DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS
CHENNAI – 600036

Coherent Optical Communication Techniques for Experimental Continuous-Variable Quantum Key Distribution

A Thesis

Submitted by

ABDULMOHSEN ALSAUI

For the award of the degree

Of

MASTER OF SCIENCE

July 2023

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS
CHENNAI – 600036

Coherent Optical Communication Techniques for Experimental Continuous-Variable Quantum Key Distribution

A Thesis

Submitted by

ABDULMOHSEN ALSAUI

For the award of the degree

Of

MASTER OF SCIENCE

July 2023

A good scientist has freed himself of concepts

and keeps his mind open to what is.

– Lao Tzu

To my parents, siblings, fiancée, and friends.

THESIS CERTIFICATE

This is to undertake that the Thesis titled **COHERENT OPTICAL COMMUNICATION TECHNIQUES FOR EXPERIMENTAL CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION**, submitted by me to the Indian Institute of Technology Madras, for the award of **Master of Science**, is a bona fide record of the research work done by me under the supervision of **Dr. Deepa Venkitesh**. The contents of this Thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Chennai 600036 **Abdulmohsen Alsaui**

Date: July 2023

Prof. Deepa Venkitesh
Research Guide
Professor
Dept. of Electrical Engineering
IIT Madras

LIST OF PUBLICATIONS

I. PRESENTATIONS IN CONFERENCE

A. Alsaui, A. Padhye, S. Vilashini, D. Venkitesh, A. Prabhakar, “Continuous-Variable Quantum Key Distribution @ IITM." Poster presented at Progress in Quantum Science and Technologies Conference; 2023 Jan 23-27; Chennai, Tamil Nadu, India.

II. PUBLICATIONS IN CONFERENCE PROCEEDINGS

A. Alsaui, Y. Alwehaibi, A. Prabhakar, and D. Venkitesh, “Digital filter design for experimental continuous-variable quantum key distribution”, in 2023 Optical Fiber Communications Conference and Exhibition (OFC), IEEE, 2023, pp. 1–3.

III. OTHER WORK

A. Alsaui, Y. Alghofaili, and D. Venkitesh, “Machine Learning Modeling and Time-Series Decomposition Analysis for Continuous-Variable Quantum Key Distribution”, European Conference on Optical Communication (ECOC), 2023 [Submitted Paper]

ACKNOWLEDGEMENTS

Words cannot express my gratitude to my parents and siblings, whose words of encouragement and motivation meant a lot to me.

Deep gratitude goes to Prof. Deepa Venkitesh, who enabled me to achieve beyond what I anticipated through her constant mentoring, guidance, and inspiration.

The gratitude is also extended to Prof. Anil Prabhakar, who had an impact in envisaging the research direction and milestones of this work.

I am also thankful to my peers, Yazeed Alwehaibi and Abdullah Almuallim, who aided me in jump-starting the early stages of the experimental work.

Great appreciation for NTIS, who funded my master's education and enabled me to run my experiments in their labs. Special thanks to Dr. Mishal Almazrooie, Prof. Turki F. Al-Somani, and Eng. Sultan Alharbi for their continuous encouragement and support throughout this research journey.

Profound appreciation for Alice, who was a source of unconditional moral support and solace as well as a great help on several non-technical aspects of the thesis.

Lastly, I appreciate the times I got to unwind from work with my friends. Thank you to Abdulrahman, Feras, Yousef, Ziyad, Ryan, Albaraa, Omar, Kareem, Naif, Yazeed, Sultan, Eyad, Chas, and Khalid for all the good times.

ABSTRACT

KEYWORDS QKD; Optical Communication; DSP

This work presents the details of implementing a continuous-variable quantum key distribution (CV-QKD) system using coherent reception. The research investigates factors that influence the secret key rate (SKR) in a practical setting, such as laser phase noise, hardware imperfections, and the considered security model. In addition, the study employs signal processing algorithms typically used in coherent optical communication utilizing homodyne detection. The experiment results demonstrate the proposed system's feasibility and highlight the importance of considering practical limitations when implementing CV-QKD in real-world applications. Overall, this work contributes to the advancement of quantum communication technology and lays the foundation for CV-QKD field implementation.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ADC analog-to-digital converter. 15, 51, 53, 65, 75, 76, 80, 96

AES advanced encryption standard. 2

BER bit error rate. 3, 90, 93, 94

BHD balanced homodyne detector. 103

BPF band-pass filter. 87–89

BS beam splitter. 103

CI confidence interval. 109, 110

CMRR common-mode rejection ratio. 85

CV-QKD continuous-variable quantum key distribution. 4–9, 12, 15, 16, 19, 21, 26, 28, 29, 36, 54, 83, 85, 95–97

CW continuous-wave. 30, 80

DAC digital-to-analog converter. 15, 43, 46, 50, 54, 65, 76, 79, 96

DDC digital down-converter. 51

DoF degrees of freedom. 109

DSP digital signal processing. 4, 6, 37, 54, 84, 90, 95, 96

DTFT discrete-time Fourier transform. 48

DUC digital up-converter. 50

DV-QKD discrete-variable quantum key distribution. 4, 5

EB entanglement-based. 21, 22

ECC error correcting code. 1, 18, 94

EM electromagnetic. 7, 9

FIR finite impulse response. 47

I/Q in-phase and quadrature. 29, 36, 76, 78, 97, 105

ICI inter-carrier interference. 46–48

IDTFT inverse discrete-time Fourier transform. 46

IF intermediate frequency. 33, 50

IID independent and identically distributed. 16

IIR infinite impulse response. 46, 54

IM/DD intensity-modulation and direct-detection. 29

ISI inter-symbol interference. 47–49, 52–54

LDPC low-density parity-check. 18

LLO local local oscillator. 5, 83, 84

LO local oscillator. 5, 30, 37, 65, 70, 71, 73, 74, 79, 80, 83, 84, 86–88, 90, 97, 103

LPF low-pass filter. 46, 47, 49, 51, 52, 85, 86

LSB least significant bit. 19

M-PSK M-ary phase-shift keying. 38, 39

M-QAM M-ary quadrature amplitude modulation. 38–41

MLC multilevel coding. 18

MS mean square. 31, 33

MSD multistage decoding. 18

MZI Mach–Zehnder interferometer. 29, 105

NEP noise-equivalent power. 73, 80, 85

NU natural units. 13

OOK on-off keying. 29

OPLL optical phase-locked loop. 37

OPM optical power meter. 91

OTP one-time pad. 2

P&M prepare-and-measure. 21, 22, 24

PCS probabilistic constellation shaping. 38, 41

PDF probability density function. 10

PDM polarization-division multiplexing. 84

PMF probability mass function. 40, 41

POVM positive operator-valued measurement. 19

PQC post-quantum cryptography. 2

PSD power spectral density. 67, 100

PSK phase-shift keying. 40

QAM quadrature amplitude modulation. 16, 40, 41

QHO quantum harmonic oscillator. 8

QKD quantum key distribution. 2–5, 16, 96

QPSK quadrature phase-shift keying. 28, 40, 43, 46, 54, 79, 90, 96, 97

QRNG quantum random number generator. 17

RC raised-cosine. 48, 49, 52, 53

RF radio frequency. 33, 43, 79

RIN relative intensity noise. 65, 67, 70, 71, 79

ROF roll-off factor. 49, 50, 53, 54, 89

RRC root raised-cosine. 49, 52, 53

RSA Rivest-Shamir-Adleman. 2

Rx receiver. 49, 52, 54, 90

SC suppressed-carrier. 43

SEC slice error correction. 18

SI international system of units. 8

SKF secret key fraction. 25, 27

SKR secret key rate. 87, 88, 93, 94, 96, 97

SNR signal-to-noise ratio. 26, 43

SNU shot-noise unit. 14, 20, 23–28, 66, 68, 79, 80, 91, 93, 103

SPD single-photon detector. 4

SSB single-sideband. 43

SSB-SC single-sideband suppressed-carrier. 43

TDM time-division multiplexing. 84

TIA transimpedance amplifier. 73, 80

TLO transmitted local oscillator. 83, 84

TMSVS two-mode squeezed vacuum state. 21, 22, 24

Tx transmitter. 49, 51, 52, 54

WLOG without loss of generality. 73

XOR exclusive or. 2

CHAPTER 1

INTRODUCTION

1.1 CRYPTOGRAPHY

The elementary form of a communication system is two parties, often referred to as Alice and Bob, who would like to exchange some information. In the presence of channel noise, the transmitted and received information will exhibit some inconsistency which can be mitigated through the use of an error correcting code (ECC). In addition to the intended message, redundant data is included to ensure error-free communication. The needed number of error-correcting bits is directly proportional to the channel noise, which was first mathematically quantified by Claude Shannon in 1948 [1].

Communication links are prone to eavesdropping, where an adversary, often named Eve, gains access to the exchanged message. The countermeasure is to conceal the raw message, known as plaintext, by encryption. The encrypted message, referred to as ciphertext, can be mapped back to the original message only by the intended recipient possessing the necessary knowledge.

Symmetric key cryptography is the case where the same key is used to encrypt and decrypt the message. The secrecy of the message may stem from the undisclosed key and the obscurity of the used cipher. The latter is known as security through obscurity, which is discouraged as design leakage will render all the developed hardware obsolete [2], similar to what happened to the Enigma machine utilized by the Germans in WWII. Therefore, the conventional practice is to utilize an unrevealed key with a reliable encryption algorithm. Some algorithms, like the substitution cipher (e.g., Caeser), are prone to elemental attacks (e.g., frequency analysis), rendering them not secure for symmetric key encryption. Once again, Claude Shannon was the one to set the foundation of modern

cryptography in his 1949 work [3], where he introduced the framework upon which ciphers are evaluated. Aside from the one-time pad (OTP), all ciphers are breakable for some available computational power. What distinguishes one cipher from another is the amount of time needed to crack it. For example, the advanced encryption standard (AES), developed in 1999 [4] and the most commonly used symmetric algorithm, requires billions of years to brute-force with the strongest existing supercomputer. In the OTP cipher, the bitwise exclusive or (XOR) operation is utilized to encrypt the message with a same-size key. As its name suggests, the OTP cipher uses the key only once, making it impractical since the pre-shared key will be quickly exhausted.

When the keys used for encryption and decryption are different, the process is called asymmetric (public-key) cryptography, elevating the burden of key sharing in symmetric cryptography. The encryption (public) key is disclosed, while the decryption (private) key is kept secret. Inspired by Ralph Merkle's work [5], the distribution of keys over a public channel was first made possible by the Diffie-Hellman algorithm in 1976 [6]. One of the oldest and most widely used public-key cryptosystems is the Rivest-Shamir-Adleman (RSA) algorithm [7]. In practice, rather than message transmission, RSA is used to distribute the keys for the less computationally demanding symmetric key cryptography, enabling high throughput secure data transmission. The security of RSA stems from the practical difficulty of factoring large prime numbers, which is threatened by the anticipated advent of quantum computers capable of running Shor's prime factorization algorithm [8].

In order to hinder the attacks posed by quantum computers, a new family of quantum-resistant ciphers has been developed lately in what is known as post-quantum cryptography (PQC). Another countermeasure is to share the keys using quantum key distribution (QKD), a physical layer approach that relies on quantum mechanical phenomena to establish symmetric keys between two authenticated parties as depicted in Figure 1.1. Unlike PQC, QKD is future-proof, in the sense that its security remains with the

advancements in hardware and software algorithms [9].

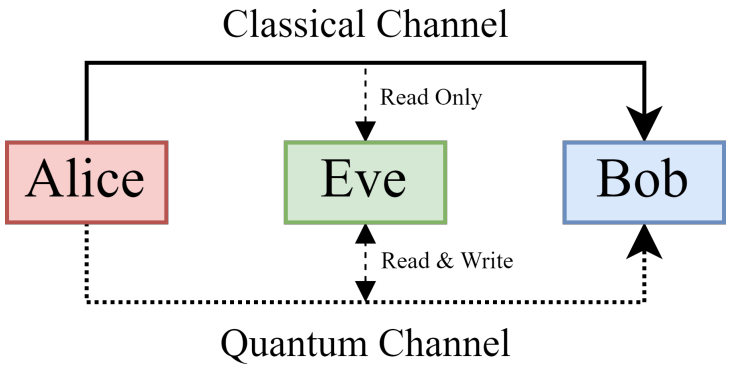


Figure 1.1: The schematic diagram of the communication channels used in QKD, where the quantum channel is susceptible to Eve's interference. In contrast, the authenticated classical channel signal can only be read by Eve.

1.2 QUANTUM KEY DISTRIBUTION (QKD)

QKD relies on the fact that quantum states cannot be observed without altering them, a concept that came to be known as the no-cloning theorem [10]. The no-cloning theorem, which originated from James Parks' work in 1970 [11], dictates that quantum states are always disturbed when measured and thus cannot be copied. By quantifying the amount of disturbance and its origins, secure quantum states can be exchanged, from which a cryptographic key is extracted. The stages of any QKD protocol are as follows

1. **Quantum Communication:** Preparation, distribution, and measurement of quantum states.

2. **Parameter Estimation:** A small subset of Alice's and Bob's data is publicly disclosed to determine the amount of information that could have leaked to Eve. The communication is aborted if the leaked information is above a certain threshold.

3. **Sifting:** Public announcements regarding the data by Alice and Bob, which allows them to obtain an equal size key with a small bit error rate (BER).

4. **Error-Correction:** The key obtained from the sifting stage is transformed into an identical pair of keys (k_{EC}) with a smaller size m using error-correction techniques.

5. **Privacy Amplification:** In order to eliminate the information leaked to Eve,

privacy amplification is performed, which further reduces the size of the key to n bits but guarantees the security of the obtained key (k_{PA}) up to a factor ϵ. This can be done through a matrix-vector multiplication operation where the vector is the error-corrected key (k_{EC}) and the matrix is a Toeplitz (diagonal-constant) [12]

$$\underbrace{\begin{pmatrix} t_{n-1} & t_n & t_{n+1} & \dots & t_{n+m-2} \\ t_{n-2} & t_{n-1} & t_n & \dots & t_{n+m-3} \\ \vdots & \ddots & & & \vdots \\ t_0 & t_1 & t_2 & \dots & t_{n-1} \end{pmatrix}}_{\text{Toeplitz Matrix}} \cdot \underbrace{\begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{m-1} \end{pmatrix}}_{k_{\mathrm{EC}}} = \underbrace{\begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{pmatrix}}_{k_{\mathrm{PA}}}. \tag{1.1}$$

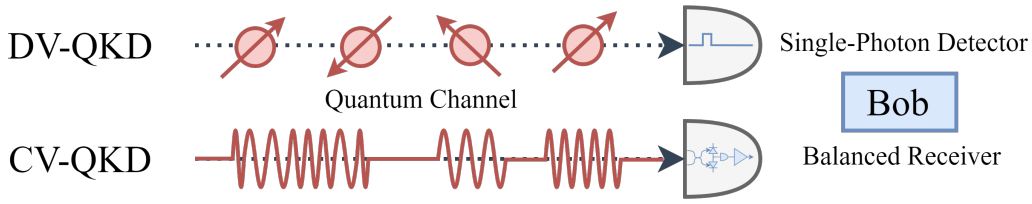


Figure 1.2: A representation highlighting the nature of the utilized quantum states in DV-QKD and CV-QKD, where the reception hardware differs for them.

The first conceived QKD protocol is the BB84 discrete-variable quantum key distribution (DV-QKD), named after its inventors Brassard and Bennett, which encodes the quantum states in the polarization of light [13]. Regarding how the signal is received, QKD can be classified into two categories: continuous-variable quantum key distribution (CV-QKD) and DV-QKD. As portrayed in Figure 1.2, the latter utilizes the discrete particle nature of light to encode the state, which is received using a single-photon detector (SPD). DV-QKD is currently more mature than CV-QKD, as it is easier to analyze using standard mathematical tools and is more heavily investigated [14]. However, the infinite-dimensional phase space of CV-QKD requires complex mathematical tools, such as symplectic transformations, making it harder to analyze compared to DV-QKD [15]. Moreover, CV-QKD requires sophisticated digital signal processing (DSP) algorithms [16].

