QUANTUM KEY DISTRIBUTION PROTOCOLS WITH HIGH RATES AND LOW COSTS

A Thesis
Presented to
The Academic Faculty

by

Zheshen Zhang

In Partial Fulfillment
of the Requirements for the Degree
Master of Science in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
May 2009

QUANTUM KEY DISTRIBUTION PROTOCOLS WITH HIGH RATES AND LOW COSTS

Approved by:

Professor Abdallah Ougazzaden,
Committee Chair
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Paul Voss, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor David Citrin
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: 6 April 2009

To my mother, who always supports me and stands by my side.

PREFACE

In the information age, massive quantitiies of information are generated every second. Some of the information generated, news, for example, is meant to be available to all who are interested in it. However, often information must be kept private or only shared between specific parties. In the latter case, information security is essential. There are various ways to protect information. One of the technical ways is cryptography, which is an area of interest for mathematicians, computer scientists, physicists, and information theorists. One new area in cryptography, a physical layer security method called quantum key distribution, has attracted much attention recently. Quantum key distribution establishes correlated random data between two parties in a way that an eavesdropper can obtain no information on this data. This thesis presents a detailed analysis of two proposed systems for quantum key distribution that allow for significantly higher clock rate operation and for lower cost than current systems. The first system uses amplified spontaneous emission as a source for continuous variable quantum key distribution. It inherits the security of other continuous variable quantum key distribution systems. The second system is based on discretely signaled continuous variable quantum key distribution and has required the development of security proofs. This second system is specifically designed in order to speed up necessary post-processing.

ACKNOWLEDGEMENTS

I would like to thank my committee, especially Prof. Voss, for guiding my research for the last two and half years. I am impressed by Prof. Voss's enthusiasm towards research and patience with his students. Discussion with him is always enjoyable and fruitful. I also would like to thank post-doc Quyen for his hard work and nice collaboration for over one year. The next person that I would like to thank is Olivier, who always makes different circuits and integrates optical devices as fast as possible for us. I also need to appreciate my life at Georgia Tech Lorraine with my colleagues. These people include Alex, Audric, Damien, David, Fred, Jaramy, Mohammed, Ning, Sarah, Satya, Peter, Vinod, Wei and Wui. It is all of us who make a relaxing and friendly atmosphere at Georgia Tech Lorraine. Last and not the least, I would like to thank my family for their continuous support on my study. Their support is the reason why I am here.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Cryptography is the study of secure transmission of information over an unprotected channel. Technically, there are two families of methods in cryptography. The first and largest family, mostly studied by mathematicians and computer scientists, uses mathematical methods to modify binary strings of information. Good examples there are cryptographic protocols such as DES, RSA, digital signature and so on. The common feature of those protocols is that they all make use of mathematical methods to provide hoped-for security. Currently used methods are believed to be secure, though none are associated with a full mathematical proof of security. The other family, which has attracted much attention recently, uses physical methods for cryptography. Compared to the first family, the second one requires a specific physical implementation, nevertheless, can be proved to be unconditionally secure.

1.1 Digital cryptography

In this section, we will review two groups of digital cryptography, i.e., private key cryptographic systems and public key cryptographic systems.

1.1.1 Private key cryptographic systems

For private key cryptographic systems, the encryption and decryption process use the same shared key. The main advantage for private key cryptographic systems is that the encryption and decryption are simple and can happen at a very high rate. However, since the encryption and decryption require a common shared private key, key distribution becomes a problem. Typical private key cryptographic systems include DES, AES and IDEA.

Essentially, private key cryptographic systems mix key and plain text in a complicated but deterministic way. The encryption process usually takes several rounds. In each round, a sub-key and the plain text are mixed up by an algorithm consisting of a series of substitution and permutation procedures. After several rounds, the original plain text is undecipherable. Security in this case is based on the assumption that due to the complexity of encryption, the best attack is an exhaustive search for the key. In Fig. 1 we show one encryption round of IDEA [32].

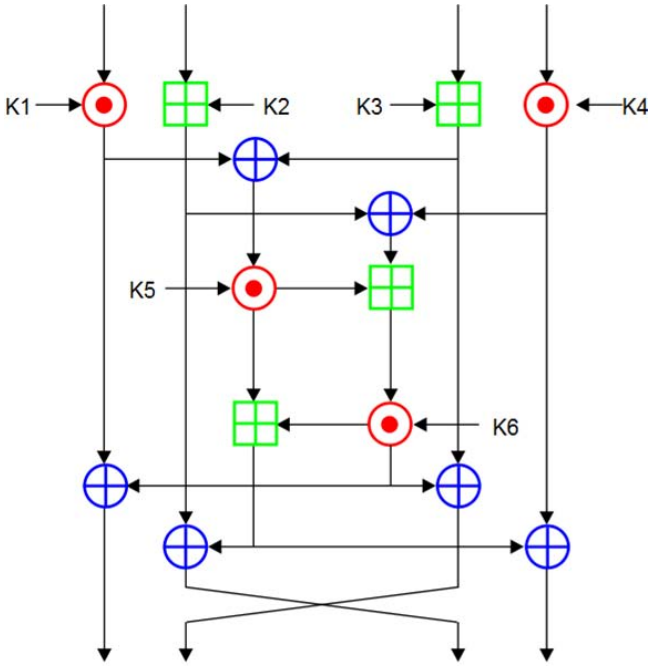


Figure 1: An encryption round of IDEA

1.1.2 Public key cryptographic systems

For public key cryptographic systems, encryption and decryption use different keys. The encryption process uses a public key that is available to any interested party. However, only the person who has the private key is able to decrypt messages that are encrypted with the public key. The main advantage of public key cryptographic systems is that there is no need for key distribution. However, compared to private key cryptographic systems, public key cryptographic systems are more computationally

intensive and thus encryption and decryption take a much longer time. Typical public key cryptographic protocols are the RSA and El-Gamal cyrptosystems. Public key principles are also used for other cyptographic primitives such as the Diffie-Hellman key exchange protocol, and the Digital Signature Algorithm. The security of these protocols is typically based on an unproven assumption that is generally considered to be true. For example, RSA is based on the generally believed proposition that the factoring of very large numbers cannot be done in a number of operations that is a polynomial function of key length. Thus with large enough numbers, one may hope that these protocols will be secure. A typical public key cryptographic system is shown in Fig. 2[33].

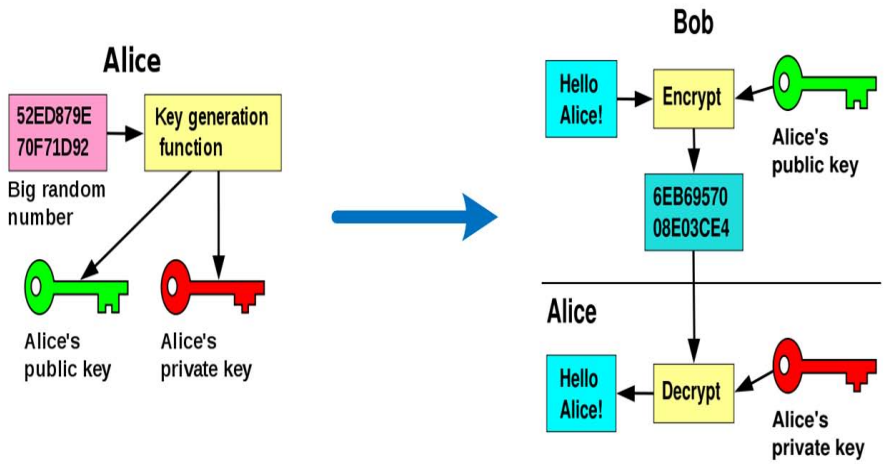


Figure 2: A typical public key cryptographic system

1.2 Physical layer security

In this section, we will give a review of quantum key distribution, which is the best developed branch of physical layer security. The fundamental idea of physical layer security is that noise in a communications channel between the sender Alice and an eavesdropper, who we call Eve, induces errors on Eve's data. Intelligent use of the channel between Alice and the intended receiver, Bob, allows transmission of data during the times when Eve makes mistakes.

1.2.1 Quantum key distribution

Quantum key distribution (QKD) systems [1, 2, 3] make use of optical quantum fluctuations to establish shared secret keys between two legitimate users (Alice and Bob) such that an eavesdropper (Eve) who makes optimal physical measurements can know, on average, none of the bits of the secret key. Because optical quantum fluctuations are universal and their properties are mathematically precise, it is possible to quantify the information between Alice and Bob as well as between Alice and Eve, and Bob and Eve. Thus one may arrive at a communication system where security is provable by fundamental principles if the protocol is followed correctly. A typical system works in the following way. After a number of samples of a correlated random variable are obtained by means of quantum measurements, a reconciliation phase assures agreement of Alice and Bob's data. Finally, a privacy amplification phase uses universal hash functions to eliminate Eve's potential partial information at the cost of shrinking the length of Alice and Bob's shared data.

The most famous quantum key distribution protocol is BB84 proposed in 1984. In BB84 QKD protocol, two communicators make use of two sets of non-orthogonal basis for encoding quantum states. By random switching of the encoding basis, two communicators will be able to know if an eavesdropper is observing the channel because quantum noise introduced by an eavesdropper making measurements, resulting in increased error rate. In Fig. 3, we show the encoding and decoding scheme proposed in BB84.

If Alice and Bob's encoding and decoding basis is the same, then they keep the bits as a part of the secure key. If their encoding and decoding basis are different, they simply abandon that time slot. Since the eavesdropper can't know Alice's encoding basis in advance and she can't measure it 100% precisely due to the limitations in fundamental quantum mechanics, any of eavesdropper's effort on obtaining information

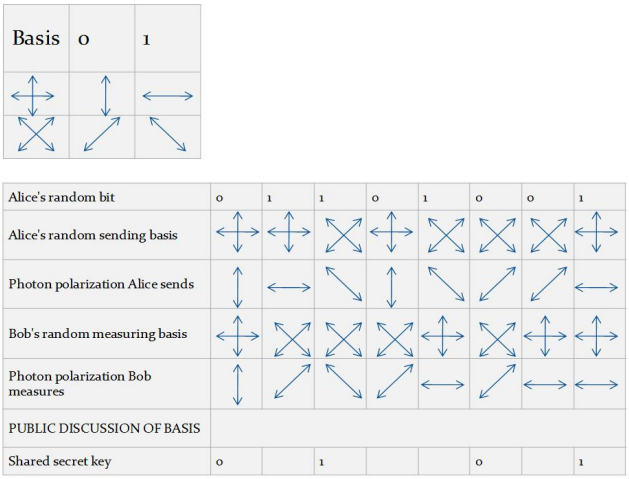


Figure 3: The encoding and decoding scheme in BB84 QKD protocol

on the key will result in an interference of the quantum state, which will be discovered by Alice and Bob by comparing Alice's sent information and Bob's measurement result.

CHAPTER II

A QUANTUM KEY DISTRIBUTION SYSTEM BASED ON AN AMPLIFIED SPONTANEOUS EMISSION SOURCE

2.1 Motivation for amplified spontaneous emission quantum key distribution

An alternative to the quantum key distribution system described in the previous chapter is to use homodyne detection instead of photon counting. This method can potentially lead to higher rate operation due to the large bandwidth of p-i-n photodiodes. Unlike photon counters, p-i-n photodiodes require no dead time to reset the detector after a measurement is performed. Potentially, such systems, called continuous variable quantum key distribution, could operate at 10 GHz clock rates or even higher. Here continuous variable refers to the fact that homodyne measurement results in a continuous real-valued spectrum as opposed to the discrete spectrum of photon counting measurements. Continuous variable systems have speed advantages, but each measurement can be thought to include noise from the electromagnetic vacuum. This always present noise results in lower performance as distances become great. A traditional CVQKD diagram is shown in Fig.4[7].

This chapter describes a physical system that can simplify continuous variable quantum key distributions. The key idea is that most CVQKD systems require that the coherent state signals sent over the channel be sent with a probability governed by a Gaussian probability in the complex plane in order to maximize the mutual information between Alice and Bob. The improvement is to take advantage of the fact that amplified spontaneous emission (ASE) is already perfectly Gaussian distributed

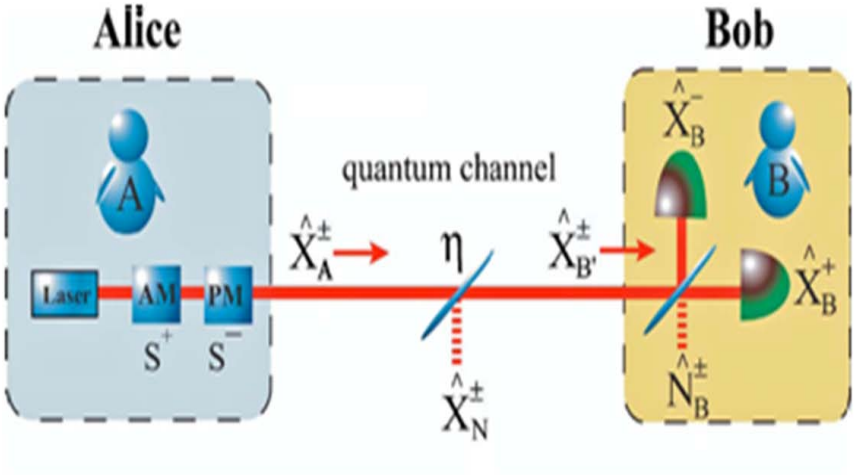


Figure 4: Traditional CVQKD diagram

in each mode.

