sigma_v^4} & \frac{\sqrt{\eta\bar{\eta}}}{2\sigma_v^2} - \frac{\sqrt{\eta\bar{\eta}}}{2}\frac{\sigma_{th}^2}{\sigma_v^4} & \frac{\sqrt{\eta}}{2}\frac{\sigma_k^2}{\sigma_v^4} \\ \frac{\sqrt{\eta\bar{\eta}}}{2\sigma_v^2} - \frac{\sqrt{\eta\bar{\eta}}}{2}\frac{\sigma_{th}^2}{\sigma_v^4} & \frac{\sqrt{\eta\bar{\eta}}}{2\sigma_v^2} - \frac{\sqrt{\eta\bar{\eta}}}{2}\frac{\sigma_{th}^2}{\sigma_v^4} & \frac{\bar{\eta}}{\sigma_v^2} + \eta\frac{\sigma_{th}^2}{\sigma_v^4} & -\sqrt{\eta}\frac{\sigma_k^2}{\sigma_v^4} \\ \frac{\sqrt{\eta}}{2}\frac{\sigma_k^2}{\sigma_v^4} & \frac{\sqrt{\eta}}{2}\frac{\sigma_k^2}{\sigma_v^4} & -\sqrt{\eta}\frac{\sigma_k^2}{\sigma_v^4} & \frac{\sigma_{th}^2}{\sigma_v^4} \end{pmatrix} \tag{E.18}$$

where $\bar{\eta} = 1 - \eta$. The two intermediate variances σ_k^2 and σ_{th}^2 introduced above are

$$\left.\begin{matrix} \sigma_{th}^2 \\ \sigma_k^2 \end{matrix}\right\} = \frac{1}{2}\left(\sigma_+^2 \pm \sigma_-^2\right) . \tag{E.19}$$

The determinant of M_y turns out to be

$$\det\left(M_y\right) = \frac{1+\delta}{4\sigma_v^8} . \tag{E.20}$$

With this, the Gaussian integration works out to be

$$\int d\vec{\mathbf{y}}\, \exp\left[-\vec{\mathbf{y}}^{\mathrm{T}} M_y \vec{\mathbf{y}}\right] = \sqrt{\frac{\pi^4}{\det(M_y)}} \tag{E.21}$$

$$= \frac{2\pi^2\sigma_v^4}{\sqrt{1+\delta}}\,. \tag{E.22}$$

Putting everything together and replacing $\hbar = 2\sigma_v^2$ (see section 11.2), we finally arrive at

$$\frac{2\pi\hbar}{(2\pi\sigma_v^2)^3}\int d\vec{\mathbf{y}}\, \exp\left[-\vec{\mathbf{y}}^{\mathrm{T}} M_y \vec{\mathbf{y}}\right] = \frac{1}{\sqrt{1+\delta}} \tag{E.23}$$

for the *y* integration.

E.2 *x* integration

For the *x* integration, we first evaluate an intermediate vector

$$\vec{\mathbf{x}}_I = M^{-1}\begin{pmatrix} x_B - \sqrt{\eta}x_A \\ \mathbf{x}_{E_1} - \sqrt{1-\eta}x_A \\ \mathbf{x}_{E_2} \end{pmatrix} \tag{E.24}$$

$$= \begin{pmatrix} \sqrt{\eta}x_B + \sqrt{1-\eta}\mathbf{x}_{E_1} - x_A \\ -\sqrt{\frac{1-\eta}{2}}x_B + \sqrt{\frac{\eta}{2}}\mathbf{x}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{x}_{E_2} \\ \sqrt{\frac{1-\eta}{2}}x_B - \sqrt{\frac{\eta}{2}}\mathbf{x}_{E_1} + \frac{1}{\sqrt{2}}\mathbf{x}_{E_2} \end{pmatrix}. \tag{E.25}$$