Table 1.1: Advantages of utilizing a homodyne detector in the continuous-variable case instead of a single photon detector (SPD) for discrete-variable (DV) QKD implementation.

QKD Class	Receiver Type	Availability	Operating Temp.	Cost	Size
DV	Photon Counting	Custom-Built	Requires Cooling	Expensive	Bulky
CV	Homodyne Detection	Commercial	Room-Temp.	Cheap	Small

Despite this, the practical implementation of CV-QKD systems is much more feasible, as summarized in Table 1.1. Unlike DV-QKD, which requires bulky, expensive, and dead time-limited single-photon detectors, CV-QKD utilizes compact and relatively inexpensive coherent receivers that operate at a higher data rate. Moreover, the existing optical telecommunication infrastructure already uses coherent receivers, making deploying CV-QKD systems easier [17]. Thus, while DV-QKD is currently more well-established, the practical advantages of CV-QKD suggest that it may become an increasingly important technique for QKD.

The most practical class of CV-QKD implementations uses coherent states to encode information, where non-commuting (therefore non-orthogonal) electric field quadratures are utilized to transmit information securely over a communication channel. By measuring the quadratures of the received signals using a homodyne detector, a measurement distribution is obtained where the expected measurement outcome is unknown due to Heisenberg's uncertainty relation for non-commuting observables. Hence, some fixed error probability is expected, inherent in the system's design. When Eve attempts to tap into the signal, an unpreventable increase of error in the receiver will happen due to her inability to discriminate between the states perfectly.

CV-QKD implementations need continual improvement in bandwidth utilization and efficient compensation for channel impairments such as time and phase synchronizations. Figure 1.3 illustrates the achieved results of different experimental efforts where recent works tend to utilize a separate local oscillator (LO) at the receiver, known as local local oscillator (LLO). The standard coherent optical communication techniques can be

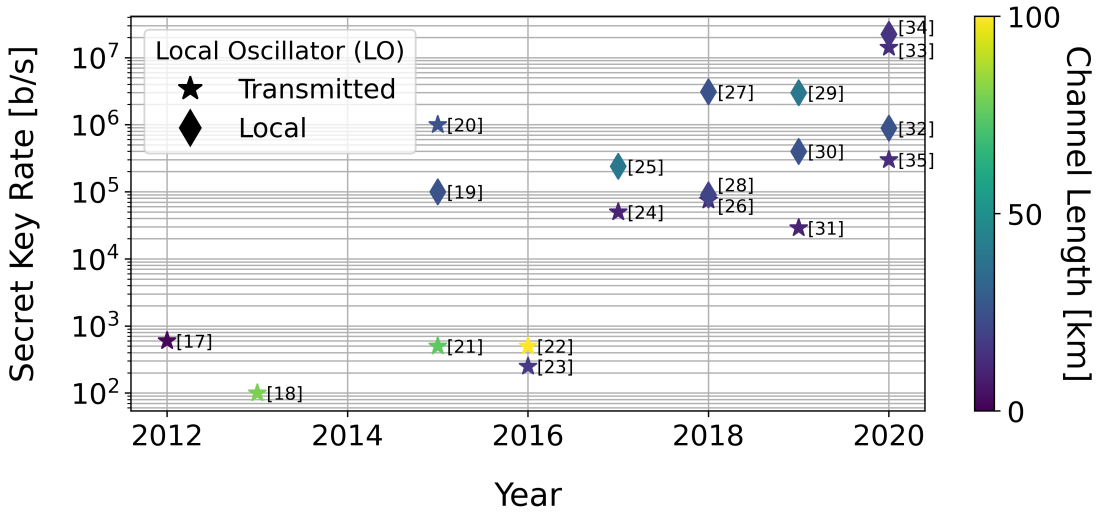


Figure 1.3: Achieved experimental result by different research groups with respect to the secret key rate (SKR), channel length, and local oscillator (LO) choice [18]–[36].

applied to improve the performance of CV-QKD systems, which entails the development of DSP algorithms targeting a CV-QKD implementation.

Our research aims to significantly improve the performance of discrete-modulated CV-QKD implementations through a combination of hardware design, system parameter optimization, and efficient DSP algorithms. Furthermore, we examine the underlying assumptions and parameters that impact the security of CV-QKD systems. The subsequent chapters are organized as follows. Chapter 2 presents the theoretical foundations of CV-QKD, encompassing the protocol description and security analysis. In Chapter 3, we discuss the fundamental concepts of coherent optical communications that are essential for understanding CV-QKD. In Chapter 4, we explore the primary sources of noise in a typical CV-QKD system. Finally, Chapter 5 delves into the system architecture and experimental implementation of CV-QKD.

CHAPTER 2

CONTINUOUS-VARIABLE QKD (CV-QKD) FUNDAMENTALS

This chapter establishes a theoretical basis for understanding the system representation and security analysis of CV-QKD and provides an in-depth discussion of the utilized protocol. Furthermore, the relevant mathematical concepts and tools used in the security analysis of CV-QKD are covered, including the derivation of the secret key rate and the study of the security parameters.

2.1 SYSTEM REPRESENTATION

2.1.1 Hilbert Space Formalism

An N-mode bosonic system can be represented by N quantized electromagnetic (EM) field modes[1], where each mode i is described by a particular Fock space ($\mathcal{F}_i$) that is spanned by an infinite Fock basis $\{|0\rangle_i, |1\rangle_i, \cdots, |n\rangle_i, \cdots\}$. The Fock state[2] $|n\rangle_i$ denotes a quantum state with n indistinguishable photons that are present in mode i. The Fock space ($\mathcal{F}_i$) may be expressed as

$$\mathcal{F}_i = \bigoplus_{n=0}^{\infty} \mathcal{H}_i^{\otimes n}, \tag{2.1}$$

where $\mathcal{H}_i^{\otimes n}$ is the n^{th} tensor power of the single-photon Hilbert space ($H_i^{\otimes 1}$) in mode i. An N-mode bosonic system is represented by the following Hilbert space

$$\begin{aligned} \mathcal{H}^{N\text{-mode}} &= \bigotimes_{i=1}^{N} \mathcal{F}_i \\ &= \bigotimes_{i=1}^{N} \left(\bigoplus_{n=0}^{\infty} \mathcal{H}_i^{\otimes n} \right), \end{aligned} \tag{2.2}$$

[1] A mode of the EM field corresponds to a specific spatial and temporal wavefunctions, energy, and polarization.

[2] The Fock state is also known as the number state.

which is also spanned by an infinite basis $|n\rangle_1 |n\rangle_2 \cdots |n\rangle_N \equiv |n_1 n_2 \cdots n_N\rangle$, since each Fock space ($\mathcal{F}_i$) is spanned by an infinite Fock basis [37]. An increase or decrease in the number of photons in a particular mode i is expressed through the creation ($\hat{a}_i^\dagger$) and annihilation ($\hat{a}_i$) ladder operators, respectively, as follows

$$\begin{aligned} \hat{a}_i^\dagger |n\rangle_i &= \sqrt{n+1}\, |n+1\rangle_i \,, \\ \hat{a}_i |n\rangle_i &= \sqrt{n}\, |n-1\rangle_i \,. \end{aligned} \tag{2.3}$$

In the international system of units (SI), the ladder operators can be modeled as a one-dimensional quantum harmonic oscillator (QHO) given by the following expressions

$$\hat{a}_i^\dagger = \frac{1}{\sqrt{2}} \left(\sqrt{\frac{m\omega}{\hbar}} \hat{x}_i - j \frac{1}{\sqrt{m\omega\hbar}} \hat{p}_i \right) \qquad \text{[SI]}, \tag{2.4}$$

$$\hat{a}_i = \frac{1}{\sqrt{2}} \left(\sqrt{\frac{m\omega}{\hbar}} \hat{x}_i + j \frac{1}{\sqrt{m\omega\hbar}} \hat{p}_i \right) \qquad \text{[SI]}, \tag{2.5}$$

where m is the particle's mass and ω_i is the angular frequency of oscillation. The factors are chosen to cancel the position($\hat{x}_i$) and momentum ($\hat{p}_i$) operators' dimensions since the ladder operators are assumed to be dimensionless. The corresponding Hamiltonian of the system is [38]

$$\begin{aligned} \hat{H} &= \sum_{i=1}^{N} \hat{H}_i \\ &= \sum_{i=1}^{N} \hbar\omega_i \left(\hat{a}_i^\dagger \hat{a}_i + \frac{1}{2} \right). \end{aligned} \tag{2.6}$$

Since an N-mode CV-QKD makes use of the infinite-dimensional Hilbert space ($\mathcal{H}^{N\text{-mode}}$), dealing with the density matrix formalism becomes quite cumbersome. Such a density matrix ($\rho^{N\text{-mode}}$) is expressed as

$$\rho^{N\text{-mode}} = \sum_{\vec{m},\vec{n}=0}^{\infty} \rho_{\vec{m},\vec{n}} \, |m_1 m_2 \cdots m_N\rangle \langle n_1 n_2 \cdots n_N| \,, \tag{2.7}$$

where $\vec{m} \equiv (m_1 m_2 \cdots m_N)$ and $\vec{n} \equiv (n_1 n_2 \cdots n_N)$. On the other hand, the phase space representation for N modes has $2N$ dimensions only [15], allowing for a simpler

representation of the states.

2.1.2 Phase Space Formalism

In general, the phase space is established by defining a canonically conjugate pair of observables $(\hat{x}_i, \hat{p}_i)$ for each mode i of the EM field. Denoting the two quadratures for each mode collectively as $\hat{r}_i$ and congregating them into a signal vector $\hat{r}$ gives

$$\begin{aligned} \hat{r} &= (\hat{r}_1, \hat{r}_2, \cdots, \hat{r}_{2N})^T \\ &= (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \cdots, \hat{x}_N, \hat{p}_N)^T, \end{aligned} \tag{2.8}$$

where T signifies the transpose operation. Equation (2.8) obeys the following bosonic commutation relation

$$\left[\hat{r}_j, \hat{r}_k\right] = 2j\Omega_{jk} \qquad (j, k = 1, ..., 2N), \tag{2.9}$$

where Ω_{jk} is a generic element of the symplectic form $2N \times 2N$ matrix[3] [15]

$$\mathbf{\Omega} = \bigoplus_{i=1}^{N} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{2.10}$$

An equivalent and more convenient description of a CV-QKD system is given by the Wigner function, which is a quasiprobability distribution defined over a real symplectic space $\left(\mathbb{R}^{2N}, \mathbf{\Omega}\right)$, known as the quantum phase space, which transforms the eigenvalues of the quadrature operators $\hat{r}$ while preserving $\mathbf{\Omega}$. In order to obtain the expression for the Wigner function, the Weyl operator is defined as

$$\hat{D}(\xi) \equiv e^{j\hat{r}^T \mathbf{\Omega} \xi}, \tag{2.11}$$

where $\hat{r}$ is given by Equation (2.8) and ξ is a $2N$-dimensional real vector. The Weyl operator translates the representation from the infinite-dimensional Hilbert space to the

[3] The symplectic form ($\mathbf{\Omega}$) defines the real symplectic matrix ($\mathbf{S}$) as

$$\mathbf{S\Omega S}^{\mathrm{T}} = \mathbf{\Omega},$$

which performs a symplectic transformation that leaves the symplectic form ($\mathbf{\Omega}$) invariant [39].

$2N$-dimensional phase space through the following relation

$$\begin{aligned} \chi_{\rho^{N\text{-mode}}}(\xi) &= \mathrm{Tr}\left[\rho^{N\text{-mode}}\hat{D}(\xi)\right], \\ &\updownarrow \\ \rho^{N\text{-mode}} &= \frac{1}{(2\pi)^{2N}}\int d^{2N}\xi \chi_{\rho^{N\text{-mode}}}(-\xi)\hat{D}(\xi), \end{aligned} \tag{2.12}$$

where $\rho^{N\text{-mode}}$ is the density matrix defined in Equation (2.7) and $\chi_{\rho^{N\text{-mode}}}(\xi)$ is the Wigner characteristic function, the Fourier transform of which defines the sought-after Wigner function as

$$W_{\rho^{N\text{-mode}}}(r) = \frac{1}{(2\pi)^{2N}}\int_{\mathbb{R}^{2N}} d^{2N}\cdot\xi\cdot e^{-jr^T\mathbf{\Omega}\xi}\cdot\chi(\xi), \tag{2.13}$$

which exhibits a quasi-probability distribution in the phase space representation. In order to characterize the Wigner function, the first two statistical moments[4] of the quantum state are used, which suffice to characterize Gaussian states fully [39]. The first moment defines the displacement vector (d) as

$$d \equiv \langle\hat{r}\rangle = \mathrm{Tr}\left(\hat{r}\hat{\rho}^{N\text{-mode}}\right), \tag{2.14}$$

while the second moment, known as the covariance matrix, is a $2N\times 2N$ symmetric positive semi-definite matrix[5] whose elements are given by[6]

[4]For a random variable (X) with probability density function (PDF) $f(x)$, the n^{th} moment is defined as the expectation value of x^n as following

$$\langle x^n\rangle = \int_{-\infty}^{\infty} x^n f(x)\,\mathrm{d}x,$$

where the first and second moments correspond to the mean and the variance, respectively [40].

[5]An $n\times n$ symmetric real-valued matrix (M) is positive semi-definite if it satisfies the following condition [41]

$$v^{\mathrm{T}}Mv \geq 0, \qquad \forall v\in\mathbb{R}^n.$$

[6]The anticommutator of two elements is defined as

$$\{A,B\} \equiv AB + BA.$$

$$
\begin{aligned}
\Gamma_{ij} &= \frac{1}{2}\left\langle\{\Delta\hat{r}_i, \Delta\hat{r}_j\}\right\rangle \\
&= \frac{1}{2}\left\langle\{\hat{r}_i - \langle\hat{r}_i\rangle, \hat{r}_j - \langle\hat{r}_j\rangle\}\right\rangle \\
&= \frac{1}{2}\Big[\Big\langle(\hat{r}_i - \langle\hat{x}_i\rangle)(\hat{r}_j - \langle\hat{r}_j\rangle) \\
&\qquad + (\hat{r}_j - \langle\hat{r}_j\rangle)(\hat{r}_i - \langle\hat{r}_i\rangle)\Big\rangle\Big] \\
&= \frac{1}{2}\Big[\Big\langle\hat{r}_i\hat{r}_j + \hat{r}_j\hat{r}_i - 2\hat{r}_i\langle\hat{r}_j\rangle \\
&\qquad - 2\hat{x}_j\langle\hat{x}_i\rangle + 2\langle\hat{r}_i\rangle\langle\hat{r}_j\rangle\Big\rangle\Big] \\
&= \frac{1}{2}\left(\langle\hat{r}_j\hat{r}_i\rangle + \langle\hat{r}_i\hat{r}_j\rangle\right) \\
&\quad + \left\langle-\hat{r}_i\langle\hat{r}_j\rangle - \hat{r}_j\langle\hat{r}_i\rangle + \langle\hat{r}_i\rangle\langle\hat{r}_j\rangle\right\rangle \\
&= \frac{1}{2}\left(\langle\hat{r}_j\hat{r}_i\rangle + \langle\hat{r}_i\hat{x}_j\rangle\right) - \langle\hat{r}_i\rangle\langle\hat{r}_j\rangle.
\end{aligned}
\tag{2.15}
$$

For the diagonal elements, plugging $j = i$ gives the variance

$$
\begin{aligned}
\Gamma_{ii} &= \langle(\hat{r}_i)^2\rangle - \langle\hat{r}_i\rangle^2 \\
&= \sigma^2_{\hat{r}_i},
\end{aligned}
\tag{2.16}
$$

while the off-diagonal elements indicate the correlation between quadratures belonging to different modes.