2.2 Description of the amplified spontaneous emission based QKD protocol

A schematic of the ASE-based QKD is presented in Fig. 5. Next, we will describe our protocol step by step.

Step 1: Alice splits broadband thermal light emitting from the source. The splitter transmission coefficient for the thermal light propagating towards Alices detectors is η_1. The rest of the light is sent to Bob through a lossy quantum channel.

Step 2: After splitting, both parts consist of a portion of the same example of a mixed state. Their classical fluctuations are the same (which have a total variance V_X), but their quantum noise is independent. Alice and Bob synchronize their measurements to a local oscillator beam generated by a laser, and measure with total efficiencies η_m and η_c respectively, where η_c includes channel propagation losses. For Alice, she makes a heterodyne measurement on both quadratures. For Bob, he randomly switches between two quadratures and makes a homodyne measurement.

Step 3: After an alignment and channel characterization procedure, and after collecting their measurement outcomes, Alice and Bob communicate on a classical

channel to perform reverse reconciliation and privacy amplification, resulting in a final secure key.

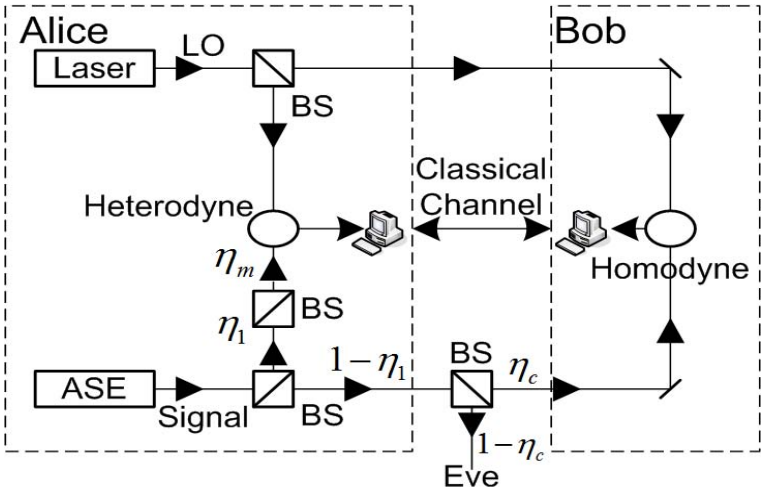


Figure 5: The experimental setup for QKD protocol based on ASE

The light source that used in our scheme is amplified spontaneous emission (ASE). ASE is regarded as superposition of the contribution of different small sources [31]. We can number those sources as $j = 1, ..., N$. When N is very large, the density operator of the entire filed can be written as,

$$\rho = \frac{1}{\pi\langle n\rangle}\int e^{-|\alpha|^2/\langle n\rangle}|\alpha\rangle\langle\alpha|d^2\alpha, \tag{1}$$

which is a Gaussian superposition of coherent states. The weight function may be written as,

$$P(\alpha) = \frac{1}{\pi\langle n\rangle}e^{-|\alpha|^2/\langle n\rangle}, \tag{2}$$

which indicates that the two quadratures of the ASE is Gaussian distributed.

The key component in the scheme is the beam splitter that Alice uses to split the output of ASE. The beam splitter has two effects. First, it guarantees Alice always have a better guess on Bob's measurement result than the eavesdropper when Alice

and Bob employ a reverse reconciliation afterwards. This means when the transmission ratio of this beam splitter is within some range, we can use information theory to prove that Alice always has a better signal noise ratio than the eavesdropper does. Therefore, in this case, Alice and Bob will be able to have positive secrecy capacity and build up a secure key. The other reason why a beam splitter is employed is to split the output of the ASE is that Alice can manually select the transmission of the beam splitter to maximize the secrecy capacity with Bob. The optimal transmission ratio is influenced by the quantum efficiency of Alice's detection and the quantum efficiency of the channel as well.

Next, we will discuss our continuous variable QKD protocol. To begin with, we first introduce some basic notations of quantum field in our scheme.

We suppose the output of ASE is $\hat{a}_s$, with both quadratures gaussian modulated. It can be presented in another form,

$$\hat{a}_s = S + \hat{N}_s, \tag{3}$$

where $S = X + iP$ is a complex random variable with X and Y being gaussian distributed real random variables. $\hat{N}_s$ is a vacuum quantum field.

Alice then use a beam splitter to split the signal. Let's assume the other input mode of the beam splitter is vacuum denoting as $\hat{N}_{BS}$, then the two outputs of the beam splitter can be denoted as,

$$\begin{aligned} \hat{a}_A &= \sqrt{\eta_1}\hat{a}_s + \sqrt{1-\eta_1}\hat{N}_{BS}, \\ \hat{a}_c &= \sqrt{\eta_1}\hat{N}_{BS} - \sqrt{1-\eta_1}\hat{a}_s, \end{aligned} \tag{4}$$

where the subscript A denotes the mode sending to Alice's detector and subscript c denotes the mode sends to the quantum channel.

The effect of a lossy quantum channel is equivalent to a beam splitter whose transmission ratio is exactly the same as the quantum efficiency of the channel. Furthermore, we assume that the channel only introduces loss into the quantum state

that is transferring on the channel but doesn't introduce any extra noise. Based on this assumption, we can constrain the action that can be taken by the Eavesdropper, also called Eve. Since Alice and Bob are able to make some kind of quantum measurements to estimate the physical parameters, such as the quantum efficiency and correlation coefficient of Alice and Bob's data, of the quantum channel, Eve's eavesdropping strategy must not violate those parameters of the channel. For a lossy but noiseless quantum channel, the best strategy for Eve is to replace the lossy channel with a lossless one and use a beam splitter, whose transmission ratio is exactly the same as the quantum efficiency of the channel, to split the input quantum state so that either Alice or Bob isn't aware of the existence of Eve because the physical parameters of the channel are not changed by Eve. Then Eve sends one output mode of the beam splitter to Bob and reserves the other mode. Eve's beam splitter is indicated in Fig. 5 where a beam splitter with transmission efficiency η_c is placed on the channel. Finally, Eve will be able to manipulate and measure her reserved quantum state. We can write Bob's received quantum mode as,

$$\begin{aligned} \hat{a}_B &= \sqrt{\eta_c}\hat{a}_c + \sqrt{1-\eta_c}\hat{N}_c \\ \hat{a}_E &= \sqrt{\eta_c}\hat{N}_c - \sqrt{1-\eta_c}\hat{a}_c. \end{aligned} \tag{5}$$

At this stage, Alice, Bob and Eve make quantum measurements and then they have some data in common forming classical correlations. For simplicity, we assume that those three parties all make homodyne measurements on only one quadrature of the quantum field. In practice, the quantum efficiency of Alice and Bob's homodyne detector is not perfect. The quantum efficiency of Bob's detector can be included in the quantum efficiency of the channel and we let the quantum efficiency of Alice's detector be η_m. Then Alice's measured quantum mode can be written as,

$$\hat{a}'_A = \sqrt{\eta_m}\hat{a}_A + \sqrt{1-\eta_m}\hat{N}_m \tag{6}$$

Those measurements result in some correlated data among Alice, Bob and Eve.

Finally, Alice and Bob can perform reverse reconciliations and privacy amplification to distill the final key.

2.3 Security analysis

In this section, we will analyze the security of our proposed experimental scheme. The security analysis will be done based on Shannon information theory. We will compare our result with those general proofs on continuous variable quantum key distribution and show that a system following our protocol is secure against gaussian and non-gaussian individual and collective attacks.

Let Alice, Bob and Eve's measurement results be gaussian distributed random variables R_A, R_B and R_E. Then those random variables can be expressed as following,

$$\begin{aligned} R_A &= \sqrt{\eta_m\eta_1}X + \sqrt{\eta_m\eta_1}R_X + \sqrt{\eta_m(1-\eta_1)}R_{BS} \\ &+ \sqrt{(1-\eta_m)}R_m \\ R_B &= -\sqrt{\eta_c(1-\eta_1)}X - \sqrt{\eta_c(1-\eta_1)}R_X \\ &+ \sqrt{\eta_1\eta_c}R_{BS} + \sqrt{1-\eta_c}R_c \\ R_E &= \sqrt{(1-\eta_1)(1-\eta_c)}X + \sqrt{(1-\eta_1)(1-\eta_c)}R_X \\ &- \sqrt{\eta_1(1-\eta_c)}R_{BS} + \sqrt{\eta_c}R_c. \end{aligned} \tag{7}$$

The mutual information between Alice and Bob is calculated to,

$$I(A;B) = -\log_2(1-\rho^2_{R_AR_B}), \tag{8}$$

where $\rho_{R_AR_B}$ is the correlation coefficient between Alice and Bob's measurement results. The correlation coefficient can be calculated as

$$\rho^2_{R_AR_B} = \frac{\mathrm{cov}^2(\mathrm{R_A},\mathrm{R_B})}{\mathrm{Var}(\mathrm{R_A})\mathrm{Var}(\mathrm{R_B})}, \tag{9}$$

where $\mathrm{cov}(\mathrm{R_A},\mathrm{R_B})$ is the covariance of R_A and R_B. $\mathrm{Var}(\mathrm{R_A})$ and $\mathrm{Var}(\mathrm{R_B})$ is the variance of R_A and R_B. Thus the mutual information between Alice and Bob is

$$I(A;B) = -\frac{1}{2}\log_2\{1 - \frac{\eta_1\eta_c\eta_m(1-\eta_1)V_X^2}{(\eta_1\eta_mV_X+1)[\eta_c(1-\eta_1)V_X+1]}\}. \tag{10}$$

Here V_X is the variance of gaussian distributed random variable X. Similarly, we can get the mutual information between Eve and Bob,

$$I(B;E) = -\frac{1}{2}\log_2\{1 - \frac{\eta_c(1-\eta_1)^2(1-\eta_c)V_X^2}{[(1-\eta_1)(1-\eta_c)V_X+1][\eta_c(1-\eta_1)V_X+1]}\}. \quad (11)$$

The secrecy capacity between Alice and Bob is

$$\begin{aligned}\Delta I &= I(A;B) - I(B;E) \\ &= \frac{1}{2}\log_2\{\frac{[(1-\eta_1)V_X+1](\eta_1\eta_m V_X+1)}{[(1-\eta_1)(1-\eta_c)V_X+1][(\eta_c+\eta_1\eta_m-\eta_1\eta_c)V_X+1]}\}\end{aligned} \quad (12)$$

Using Eq.(12), we will be able to find an optimal η_1 to maximize the secrecy capacity between Alice and Bob. The optimal η_1 and the corresponding secrecy capacity is plotted in Fig. 5, where we assume $\eta_m = 0.75, V_X = 100$ and the variance of quantum noise is normalized to 1. We also compared our result with the secrecy capacity of traditional CVQKD schemes.

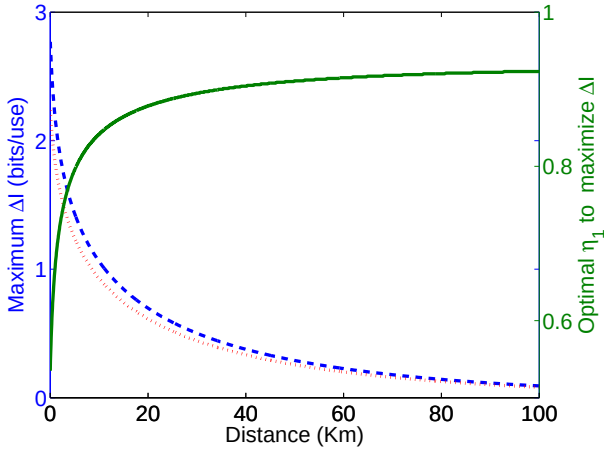


Figure 6: Optimal η_1 and the corresponding secrecy capacity. In the figure, the green curve denotes the optimal η_1 to maximize the secrecy capacity. The red curve corresponds to the secrecy capacity in our scheme and the blue curve is the secrecy capacity for traditional CVQKD schemes. ($\eta_m = 0.75$, $V_X = 100$, $V_{vac} = 1$)

¿From the figure, we can see that our secrecy capacity is lower than the secrecy capacity of traditional CVQKD schemes. This results from the fact that in our

scheme, Alice measures one quadrature of the quantum field. This measurement noise lowers the correlation between Alice and Bob's measurements. Traditional CVQKD schemes do not have this uncertainty on the transmitting side. Therefore, in traditional CVQKD schemes, Alice has a better estimation of Bob's measurement result and thus has larger mutual information with Bob. As consequence, the secrecy capacity drops when ASE instead of modulators is used for signal source. However, because the bandwidth of ASE is much larger than the bandwidth of modulators, the potential final secret key rate is also larger.