With this the x integration can be written as

$$
\begin{aligned}
&2\pi\hbar \int d\mathbf{x}_{E_1}\, d\mathbf{x}_{E_2} \\
&\quad \frac{1}{(2\pi\sigma_v^2)^3} \exp\left[-\frac{1}{2}\vec{\mathbf{x}}_I^{\mathrm{T}} \begin{pmatrix} \frac{1}{\sigma_v^2} & 0 & 0 \\ 0 & \frac{1}{\sigma_-^2} & 0 \\ 0 & 0 & \frac{1}{\sigma_+^2} \end{pmatrix} \vec{\mathbf{x}}_I - \frac{1}{2}\vec{\mathbf{x}}_I'^{\mathrm{T}} \begin{pmatrix} \frac{1}{\sigma_v^2} & 0 & 0 \\ 0 & \frac{1}{\sigma_-^2} & 0 \\ 0 & 0 & \frac{1}{\sigma_+^2} \end{pmatrix} \vec{\mathbf{x}}_I' \right] \\
=&\frac{2\pi\hbar}{(2\pi\sigma_v^2)^3} \int d\vec{\mathbf{x}} \\
&\quad \exp\begin{bmatrix} -\frac{\left(\sqrt{1-\eta}\mathbf{x}_{E_1}+\sqrt{\eta}x_B-x_A\right)^2}{2\sigma_v^2} - \frac{\left(\sqrt{1-\eta}\mathbf{x}_{E_1}+\sqrt{\eta}x_B'-x_A'\right)^2}{2\sigma_v^2} \\ -\frac{\left(\sqrt{\frac{\eta}{2}}\mathbf{x}_{E_1}+\frac{1}{\sqrt{2}}\mathbf{x}_{E_2}-\sqrt{\frac{1-\eta}{2}}x_B\right)^2}{2\sigma_-^2} - \frac{\left(\sqrt{\frac{\eta}{2}}\mathbf{x}_{E_1}+\frac{1}{\sqrt{2}}\mathbf{x}_{E_2}-\sqrt{\frac{1-\eta}{2}}x_B'\right)^2}{2\sigma_-^2} \\ -\frac{\left(-\sqrt{\frac{\eta}{2}}\mathbf{x}_{E_1}+\frac{1}{\sqrt{2}}\mathbf{x}_{E_2}+\sqrt{\frac{1-\eta}{2}}x_B\right)^2}{2\sigma_+^2} - \frac{\left(-\sqrt{\frac{\eta}{2}}\mathbf{x}_{E_1}+\frac{1}{\sqrt{2}}\mathbf{x}_{E_2}+\sqrt{\frac{1-\eta}{2}}x_B'\right)^2}{2\sigma_+^2} \end{bmatrix} \\
=&\frac{2\pi\hbar}{(2\pi\sigma_v^2)^3} \exp\begin{bmatrix} -\frac{\left(\sqrt{\eta}x_B-x_A\right)^2}{2\sigma_v^2} - \frac{\left(\sqrt{\eta}x_B'-x_A'\right)^2}{2\sigma_v^2} \\ -\frac{(1-\eta)x_B^2}{4\sigma_-^2} - \frac{(1-\eta)x_B'^2}{4\sigma_-^2} \\ -\frac{(1-\eta)x_B^2}{4\sigma_+^2} - \frac{(1-\eta)x_B'^2}{4\sigma_+^2} \end{bmatrix} \\
&\quad \times \int d\vec{\mathbf{x}}\, \exp\left[-\vec{\mathbf{x}}^{\mathrm{T}} M_x \vec{\mathbf{x}} - \vec{c}^{\mathrm{T}}\vec{\mathbf{x}}\right]
\end{aligned}
\tag{E.26}
$$

with the covariance matrix

$$
M_x = \frac{1}{\sigma_v^2} \begin{pmatrix} (1-\eta)+\eta\frac{\sigma_{th}^2}{\sigma_v^2} & \sqrt{\eta}\frac{\sigma_k^2}{\sigma_v^2} \\ \sqrt{\eta}\frac{\sigma_k^2}{\sigma_v^2} & \frac{\sigma_{th}^2}{\sigma_v^2} \end{pmatrix} \tag{E.27}
$$

and

$$\vec{c} = \frac{1}{\sigma_v^2}\begin{pmatrix} \sqrt{\eta}\,(\sqrt{\eta}(x_B + x'_B) - (x_A + x'_A)) - \sqrt{(\overline{\eta})\eta}\,\frac{\sigma_{th}^2}{\sigma_v^2}\,(x_B + x'_B) \\ \sqrt{\eta}\,\frac{\sigma_k^2}{\sigma_v^2}\,(x_B + x'_B) \end{pmatrix}. \quad \text{(E.28)}$$