2.1.3 Coherent States

The coherent state $|\alpha\rangle$, which describes a well-stabilized laser, is defined as the eigenstate of the annihilation operator ($\hat{a}$)

$$
\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.17}
$$

where $\alpha = |\alpha|e^{i\theta}$ is the complex eigenvalue and $\langle\alpha|\alpha\rangle = 1$. Applying the creation operator ($\hat{a}^\dagger$) on the coherent state gives

$$
\hat{a}^\dagger\,|\alpha\rangle = \alpha^*\,|\alpha\rangle\,. \tag{2.18}
$$

The states $|\alpha\rangle$ are not orthogonal since the annihilation operator ($\hat{a}$) is not Hermitian.

Moreover, $|\alpha\rangle$ is not an eigenstate of the number operator ($\hat{N}$) since it does not have a fixed number of photons. For the coherent state, the Weyl displacement operator is defined as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.19}$$

where α is the magnitude of displacement in phase space. In particular, the vacuum state ($|0\rangle$) can be displaced into a coherent state ($|\alpha\rangle$) by applying the Weyl displacement operator as follows

$$\begin{aligned} \hat{D}(\alpha)|0\rangle &= e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0\rangle \\ &= |\alpha\rangle . \end{aligned} \tag{2.20}$$

In order to expand $|\alpha\rangle$ in the Fock states, the Baker–Campbell–Hausdorff formula [42] is utilized, which gives

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{2.21}$$

Note that the coherent states are not orthogonal. For two coherent states $|\alpha\rangle$ and $|\beta\rangle$, their inner product gives a nonzero value as following

$$\begin{aligned} \langle\alpha|\beta\rangle &= e^{-(|\alpha|^2+|\beta|^2)/2} \sum_{n=0}^{\infty} \frac{(\alpha^*\beta)^n}{n!} \\ &= e^{-(|\alpha|^2+|\beta|^2-\alpha^*\beta)/2}, \end{aligned} \tag{2.22}$$

where the probability is

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}. \tag{2.23}$$

In CV-QKD, α and β are close, making the probability in Equation (2.23) higher, thus introducing uncertainty in the measurement. In other words, coherent states' security depends on their non-orthogonality (nonzero inner product), indicating the inability to discriminate between them perfectly [15]. As will be discussed later, the variance of the quadrature operators plays an essential role in CV-QKD protocols. Therefore, it is of interest to derive its value. Setting the value of m, ω_i, and $\hbar$ in Equation (2.4) and

Equation (2.5) to unity gives the natural units (NU) representation of the ladder operators [43]

$$\hat{a}^\dagger = \frac{1}{\sqrt{2}}(\hat{x} - j\hat{p}) \qquad \text{[NU]}, \tag{2.24}$$

$$\hat{a} = \frac{1}{\sqrt{2}}(\hat{x} + j\hat{p}) \qquad \text{[NU]}, \tag{2.25}$$

which is equivalent to following relations

$$\hat{x} = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right) \qquad \text{[NU]}, \tag{2.26}$$

$$\hat{p} = \frac{j}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right) \qquad \text{[NU]}. \tag{2.27}$$

Since the uncertainty in the two quadratures is the same for a coherent state [38], they have the same variance

$$\sigma_{\hat{x}}^2 = \sigma_{\hat{p}}^2, \tag{2.28}$$

which can be found by calculating the following expectation values

$$\begin{aligned}
\langle\hat{x}\rangle &= \langle\alpha|\,\hat{x}\,|\alpha\rangle \\
&= \frac{1}{\sqrt{2}}\left[\langle\alpha|\,\hat{a}^\dagger\,|\alpha\rangle + \langle\alpha|\,\hat{a}\,|\alpha\rangle\right] \\
&= \frac{1}{\sqrt{2}}(\alpha^* + \alpha) \\
&= \frac{1}{\sqrt{2}}\left[(x - jp) + (x + jp)\right] \\
&= \sqrt{2}x \qquad \text{[NU]},
\end{aligned} \tag{2.29}$$

$$\begin{aligned}
\langle\hat{x}^2\rangle &= \langle\alpha|\,\hat{x}^2\,|\alpha\rangle \\
&= \frac{1}{2}\langle\alpha|\,(\hat{a}^\dagger + \hat{a})^2\,|\alpha\rangle \\
&= \frac{1}{2}\left[\,\langle\alpha|\,(\hat{a}^\dagger)^2\,|\alpha\rangle + \langle\alpha|\,\hat{a}^2\,|\alpha\rangle + \langle\alpha|\,\hat{a}^\dagger\hat{a}\,|\alpha\rangle + \langle\alpha|\,\hat{a}\hat{a}^\dagger\,|\alpha\rangle\,\right] \\
&= \frac{1}{2}\left[\alpha^2 + (\alpha^*)^2 + 2\alpha^*\alpha + 1\right] \\
&= \frac{1}{2}\left[(x^2 - p^2 + 2jxp) + (x^2 - p^2 - 2jxp) + 2(x^2 + p^2) + 1\right] \\
&= 2x^2 + \frac{1}{2} \qquad \text{[NU]},
\end{aligned} \tag{2.30}$$

where the fact that $[\hat{a}, \hat{a}^\dagger] = 1$ was used. Therefore, the variance can be found as

$$\begin{aligned} \sigma_{\hat{x}}^2 &= \langle \hat{x}^2 \rangle - \langle \hat{x} \rangle^2 \\ &= 2x^2 + \frac{1}{2} - 2x^2 \\ &= \frac{1}{2} \qquad [\text{NU}]. \end{aligned} \tag{2.31}$$

In shot-noise unit (SNU), the variance of the vacuum noise is normalized to unity by multiplying Equation (2.26) and Equation (2.27) by $\sqrt{2}$ which gives [15]

$$\hat{x} = \left(\hat{a}^\dagger + \hat{a}\right) \qquad [\text{SNU}], \tag{2.32}$$

$$\hat{p} = j\left(\hat{a}^\dagger - \hat{a}\right) \qquad [\text{SNU}], \tag{2.33}$$

with the equivalent representation

$$\hat{a}_i^\dagger = \frac{1}{2}\left(\hat{x}_i - j\hat{p}_i\right) \qquad [\text{SNU}], \tag{2.34}$$

$$\hat{a}_i = \frac{1}{2}\left(\hat{x}_i + j\hat{p}_i\right) \qquad [\text{SNU}], \tag{2.35}$$

which results in the following expectation values

$$\langle \hat{x} \rangle = 2x \qquad [\text{SNU}], \tag{2.36}$$

$$\langle \hat{x}^2 \rangle = 4x^2 + 1 \qquad [\text{SNU}], \tag{2.37}$$

which gives a unity quadrature variance

$$\begin{aligned} \sigma_{\hat{x}}^2 &= \langle \hat{x}^2 \rangle - \langle \hat{x} \rangle^2 \\ &= 4x^2 + 1 - 4x^2 \\ &= 1 \qquad [\text{SNU}]. \end{aligned} \tag{2.38}$$

A depiction of the SNU in phase space for the coherent state is shown in Figure 2.1. A summary of the different representations of the quadratures and their variance is given in Table 2.1.

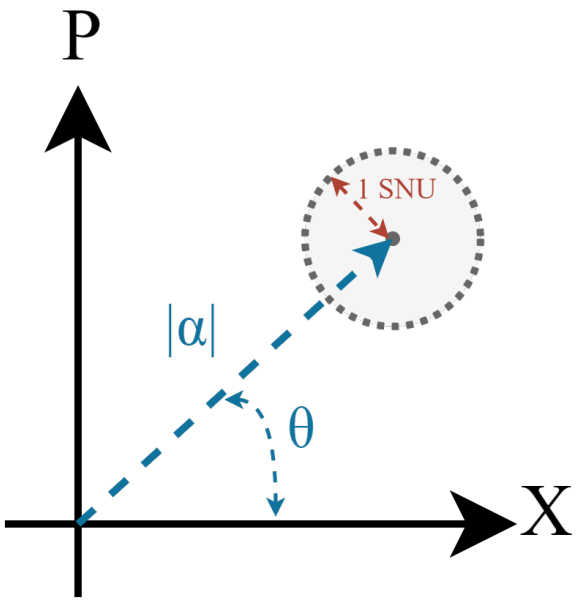


Figure 2.1: Argand diagram depicting the coherent state in phase space with unity variance in SNU.

Table 2.1: Representation of the quadratures and the corresponding standard variance σ^2 in the international system of units (SI), natural units (NU), and shot-noise unit (SNU).

	SI	**NU**	**SNU**
$\hat{x}$	$\sqrt{\frac{\hbar}{2m\omega}}\left(\hat{a}^\dagger + \hat{a}\right)$	$\frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right)$	$\left(\hat{a}^\dagger + \hat{a}\right)$
$\hat{p}$	$j\sqrt{\frac{m\omega\hbar}{2}}\left(\hat{a}^\dagger - \hat{a}\right)$	$\frac{j}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right)$	$j\left(\hat{a}^\dagger - \hat{a}\right)$
σ^2	$\frac{\hbar}{2}$	$\frac{1}{2}$	1

2.2 PROTOCOL

The modulation format of the quantum states can either be continuous, following a Gaussian distribution, or discrete. From a theoretical point of view, Gaussian modulation offers better system performance and more understood security proofs. On the other hand, ideal Gaussian modulation is impractical due to the finite quantization resolution of the analog-to-digital converter (ADC) and digital-to-analog converter (DAC). Moreover, as will be outlined, continuous-modulated CV-QKD requires a complex reconciliation

procedure. Therefore, the chosen scheme is the discrete modulation, which shares many similarities with the quadrature amplitude modulation (QAM) format used in classical optical communication, easing the post-processing procedure. Recently, the development of security proofs for discrete-modulated CV-QKD has been catching up [44], [45], further motivating the selection of this protocol. For ease of reference, the QKD stages outlined in Section 1.2 are depicted in Figure 2.2 with a slight modification for the chosen protocol.

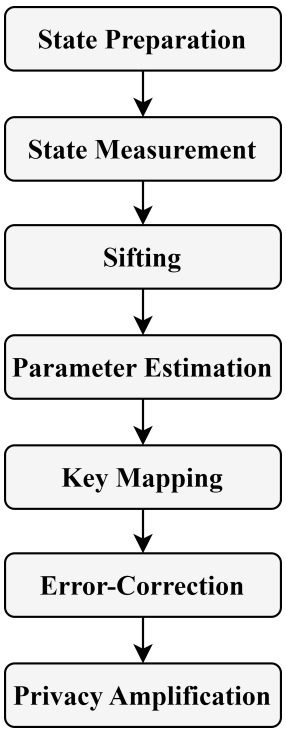


Figure 2.2: Considered stages for the targeted CV-QKD protocol.

2.2.1 Continuous-Modulated CV-QKD

The first developed CV-QKD protocol is the continuous-modulated GG02, named after Grosshans and Grangier, who invented it in 2002 [46]. In this protocol, Alice starts by preparing N coherent states $|\alpha_n\rangle = |x_n + ip_n\rangle$, $n \in \{1, \cdots, N\}$ which are Gaussian-modulated. The quadrature variables x_n and p_n are sampled from the independent and identically distributed (IID) random variables $\mathcal{X}$ and $\mathcal{P}$, respectively, which follow a

Gaussian distribution with zero mean (μ) and variance[7] σ_A^2 such that $\mathcal{X}, \mathcal{P} \sim N(0, \sigma_A^2)$. Figure 2.3 illustrates such a distribution in the complex plane, also known as the Argand (phase space) diagram, for 500 samples[8]. From the incoming states, Bob only measures one of the quadratures. The choice of which quadrature (x or p) to measure is randomized using a quantum random number generator (QRNG), as shown in Figure 2.4.

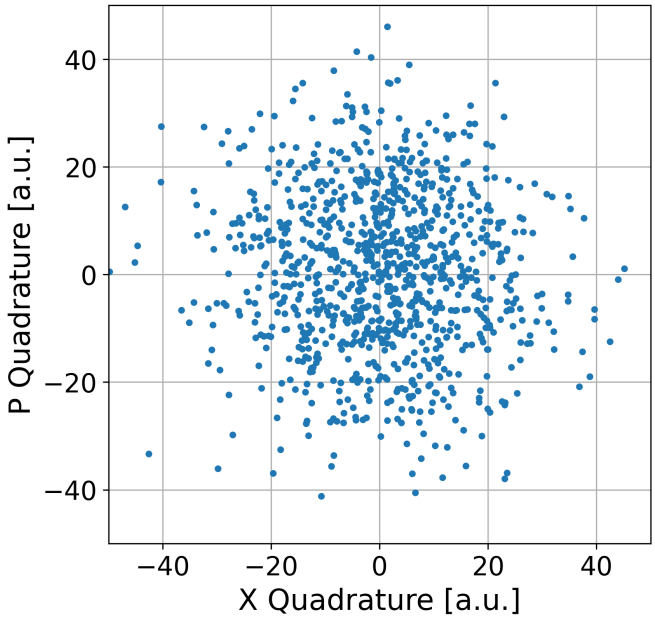


Figure 2.3: Argand (phase space) diagram for 500 randomly generated coherent states with $\mu = 0$ and $\sigma = 15$. The 99% confidence interval (CI) of estimating the standard deviation from the obtained samples $\sigma_s = 14.83$ is $12.61 \leq \sigma \leq 17.5$.

The obtained decimal-valued measurements are discretized into a binary representation, where the number of binary numbers depends on the resolution of Alice's and Bob's hardware. Then, sifting is done, where Bob informs Alice of his quadrature choices. Then, Alice discards the N quadrature values that Bob did not measure. Next, parameter estimation is performed, which involves Alice and Bob disclosing a subset of size k from

[7] Recall that the variance σ_x^2 for a signal x is

$$\sigma_x^2 \equiv \left\langle (\Delta x)^2 \right\rangle,$$

which quantifies the average fluctuation of the signal.

[8] The number of needed samples to truthfully represent the standard deviation for the normal distribution is discussed in Appendix D.

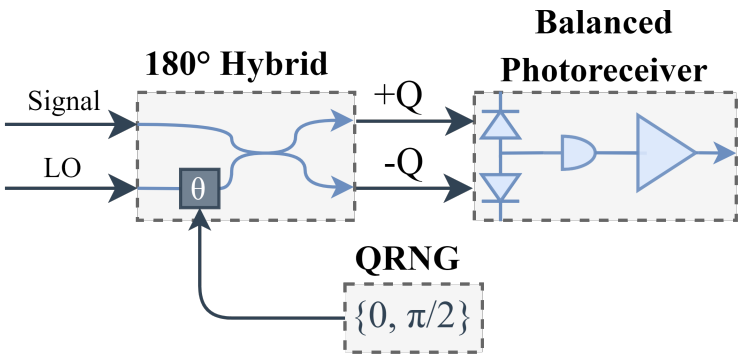


Figure 2.4: Coherent reception configuration where one of the quadratures is randomly chosen to be measured by adjusting the phase modulator.

their data over an authenticated classical. The disclosed data are used to estimate the parameters upper bounding Eve's information, which determines the length l of the final key. Now, Alice and Bob share $m = N - k$ correlated pairs of binary data.

The m pairs of data shared by Alice and Bob are not identical. A procedure known as reconciliation is utilized to correct the errors between the variables. The reconciliation procedure is called direct (reverse) when only Alice (Bob) communicates to Bob (Alice), while Bob (Alice) performs the computationally expensive decoding process of the ECC. Reconciliation allows Alice and Bob to obtain an equal-length bit string with a low probability of error.