It is important to discuss how those general proofs[15, 17, 16, 19] on continuous variable QKD can be applied to our scheme. First of all, let's briefly review those security proofs on continuous variable QKD. Grosshans proved that continuous variable QKD is secure against non-gaussian attacks[15]. Navascués[17] deduced security bounds for continuous variable QKD based on a general result of the secure key rate by Christandl[18]. Grosshans then proved that continuous variable QKD is secure against collective attacks[16]. Finally, García-Patrón and Navascués proved the unconditional optimality of gaussian attacks against continuous variable QKD[19, 20]. In order to prove that our protocol inherits those security proofs, we should note that the maximal possible mutual information between Bob and Eve only depends on the energy inputting to the channel and the channel's quantum efficiency. Now let's assume that those previous results prove that for input energy E_c and quantum efficiency η_c is secure for the normal continuous variable QKD scheme. It implies that for E_c and η_c, we have $\Delta I > 0$ for Alice and Bob. In our scheme, we let the input energy to the channel and the channel efficiency remains the same as E_c and η_c. Therefore, the mutual information between Bob and Eve doesn't change. The only difference is that in traditional CVQKD schemes, Alice knows exactly the precise value of both quadratures but in our schemes, there remains some uncertainty for Alice to determine the average value of the quadrature. For traditional CVQKD schemes, we let

the average value for one quadrature to be X and The mutual information between Alice and Bob to be $I(X;B)$. For our scheme, the mutual information of Alice and Bob is $I(A;B)$. Apparently, $I(A;B) < I(X;B)$ always satisfies for arbitrarily signal variance and quantum efficiency of the channel. However, we can do the following manipulations. We can arbitrarily increase the variance of the output of ASE and change the transmission coefficient of Alice's beam splitter keep the input energy of the channel, e.g., the variance of the signal at the input side, $V_c = (1-\eta_1)V_X$ a constant. Then we can write Alice and Bob's correlation coefficient in the form of V_c,

$$\rho^2_{R_A R_B} = \frac{\eta V_c^2}{(V_c + \frac{1-\eta_1}{\eta_1 \eta_m})(\eta_c V_c + 1)}. \tag{13}$$

For traditional CVQKD schemes, the correlation coefficient is

$$\rho^2_{X R_B} = \frac{\eta_c V_c^2}{V_c(\eta_c V_c + 1)}. \tag{14}$$

We can plot the mutual information between Alice and Bob as a function of η_1 in Fig. 7,

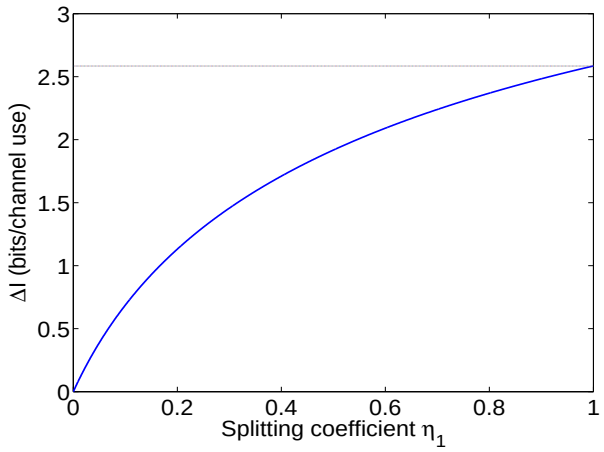


Figure 7: The mutual information between Alice and Bob as a function of η_1 ($\eta_m = 0.75$, $V_c = 10$, $V_{vac} = 1$). The blue curve is the mutual information between Alice and Bob in our scheme and the brown line is the mutual information between Alice and Bob in traditional CVQKD schemes.

It is very easy to check that when $\eta_1 \to 1$,i.e. When $V_X \to \infty$ we get

$$\lim_{V_X \to \infty} I(A;B) = I(X;B). \tag{15}$$

In other words, $\exists V_X$ and corresponding η_1 that make $\Delta I > 0$ for given E_c and η_c. Therefore, those secrecy results in previous work for continuous variable QKD can also applied to our scheme.

2.4 Experimental Issues

There are several issues that could happen in experiment need to be considered. The first issue is the fluctuation of polarization. The fluctuation of polarization can be compensated by polarization controllers that are placed before homodyne detectors. Since the fluctuation of polarization is not very rapid, what we need to do is adjust those polarization controllers to maximize the output of homodyne detectors when we start the experiment and make some periodically tiny calibration later.

Another issue is the fluctuation of phases. If the phase of the local oscillator doesn't accord with the phase of the signal beam, Alice and Bob will measure different quadratures and thus the mutual information between them will drop. However, since Eve can always measure the same quadrature as Bob, the fluctuation of phase actually doesn't decrease Eve's information on Bob's measurement result. As a result, the secrecy capacity between Alice and Bob drops as some phase fluctuation introducing into the system. Next we will give mathematical analysis on how the phase fluctuation influence the secrecy capacity of the system and compare our scheme with previous continuous variable QKD schemes.

Let the difference of the phase between the local oscillator and signal is $\delta\theta$. Since Eve always measures the same quadrature as Bob does, it is convenient to assume that Alice's local oscillator has a phase drift $\delta\theta$ from her signal beam. Then, Alice's measured random variable becomes

$$R'_A = \cos\delta\theta R_A + \sin\delta\theta(Y + R_Y), \tag{16}$$

where Y is random variable that denotes the quadrature orthogonal with X and R_Y

is the corresponding quantum noise. The correlation coefficient between Alice and Bob's measurement results is

$$\rho_{R'_A R_B} = \frac{\eta_1 \eta_c \eta_m (1-\eta_1) V_X^2 \cos^2 \delta\theta}{(\eta_1 \eta_m V_X \cos^2 \delta\theta + \eta_1 \eta_m V_Y \sin^2 \delta\theta + 1)[\eta_c (1-\eta_1) V_X + 1]} \tag{17}$$

Then we can find optimal secrecy capacity for different channel efficiency η_c. For traditional CVQKD schemes, the correlation coefficient between Alice and Bob's measurement results becomes

$$\rho'_{X R_B} = \frac{\eta_c \cos^2 \delta\theta V_c^2}{(V_X \cos^2 \delta\theta + V_Y \sin^2 \delta\theta)(\eta_c V_X + 1)}, \tag{18}$$

where $V_c = (1-\eta_1)V_X$ is the energy that Alice sends into the quantum channel. Then we can compare the two difference cases in Fig. 8.

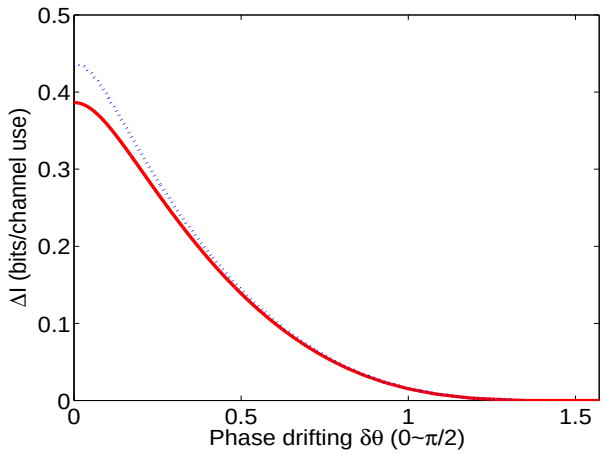


Figure 8: Comparison of the secrecy capacity between our scheme and traditional CVQKD schemes. The blue curve is for traditional CVQKD schemes and the red curve is for our scheme. We let $\eta_c = 0.5, V_X = V_Y = 100, \eta_m = 0.75$.

We can see that there are almost no differences in secrecy capacity for our scheme and traditional CVQKD schemes. In other words, as long as we can control the phase drift within $\pi/4$, we will be able to run the system at a relative low rate without any devices calibrating the phase. In this situation, the performance of our system is almost equivalent to traditional CVQKD schemes.

Finally, we briefly discuss the availability of fast detector in our system. As we have mentioned, the bandwidth of the signal source is very large in our scheme. In

order to improve the final key rate, we also have to increase the bandwidth of the detection subsystem. FPGAs can greatly improve the bandwidth of the detection circuit. Furthermore, some efficient reconciliation and privacy amplification algorithms are also available.

CHAPTER III

A QKD PROTOCOL BASED ON DISCRETELY SIGNALED CONTINUOUS VARIABLE QUANTUM KEY DISTRIBUTION

We propose a protocol for discretely signaled CVQKD that is designed for simple implementation with normal network hardware and with the goal of improving reconciliation speed. The protocol uses reverse reconciliation only and can optionally use post-selection. We prove security for collective attacks on a lossy, noisy channel. The novel contributions of this thesis are the combination of discrete signaling with tomography on a subset of data to restrict Eve's attacks, the use of novel analytical and computational techniques for calculating collective security with channel excess noise, and the level of attention that is paid to reconciliation speed in the design and analysis.

3.1 Previous work

Systems that measure arrivals of single photons are called discrete variable systems, while those that use homodyne or heterodyne detection to measure the continuous-valued electromagnetic field and are called continuous variable systems[12]. Discrete QKD is well developed in terms of security analyses, experiments, and commercial products. One important avenue of research for QKD systems seeks to improve rates. The counting rate limitations for non-cryogenic detectors are 15 MHz for Si photon counters and new greatly improved counter speed of approximately 100 MHz for InGaAs photon counters. These limits are due to dead times required to clear avalanche carriers, which produces spurious afterpulsing counts.

Unlike photon counters, homodyne and heterodyne detectors do not require dead times and thus continuous variable QKD (CVQKD) systems [13, 4, 14] are in principle scalable to standard telecom rates, such as 10 GHz. However, homodyne and heterodyne measurements see at minimum the presence of vacuum noise manifesting itsself as Gaussian distributed randomness with noise power that remains constant as signals attenuate with length. This limits the achievable secure link length to a smaller distance than is achievable for discrete QKD. Thus CVQKD may be preferable at short and medium distances.

One may divide CVQKD systems into those that use continuous signaling [4] and those that use discrete signaling[22]. Continuous signaling, where Alice sends 2 independent Gaussian distributed random variables in the x and y quadratures of the field, is the most studied because proofs against individual and collective attacks exist [16, 17, 19, 20]. These proofs exist because the Gaussian-distributed coherent states reach the channel capacity between Alice and Bob and also allow for quantification of Eve's knowledge. An individual attack describes manipulation of individual timeslots and optimal quantum measurement by Eve on light in that timeslot, while collective attacks describe manipulation of individual timeslots and optimal joint measurement of several or many timeslots. State-of-the-art continuously signaled experiments provide security against collective attacks, and demonstrate final key rate limited to 2 kB/sec [7]. This limitation is due not to the physical layer, but to the time required to implement reconciliation on a typical microprocessor. Attempts to increase speed have led to proposals for post-selection, and recently to a protocol that can be proved secure against collective attacks if infinite dimensional conditional homodyne tomography can be implemented on a subset of data[21]. It has been clear to many CVQKD researchers that a discretely signaled CVQKD protocol would be advantageous in terms of simplicity and several have been proposed. However, it has been pointed out that the security of discretely signaled systems under collective attacks

remains an open problem for the practical case of excess noise in the channel[6].

In order to increase distance, the technique of post-selection has been proposed for CVQKD [8, 9, 10, 11]. In post-selection schemes, only a subset of the data is used. By post-selection, Alice and Bob obtain a signal-to-noise ratio advantage over Eve. CVQKD experiments have been implemented using post-selection systems with post-selection[9, 10, 11], but without security proofs. Although Gaussian attacks have been proved to be optimal against continously signaled CVQKD systems, the optimal attack for post-selection based CVQKD protocols is unknown yet. The recent progress on the security analysis of post-selection [21] gave a proof of a post-selection protocol when there is excess gaussian noise introduced into the channel. The protocol presented in their paper requires full state conditional tomography. Therefore, theoretically an infinite number of tomographic measurements is to be made.