The vector $\vec{\mathbf{x}} = (\mathbf{x}_{E_1}, \mathbf{x}_{E_2})^{\mathrm{T}}$. The remaining Gaussian integral can be evaluated by diagonalising M_x and the resulting expression is

$$\int d\vec{\mathbf{x}}\, \exp\left[-\vec{\mathbf{x}}^{\mathrm{T}} M_x \vec{\mathbf{x}} - \vec{c}^{\mathrm{T}}\vec{\mathbf{x}}\right] = \sqrt{\frac{\pi^2}{\det M_x}}\exp\left[\frac{b_1^2}{4\lambda_1} + \frac{b_2^2}{4\lambda_2}\right] \quad \text{(E.29)}$$

where

$$\left.\begin{matrix}\lambda_1 \\ \lambda_2\end{matrix}\right\} = \frac{1}{2\sigma_v^2(1-\eta)}\left(2(1-\eta) + (1+\eta)\,\delta \pm \sqrt{8(1-\eta)\eta\delta + (1+\eta)^2\delta^2}\right) \quad \text{(E.30)}$$

are the eigenvalues of M_x. The b's are obtained from

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = S \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \quad \text{(E.31)}$$

where

$$S = \sqrt{2\eta(2+\delta-2\eta)}\begin{pmatrix} -\frac{1}{\sqrt{W+Y}} & \frac{1}{\sqrt{W-Y}} \\ -\frac{1}{\sqrt{W-Y}} & -\frac{1}{\sqrt{W+Y}} \end{pmatrix} \quad \text{(E.32)}$$

with

$$W = 8\eta(1-\eta) + \delta(1+\eta)^2 \tag{E.33}$$

$$Y = (1-\eta)\sqrt{\delta}\sqrt{8\eta(1-\eta) + \delta(1+\eta)^2}\,. \tag{E.34}$$

S is the unitary matrix that diagonalises M_x

$$SM_xS^{\mathrm{T}} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\,. \tag{E.35}$$

The term $b_1^2/4\lambda_1 + b_2^2/4\lambda_2$ can be simplified to get

$$\begin{aligned} \frac{b_1^2}{4\lambda_1} + \frac{b_2^2}{4\lambda_2} =& \frac{(1+\delta-\eta)\left(x_A + x_A'\right)^2}{4(1+\delta)\sigma_v^2} + \frac{\delta(2+\delta)\left(x_B + x_B'\right)^2}{4(1+\delta)\sigma_v^2} \\ & - \frac{2\delta\sqrt{\eta}\left(x_B + x_B'\right)\left(x_A + x_A'\right)}{4(1+\delta)\sigma_v^2}\,. \end{aligned} \tag{E.36}$$

The determinant of M_x is

$$\det M_x = \frac{1+\delta}{\sigma_v^4}\,. \tag{E.37}$$

Putting all this together, the x-integration becomes

$$\begin{aligned}
&\frac{2\pi\hbar}{(2\pi\sigma_v^2)^3}\exp\left[\begin{array}{c} -\frac{\left(\sqrt{\eta}x_B-x_A\right)^2}{2\sigma_v^2}-\frac{\left(\sqrt{\eta}x'_B-x'_A\right)^2}{2\sigma_v^2} \\ -\frac{(1-\eta)x_B^2}{4\sigma_-^2}-\frac{(1-\eta)x_B'^2}{4\sigma_-^2} \\ -\frac{(1-\eta)x_B^2}{4\sigma_+^2}-\frac{(1-\eta)x_B'^2}{4\sigma_+^2} \end{array}\right] \\
&\times\int d\vec{\mathbf{x}}_E\ \exp\left[-\vec{\mathbf{x}}_E^{\mathrm{T}}M_x\vec{\mathbf{x}}_E-\vec{c}^{\mathrm{T}}\vec{\mathbf{x}}_E\right] \\
=&\frac{1}{2\pi^2\sigma_v^4}\exp\left[\begin{array}{c} -\frac{\left(\sqrt{\eta}x_B-x_A\right)^2}{2\sigma_v^2}-\frac{\left(\sqrt{\eta}x'_B-x'_A\right)^2}{2\sigma_v^2} \\ -\frac{(1-\eta)}{4\sigma_-^2}\left(x_B^2+x_B'^2\right) \\ -\frac{(1-\eta)}{4\sigma_+^2}\left(x_B^2+x_B'^2\right) \end{array}\right] \\
&\times\frac{\pi\sigma_v^2}{\sqrt{1+\delta}}\exp\left[\begin{array}{c} \frac{(1+\delta-\eta)}{4(1+\delta)\sigma_v^2}\left(x_A+x'_A\right)^2 \\ +\frac{\delta(2+\delta)}{4(1+\delta)\sigma_v^2}\left(x_B+x'_B\right)^2 \\ -\frac{2\delta\sqrt{\eta}}{4(1+\delta)\sigma_v^2}\left(x_B+x'_B\right)\left(x_A+x'_A\right) \end{array}\right] \qquad \text{(E.38)} \\
=&\frac{1}{2\pi\sigma_v^2\sqrt{1+\delta}}\exp\left[\begin{array}{c} -\frac{\left(\sqrt{\eta}x_B-x_A\right)^2}{2\sigma_v^2}-\frac{\left(\sqrt{\eta}x'_B-x'_A\right)^2}{2\sigma_v^2} \\ -\frac{(1+\delta-\eta)}{2\sigma_v^2}\left(x_B^2+x_B'^2\right) \\ +\frac{(1+\delta-\eta)}{4(1+\delta)\sigma_v^2}\left(x_A+x'_A\right)^2 \\ +\frac{\delta(2+\delta)}{4(1+\delta)\sigma_v^2}\left(x_B+x'_B\right)^2 \\ -\frac{\delta\sqrt{\eta}}{2(1+\delta)\sigma_v^2}\left(x_B+x'_B\right)\left(x_A+x'_A\right) \end{array}\right]. \qquad \text{(E.39)}
\end{aligned}$$