One famous reconciliation method is slice error correction (SEC) reconciliation, which is a two-stage procedure as seen in Figure 2.5. First, Alice's and Bob's continuous variables are converted to binary values by quantizing them using a slice (quantization) function. Then, a binary correction protocol is performed where a multilevel coding (MLC) with multistage decoding (MSD) is used for channel coding while the error correction is done using low-density parity-check (LDPC) codes [47].

In the quantization step, the slice (quantization) function $Q(b) : \mathbb{R} \rightarrow \{0,1\}^m$ maps the continuous variables to m-bit binary numbers. Thus, $Q(b) = (Q_1(b), \cdots, Q_m(b))$ is a vector of binary slices where Q_i picks up the i^{th} bit q^i_j from the binary representation

of y_j. Bob then discloses the first t slices $(Q_1(b), \cdots, Q_t(b))$ corresponding to the least significant bits (LSBs). For the remaining $m - t$ slices, Bob encodes each slice $Q_k(b), k \in \{t+1, \cdots, m\}$ and sends it to Alice for the error correction stage. Then, Alice recovers the bits using her Gaussian variables, Bob's encoded slices, and the output of the previous decoder [47].

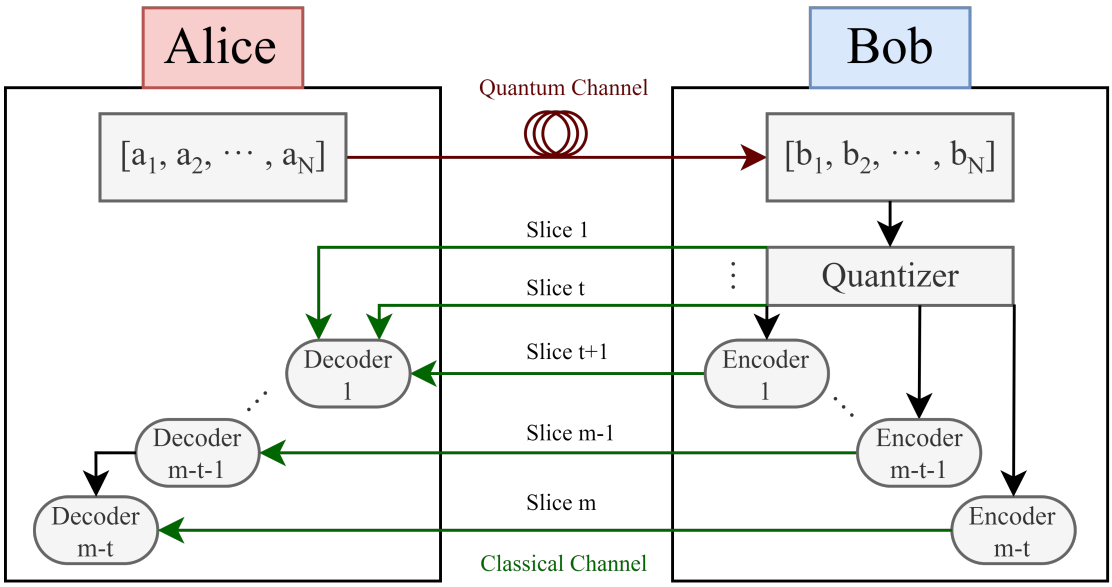


Figure 2.5: Reverse slice reconciliation using the multilevel coding (MLC) with multistage decoding (MSD) scheme for continuous-modulated CV-QKD protocol. In addition to the known transmitted states, Alice utilizes the output of the previous decoders to obtain an error-free key.

2.2.2 Discrete-Modulated CV-QKD

The protocol of interest for this work is the discrete-modulated CV-QKD. In the discrete modulation, Alice prepares N coherent states $\left|\psi_a^i\right\rangle$ where $i \in \{1, 2, \cdots N\}$, which are randomly selected from the set $\{|\alpha\rangle, |-\alpha\rangle, |j\alpha\rangle, |-j\alpha\rangle\}$ for some specified $\alpha \in \mathbb{R}$. At Bob's side, for each received state $\left|\psi_b^i\right\rangle$, Bob measures both quadratures which is described by the positive operator-valued measurement (POVM) $E_{y_b} = \frac{1}{\pi} |y_b\rangle \langle y_b|$, obtaining the outcome $y_b^i \in \mathbb{C}$. The N exchanged states are partitioned into two subsets $\mathcal{I}_{\text{key}}$ and $\mathcal{I}_{\text{test}}$ that are used for the sifting and parameter estimation stages, respectively. In the sifting stage, Alice maps her states $\left|\psi_a^k\right\rangle$ for $k \in \mathcal{I}_{\text{key}}$ to symbols S_a^k according to

the following rule

$$S_a^k = \begin{cases} 0, & \left|\psi_a^k\right\rangle = |\alpha\rangle\,, \\ 1, & \left|\psi_a^k\right\rangle = |j\alpha\rangle\,, \\ 2, & \left|\psi_a^k\right\rangle = |-\alpha\rangle\,, \\ 3, & \left|\psi_a^k\right\rangle = |-j\alpha\rangle\,, \end{cases} \tag{2.39}$$

where the symbols 0, 1, 2, and 3 map to the binary pairs 00, 01, 10, and 11, respectively. Then, parameter estimation is performed where the small subset of Alice's and Bob's data ($\mathcal{I}_{\text{test}}$) is publicly disclosed to determine the amount of information that could have leaked to Eve. The communication is aborted if the leaked information is above a certain threshold. After that, Bob maps the measurements $y_b^k = \left|y_b^k\right| e^{j\theta_b^k}$ where $k \in \mathcal{I}_{\text{key}}$ and $\theta_b^k \in \left[-\frac{\pi}{4}, \frac{7\pi}{4}\right)$ to symbols (S_b^k) according to the following rule [44]

$$S_b^k = \begin{cases} 0, & \theta_b^k \in \left[-\frac{\pi}{4} + \Delta_\theta, \frac{\pi}{4} - \Delta_\theta\right) \text{ and } \left|y_b^k\right| \geq \Delta_\alpha, \\ 1, & \theta_b^k \in \left[\frac{\pi}{4} + \Delta_\theta, \frac{3\pi}{4} - \Delta_\theta\right) \text{ and } \left|y_b^k\right| \geq \Delta_\alpha, \\ 2, & \theta_b^k \in \left[\frac{3\pi}{4} + \Delta_\theta, \frac{5\pi}{4} - \Delta_\theta\right) \text{ and } \left|y_b^k\right| \geq \Delta_\alpha, \\ 3, & \theta_b^k \in \left[\frac{5\pi}{4} + \Delta_\theta, \frac{7\pi}{4} - \Delta_\theta\right) \text{ and } \left|y_b^k\right| \geq \Delta_\alpha, \\ \perp, & \text{Otherwise}, \end{cases} \tag{2.40}$$

where Δ_θ and Δ_α are non-negative post-selection parameters in SNU to be optimized for, and $\perp$ signifies a discarded measurement as depicted in Figure 2.6. The minimum permissible coherent state amplitude (Δ_α) distills the weak signals that result in insignificant shared information between Alice and Bob. Similarly, Δ_θ filters out the high uncertainty regions by setting the maximum permissible phase deviation from the ideal constellation point. Intuitively, the post-selection scheme can be viewed as an optimization mechanism between the information leaked to Eve and the mutual information between Alice and Bob. Both increase as the uncertainty regions are limited.

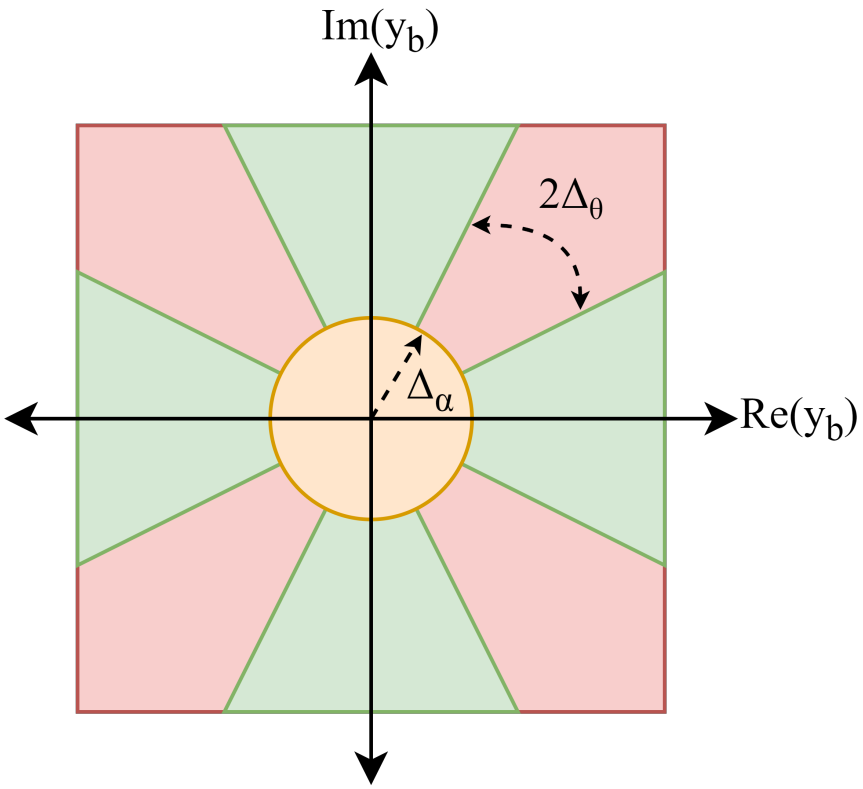


Figure 2.6: The post-selection strategy discards the states existing in the extreme uncertainty regions (red-colored) that prohibit Alice and Bob from agreeing on a key. The green regions correspond to the optimal trade-off between having significant mutual information between Alice and Bob with enough uncertainty to limit the information leaked to Eve.

2.3 SECURITY ANALYSIS

CV-QKD can be implemented using two equivalent approaches: the entanglement-based (EB) and the prepare-and-measure (P&M) [48]. The two variations are compared in Table 2.2. In the P&M implementation, Alice communicates displaced coherent states to Bob through a Gaussian channel. For the EB version, a two-mode squeezed vacuum state (TMSVS)[9] is prepared by Alice, where she will measure the quadratures of one mode and sends the other mode to Bob as Figure 2.7 shows. The equivalence between the two approaches stems from the fact that the partial measurement on the bipartite EB version (measuring the second mode) can be projected into the P&M states (statistical mixture of

[9] A TMSVS is a quantum light state with high correlations between its electromagnetic modes.

coherent states) [49]. From a mathematical point of view, the security analysis is more straightforward for the EB version. On the other hand, practically, it is much easier to implement the P&M version. Therefore, in what follows, the security is considered for the EB version, while the experimental implementation is based on the P&M scheme.

Table 2.2: Comparison between the two approaches to implementing CV-QKD concerning the nature of the exchanged signal and the complexity of implementation and analysis.

Approach	**Prepared Signal**	**Implementation**	**Analysis**
Prepare-and-Measure (P&M)	Coherent State	Simple	Complex
Entanglement-Based (EB)	Two-Mode Squeezed Vacuum State (TMSVS)	Complex	Simple

2.3.1 Entanglement-Based (EB) CV-QKD

The covariance matrix of the TMSVS at Alice's side is [50]

$$\begin{aligned}\Gamma_{\mathrm{A}} &= \begin{bmatrix} \sigma_{\hat{q}}^2 & 0 & Z & 0 \\ 0 & \sigma_{\hat{q}}^2 & 0 & -Z \\ Z & 0 & \sigma_{\hat{q}}^2 & 0 \\ 0 & -Z & 0 & \sigma_{\hat{q}}^2 \end{bmatrix} \\ &= \begin{bmatrix} \sigma_{\hat{q}}^2 \cdot I_2 & Z \cdot \sigma_z \\ Z \cdot \sigma_z & \sigma_{\hat{q}}^2 \cdot I_2 \end{bmatrix},\end{aligned} \tag{2.41}$$

where $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity matrix, $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ is Pauli Z matrix, $Z = f(\sigma_{\hat{q}}^2)$ is a correlation factor between the two quadratures that is a function of $\sigma_{\hat{q}}^2$, which depends on the distribution of the states, and $\sigma_{\hat{q}}^2$ is the quadrature operators' variance given by

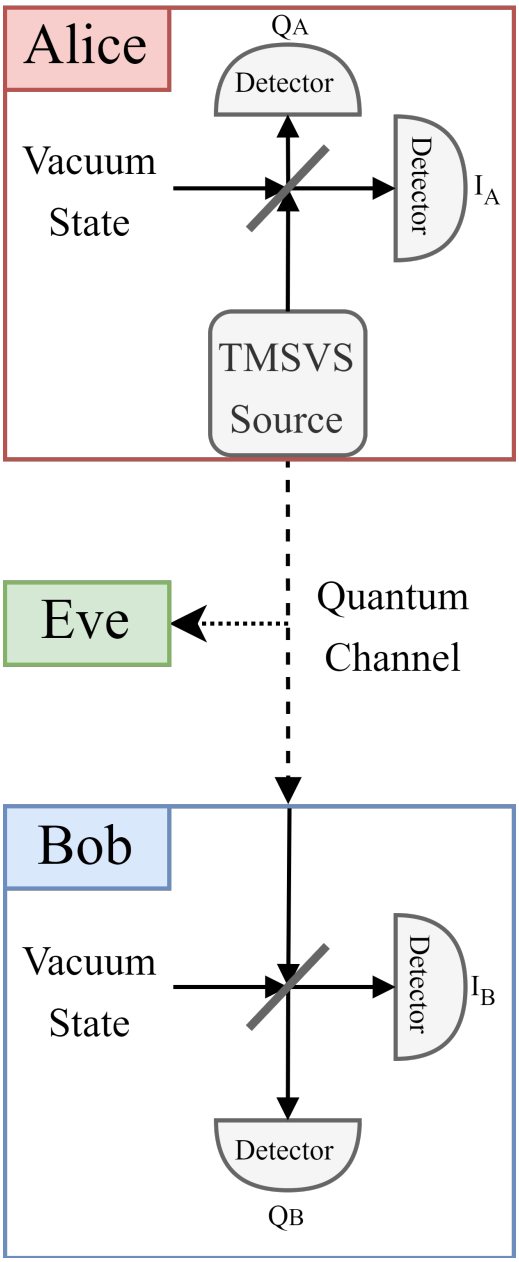


Figure 2.7: Schematic diagram of the entanglement-based (EB) CV-QKD protocol where a two-mode squeezed vacuum state (TMSVS) is prepared, and one is sent to Bob. Alice and Bob measure both quadratures of their respective mode.