In order to permit faster and longer links, one needs to overcome the following obstacles. First, a very efficient reconciliation protocol is needed. Although theoretically, reverse reconciliation enables CVQKD links of infinite distance, as CVQKD link length increases, the minimum reconciliation efficiency required for positive secrecy capacity, β_0, approaches 1. This differs from discrete QKD. Second, reconciliation needs to be simple and fast. In order to correct errors between Alice and Bob, one usually seeks continuous variable based error correction codes to be as efficient as possible. However, highly efficient error correction codes are also slow. In addition, codes for binary symmetric channel are usually the simplest and fastest. By turning the continuous variable based error correction problem into a binary based error correction problem, several advantages come. First, it is easier to find corresponding error correction codes working at a rate very close to Shannon limit while keeping a lower decoding complexity. Furthermore, if the required error correction efficiency is lowered for a given distance, then we may be able to find a reconciliation code with corresponding lower efficiency but greater speed. As a result, the distance and

throughput of CVQKD systems would be greatly improved.

3.2 Description of the quantized input-quantized output CVQKD protocol

According the previous discussions, binary reconciliation is attractive in order to improve CVQKD distance and speed. In 2006, Namiki proposed a CVQKD scheme using discrete encoding and post-selection[22]. Although the protocol then results in binary reconciliation, the security analaysis was only developed for individual attacks. Second, the experimentally relevant case of excess noise in the channel was not treated. This case is important because system imperfections typically result in some additional noise present, which should be treated for security purposes as if Eve controls it. Third, for low channel efficiency, the possibility of selecting a quantum state is low enough that most of the measurements are discarded.

In order to obtain positive secrecy capacity, it is desirable that Alice and Bob nearly achieve the capacity of the channel given the signal-to-noise ratio. Recently, a new result of classical information theory [23] shows that for a lossy gaussian channel with given signal-to-noise ratio, when Bob quantizes the received data, the optimal way for Alice to encode data is to also send quantized data. Specifically, under the condition that Bob performs binary quantization, Alice needs only send binary data and achieve the channel capacity. This result is significant for reverse-reconciliation CVQKD because it indicates that if Bob quantizes the data received, then Alice doesn't need to send gaussian modulated signals but should send binary signals.

The quantized input-quantized output(QIQO) CVQKD protocol is described below:

Step 1: Alice randomly picks up a random variable $x_k \in \{1, 2, 3, 4\}$ and encodes a coherent state $|\varphi_{x_k}\rangle_k \in \{|\alpha_1\rangle = |r + ri\rangle, |\alpha_2\rangle = |r - ri\rangle, |\alpha_3\rangle = |-r + ri\rangle, |\alpha_4\rangle = |-r - ri\rangle\}$,where r is a positive real number depending on Bob's signal-to-noise ratio and k denotes the index of time slot, and sends it through a lossy and noisy quantum

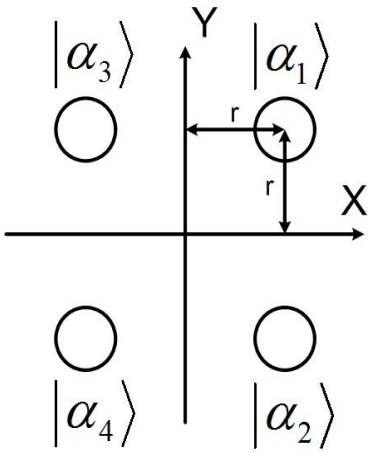


Figure 9: Alice's encoding scheme in which she only sends four different coherent states.

channel. Alice's encoding scheme can be described in Fig. 9.

Step 2 Bob receives a quantum state from the quantum channel. With probability p, each measurement is assigned to channel characterization, where Bob randomly chooses a local oscillator phase ϕ_k of 0, $\pi/4$ or $\pi/2$, makes a homodyne measurement and records the real result[27]. With probability $1-p$, that measurement is assigned a data collection index k, where Bob randomly chooses a local oscillator phase ϕ_k of 0 or $\pi/2$ before performing homodyne detection. If his measurement result is greater than T, where $T \geq 0$ is Bob's decision threshold, then he quantizes the result to $q_k = 1$. If Bob's measurement result is less than $-T$ otherwise, he quantizes the data to $q_k = -1$. For other cases where his measurement result is between $-T$ and T, Bob quantizes his data to $q_k = 0$. When $q_k = 0$, the data from the corresponding time slot won't be selected in the post classical processing. We note here that we have added post-selection into the protocol. When $T = 0$, it reduces to the case without post-selection.

To summarize these two steps, Alice uses random QPSK signaling but Bob's collected data are digitized BPSK.

Step 3: When all quantum communication has been finished, Bob reveals to

Alice which time slots that were used for characterization phase measurements. Alice reveals to Bob the state that she has sent for those time slots. Then Bob performs conditional quantum tomography for each one of the four particular coherent states that Alice sent. Only three different collection angles are required to achieve a good estimate of the received state[27]. We know that without Eve, the channel can be modeled as a beamsplitter with two inputs, one of which is Alice's output to the quantum channel and the other one is the excess channel noise mode.

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{\varepsilon}_n, \tag{19}$$

where $\hat{b}$ is the output of beamsplitter going to Bob's detectors. For any field quadrature of Bob, we have

$$\hat{Q}_b = \sqrt{\eta}\hat{Q}_a + \sqrt{1-\eta}\hat{Q}_{\varepsilon_n}. \tag{20}$$

Assume $p_b(q)$, $p_a(q)$ and $p_{\varepsilon_n}(q)$ are the possibility distributions of the three quadratures, we have

$$p_b(q) = p_a(\sqrt{\eta}q) * p_{\varepsilon_n}(\sqrt{1-\eta}q), \tag{21}$$

where * is a convolution. By Fourier transform techniques, we can simply get $p_\varepsilon(q)$ once we know $p_a(q)$ and got $p_b(q)$ from tomography. Therefore, we can also reconstruct $\hat{\rho}_{\varepsilon_n}$ based on quantum tomography on $\hat{\rho}_b$. For the protocol, Bob does quantum conditional tomography for all four cases. Then Bob can reconstruct $\hat{\rho}_{\varepsilon_n}$ for all four cases. The protocol requires that the reconstructed $\hat{\rho}_{\varepsilon_n}$ for all four cases to be the same. Otherwise, Alice and Bob abort the protocol.

Step 4: For each data collection time slot, Bob reveals the local oscillator phase that was chosen. If Bob used $\phi_k = 0$, then Alice records $a_k = 1$ for the case where $x_k = 0$ or $x_k = 1$ and $a_k = -1$ for the case where $x_k = 2$ or $x_k = 3$. If Bob used $\phi_k = \frac{1}{2}\pi$, then Alice records $a_k = 1$ for the case where $x_k = 0$ or $x_k = 2$ and $a_k = -1$ for the case where $x_k = 1$ or $x_k = 3$.

Step 5: Bob sends checkbits to Alice over a public channel, i.e. *reverse reconciliation*. The reconciliation is strictly one-way.

Step 6: Alice and Bob perform privacy amplification to distill the final secure key.

3.3 Security analysis

In this section, we analyze the security of the QIQO CVQKD protocol against collective attacks, where Eve interacts with incoming quantum states individually and makes joint multi-timeslot measurements after knowing Bob's measurement basis. The security of CV QKD systems can be guaranteed by fundamental limits of the noise coming from the quantum measurements. However, since the quantum channel can always introduce some excess noise, this amount of noise could potentially have been introduced by Eve, and may thus weaken the security of the system. We treat the excess channel noise rigorously. We divide this section into two subsections. In the first subsection, we analyze the simpler case where there is no excess channel noise but Bob's homodyne detector has a given quantum efficiency and Bob also has some additive gaussian electronic noise. We will give analytical solution for this case. In the second subsection, we analyze the case where channel excess noise is present.

For collective attacks, the secrecy capacity between Alice and Bob in bits per channel use is defined to be

$$\Delta I = I(A;B) - \chi(B;E), \tag{22}$$

where $I(A;B)$ is the mutual information between Alice and Bob. For the binary symmetric channel in our protocol, $I(A;B)$ can be completely determined by the signal-to-noise ratio of Bob. $I(A;B)$ can be calculated as Eq. 23 and Eq. 24,

$$e_{AB} = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\sqrt{SNR}} e^{-\frac{x^2}{2}} dx. \tag{23}$$

$$I(A;B) = 1 - h(e_{AB}), \tag{24}$$

where $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function.

$\chi(B;E)$ is the Holevo information between Bob and Eve, which is definined to be

$$\chi(B;E) = S(\hat{\rho}_E) - \sum_i p_i S(\hat{\rho}_{E|q=i}), \tag{25}$$

where $S(\hat{\rho}_E)$ is the von Neumann entropy of Eve's mixed state. $\hat{\rho}_{E|q=i}$ is Eve's mixed state given Bob's measurement result and p_i is the probability that Bob's measurement is i. For our binary symmetric case, we can rewrite $\chi(B;E)$ to be

$$\chi(B;E) = S(\hat{\rho}_E) - \frac{1}{2}S(\hat{\rho}_{E|q=-1}) - \frac{1}{2}S(\hat{\rho}_{E|q=1}) = S(\hat{\rho}_E) - S(\hat{\rho}_{E|q=1}) \tag{26}$$

3.3.1 Analytical solution for no excess channel noise case

When there is no excess channel noise, Bob's received state is a coherent state given Alice sent a particular quantum state. When the tomographic subset verifies Bob's received state, Eve's only possible attack is a beam splitter attack, where Eve replaces the lossy channel with a perfect one and uses a beam splitter to simulate the lossy effect of the channel. Suppose the quantum efficiency of the quantum channel is η, then Bob's received quantum states are $|\sqrt{\eta}\alpha_i\rangle$ and Eve's received quantum states are $|\sqrt{1-\eta}\alpha_i\rangle$. It is straight forward to give the expression for $\hat{\rho}_E$,

$$\hat{\rho}_E = \sum_{i=1}^{4} \frac{1}{4} |\sqrt{1-\eta}\alpha_i\rangle\langle\sqrt{1-\eta}\alpha_i|. \tag{27}$$

The second term of $\chi(B;E)$ relates directly to the error rate of the binary symmetric channel. Let's consider the case where Bob chose $\phi = 0$ as the phase for homodyne detection. Given Bob's quantized data $q = 1$, the possibility that Alice sent $|\alpha_1\rangle$, $|\alpha_2\rangle$, $|\alpha_3\rangle$ and $|\alpha_4\rangle$ are $p_{1|q=1} = \frac{1}{2}(1-e_{AB})$, $p_{2|q=1} = \frac{1}{2}e_{AB}$, $p_{3|q=1} = \frac{1}{2}(1-e_{AB})$ and $p_{4|q=1} = \frac{1}{2}e_{AB}$ respectively. Therefore, the second term of $\chi(B;E)$ is

$$\hat{\rho}_{E|q=1} = \sum_{i=1}^{4} p_{i|q=1} |\sqrt{\eta - 1}\alpha_i\rangle\langle\sqrt{\eta - 1}\alpha_i|. \tag{28}$$

The error rate e_{AB} is directly related to the signal-to-noise ratio of Bob. Suppose the vacuum variances of both quadratures are $\langle \Delta X^2 \rangle = \langle \Delta Y^2 \rangle = V_S = \frac{1}{4}$ and the variance of electronic noise is V_{el}, then variance of Bob's detection noise is

$$V_B = V_S + V_{el}. \tag{29}$$

The signal-to-noise ratio then reads,

$$SNR = \frac{u_i^2}{V_B}, \tag{30}$$

where $u_i = \Re\{\sqrt{\eta\eta_m}\alpha_i\}$ is Bob's average value of X quadrature when Alice sent α_i. η_m is the detection efficiency of the homodyne detector. Combining Eq. 29 and Eq. 30, we have

$$SNR = \frac{\Re^2\{\sqrt{\eta\eta_m}\alpha_i\}}{V_S + V_{el}}. \tag{31}$$

Together with Eq. 23, we calculate the error rate of the binary symmetric channel between Alice and Bob. Combining the above equations, we get the analytical expression for the secrecy capacity between Alice and Bob for the case where there is no excess noise.

3.3.2 Numerical simulation for the general case with excess channel noise

In the case where there some excess noise is introduced into the quantum channel, the analysis is more complicated. Here numerical simulations are required. We will prove that with small amounts of excess noise, the security of the QIQO CVQKD scheme can still be guaranteed.