In the last equality, we write σ_- and σ_+ in terms of η and δ using the relation

$$(1-\eta)\sigma_{th}^2+\eta\sigma_v^2=(1+\delta)\sigma_v^2\,. \qquad \text{(E.40)}$$

This completes the x integration.

E.3 Putting them together

Combining the results for the y integration and the x integration, the inner product $\left|\left\langle \psi_E\left(x_A,x_B\right)\left|\psi_E\left(x'_A,x'_B\right)\right\rangle\right|^2$ works out to be

$$\begin{aligned}&\left|\left\langle \psi_E\left(x_A,x_B\right)\left|\psi_E\left(x'_A,x'_B\right)\right\rangle\right|^2\\&\quad=\frac{1}{2\pi\sigma_v^2(1+\delta)}\exp\left[\begin{array}{c}-\frac{\left(\sqrt{\eta}x_B-x_A\right)^2}{2\sigma_v^2}-\frac{\left(\sqrt{\eta}x'_B-x'_A\right)^2}{2\sigma_v^2}\\-\frac{(1+\delta-\eta)}{2\sigma_v^2}\left(x_B^2+x_B'^2\right)\\+\frac{(1+\delta-\eta)}{4(1+\delta)\sigma_v^2}\left(x_A+x'_A\right)^2\\+\frac{\delta(2+\delta)}{4(1+\delta)\sigma_v^2}\left(x_B+x'_B\right)^2\\-\frac{\delta\sqrt{\eta}}{2(1+\delta)\sigma_v^2}\left(x_B+x'_B\right)\left(x_A+x'_A\right)\end{array}\right].\end{aligned}\tag{E.41}$$

Bibliography

[1] Daniel J. Alton. *The effect of state impurity on the security of continuous variable quantum key distribution*. Honour's thesis, The Australian National University, 2006.

[2] Leslie E. Ballentine. *Quantum mechanics: a modern development*. World Scientific Publishing Company, 1998.

[3] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Communicating with qubit pairs. In Ranee K. Brylinski and Goong Chen, editors, *Mathematics of Quantum Computation*, chapter 14, pages 361–403. Chapman & Hall/CRC, 2002.

[4] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Secure communication with a publicly known key. *Acta Phys. Pol. A*, 101:357, 2002; 101:901, 2002.

[5] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Secure communication with single-photon two-qubit states. *J. Phys. A*, 35:L407–L413, 2002.

[6] Giuliano Benenti, Giulio Casati, and Giuliano Strini. *Principles of quantum computation and information, Volume II: Basic tools and special tools*. World Scientific, 2007.

[7] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, December 1984. IEEE.

[8] Charles H. Bennett, Gilles Brassard, Claude Crpeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41(6):1915–1923, 1995.

[9] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology EUROCRYPT 93*, pages 410–423. Springer-Verlag, 1994.

[10] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, Oct 1998.

[11] G. S. Buller and R. J. Collins. Single-photon generation and detection. *Measurement Science and Technology*, 21(1):012002+, 2010.

[12] N. J. Cerf, S. Iblisdir, and G. Van Assche. Cloning and cryptography with quantum continuous variables. *The European Phycial Journal D*, 18:211, 2002.

[13] M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key distribution, 2004, quant-ph/0402131.

[14] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Appl. Opt.*, 35(12):1956–1976, 1996.