Equation (2.37)

$$\begin{aligned}\sigma^2_{\hat{q}} &= 4\sigma^2_{\hat{\mathrm{A}}} + 1 \\ &= \sigma^2_{\hat{\mathrm{A}}} + 1 \\ &= 2|\alpha|^2 + 1 \\ &= 2\langle n\rangle + 1 \qquad \text{[SNU]},\end{aligned} \tag{2.42}$$

where σ^2_{A} and $\sigma^2_{\hat{\mathrm{A}}}$ are the modulation variance of the quadrature components (x and p) and operators ($\hat{x}$ and $\hat{p}$) in the P&M scheme, respectively, α is the coherent state amplitude, and $\langle n \rangle$ is the average number of photons per symbol at the channel input. The TMSVS received by Bob has the following covariance matrix

$$\Gamma_{\mathrm{AB}} = \begin{bmatrix} \left(\sigma^2_{\hat{\mathrm{A}}} + 1\right) \cdot I_2 & \sqrt{T_{\mathrm{tot}}} Z \cdot \sigma_z \\ \sqrt{T_{\mathrm{tot}}} Z \cdot \sigma_z & \left[1 + T_{\mathrm{tot}} \sigma^2_{\hat{\mathrm{A}}} + \xi_{\mathrm{tot}}\right] \cdot I_2 \end{bmatrix} \quad \text{[SNU]}, \tag{2.43}$$

where ξ_{tot} is the total excess noise referred to at the input of Bob's equipment (after the channel), and T_{tot} is the total transmittance incorporating the following loss sources

$$T_{\mathrm{tot}} = T_{\mathrm{ch}} \cdot T_{\mathrm{hyb}} \cdot \eta_{\mathrm{det}}, \tag{2.44}$$

for a detector with quantum efficiency η_{det} and channel transmittance T_{ch} given by

$$T_{\mathrm{ch}} = 10^{-\frac{L_{\mathrm{ch}} \cdot \alpha_{\mathrm{ch}}}{10}}, \tag{2.45}$$

for a channel of length L_{ch} with an attenuation rate α_{ch}, while T_{hyb} depends whether or not a 3 dB coupler is utilized in the optical hybrid

$$T_{\mathrm{hyb}} = \begin{cases} 1, & \text{Homodyne (Single Quadrature)} \\ T_{3\ \mathrm{dB}} \approx 0.5, & \text{Heterodyne (Two Quadratures)} \end{cases}, \tag{2.46}$$

whereas the correlation factor for the Gaussian-distributed coherent states is given in SNU by, respectively, the following matrices

$$\begin{aligned} Z^{\mathrm{Gaus}} &= \sqrt{\sigma^4_{\hat{q}} - 1} \\ &= \sqrt{\left(\sigma^2_{\hat{\mathrm{A}}} + 1\right)^2 - 1} \\ &= \sqrt{\sigma^4_{\hat{\mathrm{A}}} + 2\sigma^2_{\hat{\mathrm{A}}}} \\ &= \sqrt{\sigma^2_{\hat{\mathrm{A}}} \left(\sigma^2_{\hat{\mathrm{A}}} + 2\right)} \qquad \text{[SNU]}, \end{aligned} \tag{2.47}$$

which closely approximates that of the discrete modulation scheme for small variances [50]. Plugging Equation (2.47) in Equation (2.43) gives

$$\Gamma_{\mathrm{AB}}^{\mathrm{Gaus}} = \begin{bmatrix} \left(\sigma_{\hat{\mathrm{A}}}^2 + 1\right) \cdot I_2 & \sqrt{T_{\mathrm{tot}} \cdot \sigma_{\hat{\mathrm{A}}}^2 \left(\sigma_{\hat{\mathrm{A}}}^2 + 2\right)} \cdot \sigma_z \\ \sqrt{T_{\mathrm{tot}} \cdot \sigma_{\hat{\mathrm{A}}}^2 \left(\sigma_{\hat{\mathrm{A}}}^2 + 2\right)} \cdot \sigma_z & \left[1 + T_{\mathrm{tot}} \sigma_{\hat{\mathrm{A}}}^2 + \xi_{\mathrm{tot}}\right] \cdot I_2 \end{bmatrix} \quad [\mathrm{SNU}]. \tag{2.48}$$

The post-measurement state for the homodyne and heterodyne cases are given by [37]

$$\Gamma_{\mathrm{AB|b}}^{\mathrm{Hom}} = \begin{bmatrix} \left(\sigma_{\hat{\mathrm{A}}}^2 + 1 - \frac{\sigma_{\hat{\mathrm{A}}}^2 \left(\sigma_{\hat{\mathrm{A}}}^2 + 2\right)}{T_{\mathrm{tot}} \left(\sigma_{\hat{\mathrm{A}}}^2 + \xi\right) + 1}\right) \cdot I_2 & 0 \\ 0 & \left(\sigma_{\hat{\mathrm{A}}}^2 + 1\right) \cdot I_2 \end{bmatrix} \quad [\mathrm{SNU}], \tag{2.49}$$

$$\Gamma_{\mathrm{AB|b}}^{\mathrm{Het}} = \begin{bmatrix} \left(\sigma_{\hat{\mathrm{A}}}^2 + 1 - \frac{\sigma_{\hat{\mathrm{A}}}^2 \left(\sigma_{\hat{\mathrm{A}}}^2 + 2\right)}{T_{\mathrm{tot}} \left(\sigma_{\hat{\mathrm{A}}}^2 + \xi\right) + 2}\right) \cdot I_2 & 0 \\ 0 & \left(\sigma_{\hat{\mathrm{A}}}^2 + 1 - \frac{\sigma_{\hat{\mathrm{A}}}^2 \left(\sigma_{\hat{\mathrm{A}}}^2 + 2\right)}{T_{\mathrm{tot}} \left(\sigma_{\hat{\mathrm{A}}}^2 + \xi\right) + 2}\right) \cdot I_2 \end{bmatrix} \quad [\mathrm{SNU}]. \tag{2.50}$$

2.3.2 Security Under Collective Attacks

The secret key fraction (SKF) is defined as following

$$R_{\mathrm{SK}} \equiv \frac{N_{\mathrm{sec}}}{N_{\mathrm{exch}}}, \tag{2.51}$$

where N_{sec} and N_{exch} are the number of obtained secure bits and exchanged quantum states, respectively. For Gaussian-modulated states, the SKF in the asymptotic limit against collective attacks is given by

$$R_{\mathrm{SK}}^{\mathrm{CA}} = I(A : B) - S(B : E), \tag{2.52}$$

where $I(A : B)$ is the Shannon mutual information between the classical data of Alice and Bob after error correction, and $S(B : E)$ is the Holevo bound between Eve's quantum state and Bob's error-corrected classical data. The Holevo bound is an upper limit on the amount of classical information that Eve can extract from the quantum system. Security against collective attacks entails that Eve's capability is limited only by quantum mechanics. In practice, the error correction procedure is not perfect and is quantified by

the reconciliation efficiency (β) as following

$$R_{\mathrm{SK}}^{\mathrm{CA,\ prac}} = \beta I(A:B) - S(B:E). \tag{2.53}$$

From Equation (2.48), the quadrature operators variance at Bob's side is

$$\sigma^2_{\hat{q}_{\mathrm{B}}} = \underbrace{T_{\mathrm{tot}}\sigma^2_{\hat{\mathrm{A}}}}_{\text{Signal}} + \underbrace{1+\xi_{\mathrm{tot}}}_{\text{Noise}} \qquad [\mathrm{SNU}], \tag{2.54}$$

where the signal and noise components are accordingly labeled. Therefore, the signal-to-noise ratio (SNR) is

$$\mathrm{SNR} = \frac{T_{\mathrm{tot}}\sigma^2_{\hat{\mathrm{A}}}}{1+\xi_{\mathrm{tot}}}. \tag{2.55}$$

For heterodyne measurement, the Shannon mutual information is given by

$$\begin{aligned} I(A:B) &= \log_2(1+\mathrm{SNR}) \\ &= \log_2\left(1+\frac{T_{\mathrm{tot}}\sigma^2_{\hat{\mathrm{A}}}}{1+\xi_{\mathrm{tot}}}\right), \end{aligned} \tag{2.56}$$

which is twice that of the homodyne case.

The Holevo information for discrete-modulated CV-QKD can be upper bounded by utilizing the fact that the Holevo bound is maximized for Gaussian states. Therefore, security proofs for Gaussian modulation can be used to prove the security of discrete-modulated CV-QKD given that the signal power does not exceed a few SNUs [45]. The binary entropy is defined as

$$g(x) = \left(\frac{x+1}{2}\right)\log_2\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log_2\left(\frac{x-1}{2}\right), \tag{2.57}$$

which is used to compute the Holevo bound as following

$$S(B:E) = g(\nu_1) + g(\nu_2) - g(\nu_3), \tag{2.58}$$

where ν_1, ν_2, and ν_3 are the symplectic eigenvalues of the covariance matrix (Γ_{AB}^{Gaus}) in Equation (2.48). To estimate the SKF, a simple form for the total excess noise (ξ_{tot}) is defined as follows[10]

$$\xi_{tot} = T_{tot} \cdot \xi_{exc} + \xi_{el} \qquad [SNU], \tag{2.59}$$

and the following parameters are assumed for heterodyne measurement:

- $\alpha_{ch} = 0.25$ dB/km,
- $\xi_{exc} = 0.05$ SNU,
- $\xi_{el} = 0.15$ SNU,
- $\eta_{det} = 0.7$,
- $\beta = 0.85$,

where the resulting SKFs for difference channel lengths and signal powers are visualized in Figure 2.8.

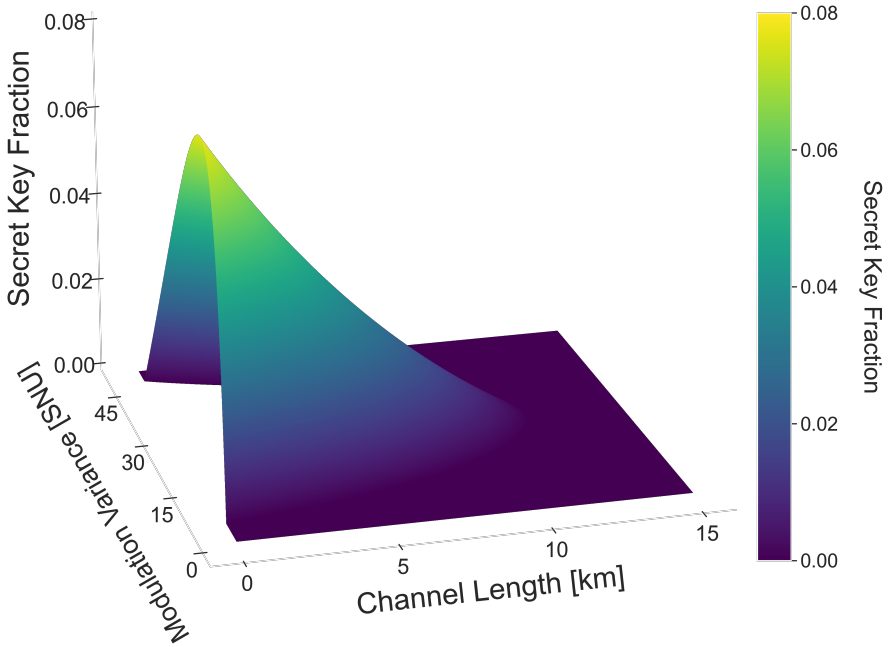


Figure 2.8: A 3D heatmap depicting the secret key fraction (SKF) as a function of the modulation variance ($\sigma^2_{\hat{A}}$) and channel length. Each channel length has a corresponding optimal signal power.

[10]The sources of noise in a practical settings are analyzed in Chapter 4.

In practice, the modulation variance ($\sigma^2_{\hat{A}}$) needs to be optimized for each channel length to achieve the best system performance. Moreover, limiting the excess noise (ξ_{exc}) is essential to operate the system at long channel lengths. Since the formulated security proofs is for the continuous-modulated CV-QKD, care must be taken when setting the symbol power for the discrete modulation case. In [51], it was illustrated that the security of quadrature phase-shift keying (QPSK)-modulated CV-QKD matches the Gaussian modulation case for modulation variances not exceeding 1.5 SNU, given an excess noise $\xi_{\text{exc}} = 0.001$ SNU. This corresponds to around 0.75 photons/symbol for 50 MBd symbol rate. Therefore, the maximum power for the targeted QPSK-modulated CV-QKD system should be limited depending on the excess noise (ξ_{exc}) and the channel transmittance (T_{tot}). Alternatively, the security framework by [44] may be utilized, where a MATLAB package was developed.

CHAPTER 3

COHERENT OPTICAL COMMUNICATION FUNDAMENTALS

The first conceived optical communication links used what is known as the intensity-modulation and direct-detection (IM/DD) scheme, where the information is encoded solely in the intensity degree of freedom of light, like in the on-off keying (OOK) modulation format. With the advancement of the available hardware, schemes utilizing a higher bandwidth with other degrees of freedom (e.g., phase or polarization) were possible. Such methods that use complex signals to transmit information fall under a communication class known as coherent optical communication.

Classical coherent optical communication technologies can improve the performance of CV-QKD systems in more than one way. By applying a filter on the transmitted signal, classical coherent optical communication makes better use of the available bandwidth. With some modification, a similar outcome can be achieved for CV-QKD. Moreover, compensation for different channel effects can be incorporated into CV-QKD systems with techniques typically used in classical coherent optical communication. The ability to compensate for channel effect and utilize the available bandwidth more efficiently allows for a higher rate CV-QKD implementation.

3.1 COHERENT OPTICAL DETECTION

A coherent communication system uses a laser to generate an optical carrier signal modulated with the information transmitted using an in-phase and quadrature (I/Q) modulator. As discussed in Appendix C, the I/Q modulator consists of two Mach–Zehnder interferometers (MZIs) that are controlled by electrical signals representing the amplitude and phase information of the modulating signal. Then, the modulated signal is transmitted

over the optical channel to the receiver, where it is detected and digitally processed to recover the original information.

3.1.1 Balanced Receivers

180° Optical Hybrid

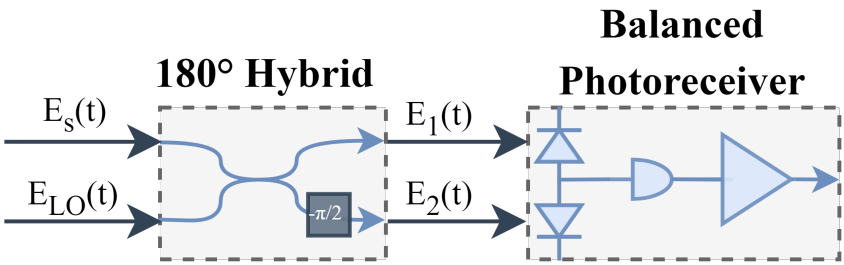


Figure 3.1: Coherent receiver configuration for the 180° hybrid.