3.3.2.1 Validity of channel model

We will show that Eve's optimal collective attack is the entangling beamsplitter attack (see Fig. 10), where Eve replaces the lossy fiber with a lossless channel and mixes one

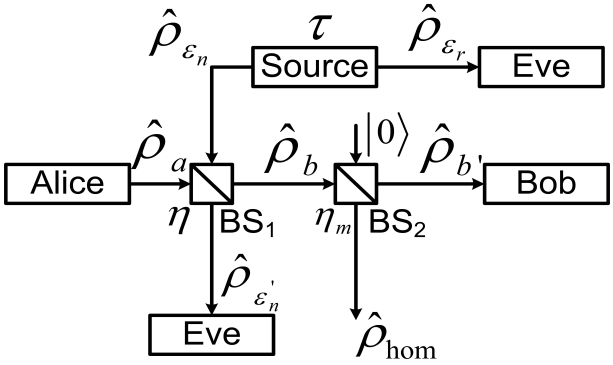


Figure 10: Model of the transmission channel. $\hat{\rho}_{\varepsilon_{\rm n}}$ and $\hat{\rho}_{\varepsilon_{\rm r}}$, density matrices produced by Eve's EPR source; $\hat{\rho}_{\rm a}$, density matrix of signal sent by Alice, $\hat{\rho}_{\rm b}$ and $\hat{\rho}_{\rm b'}$, density matrix before Bob's detector inefficiencies and that after detector inefficiencies. $\hat{\rho}_{\varepsilon_{\rm n'}}$, density matrix post-beamsplitter, measured by Eve, and $\hat{\rho}_{\rm hom}$ density matrix of equivalent mode consisting of light lost to detector inefficiencies. τ is the gain of EPR source, η is the channel efficiency, and $\eta_{\rm m}$ is Bob's detector efficiency.

of two entangled beams ($\hat{\rho}_{\varepsilon_n}$) on a beamsplitter while additionally monitoring one of the outputs ($\hat{\rho}_{\varepsilon_r}$). *Conditional* homodyne tomography serves to make the optimality of the entangled beamsplitter attack provable.

First of all, we need to note that Eve's attack is a unitary operator which maps the product state of Eve's original ancillary state and Alice's output state into the input state to Bob's detectors and final ancillary state. If the input ancillary state and Alice's output state are given, and the output states of the unitary operator are also given, then the unitary operator can be regarded as a black box. In this case, the internal structure of the black box doesn't matter because the secrecy capacity of the system is only a function of the output of the black box. In another word, only the output quantum state matters and how the state was generated doesn't matter. Eve's unitary operation can be denoted as

$$|\Phi_i\rangle = \hat{M}(|\Psi\rangle_E \otimes |\alpha_i\rangle), \tag{32}$$

where i denotes Alice's picked state and $|\Psi\rangle_E$ denotes Eve's original ancillary states. Then Bob's incoming density matrices are given by a trace over Eve's Hilbert space

$$\rho_{b_i} = Tr_E(|\Phi_i\rangle\langle\Phi_i|). \tag{33}$$

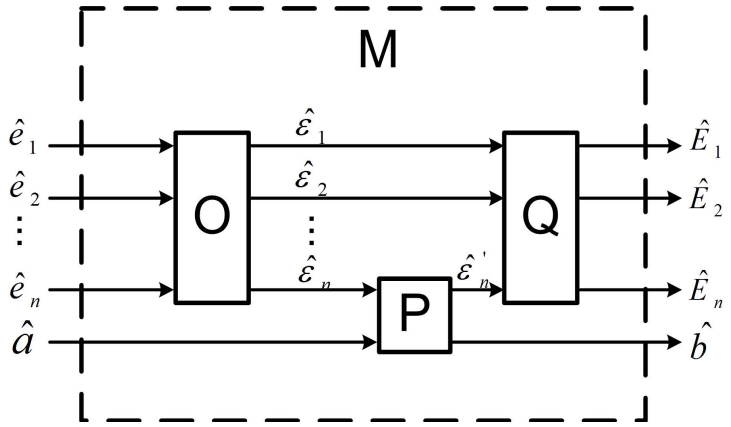


Figure 11: Any Eve's attack operator $\hat{M}$ can be decomposed into three sub-operators $\hat{O}$,$\hat{P}$ and $\hat{Q}$, which give the same output quantum states.

We know that ρ_{b_i} can be obtained by quantum conditional tomography and according to Eq.19, each $\hat{b}_i$ can be expresses as a superposition of Alice's mode and another excess noise mode, we can decompose $\hat{M}$ into three different unitary operators $\hat{O}$, $\hat{P}$ and $\hat{Q}$. $\hat{O}$ creates $\hat{\rho}_{\varepsilon_n}$ from Eve's original ancillary states

$$\hat{\rho}_{\varepsilon_n} = Tr_r[\hat{O}^\dagger(|\Psi\rangle_E\langle\Psi|)\hat{O}], \tag{34}$$

where Tr_r denotes the trace over the rest Eve's state beside ε_n. The role of operator $\hat{P}$ is to interact $\hat{\rho}_{\varepsilon_n}$ with $|\alpha_i\rangle$ on a beamsplitter to create ρ_{b_i}. $\hat{P}$ can be written as

$$\hat{P} = \begin{bmatrix} -\sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix}. \tag{35}$$

The role of $\hat{Q}$ is to map the final state back to $|\Phi_i\rangle$. We have

$$\hat{Q} = \hat{M}\hat{O}^\dagger\hat{P}^\dagger. \tag{36}$$

Since for all four cases, $\hat{M}$ and $\hat{O}$, $\hat{P}$, $\hat{Q}$ give the same output, the decomposition is therefore equivalent to the unitary operator $\hat{M}$. The idea of decomposition can be found in Fig.11.

We note here that the operator $\hat{Q}$ is a post-processing on Eve's states. According to quantum data processing theorem[24], this operation doesn't increase Eve's accessible information. Therefore, we can safely only consider the system without $\hat{Q}$ since

$\hat{Q}$ can only decrease Eve's accessible information. In anther word, considering ρ_{ε_r} and $\rho_{\varepsilon'_n}$ is enough for calculating Eve's accessible information.

3.3.2.2 Mathematical description of the channel model

As an example, we calculate an representative case where the excess channel noise is thermal. If the channel noise is not thermal, as long as we reconstruct ρ_{ε_n}, we still can use the same method to calculate the secrecy capacity. In Fig.10, $\hat{\rho}_{\varepsilon_n}$ is Eve's input mode to the operator $\hat{P}$. Whatever Bob's state, he can infer Eve's input mode because he also knows Alice's sent state. Mathematically, $\hat{\rho}_{\varepsilon_n}$ can be written as,

$$\hat{\rho}_{\varepsilon_n} = (1-\tau^2)\sum_{n=0}^{\infty}\tau^{2n}|n\rangle\langle n|. \tag{37}$$

In the Schroedinger picture, let's assume Eve's State is a pure state $|\Psi\rangle_{\varepsilon_n,\varepsilon_r}$, where the subscript ε_r denotes the rest of the system modes besides ε_n. One should note that although the notation here implies that Eve is using a two mode state, Eve is not actually limited to a two mode state. The quantum tomography only guarantees that the input mode ε_n to the beamsplitter be a thermal state. Subscript ε_r denotes Eve's arbitrary number of modes, that remain besides ε_n. Since Eve's entire quantum state is pure, the condition in Eq. 38 must satisfy,

$$\hat{\rho}_{\varepsilon_n} = \mathrm{Tr}_{\varepsilon_r}(|\Psi\rangle_{\varepsilon_n,\varepsilon_r}\langle\Psi|), \tag{38}$$

Without loss of generality, one can assume $|\Psi\rangle_{\varepsilon_n,\varepsilon_r}$ has the form in Eq. 39,

$$|\Psi\rangle_{\varepsilon_n,\varepsilon_r} = \sqrt{1-\tau^2}\sum_{n=0}^{\infty}\tau^n|n\rangle_{\varepsilon_n}|\phi(n)\rangle_{\varepsilon_r}, \tag{39}$$

where $\langle\phi(n)|\phi(n')\rangle = \delta_{n,n'}$.

Similar to other security proofs of CVQKD schemes, we make use of an entanglement based picture. We assume Alice also has a entanglement source that generates the quantum state in Eq. 40,

$$|\psi\rangle_A = \sum_{i=1}^{4} \frac{1}{2} |\alpha_i\rangle_a |i\rangle_{a'}, \tag{40}$$

which is a two mode state. In mode a', the state is expressed in the Fock basis and in mode a the state is expressed in the coherent basis. Alice then makes a photon number counting measurement on mode a', which projects the state of mode a into one of the four coherent states, i.e., $\hat{\rho}_a = \mathrm{Tr}_{a'}({}_A|\psi\rangle_{a,a'}\langle\psi|_A) = \sum_{i=1}^{4} \frac{1}{4} |\alpha_i\rangle_a\langle\alpha_i|$, which corresponds to the case where Alice randomly chooses one of the four coherent states and sends it through the quantum channel. The quantum state of the entire system becomes

$$|\Phi\rangle = \hat{B}_{b,hom}(\eta_m)\hat{B}_{a,\varepsilon_n}(\eta)|\psi\rangle_A|\Psi\rangle_{\varepsilon_n,\varepsilon_r}|0\rangle_{hom}, \tag{41}$$

where $\hat{B}_{b,hom}(\eta_m)$ and $\hat{B}_{a,\varepsilon_n}(\eta)$ denote the unitary operator of BS_1 and BS_2.

Bob then makes a homodyne measurement on mode b'. Each measurement results, by the state reduction postulate of quantum mechanics, in the rest of the system is collapsing into a pure quantum state. Suppose Bob's homodyne measurement results in a real-valued number X, then the system collapses into the state

$$|\Xi^X\rangle = \frac{{}_{b'}\langle X|\Phi\rangle}{\sqrt{\langle\Phi|X\rangle_{b'}\langle X|\Phi\rangle}}, \tag{42}$$

Tracing over Alice's mode a' and the *hom* mode, one obtains Eve's density matrix given the measurement result X,

$$\hat{\rho}_E^X = \mathrm{Tr}_{a',hom}(|\Xi^X\rangle\langle\Xi^X|). \tag{43}$$

The probability that $\hat{\rho}_E^X$ is generated is

$$p(\hat{\rho}_E^X) = \langle\Phi|X\rangle_{b'}\langle X|\Phi\rangle. \tag{44}$$

Eve's density matrix $\hat{\rho}_E$ is then of the form Eq. 45,

$$\hat{\rho}_E = \int p(\hat{\rho}_E^X)\hat{\rho}_E^X dx \tag{45}$$

Experimental homodyne measurements result in classical electronic noise, resulting in a real value measurement $r_B = X + N_{el}$ that is the sum of X, from the homodyne measurement, and N_{el}, which is a Gaussian distributed random variable denoting the electronic noise. *Without* post-selection, the protocol requires that Bob quantize r_B according to its sign. If $r_B > 0$ Bob sets $q = 1$, otherwise, Bob sets $q = -1$. We are interested in the conditional density matrix of Eve given Bob's quantization result. Without loss of generality, we only analyze the case in which $q = 1$.

Because the system begins in a pure state, Eve's density matrix becomes a function of Bob's homodyne measurement result X. However, Bob's quantization result not only depends on X, but also depends on N_{el}, which is independent of X. We can always regard Eve's conditional density matrix as a superposition of different $\hat{\rho}_E^X$ with different probability $p(\hat{\rho}_E^X|q = 1)$. Therefore, Eve's conditional density matrix can be written as Eq.46,

$$\hat{\rho}_{E|q=1} = \int p(\hat{\rho}_E^X|q = 1)\hat{\rho}_E^X dx. \tag{46}$$

We are now interested in $p(\hat{\rho}_E^X|q = 1)$. According Bayes' theorem,

$$p(\hat{\rho}_E^X|q = 1) = \frac{p(\hat{\rho}_E^X)p(q = 1|\hat{\rho}_E^X)}{p(q = 1)}. \tag{47}$$

We have the expression for $p(\hat{\rho}_E^X)$ from Eq. 44 and because of Alice's symmetric signaling, we have $p(q = 1) = \frac{1}{2}$. $p(q = 1|\hat{\rho}_E^X)$ also depends on V_{el}, which is the variance of the electronic noise.

$$p(q = 1|\hat{\rho}_E^X) = \frac{1}{\sqrt{2\pi V_{el}}} \int_{-\infty}^{X} \exp(-\frac{x^2}{2V_{el}})dx. \tag{48}$$

Next we deduce e_{AB}. According to Eq. 23, in order to obtain e_{AB}, we have to calculate the signal-to-noise ratio of Bob. When the quantum channel is introduced with some excess thermal noise, Bob's noise is actually made up of three different parts. The first part is the vacuum noise, whose variance is always $\frac{1}{4}$. The second part is the electronic noise, whose variance is V_{el}. And the third part is the thermal

noise. The variance of the thermal noise depends on τ, which is the squeezing factor of Eve's EPR source, and η, which is the quantum efficiency of the channel. Let the average thermal photon number be $\langle n_{th} \rangle$. We have

$$\langle n_{th} \rangle = (1 - \tau^2) \sum_{n=0}^{\infty} n\tau^{2n} = \frac{\tau^2}{1 - \tau^2}. \tag{49}$$

Then Bob's noise variance reads

$$V_B = V_S + \frac{1}{2}(1 - \eta)\eta_m \langle n_{th} \rangle + V_{el}. \tag{50}$$

Using Eq. 50 and Eq. 30, we can get the expression for signal-to-noise ratio for the case with excess noise, which is

$$SNR = \frac{\Re^2\{\sqrt{\eta\eta_m}\alpha_i\}}{V_S + \frac{1}{2}(1 - \eta)\eta_m \frac{\tau^2}{1-\tau^2} + V_{el}}. \tag{51}$$

3.3.3 QIQO CVQKD with post-selection

As discussed in the Section 1, the practical limitation on the key generation rate of CVQKD systems is computational time for reconciliation. Treating the channel as if it were symmetric binary channel for reconciliation purposes, the complexity of error correction codes used in reconciliation decreases. Suppose that for a given code, the code length is N and the code rate is $R = (1 - \varepsilon)C$, where C is the channel capacity, in this case decoding time complexity is function of ε and N. Typically, it grows polynomially with N. It has also been conjectured in [25] that per-bit complexity of message-passing decoding of LDPC code over any "typical" channel, such as binary erasure channel or binary symmetric channel, is $O(\log \frac{1}{\pi}) + O(\frac{1}{\varepsilon} \log \frac{1}{\varepsilon})$, where π is the decoding error rate. So the closer the code approaches the Shannon limit, the more complex the code. In other word, the requirement of high β_0 leads to very complex codes. Even so, the decoding error probability drops only polynomially with code length for LDPC codes, so that this requires even more time complexity to reduce the block error rate to suitable levels.