[15] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2nd edition, June 2006.

[16] Imre Csiszár and János Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, 1978.

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

[18] Berthold-Georg Englert. *Lectures on quantum mechanics: simple systems*. World Scientific Publishing Company, 2006.

[19] Berthold-Georg Englert, Dagomir Kaszlikowski, Hui Khoon Ng, Wee Kang Chua, Jaroslav Řeháček, and Janet Anders. Highly efficient quantum key distribution with minimal state tomography, 2004, quant-ph/0405084.

[20] Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Universal unitary gate for single-photon two-qubit states. *Phys. Rev. A*, 63(3):032303, Feb 2001.

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

[22] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography

with continuous variables. *Quantum Information and Computation*, 3:535–552, 2003, quant-ph/0306141.

[23] Frederic Grosshans and Philippe Grangier. Continuous variable quantum cryptograhy using coherent states. *Phys. Rev. Lett.*, 88(5):057902, 2002.

[24] Masahito Hayashi. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Phys. Rev. A*, 76, 2007.

[25] Matthias Heid and Norbert Lütkenhaus. Security of coherent-state quantum cryptography in the presence of Gaussian noise. *Phys. Rev. A*, 76(2):022313, Aug 2007.

[26] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61(2):022309, Jan 2000.

[27] A. S. Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 4(4):337–394, 1973.

[28] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory*, 44:269–273, 1998.

[29] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501, Aug 2005.

[30] Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.*, 95:180503, 2005.

[31] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White. Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement. *PRL*, 99(25):250505, Dec 2007.

[32] L. B. Levitin. Optimal quantum measurements for two pure and mixed states. In V. P. Belavkin, O. Hirota, and R. L. Hudson, editors, *Quantum Communications and Measurement*, pages 439–447. Plenum Press, 1995.

[33] Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency. *Opt. Express*, 16(5):3032–3040, 2008.

[34] Hoi-Kwong Lo. Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Inf. Comput.*, 1:81–94, 2001.

[35] Hoi-Kwong Lo and Yi Zhao. Quantum cryptography, Mar 2008, quant-ph/0803.2507.

[36] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection. *Phys. Rev. A*, 74(4):042326, Oct 2006.

[37] Chao-Yang Lu, Daniel E. Browne, Tao Yang, and Jian-Wei Pan. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *PRL*, 99(25):250504, Dec 2007.

[38] Ryo Namiki and Takuya Hirano. Practical limitation for continuous-variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 92:117901, 2004.

[39] John Preskill. Lecture notes for Physics 229: Quantum information and computation, http://www.iqi.caltech.edu.

[40] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61(1):010303, Dec 1999.

[41] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45:2171, 2004.

[42] R. Renner and J. I. Cirac. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102(11):110504, 2009.

[43] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Computing*, 6(1):1–127, 2008, quant-ph/0512258.

[44] Danna Rosenberg, Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A*, 71(6):061803, Jun 2005.

[45] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301, 2009.

[46] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100(20), May 2008.

[47] Benjamin Schumacher. Quantum coding. *Phys. Rev. A*, 51(4):2738–2747, Apr 1995.

[48] Benjamin Schumacher and Michael D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56(1):131–138, Jul 1997.

[49] Claude E. Shannon. A mathematical theory of communication. *Bell Systems Tech. J.*, 27:379–423, 623–656, 1948.

[50] Peter W. Shor. Algorithm for quantum computation: Discrete logarithm and factoring. In *Proceedings*, 35^{th} *Annual Symposium on Foundation of Computer Science*, pages 124–134, Los Alamitos, CA, 1994. IEEE Press.

[51] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, Jul 2000.

[52] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Phys. Rev. Lett.*, 89(16):167901, Sep 2002.

[53] R. Simon, N. Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. *Phys. Rev. A*, 49(3):1567–1583, Mar 1994.

[54] Thomas Symul, Daniel J. Alton, Syed M. Assad, Andrew M. Lance, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Phys. Rev. A*, 76:030303, 2007.

[55] G. Van Assche, J. Cardinal, and N. J. Cerf. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory*, 50(2):394–400, 2004.

[56] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883–887, 2001.

[57] Jaroslav Řeháček, Berthold-Georg Englert, and Dagomir Kaszlikowski. Iterative procedure for computing accessible information in quantum communication. *Phys. Rev. A*, 71:054303, 2005, quant-ph/0408134.

[58] D. F. Walls and Gerard J. Milburn. *Quantum optics*. Springer, 2008.

[59] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.