Coherent detection allows for measuring the complex amplitude of an optical signal mixed with a continuous-wave (CW) local oscillator (LO) as shown in Figure 3.1. The electric fields of the incoming signal of interest (E_s) and the LO signal (E_LO) can be expressed in phasor representation as

$$E_\mathrm{s}(t) = A_\mathrm{s}(t)e^{j[\omega_\mathrm{s}t+\theta_\mathrm{s}(t)]}, \tag{3.1}$$

$$E_\mathrm{LO}(t) = A_\mathrm{LO}e^{j[\omega_\mathrm{LO}t+\theta_\mathrm{LO}(t)]}, \tag{3.2}$$

where $A_\mathrm{s}(t)$ and A_LO are the real-valued complex amplitudes, ω_s and ω_LO are the angular frequencies, whereas $\theta_\mathrm{s}(t)$ and $\theta_\mathrm{LO}(t)$ represent the unknown phase noise. Note that the amplitude of the LO (A_LO) is kept constant. The real signals are

$$\begin{aligned}\mathbb{E}_\mathrm{s}(t) &= \mathrm{Re}\left\{A_\mathrm{s}(t)e^{j[\omega_\mathrm{s}t+\theta_\mathrm{s}(t)]}\right\} \\ &= A_\mathrm{s}(t)\cos[\omega_\mathrm{s}t+\theta_\mathrm{s}(t)],\end{aligned} \tag{3.3}$$

$$\begin{aligned}\mathbb{E}_\mathrm{LO}(t) &= \mathrm{Re}\left\{A_\mathrm{LO}e^{j[\omega_\mathrm{LO}t+\theta_\mathrm{LO}(t)]}\right\} \\ &= A_\mathrm{LO}\cos[\omega_\mathrm{LO}t+\theta_\mathrm{LO}(t)].\end{aligned} \tag{3.4}$$

The power of the signals is taken to be their mean square (MS) values[1] as following

$$\begin{aligned} P_{\mathrm{s}}(t) &= [\mathbb{E}_{\mathrm{s}}(t)]^{\mathrm{MS}} \\ &= \frac{A_{\mathrm{s}}(t)^2}{2}, \end{aligned} \tag{3.5}$$

$$\begin{aligned} P_{\mathrm{LO}} &= [\mathbb{E}_{\mathrm{LO}}(t)]^{\mathrm{MS}} \\ &= \frac{A_{\mathrm{LO}}^2}{2}. \end{aligned} \tag{3.6}$$

The 2×2 3-dB optical coupler is a four-terminal device with the following scattering matrix [52]

$$\mathbb{T}_{2\times 2} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & j \\ j & 1 \end{bmatrix}, \tag{3.7}$$

where the cross-coupling components ($= j$) are phase shifted by 90° with respect to the direct pass components ($= 1$). To construct a 180° optical hybrid, a −90° phase shifter is added to the bottom arm. Utilizing the transfer matrix in Equation (3.7), the output ports in Figure 3.1 are given by

$$\begin{aligned} E_1(t) &= \frac{1}{\sqrt{2}} \left[E_{\mathrm{s}}(t) + jE_{\mathrm{LO}}(t)\right] \\ &= \frac{1}{\sqrt{2}} \left\{A_{\mathrm{s}}(t)e^{j[\omega_{\mathrm{s}}t+\theta_{\mathrm{s}}(t)]} + A_{\mathrm{LO}}e^{j[\omega_{\mathrm{LO}}t+\theta_{\mathrm{LO}}(t)+\frac{\pi}{2}]}\right\}, \end{aligned} \tag{3.8}$$

$$\begin{aligned} E_2(t) &= \frac{1}{\sqrt{2}} \left[jE_{\mathrm{s}}(t) + E_{\mathrm{LO}}(t)\right] \cdot e^{-\frac{\pi}{2}} = \frac{1}{\sqrt{2}} \left[E_{\mathrm{s}}(t) - jE_{\mathrm{LO}}(t)\right] \\ &= \frac{1}{\sqrt{2}} \left\{A_{\mathrm{s}}(t)e^{j[\omega_{\mathrm{s}}t+\theta_{\mathrm{s}}(t)]} + A_{\mathrm{LO}}e^{j[\omega_{\mathrm{LO}}t+\theta_{\mathrm{LO}}(t)-\frac{\pi}{2}]}\right\}. \end{aligned} \tag{3.9}$$

Note that $E_1(t)$ and $E_2(t)$ have a relative phase shift of 180°, which explains the naming of the structure in Figure 3.1. The ratio of the generated photocurrent (I_{ph}) to the incident

[1] The MS of a signal $f(t)$ with period T is defined as

$$[f(t)]^{\mathrm{MS}} = \frac{1}{T}\int_0^T f(t)^2 dt.$$

power (P_{inc}) defines the responsivity (R) of a photodiode as [52]

$$\begin{aligned} R &= \frac{I_{\text{ph}}}{P_{\text{inc}}} \\ &= \eta \frac{e}{\hbar \omega_{\text{inc}}}, \end{aligned} \tag{3.10}$$

where η is the photodiode quantum efficiency, e is the electron charge, $\hbar$ is the reduced Planck's constant, and ω_{inc} is the angular frequency of the incident signal. When $E_1(t)$ and $E_2(t)$ are incident on the photodiodes, the generated photocurrents are

$$\begin{aligned} I_1(t) &= RP_1(t) \\ &= R\left[\mathbb{E}_1(t)\right]^{\text{MS}}, \end{aligned} \tag{3.11}$$

$$\begin{aligned} I_2(t) &= RP_2(t) \\ &= R\left[\mathbb{E}_2(t)\right]^{\text{MS}}, \end{aligned} \tag{3.12}$$

where the real signals are given by

$$\begin{aligned} \mathbb{E}_1(t) &= \text{Re}\left[E_1(t)\right] \\ &= \frac{1}{\sqrt{2}}\left[A_{\text{s}}(t)\cos\left(\omega_{\text{s}}t + \theta_{\text{s}}(t)\right) + A_{\text{LO}}\cos\left(\omega_{\text{LO}}t + \theta_{\text{LO}}(t) + \frac{\pi}{2}\right)\right] \\ &= \frac{1}{\sqrt{2}}\left[A_{\text{s}}(t)\cos\left(\omega_{\text{s}}t + \theta_{\text{s}}(t)\right) - A_{\text{LO}}\sin\left(\omega_{\text{LO}}t + \theta_{\text{LO}}(t)\right)\right], \end{aligned} \tag{3.13}$$

$$\begin{aligned} \mathbb{E}_2(t) &= \text{Re}\left[E_2(t)\right] \\ &= \frac{1}{\sqrt{2}}\left[A_{\text{s}}(t)\cos\left(\omega_{\text{s}}t + \theta_{\text{s}}(t)\right) + A_{\text{LO}}\cos\left(\omega_{\text{LO}}t + \theta_{\text{LO}}(t) - \frac{\pi}{2}\right)\right] \\ &= \frac{1}{\sqrt{2}}\left[A_{\text{s}}(t)\cos\left(\omega_{\text{s}}t + \theta_{\text{s}}(t)\right) + A_{\text{LO}}\sin\left(\omega_{\text{LO}}t + \theta_{\text{LO}}(t)\right)\right]. \end{aligned} \tag{3.14}$$

which results in the following photocurrents[2]

$$\begin{aligned} I_1(t) &= \frac{R}{2}\left[A_s(t)^2 + A_{LO}^2 \right. \\ &\qquad \left. - 2A_{LO}A_s(t)\cos\left(\omega_s t + \theta_s(t)\right)\sin\left(\omega_{LO}t + \theta_{LO}(t)\right)\right] \\ &= \frac{R}{2}\left\{A_s(t)^2 + A_{LO}^2 - A_{LO}A_s(t)\left[\sin\left((\omega_{LO} - \omega_s)t + \theta_{LO}(t) - \theta_s(t)\right)\right.\right. \\ &\qquad \left.\left. + \sin\left(\left(\omega_{LO} + \omega_s\right)t + \theta_{LO}(t) + \theta_s(t)\right)\right]\right\} \\ &= \frac{R}{2}\left[A_s(t)^2 + A_{LO}^2 - A_{LO}A_s(t)\sin\left(\omega_{IF}t + \Delta\theta(t)\right)\right], \end{aligned} \tag{3.15}$$

and similarly

$$I_2(t) = \frac{R}{2}\left[A_s(t)^2 + A_{LO}^2 + A_{LO}A_s(t)\sin\big(\omega_{IF}t + \Delta\theta(t)\big)\right], \tag{3.16}$$

where $\omega_{IF} \equiv \omega_{LO} - \omega_s$ is the intermediate frequency (IF) and $\Delta\theta(t) \equiv \theta_{LO}(t) - \theta_s(t)$. The omitted high-frequency component corresponds to the sum-frequency term, usually filtered out by the subsequent radio frequency (RF) circuit. In order to eliminate the DC component, the photodiodes are connected in a balanced configuration, generating a current ($I(t)$) given by their difference

$$\begin{aligned} I(t) &= I_1(t) - I_2(t) \\ &= -RA_{LO}A_s(t)\sin\big(\omega_{IF}t + \Delta\theta(t)\big). \end{aligned} \tag{3.17}$$

90° Optical Hybrid

Another configuration for balanced detection is the 90° hybrid which utilizes four 3-dB couplers and a 90° phase shifter as shown in Figure 3.2. The scattering matrix of the

[2]The MS is applied on single-tone components. For the mixing terms, direct multiplication is performed.

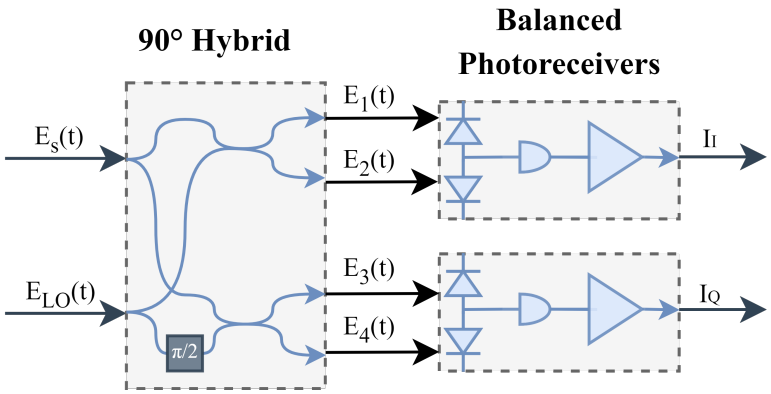


Figure 3.2: Coherent receiver configuration for the 90° hybrid.

configuration is as follows

$$\begin{aligned}\mathbb{T}_{4\times4} &= \begin{bmatrix} \mathbb{T}_{2\times2} & 0 \\ 0 & \mathbb{T}_{2\times2} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & j & 0 \end{bmatrix} \begin{bmatrix} \mathbb{T}_{2\times2} & 0 \\ 0 & \mathbb{T}_{2\times2} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbb{T}_{2\times2} & 0 \\ 0 & \mathbb{T}_{2\times2} \end{bmatrix} \begin{bmatrix} 1 & j & 0 & 0 \\ 0 & 0 & j & 1 \\ j & 1 & 0 & 0 \\ 0 & 0 & j & -1 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 & j & -1 & j \\ j & -1 & j & 1 \\ j & 1 & -1 & -j \\ -1 & j & j & -1 \end{bmatrix}. \end{aligned} \tag{3.18}$$

The corresponding outputs of the structure are

$$\begin{bmatrix} E_1(t) \\ E_2(t) \\ E_3(t) \\ E_4(t) \end{bmatrix} = \mathbb{T}_{4\times4} \begin{bmatrix} E_s(t) \\ 0 \\ E_{LO}(t) \\ 0 \end{bmatrix}, \tag{3.19}$$

which results in the following expressions when evaluated

$$E_1(t) = \frac{1}{2}\left[E_s(t) - E_{LO}(t)\right], \tag{3.20}$$

$$E_2(t) = \frac{j}{2}\left[E_s(t) + E_{LO}(t)\right], \tag{3.21}$$

$$E_3(t) = \frac{j}{2}\left[E_s(t) + jE_{LO}(t)\right], \tag{3.22}$$

$$E_4(t) = -\frac{1}{2}\left[E_s(t) - jE_{LO}(t)\right], \tag{3.23}$$

with the real representations being

$$\begin{aligned}\mathbb{E}_1(t) &= \mathrm{Re}[E_1(t)] \\ &= \frac{1}{2}\left[A_s(t)\cos\left(\omega_s t + \theta_s(t)\right) - A_{LO}\cos\left(\omega_{LO} t + \theta_{LO}(t)\right)\right],\end{aligned} \tag{3.24}$$

$$\begin{aligned}\mathbb{E}_2(t) &= \mathrm{Re}[E_2(t)] \\ &= -\frac{1}{2}\left[A_s(t)\sin\left(\omega_s t + \theta_s(t)\right) + A_{LO}\sin\left(\omega_{LO} t + \theta_{LO}(t)\right)\right],\end{aligned} \tag{3.25}$$

$$\begin{aligned}\mathbb{E}_3(t) &= \mathrm{Re}[E_3(t)] \\ &= -\frac{1}{2}\left[A_s(t)\sin\left(\omega_s t + \theta_s(t)\right) + A_{LO}\cos\left(\omega_{LO} t + \theta_{LO}(t)\right)\right],\end{aligned} \tag{3.26}$$

$$\begin{aligned}\mathbb{E}_4(t) &= \mathrm{Re}[E_4(t)] \\ &= -\frac{1}{2}\left[A_s(t)\cos\left(\omega_s t + \theta_s(t)\right) + A_{LO}\sin\left(\omega_{LO} t + \theta_{LO}(t)\right)\right],\end{aligned} \tag{3.27}$$

and the corresponding photocurrents are

$$\begin{aligned}I_1(t) &= R\left[\mathbb{E}_1(t)\right]^{\mathrm{MS}} \\ &= \frac{R}{4}\Big[A_s(t)^2 + A_{LO}^2 \\ &\qquad - 2A_s(t)A_{LO}\cos\big(\omega_s t + \theta_s(t)\big)\cos\big(\omega_{LO} t + \theta_{LO}(t)\big)\Big],\end{aligned} \tag{3.28}$$

$$\begin{aligned}I_2(t) &= R\left[\mathbb{E}_2(t)\right]^{\mathrm{MS}} \\ &= \frac{R}{4}\Big[A_s(t)^2 + A_{LO}^2 \\ &\qquad + 2A_s(t)A_{LO}\sin\big(\omega_s t + \theta_s(t)\big)\sin\big(\omega_{LO} t + \theta_{LO}(t)\big)\Big],\end{aligned} \tag{3.29}$$

$$
\begin{aligned}
I_3(t) &= R\,[\mathbb{E}_3(t)]^{\mathrm{MS}} \\
&= \frac{R}{4}\Big[A_{\mathrm{s}}(t)^2 + A_{\mathrm{LO}}^2 \\
&\qquad + 2A_{\mathrm{s}}(t)A_{\mathrm{LO}}\sin\big(\omega_{\mathrm{s}}t + \theta_{\mathrm{s}}(t)\big)\cos\big(\omega_{\mathrm{LO}}t + \theta_{\mathrm{LO}}(t)\big)\Big],
\end{aligned}
\tag{3.30}
$$

$$
\begin{aligned}
I_4(t) &= R\,[\mathbb{E}_4(t)]^{\mathrm{MS}} \\
&= \frac{R}{4}\Big[A_{\mathrm{s}}(t)^2 + A_{\mathrm{LO}}^2 \\
&\qquad + 2A_{\mathrm{s}}(t)A_{\mathrm{LO}}\cos\big(\omega_{\mathrm{s}}t + \theta_{\mathrm{s}}(t)\big)\sin\big(\omega_{\mathrm{LO}}t + \theta_{\mathrm{LO}}(t)\big)\Big].
\end{aligned}
\tag{3.31}
$$

Thus, the output currents in Figure 3.2 are[3]

$$
\begin{aligned}
I_I(t) &= I_1(t) - I_2(t) \\
&= -\frac{RA_{\mathrm{s}}(t)A_{\mathrm{LO}}}{2}\cos\big(\omega_{\mathrm{IF}}t + \Delta\theta(t)\big),
\end{aligned}
\tag{3.32}
$$

$$
\begin{aligned}
I_Q(t) &= I_3(t) - I_4(t) \\
&= -\frac{RA_{\mathrm{s}}(t)A_{\mathrm{LO}}}{2}\sin\big(\omega_{\mathrm{IF}}t + \Delta\theta(t)\big),
\end{aligned}
\tag{3.33}
$$

which represents the I/Q components of the photocurrent.

3.1.2 Regimes of Operation

Let the bandwidth of the incoming signal ($E_{\mathrm{s}}(t)$) be B_{s}. Then, three possible operation regimes are the homodyne, heterodyne, and intradyne.[4]

Homodyne

Homodyne detection refers to the condition $\omega_{\mathrm{IF}} = 0$. For the 180° hybrid, the photocurrent in Equation (3.17) becomes

$$
I(t) = -RA_{\mathrm{LO}}A_{\mathrm{s}}(t)\sin\big(\Delta\theta(t)\big),
\tag{3.34}
$$

[3] The trigonometric identities $2\cos(\alpha)\cos(\beta) = \cos(\alpha-\beta) + \cos(\alpha+\beta)$, $2\sin(\alpha)\sin(\beta) = \cos(\alpha-\beta) - \cos(\alpha+\beta)$, and $2\sin(\alpha)\cos(\beta) = \sin(\alpha-\beta) - \sin(\alpha+\beta)$ were used.