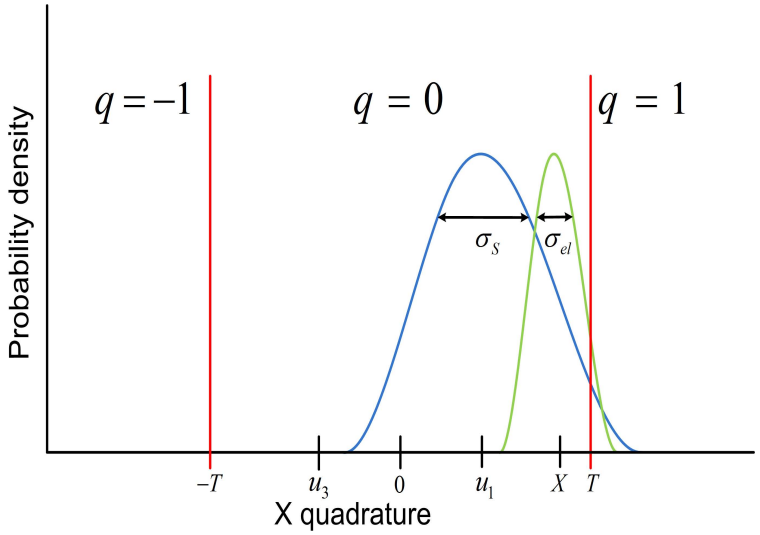


Figure 12: Bob's decision rule under post-selection. Here $\sigma_S = \sqrt{V_S}$ and $\sigma_{el} = \sqrt{V_{el}}$.

For the proposed QIQO CVQKD scheme, in order to have positive secrecy capacity, Bob's signal-to-noise ratio must be very low, i.e., around 0.5, which causes e_{AB} to be very high, i.e., around 25%. In order to fit the error rate to the requirements of those good codes, we need to modify e_{AB} while also changing β_0 little. Post-selection satisfies these requirements.

Bob's final measurement result is $r_B = X + N_{el}$ when electronic noise is included. According to the proposed protocol, when $r_B > 0$, Bob quantizes it into $q = 1$, otherwise Bob quantizes it into $q = -1$. With post-selection, we set a threshold $T > 0$. Bob's quantization rule is modified as follows: for the case $r_B > T$, he quantizes $q = 1$, for the case $-T \leq r_B \leq T$, he sets $q = 0$ and for the case $r_B < -T$, he sets $q = -1$. Finally, Alice and Bob discard data where $q = 0$ and only make error correction on those data where $q \neq 0$. Bob's decision rule for post-selection can be visualized in Fig. 12:

In order to get the expression for $\hat{\rho}_E$ under post-selection, we need to reevaluate the probability of each $\hat{\rho}_E^X$. We denote the new possibility as $p(\hat{\rho}_E^X | q \neq 0)$. Using

Bayes' theorem, it is rewritten to be

$$p(\hat{\rho}_E^X|q\neq 0)=\frac{p(q\neq 0|\hat{\rho}_E^X)p(\hat{\rho}_E^X)}{p(q\neq 0)} \tag{52}$$

The first term of the numerator can be expanded as

$$p(q\neq 0|\hat{\rho}_E^X)=\frac{1}{\sqrt{2\pi V_{el}}}[\int_{-\infty}^{-(T-X)}\exp(-\frac{x^2}{2V_{el}})+\int_{-\infty}^{-(T+X)}\exp(-\frac{x^2}{2V_{el}})]. \tag{53}$$

The second term of the numerator can be had from Eq. 44. The denominator is the probability of selecting a result. It directly relates to the amplitude of the signal u_i, the variance of noise V_B and the T, and can be written as:

$$p(q\neq 0)=\frac{1}{\sqrt{2\pi V_B}}[\int_{-\infty}^{-(T-u_i)}\exp(-\frac{x^2}{2V_B})+\int_{-\infty}^{-(T+u_i)}\exp(-\frac{x^2}{2V_B})]. \tag{54}$$

$\hat{\rho}_E^X$ can be therefore written as

$$\hat{\rho}_E^X=\int p(\hat{\rho}_E^X|q\neq 0)\hat{\rho}_E^X dx. \tag{55}$$

One must next calculate $p(\hat{\rho}_E^X|q=1)$. According to Eq. 47, several terms must be calculated. The first term on the numerator is exactly the same as Eq. 44. The second term of the numerator can be expanded to

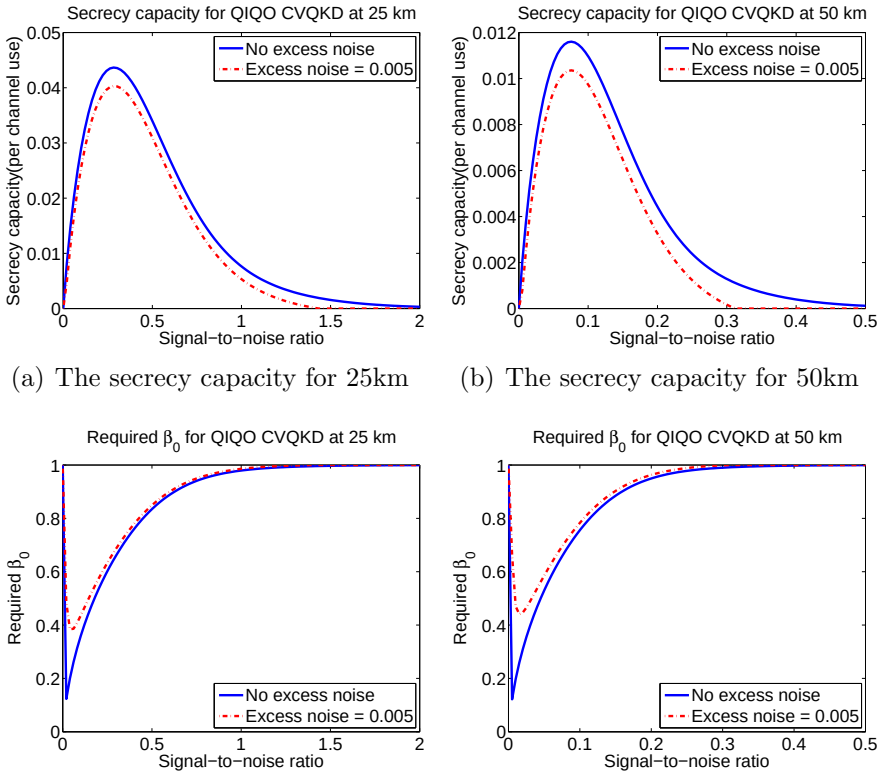
$$p(q=1|\hat{\rho}_E^X)=\frac{1}{\sqrt{2\pi V_{el}}}\int_{-\infty}^{-(T-X)}\exp(-\frac{x^2}{2V_{el}})dx. \tag{56}$$

Having obtained the preceding probabilities, we get $\chi(B;E)$ according to Eq. 26.

Finally, we calculate e_{AB} for post-selection. The symmetry of the states implies that the error rate is the same. So for simplicity, we only calculate the error rate when Alice encodes $|\alpha_1\rangle$. We obtain:

$$e_{AB}=\frac{p(q=-1|\text{Alice encodes}|\alpha_1\rangle)}{p(q\neq 0)}=\frac{\int_{-\infty}^{-(T+u_i)}\exp(-\frac{x^2}{2V_B})}{\int_{-\infty}^{-(T-u_i)}\exp(-\frac{x^2}{2V_B})+\int_{-\infty}^{-(T+u_i)}\exp(-\frac{x^2}{2V_B})}. \tag{57}$$

The secrecy capacity for post-selection is obtained straightforwardly. We present numerical simulation results and compare them to the case without post-selection in Fig. 14.



(a) The secrecy capacity for 25km

(b) The secrecy capacity for 50km

(c) The required reconciliation efficiency β_0 for 25km

(d) The required reconciliation efficiency β_0 for 50km

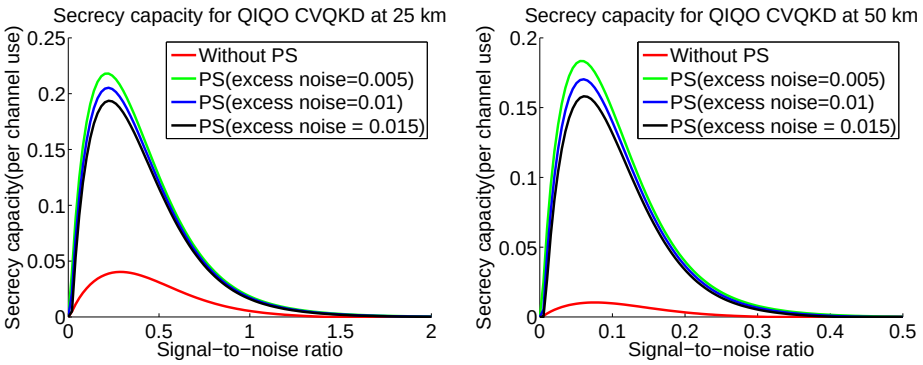
Figure 13: The secrecy capacity and required reconciliation efficiency for the system without post-selection.

We note that the post-selection we have proposed does not require high rate multi-bit A/D conversion. It requires only a hard threshold decision. For the case where $T = 1$, almost 10% of the data is selected. Therefore, if the clock rate is high enough, post-selection will not be the factor that limits the system.

3.4 Discussion of results

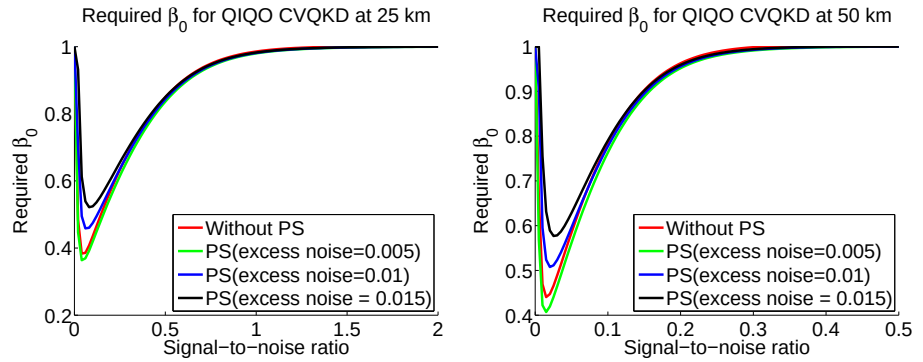
In this section, we discuss results. The numerical simulation gives the results in Fig. 13.

Several observations are in order. First, as expected, it is clear that excess noise reduces secrecy capacity and lowers β_0. This is as expected because we assumed that Eve could make use of the excess noise and thus achieve higher mutual information



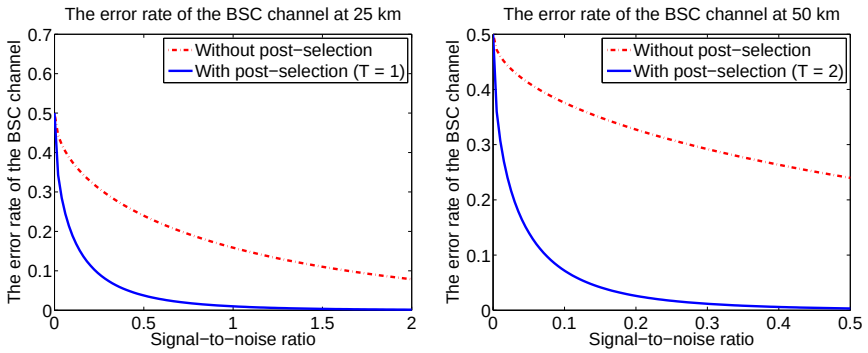
(a) The secrecy capacity of the system with post-selection at 25km

(b) The secrecy capacity of the system with post-selection at 50km



(c) The required β_0 for the system with post-selection at 25km

(d) The required β_0 for the system with post-selection at 50km



(e) The error rate of the BSC channel at 25km

(f) The error rate of the BSC channel at 50km

Figure 14: The secrecy capacity, required reconciliation efficiency and the error rate on the BSC channel of the system with post-selection

with Bob. Secondly, it is also clear why β_0 increases with increasing signal-to-noise ratio. This is because at higher SNRs, the signal amplitude increases, which leads Eve to better discrimination between the four states sent by Eve. In order to take advantage of coding, we require a relatively low β_0 and thus we require error correcting codes that work at low SNR. However, at low SNR, the error probability of the binary symmetric channel increases. As discussed in the previous section, very good codes have been found for binary symmetric channels but they are very sensitive to the error probability of the channel. In order to make those codes applicable to our case, we use post-selection on Bob's received data so that the secrecy capacity (per retained bit) between Alice and Bob goes up dramatically, the error probability (per retained bit) drops dramatically, while the required β_0 remains almost constant. For $25km$ QIQO CVQKD, a threshold of $T = 1$ is set for post-selection. This leads to postselection of 10% of Bob's data. For $50km$ QIQO CVQKD, a threshold $T = 2$ leads to retention of about 1% of Bob's data. For example, with a broadband source with a symbol rate of 10GS/sec, the retained 1 GS/sec and 100 MS/sec for $25km$ and $50km$ QIQO CVQKD respectively. Therefore, the post-selection would not limit the clock rate of the system. For $25km$ QIQO CVQKD with post-selection, the ideal working region is at a signal-to-noise ratio about 0.25, where the secrecy capacity is 0.2bit/channel use, the error probability is less than 10% and the required β_0 is about 60%. For $50km$ QIQO CVQKD, the ideal working region is at signal-to-noise ratio about 0.15, where the secrecy capacity is 0.15bit/channel use, the error probability is less than 10% and the required β_0 is about 75%.

We have also made initial simulations on a simple error correction code and compared the results to previous CVQKD experiments based on post-selection. For 25km QKD, after the post-selection process, we have an error rate about 7% on the BSC channel. We then use a standard unoptimized LDPC code that corrects all the errors. Running on a Mac laptop, we were able to decode at a processing rate of 600

kbps at an reconciliation efficiency of $\beta = 80\%$. The secrecy key rate per channel use when we take the inefficiency of the error correction code into account is $\Delta I = \beta I(A;B) - \chi(B;E) = 0.1$ at 25km at signal-to-noise ratio 0.45. This results after privacy amplification in a final key rate of 60 kbps at 25km with channel loss 70%. This provides a speed-up by a factor of 25 over the existing experiment that uses a protocol secure against collective attacks.

Recently, we have become aware of a security analysis on binary modulated CVQKD system has been posted[26] after we presented most of these results[30]. That protocol uses two-state modulation instead of four-state modulation. It does not require quantum tomography. Instead, inequalities and maximum eigenvalues are found to get a upper bound for Eve. The inequalities result in an upper bound less tight than that found in this paper, which makes that protocol more sensitive to channel excess noise. We also compare out result with [11], which is limited to 50km with no excess noise. but our scheme can go more than 50km with excess noise and still has high secrecy capacity.

3.5 Numerical simulation techniques

It is difficult to obtain analytical solutions for continuous variable quantum state, because it has infinite dimension. Unlike those protocols based on gaussian modulation of signal, discrete modulation only gives *conditional* gaussian states instead of global gaussian states. If the global state, such as $\hat{\rho}_E$, is not Gaussian, it's difficult to find a analytical solution for von Neumann entropy when there excess noise is introduced into the channel. Fortunately, as long as the amount of excess noise is small, it's still possible to get numerical solutions.

¿From Eq. 39, one may see that if Eve's two mode quantum state is expanded into Fock spaces, there would be infinite number of terms. But one may truncate the state into finite number of terms since when τ is small, the amplitudes for large

photon numbers are so small that those terms are negligible. For this simulation, we have the excess noise about 0.005 of one shot noise unit and this leads to $\tau = 0.033$ for $25km$ and $\tau = 0.0167$ for $50km$. Using only the first three terms of the expansion is then justified. In other words, the terms up to 2 photons are preserved. We let $EMAX = 2$ denoting the maximal number of photons.

Now we can approximate Eve's two mode state using the form in Eq. 58:

$$|\Psi\rangle_{\varepsilon_n,\varepsilon_r} = \sqrt{1-\tau^2}\sum_{n=0}^{EMAX}\tau^n|n\rangle_{\varepsilon_n}|\phi(n)\rangle_{\varepsilon_r}. \tag{58}$$

Then mode ε_n is interacted with mode a. However, since the quantum state in mode ε_n is represented in Fock space, it needs to be transformed into coherent form so that the operation of BS_1 is performed on two coherent states and the outcome of the operation is also coherent states. Here we use another approximation where $|n\rangle$ is represented as the superposition of $n+1$ coherent states[28].

$$|n,r\rangle = c(r)\frac{\sqrt{n!}e^{\frac{r^2}{2}}}{(n+1)r^n}\sum_{k=0}^{n}e^{\frac{2\pi i}{n+1}k}|re^{\frac{2\pi i}{n+1}k}\rangle, \tag{59}$$

where $c(r)$ is used to normalize $|n,r\rangle$. We have

$$|n,r\to 0\rangle = |n\rangle. \tag{60}$$

The accuracy of the approximation is

$$1-|c_n|^2 = \frac{n!}{(2n+1)!}r^{2(n+1)} + o(r^{4(n+1)}), \tag{61}$$

where $|c_n|^2$ is the probability amplitude of $|n\rangle$ in $|n,r\rangle$. In practice, we set $r=0$ for $|0\rangle$ and $r=0.1$ for other Fock states.

Thus, we write $|\Phi\rangle$ in Eq. 62,

$$\begin{aligned}|\Phi\rangle = c(r)\sqrt{1-\tau^2}\sum_{j=1}^{4}\frac{1}{2}|j\rangle_{a'}\sum_{n=0}^{EMAX}\tau^n|n\rangle_{\varepsilon_r}\frac{\sqrt{n!}e^{\frac{(r_n)^2}{2}}}{(n+1)(r_n)^n}\\ \sum_{k=0}^{n}e^{\frac{2\pi ik}{n+1}}|\sqrt{\eta_m}(\sqrt{\eta}\alpha_j+\sqrt{1-\eta}r_ne^{\frac{2\pi ik}{n+1}})\rangle_{b'}\\ |\sqrt{1-\eta_m}(\sqrt{\eta}\alpha_j+\sqrt{1-\eta}r_ne^{\frac{2\pi ik}{n+1}})\rangle_{hom}|\sqrt{1-\eta}\alpha_j-\sqrt{\eta}r_ne^{\frac{2\pi ik}{n+1}}\rangle_{\varepsilon_n'}.\end{aligned} \tag{62}$$

We first trace over a' mode to get the density matrix of mode b', ε'_n, ε_r and hom.

$$\hat{\rho}_{b',\varepsilon'_n,\varepsilon_r,hom} = \mathrm{Tr}_{a'}(|\Phi\rangle\langle\Phi|) = \sum_{i=1}^{4} \frac{1}{4}|\Omega_i\rangle\langle\Omega_i|, \tag{63}$$

i.e., the density matrix for mode b', ε'_n, ε_r and hom is made up of 4 different pure states $|\Omega_i\rangle$ depending Alice's measurement of the photon counting on mode a'. This exactly corresponds to the case in which Alice prepares one of the four coherent states and sends it to Bob. For each of the $|\Omega_i\rangle$, Bob then make a homodyne measurement on his mode b'. As have been discussed, the outcome of the homodyne measurement is a gaussian distributed continuous random variable with average value $u_i = \Re(\sqrt{\eta\eta_m}\alpha_i)$ and variance V_S. Physically, for each of the $|\Omega_i\rangle$, Bob's measurement outcome has infinite possibilities. However, only those values distributed close to u_i occur with high possibility. As an approximation, out simulation only takes the value in the range of $[u_i - 6\sqrt{V_S}, u_i + 6\sqrt{V_S}]$. Another approximation is that instead of processing the continuous data in the range $[u_i - 6\sqrt{V_S}, u_i + 6\sqrt{V_S}]$, we divided it into $XMAX$ bins with equal widths and made un approximation that Bob's measurement only has $XMAX$ different possibilities instead of infinite possibilities. Suppose each bin has left bound $lb_{i,k}$ and right bound $rb_{i,k}$, with $1 \le k \le XMAX$. Then the measurement result is $X_{i,k} = (lb_{i,k} + rb_{i,k})/2$ with possibility $p(X_{i,k}) = \frac{1}{\sqrt{2\pi V_S}} \int_{lb_{i,k}}^{rb_{i,k}} \exp(-\frac{(x-u_i)^2}{2V_S})dx$. The density matrix for mode ε'_n, ε_r and hom can be approximately written as

$$\begin{aligned}
\hat{\rho}_{\varepsilon'_n,\varepsilon_r,hom} &= \mathrm{Tr}'_b(\hat{\rho}_{b',\varepsilon'_n,\varepsilon_r,hom}) = \sum_{i=1}^{4} \frac{1}{4} \sum_{k=1}^{XMAX} p(X_{i,k}) \frac{\langle X_{i,k}|\Omega_i\rangle\langle\Omega_i|X_{i,k}\rangle}{\langle\Omega_i|X_{i,k}\rangle\langle X_{i,k}|\Omega_i\rangle} \\
&= \sum_{i=1}^{4} \frac{1}{4} \sum_{k=1}^{XMAX} p(X_{i,k})|\psi_{i,k}\rangle\langle\psi_{i,k}|,
\end{aligned} \tag{64}$$

where $|\psi_{i,k}\rangle = \frac{\langle X_{i,k}|\Omega_i\rangle}{\sqrt{\langle\Omega_i|X_{i,k}\rangle\langle X_{i,k}|\Omega_i\rangle}}$. In order get $\hat{\rho}_E$, we further trace $|\psi^{i,k}\rangle\langle\psi^{i,k}|$ over mode hom. For low signal-to-noise ratio, the average photon number in mode hom is also low. If we use Fock basis to expand mode hom, we can neglect those quantum states with large photon numbers. Suppose we can present mode hom in Fock space

and only keep the states up to $HMAX$ photons. Then

$$\mathrm{Tr}_{hom}(\hat{\rho}^{i,k}_{\varepsilon'_n,\varepsilon_r,hom}) = \sum_{j=0}^{HMAX} {}_{hom}\langle j|\psi_{i,k}\rangle\langle\psi_{i,k}|j\rangle_{hom}. \tag{65}$$

Therefore, $\hat{\rho}_E$ can be written as

$$\begin{aligned}\hat{\rho}_E &= \sum_{i=1}^{4}\frac{1}{4}\sum_{k=1}^{XMAX} p(X_{i,k}) \sum_{j=0}^{HMAX} \langle j|\psi_{i,k}\rangle\langle\psi_{i,k}|j\rangle \\ &= \sum_{i=1}^{4}\frac{1}{4}\sum_{k=1}^{XMAX} p(X_{i,k}) \sum_{j=0}^{HMAX} p(j|X_{i,k})|\epsilon_{i,j,k}\rangle\langle\epsilon_{i,j,k}|,\end{aligned} \tag{66}$$

where $|\epsilon_{i,j,k}\rangle = \frac{\langle j|\psi_{i,k}\rangle}{\sqrt{\langle\psi_{i,k}|j\rangle\langle j|\psi_{i,k}\rangle}}$ and $p(j|X_{i,k}) = \langle\psi_{i,k}|j\rangle\langle j|\psi_{i,k}\rangle$. Here we ignored the subscript for $|j\rangle_{hom}$. We define a global possibility $p(|\epsilon_{i,j,k}\rangle) = \frac{1}{4}p(X_{i,k})p(j|X_{i,k})$, then we can rewrite $\hat{\rho}_E$ in the Eq. 67

$$\hat{\rho}_E = \sum_{i,j,k} p(|\epsilon_{i,j,k}\rangle)|\epsilon_{i,j,k}\rangle\langle\epsilon_{i,j,k}|, \tag{67}$$

where we omitted the subscript E used to describe the mode. The problem of calculating the von Neumann entropy $S(\hat{\rho}_E)$ is equivalent to solving the eigenvalue of the corresponding Gram matrix[29]. Each element of the Gram matrix is

$$G_{ijk,i'j'k'} = \sqrt{p(|\epsilon_{i,j,k}\rangle)p(|\epsilon_{i',j',k'}\rangle)}\langle\epsilon_{i,j,k}|\epsilon_{i',j',k'}\rangle. \tag{68}$$