[4] In the CV-QKD literature, the case when using a 180° hybrid with $\omega_{\mathrm{IF}} = 0$ is known as *homodyne* detection. For all the other cases, where both quadratures are simultaneously measured, they are referred to as *heterodyne* detection [15].

which represents the imaginary part of the signal. Consequently, the incoming signal's quadrature (Q) component is known. In order to measure the in-phase (I) component, a phase shift of $\pi/2$ has to be introduced. In other words, depending on the chosen phase, only one quadrature can be measured in the 180° hybrid structure. On the other hand, both quadratures of the incoming signal can be measured in the 90° hybrid configuration. In order to realize the homodyne regime, the phases of the incoming signal and the reference laser have to be synchronized using an optical phase-locked loop (OPLL). The OPLL is generally complex to implement [53], making it not desirable to operate the receiver in the homodyne regime.

Heterodyne

When the signal and LO are not derived from the same source, the detection is said to be heterodyne. For the case when $|\omega_{\mathrm{IF}}| > B_{\mathrm{s}}/2$, as illustrated in Figure 3.3, the whole spectrum is accessible by both optical hybrid structures, making it possible for both quadratures to be simultaneously measured. The downside of this regime is that the uncertainty principle limits the information gained in simultaneously measuring the two quadratures and the noise acquired when downsampling the signal to the baseband [54].

In the range where $0 < |\omega_{\mathrm{IF}}| < B_{\mathrm{s}}/2$, the positive and negative images of the signal partially overlap, necessitating the use of information from both quadratures for signal retrieval. In this scenario, the 90° hybrid becomes essential as it enables the recovery of complete signal information, whereas the 180° hybrid only provides one quadrature. A notable advantage of this regime is that it eliminates the need for an OPLL, leveraging DSP techniques to compensate for any frequency offset. This makes it an optimal choice for signal processing.

The homodyne operation regime is the current popular choice in coherent optical communication[55]. The signal and LO originate from the same laser in this work. Thus, their frequencies should be matched in an ideal situation indicating a homodyne

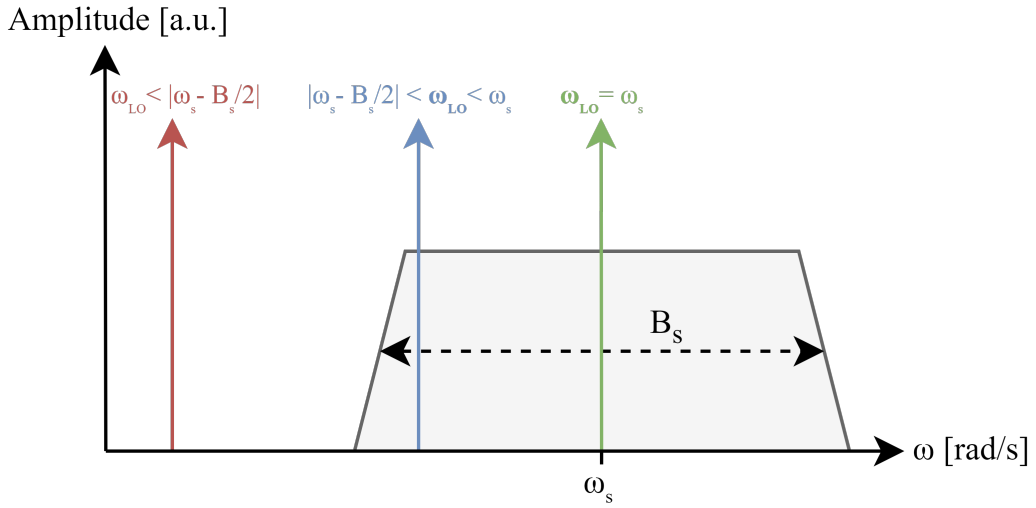


Figure 3.3: The operation regimes based on the relationship between ω_{IF} and the bandwidth B_{s} of the incoming signal. The green color represents the homodyne regime, while the remaining two cases depict different scenarios within the heterodyne regime.

operation regime. However, slight frequency drifts and the different propagation path lengths can cause the operation to be in the heterodyne regime.

3.2 DIGITAL SIGNAL PROCESSING (DSP)

The utilized signal processing stack is shown in Figure 3.4, where each block will be elaborated on in the following subsections.

3.2.1 Modulation

Quantum Signal

As discussed in Section 2.2, the discrete modulation schemes are implemented for the quantum signal. Specifically, M-ary phase-shift keying (M-PSK) and M-ary quadrature amplitude modulation (M-QAM) with probabilistic constellation shaping (PCS) are chosen. The M-PSK coherent states are given by

$$|\psi_{\text{M-PSK}}\rangle = \left|\alpha e^{j(2k+1)\pi/M}\right\rangle, \tag{3.35}$$

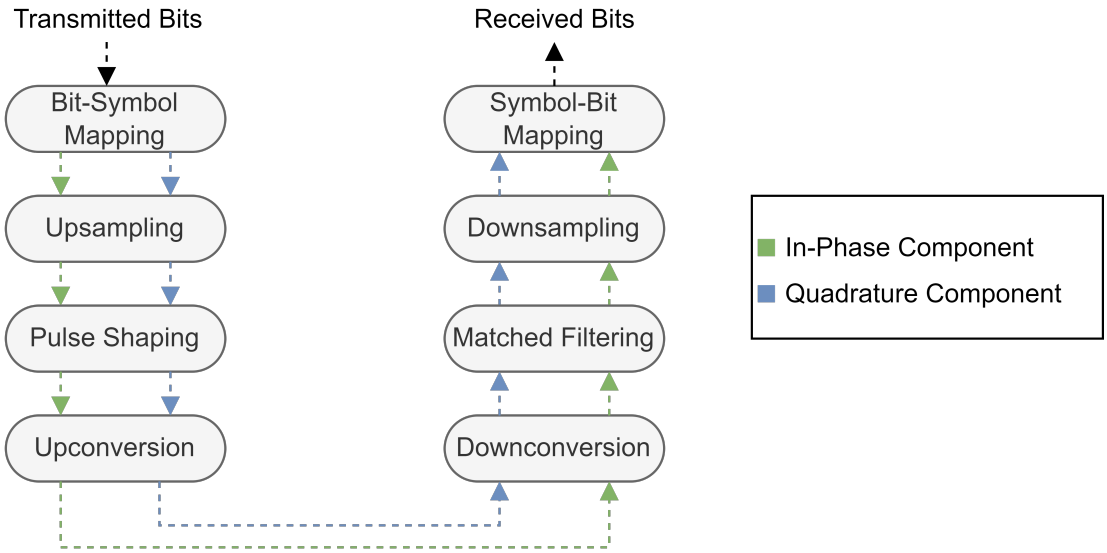


Figure 3.4: The signal processing suite at used at the transmitter (Tx) and receiver (Rx).

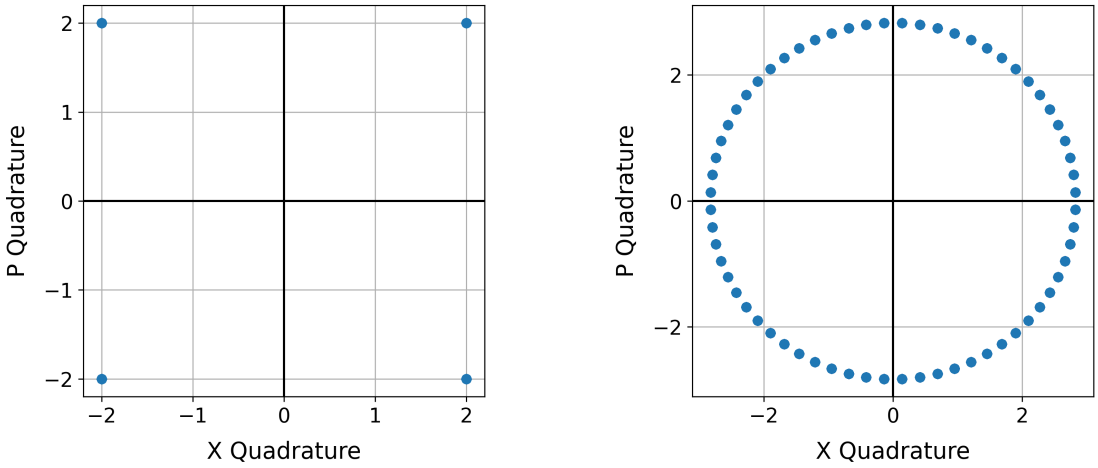
where $k \in \{0, 1, \cdots, M-1\}$, M is the number of used symbols, and α is the coherent state amplitude whose magnitude-squared is given by Equation (2.42) as

$$\begin{aligned} |\alpha|^2 &= \langle n_s \rangle \\ &= \frac{\sigma_{A'}^2}{2} \\ &= 2\sigma_A^2, \end{aligned} \tag{3.36}$$

where $\sigma_{A'}^2$ and σ_A^2 are the modulation variance of the quadrature operator and variable, respectively, and $\langle n_s \rangle$ is the average number of photons of the signal. Without any noise, the constellation diagrams of the ideal M-PSK modulation are depicted in Figure 3.5. The density matrix of the M-PSK modulation is expressed as

$$\begin{aligned} \rho_{\text{M-PSK}} &= \frac{1}{M} \sum_{k=0}^{M-1} |\alpha_{\text{M-PSK}}\rangle \langle \alpha_{\text{M-PSK}}| \\ &= \frac{1}{M} \sum_{k=0}^{M-1} \left|\alpha e^{j(2k+1)\pi/M}\right\rangle \left\langle \alpha e^{j(2k+1)\pi/M}\right|. \end{aligned} \tag{3.37}$$

In M-QAM, the two quadratures need to be completely independent to prevent Eve from gaining information on one quadrature from the other. Thus, the constellation diagram



(a) 4-PSK (QPSK)

(b) 64-PSK

Figure 3.5: The constellation diagram of Alice's ideal M-PSK modulated quantum signal for (a) M = 4, known as QPSK, and (b) M = 64 with the quadrature variable variance being $\sigma_{\mathrm{A}}^2 = 4$, corresponding to $\alpha = 2\sqrt{2}$.

should be square-shaped, corresponding to M being a power of four. The M-QAM coherent states are expressed as

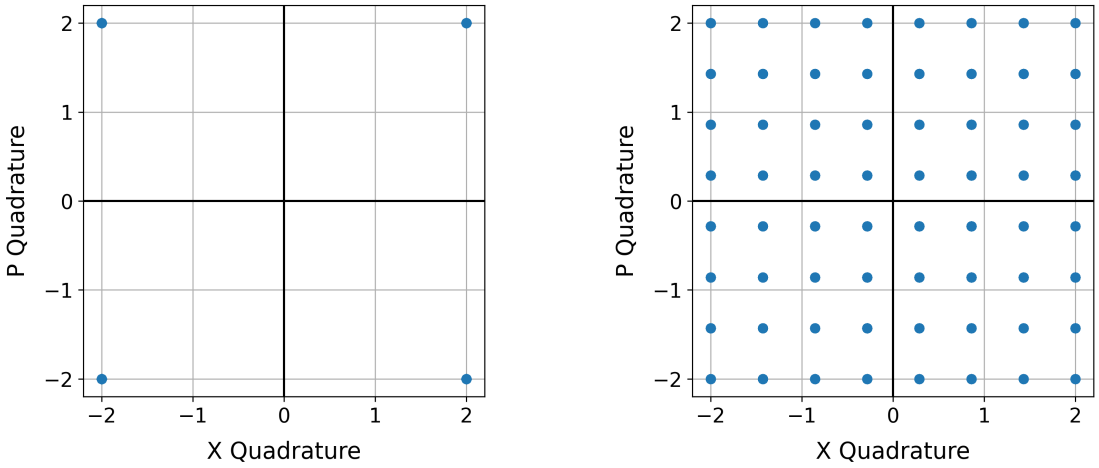
$$\left|\psi_{\text{M-QAM}}\right\rangle = \left|A_{\text{quad}}^{\max}\,(x + jp)\right\rangle, \tag{3.38}$$

where $A_{\text{quad}}^{\max} = \frac{\alpha}{\sqrt{2}}$ is the maximum amplitude a quadrature can have. Thus, the possible quadrature points x and p are normalized. Namely, $x,\ p \in \{-1, -1 + S, \cdots, 1 - S, 1\}$ for a spacing $S = \frac{2}{\sqrt{M}-1}$ between the coordinates. The ideal constellation diagrams of M-QAM are shown in Figure 3.6. Note that the 4-QAM is equivalent to the 4-phase-shift keying (PSK), also known as QPSK.

The independence of the two quadratures of M-QAM is expressed by the following probability mass function (PMF) relation

$$P_{X+jP}(x + jp) = P_X(x)P_P(p), \tag{3.39}$$

where $P_X(x)$ and $P_P(p)$ are the PMFs of the X and P quadratures, respectively. To approximate the continuous Gaussian states which possess the desired security aspects,



(a) 4-QAM (b) 64-QAM

Figure 3.6: The constellation diagram of Alice's ideal M-QAM modulated quantum signal for (a) M = 4 and (b) M = 64 with the quadrature variable variance being $\sigma_A^2 = 4$, corresponding to $\alpha = 2\sqrt{2}$.

the utilized PCS for the two quadratures is the discrete Boltzmann-Maxwell distribution with the following PMFs [56]

$$P_\nu(x) = \frac{e^{-\nu x^2}}{\sum_{x \in \mathcal{X}} e^{-\nu x^2}}, \tag{3.40}$$

where $\nu > 0$ is the free parameter. Thus, the PMFs of the M-QAM coherent state is expressed by

$$P_{X+jP}(x + jp) = \frac{e^{-\nu(x^2+p^2)}}{\sum_{x,\, p=-\frac{\sqrt{M}}{2}}^{\frac{\sqrt{M}}{2}} e^{-\nu(x^2+p^2)}}. \tag{3.41}$$

In practice, the free parameter ν is tuned to achieve optimal performance. The constellation diagram of the PCS 64-QAM following the discrete Boltzmann-Maxwell distribution is shown in Figure 3.7 for multiple values of ν. When $\nu = 0$, the PCS M-QAM reduces to the traditional M-QAM modulation since all the coordinates will have an equal probability.