The non-zero eigenvalues of G are equivalent to the non-zero eigenvalues of $\hat{\rho}_E$. Suppose the non-zero eigenvalues of G are $\{\lambda_1, \lambda_2, ..., \lambda_n\}$, then

$$S(\hat{\rho}_E) = \sum_{i=1}^{n} -\lambda_i \log_2(\lambda_i). \tag{69}$$

The next thing that we are interested in is $p(|\epsilon_{i,j,k}\rangle|q=1)$ for calculating $S(\hat{\rho}_{E|q=1})$. We first rewrite $p(|\epsilon_{i,j,k}\rangle|q=1)$ according to Bayes' theorem,

$$p(|\epsilon_{i,j,k}\rangle|q=1) = \frac{p(q=1||\epsilon_{i,j,k}\rangle)p(|\epsilon_{i,j,k}\rangle)}{p(q=1)}. \tag{70}$$

What we need to calculate is just the first term of the nominator. This was calculated as follows:

$$p(q=1||\epsilon_{i,j,k}\rangle) = \frac{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp[-\frac{(x-u_i)^2}{2V_S}]\frac{1}{\sqrt{2\pi V_{el}}}\int_0^{\infty}\exp[-\frac{(y-x)^2}{2V_{el}}]dydx}{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}}\exp[-\frac{(x-u_i)^2}{2V_S}]dx}. \tag{71}$$

$\hat{\rho}_{E|q=1} = \sum_{i,j,k} p(|\epsilon_{i,j,k}\rangle|q=1)|\epsilon_{i,j,k}\rangle$ we can calculate $S(\hat{\rho}_{E|q=1})$ following the Gram matrix that we have discussed above.

For the post-selection case, we need to calculate $p(|\epsilon_{i,j,k}\rangle|q \neq 0)$. As what we've done above, we first rewrite it according to the Bayes' theorem.

$$p(|\epsilon_{i,j,k}\rangle|q \neq 0) = \frac{p(q \neq 0||\epsilon_{i,j,k}\rangle)p(|\epsilon_{i,j,k}\rangle)}{p(q \neq 0)}. \tag{72}$$

What we need to calculate is just the first term of the nominator. The method that we used to calculate this term is

$$p(q \neq 0||\epsilon_{i,j,k}\rangle) = \frac{\frac{1}{\sqrt{2\pi V_S}} \int_{lb_{i,k}}^{rb_{i,k}} \exp[-\frac{(x-u_i)^2}{2V_S}] \frac{1}{\sqrt{2\pi V_{el}}} (\int_{-\infty}^{-T} \exp[-\frac{(y-x)^2}{2V_{el}}] + \int_{T}^{\infty} \exp[-\frac{(y-x)^2}{2V_{el}}]) dydx}{\frac{1}{\sqrt{2\pi V_S}} \int_{lb_{i,k}}^{rb_{i,k}} \exp[-\frac{(x-u_i)^2}{2V_S}] dx}. \tag{73}$$

Then $\hat{\rho}_E = \sum_{i,j,k} p(|\epsilon_{i,j,k}\rangle|q \neq 0)|\epsilon_{i,j,k}\rangle$. We can then use the Gram matrix to calculate $S(\hat{\rho}_E)$.

In order to calculate $S(\hat{\rho}_{E|q=1})$ in the case with post-selection, we need to calculate the possibility $p(|\epsilon_{i,j,k}\rangle|q=1)$. We first rewrite it according to Bayes' theorem, which can be found in Eq. 70. But now the first term must be calculated differently. We can calculate it as Eq. 74,

$$p(q=1||\epsilon_{i,j,k}\rangle) = \frac{\frac{1}{\sqrt{2\pi V_S}} \int_{lb_{i,k}}^{rb_{i,k}} \exp[-\frac{(x-u_i)^2}{2V_S}] \frac{1}{\sqrt{2\pi V_{el}}} \int_{T}^{\infty} \exp[-\frac{(y-x)^2}{2V_{el}}] dydx}{\frac{1}{\sqrt{2\pi V_S}} \int_{lb_{i,k}}^{rb_{i,k}} \exp[-\frac{(x-u_i)^2}{2V_S}] dx}. \tag{74}$$

Finally, we can get $\hat{\rho}_{E|q=1}$ and calculate $S(\hat{\rho}_{E|q=1})$ according the above methods.

In order to demonstrate the accuracy of our numerical simulation results, we first compare it with the analytical solution in the limit of no excess noise. Here we picked up $\tau = 1 \times 10^{-6}$ in our numerical simulation. It shows that the difference of ΔI is only 6.5804×10^{-7} between numerical simulation and analytical results.

In the end, we give the comparison of the result we get by setting different parameters, i.e., $EMAX$, $XMAX$, $HMAX$ and r_k. We can see that when $EMAX > 2$, $XMAX > 20$, $HMAX > 6$ and $r_k < 0.1$, we can see only tiny difference among

Table 1: Differences of the secrecy capacity with ΔI_{ref}. Here 25km denotes the case of 25km QIQO CVQKD without post-selection. 25km-ps denotes the case of 25km QIQO CVQKD with post-selection. 50km denotes the case of 50km QIQO CVQKD without post-selection. 50km-ps denotes the case of 50km QIQO CVQKD with post-selection.

	$\overline{\lvert\Delta I_{ref} - \Delta I_*\rvert}$			
	25km	25km-ps	50km	50km-ps
$\Delta I_{XMAX=10}$	7.35×10^{-5}	9.97×10^{-5}	4.25×10^{-5}	1.04×10^{-4}
$\Delta I_{XMAX=30}$	4.58×10^{-6}	5.84×10^{-6}	1.93×10^{-6}	5.46×10^{-6}
$\Delta I_{r=0.5}$	5.89×10^{-5}	4.01×10^{-4}	4.54×10^{-5}	3.50×10^{-3}
$\Delta I_{r=0.05}$	2.98×10^{-6}	8.23×10^{-6}	1.51×10^{-6}	9.42×10^{-5}
$\Delta I_{EMAX=1}$	2.63×10^{-6}	2.42×10^{-5}	9.85×10^{-7}	9.78×10^{-5}
$\Delta I_{EMAX=3}$	1.31×10^{-7}	5.60×10^{-7}	3.83×10^{-10}	1.22×10^{-8}
$\Delta I_{HMAX=4}$	1.41×10^{-5}	3.16×10^{-5}	1.51×10^{-6}	9.42×10^{-5}
$\Delta I_{HMAX=8}$	5.22×10^{-8}	9.26×10^{-8}	1.28×10^{-12}	7.28×10^{-12}

different simulations. We believe that the simulation results are accurate enough for those parameters.

The simulation results with different parameters are shown in the TABLE 1. We took the secrecy capacity obtained at $25km$ without post-selection with $EMAX = 2$, $XMAX = 20$, $HMAX = 6$ and $r = 0.1$ as a reference and note it as ΔI_{ref}. We give the difference of ΔI_* with the reference. We calculated $\overline{|\Delta I_{ref} - \Delta I_*|}$ and put the values into the TABLE 1.

¿From the results, we see that if we set $EMAX = 2$, $XMAX = 20$, $HMAX = 6$ and $r = 0.1$, we are already very close to the limit because if we further adjust the parameters, we get much less differences. In our final results, we just set $EMAX = 3$, $XMAX = 30$, $HMAX = 8$ and $r = 0.05$. We believe that these parameters give us numerical simulation results that are extremely close to the exact results.

CHAPTER IV

CONCLUSIONS

In this thesis, we have proposed an experimental continuous variable QKD scheme that uses high bandwidth ASE as the signal source. This system has extremely high bandwidth and low cost but does not improve the post-processing time required for reconciliation. We have used information theory to analyze the security of our scheme and compared our result with those previous results for traditional CVQKD schemes. Finally, we showed that the results of security proofs for traditional CVQKD schemes can also be applied to our scheme with simple arguments.

Second, we have proposed a quantized input-quantized output continuous variable quantum key distribution protocol. By quantizing the data into binary, the decoding complexity is dramatically decreased. We have given a general proof for general collective attacks and shown numerical simulation results. In order to make the proposed system compatible with the requirements of existing high efficiency and high decoding speed codes, we have also proposed post-selection to allow choosing of the error rate of the binary symmetric channel such that β_0 remains constant.

For future works, the experiment has been undertaken. We are making use of continuous wave instead of pulsed source in optical fibers. The continuous wave benefits us with high bandwidth. The experimental work is to be included in my PhD proposal.

REFERENCES

[1] C. H. Bennett and G. Grassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, Newyork, 1984), pp. 175-179.

[2] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem,"Phys. Rev. Lett. **67**, 661 (1991).

[3] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," (Cambridge University Press, UK, 2000).

[4] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables,"quant-ph/0204127 (2002).

[5] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States,"Phys. Rev. Lett., **88**, 057902 (2002)

[6] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, "Title: A Framework for Practical Quantum Cryptography,"arXiv:0802.4155(2008).

[7] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J. Cerf, R. Tualle-Brouri, S.W. McLaughlin, P. Grangier, "Quantum key distribution over 25km with an all-fiber continuous-variable system,"Phys. Rev. A, **76**, 042305 (2007).

[8] Ch. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit,"Phys. Rev. A, **89**, 167901 (2002).

[9] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Coherent-state quantum key distribution without random basis switching,"Phys. Rev. A, **73**,022316 (2006).

[10] A.M. Lance, T. Symul, V. Sharma, C. Weedbrook, T.C. Ralph,P.K. Lam, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light,"Phys. Rev. A, **95**, 180503 (2005).

[11] T. Symul, D.J. Alton, S.M. Assad, A.M. Lance, C. Weedbrook, T.C. Ralph, P.K. Lam, "Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise,"Phys. Rev. A, **76**, 030303(R) (2007).

[12] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables,"Rev. of Mod. Phys. **77** (2005).

[13] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238-241 (2003).

[14] N. J. Cerf, M. Lévy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states,"Phys. Rev. A, **63**, 052311 (2001).

[15] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).

[16] F. Grosshans, "CollectiveAttacks and Unconditional Security in Continuous Variable Quantum KeyDistribution ,"Phys. Rev. Lett., **94**, 020504 (2005).

[17] M. Navascués and A. Acín, "SecurityBounds for Continuous Variables Quantum Key Distribution," Phys. Rev. Lett., **94**, 020505 (2005).

[18] M. Christandl, R. Renner and A. K. Ekert, quant-ph/0402131.

[19] R. García-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution," Phys. Rev. Lett., **97**, 190503 (2006).

[20] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," Phys. Rev. Lett., **97**, 190502 (2006).

[21] H. Heid and N. Lütkenhaus, "Security of coherent-state quantum cryptography in the presence of Gaussian noise," Phys. Rev. A, **76**, 022313 (2007).

[22] R. Namiki and T. Hirano, "Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection," Phys. Rev. A, **74**, 032302 (2006).

[23] J. Singh, O. Dabeer and U. Madhow, "Capacity of the Discrete-Time AWGN Channel Under Output Quantization," arXiv:0801.1185v1 (2008).

[24] R. Ahlswede and P. Lober, "Quantum data processing," IEEE Trans. Inf. Theory, **47**, 1 (2001).

[25] K. Khandekar and R. J. McEliece, "On the complexity of reliable communication on the erasure channel," in Proc. IEEE Int. Symp. Information Theory, Washington, DC, Jun. 2001, p.1.

[26] Y. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," Phys. Rev. A, **79**, 012307 (2009).

[27] V. Bužek and G. Drobný, "Quantum tomography via the MaxEnt principle," J. of Mod. Optics, **47**, 14/15 (2000).

[28] J. Janszky, P. Domokos, S.Szabó, and P. Adam, "Quantum-state engineering via discrete coherent-state superpositions," Phys. Rev. A, **51**, 5 (1995).

[29] R. Jozsa and J. Schlienz, "Distinguishability of States and von Neumann Entropy," arXiv:quant-ph/9911009v1, 3 (1999).

[30] Z. Zhang and P. L. Voss, "A path towards 10 Gb/s continuous variable QKD," LPHYS08, Trondheim, Norway. July 2008.

[31] R. J. Glauber, Phys. Rev. **131**, 6 (1963).

[32] http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

[33] http://en.wikipedia.org/wiki/Public_key