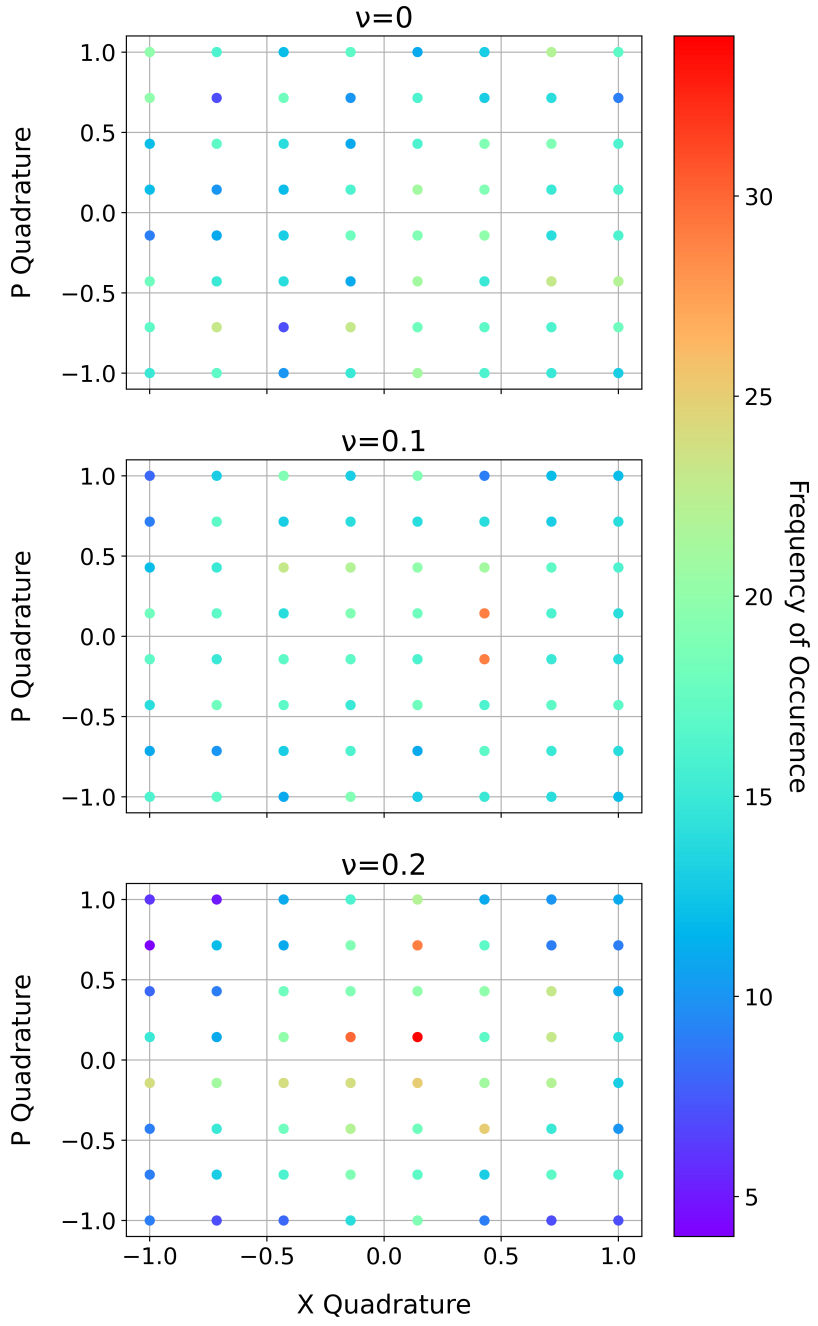


Figure 3.7: The constellation diagrams of 10^5 probabilistic constellation-shaped 64-QAM signals using different values for the free parameter (ν) with the quadrature variable variance being $\sigma_A^2 = 4$, corresponding to $\alpha = 2\sqrt{2}$.

Pilot Tone

As will be discussed in Section 5.1, a pilot tone is needed to establish a phase reference since the quantum signal is feeble. One scheme of generating the pilot is known as

single-sideband suppressed-carrier (SSB-SC) modulation. Since the same information is carried by both bands, suppressing the other band in single-sideband (SSB) modulation is spectrally and power efficient. Moreover, reducing the power results in less crosstalk between the quantum and pilot signals. Another advantage that SSB modulation offers is immunity against dispersion [57].

Furthermore, for the heterodyne regime of operation $\left(\left|f_{\mathrm{LO}} - f_{\mathrm{sig}}\right| < B_{\mathrm{sig}}/2\right)$, not suppressing the other band will result in RF fading since the two bands will self-interfere after being projected to almost the same RF frequency [30], [58], [59]. The crosstalk between the carrier and the quantum signal at the receiver can be eliminated using the suppressed-carrier (SC) technique [30], [58], which is implemented along with SSB, the so-called SSB-SC modulation. Suppressing the carrier would also enhance the pilot tone's SNR, a desirable outcome.

3.2.2 Upsampling

The initial form of the modulated signal is a series of values representing the symbols in the discrete-time domain. A QPSK modulated signal is obtained from 13,106 pseudorandomly generated bits that are mapped as displayed in Table 3.1.

Table 3.1: Followed convention in mapping the bits pair to the QPSK symbols.

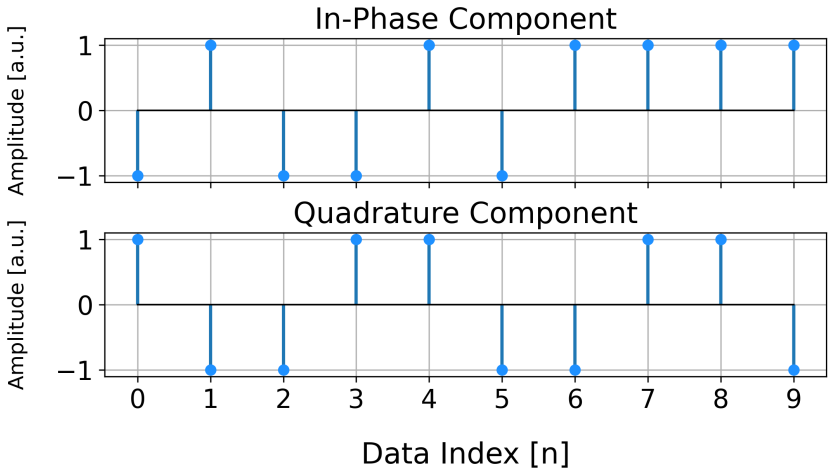
Bits	00	01	10	11
Symbol	-1-j	-1+j	1-j	1+j

The original discrete-time representation is shown in Figure 3.8 along with its normalized [5] and raw frequency responses. In practice, multiple samples represent each symbol through the upsampling operation. Considering that the original symbol period is $T_{\mathrm{sym}}^{\mathrm{orig}}$, the upsampling by L operation increases the symbol period to $T_{\mathrm{sym}}^{\mathrm{us}} = LT_{\mathrm{sym}}^{\mathrm{orig}}$.

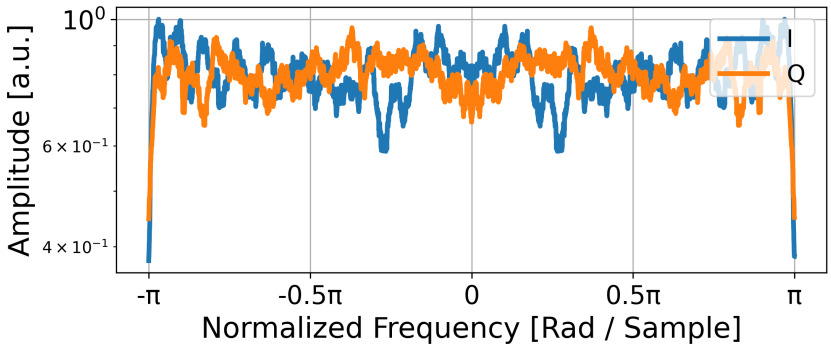
[5] The normalized frequency ω is related to the traditional raw frequency Ω by the following relation

$$\omega = \frac{\Omega}{f_{\mathrm{s}}^{\mathrm{Tx}}},$$

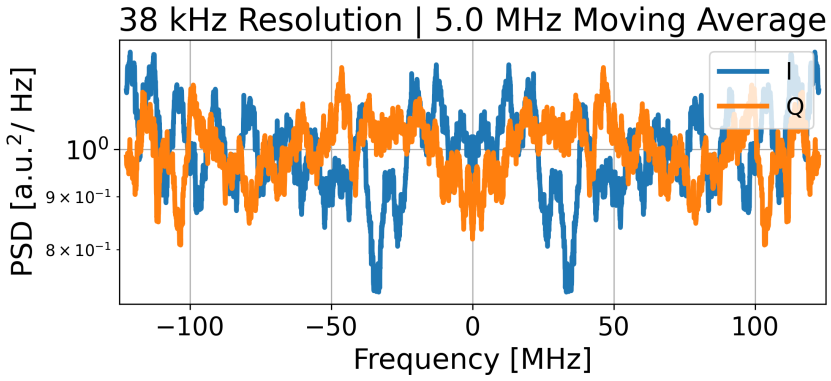
where $f_{\mathrm{s}}^{\mathrm{Tx}}$ is the sampling frequency of the DAC.



(a)



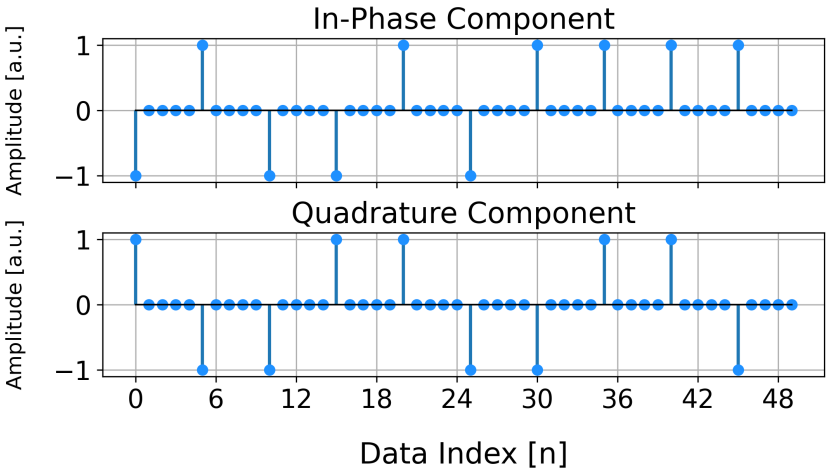
(b)



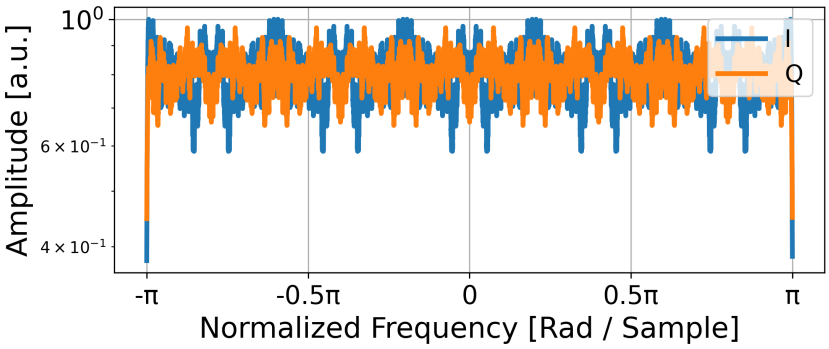
(c)

Figure 3.8: The (a) original discrete form of a random QPSK modulated signal for ten symbols, (b) its normalized frequency response, and (c) the raw frequency response assuming a sampling frequency $f_s^{\mathrm{Tx}} = 250$ MSa/s.

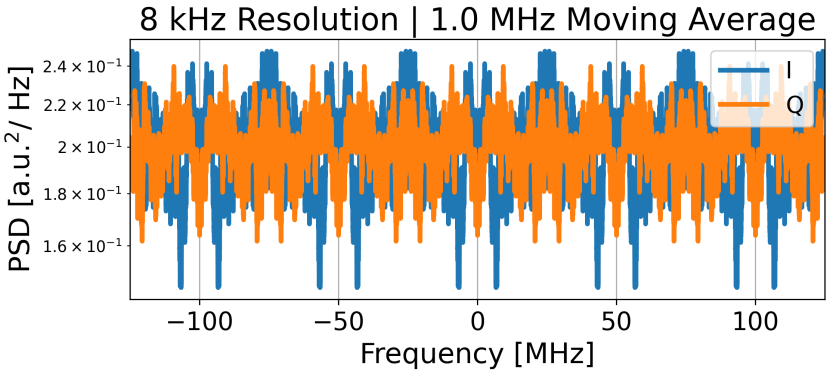
Equivalently, the original symbol rate $f_{\mathrm{sym}}^{\mathrm{orig}}$ is reduced to $f_{\mathrm{sym}}^{\mathrm{us}} = f_{\mathrm{sym}}^{\mathrm{orig}}/L$. To upsample a signal with a factor L, a two-step procedure is performed. First, zero-padding is



(a)



(b)



(c)

Figure 3.9: The first stage of the upsampling procedure involves zero-padding the modulated signal of Figure 3.8 in the time domain, as shown in (a). In contrast, (b) and (c) illustrate the frequency domain representation of the signal, highlighting the duplication of the original frequency component after being compressed.

implemented by inserting $L-1$ zeros between each two consecutive symbols. The zero-padding operation is represented by

$$x_{\text{zp}}[n] = \begin{cases} x_{\text{orig}}\left[\frac{n}{L}\right] & \text{for } n = kL,\ k \in \mathbb{Z}, \\ 0 & \text{otherwise,} \end{cases} \tag{3.42}$$

where x_{orig} and x_{zp} are the original and zero-padded versions of the signal, respectively. The zero-padded version of Alice's QPSK signal is shown in Figure 3.9 for $L = 5$. For a DAC with sampling frequency $f_{\text{s}}^{\text{Tx}} = 250$ MSa/s, the resulting symbol period is

$$\begin{aligned} T_{\text{sym}}^{\text{us}} &= L T_{\text{sym}}^{\text{orig}} \\ &= \frac{L}{f_{\text{s}}^{\text{Tx}}} \\ &= \frac{5}{250 \times 10^6} \\ &= 20 \quad \text{ns}, \end{aligned} \tag{3.43}$$

which corresponds to 50 MBd. The second stage of upsampling is an interpolation process, where the inserted zeros are given a value that depends on the neighboring samples using a filter. From the frequency domain perspective, each inserted zero results in an additional spectral image of the original signal, which must be filtered using a low-pass filter (LPF). The unwanted $L-1$ spectral images are omitted by setting the cutoff frequency of the LPF to $\omega_{\text{c}} = \frac{\pi}{L}$ [60]. In order to completely suppress the interference between channels utilizing neighboring frequency ranges, a phenomenon known as inter-carrier interference (ICI), the utilized LPF should have a rectangular-shaped spectrum. The frequency response of the ideal LPF is given by

$$H_{\text{LPF}}^{\text{ideal}}(\omega) = \begin{cases} 1 & \text{for } \omega \leq \omega_{\text{c}}, \\ 0 & \text{for } \omega > \omega_{\text{c}}, \end{cases} \tag{3.44}$$

which cannot be realistically implemented since it is an infinite impulse response (IIR) filter, requiring an infinite number of coefficients to realize it[6]. On the other

[6]The reason is that the inverse discrete-time Fourier transform (IDTFT) of the ideal LPF $H_{\text{LPF}}^{\text{ideal}}(\omega)$ is

hands, finite impulse response (FIR) filters are utilized in practice such as the one in Figure 3.10. Utilizing the LPF of Figure 3.10, upsampling is achieved after interpolating the zero-padded signal as shown in Figure 3.11.

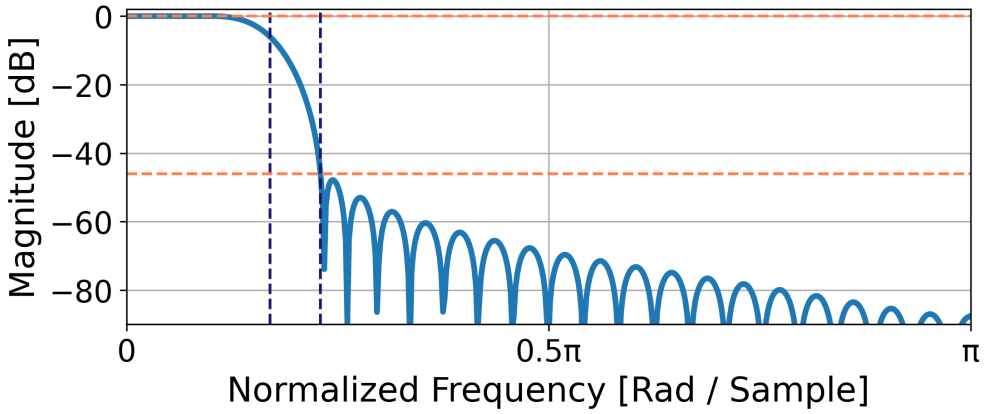


Figure 3.10: The frequency response of a finite impulse response (FIR) filter where $\omega_c \approx \frac{\pi}{5}$. The FIR filter was designed using the Kaiser–Bessel window method with the passband (PB) and stopband (SB) edges being 0.17π and 0.23π rad/sample, respectively.

3.2.3 Pulse Shaping

The time-domain analog to the ICI phenomenon is inter-symbol interference (ISI), where adjacent pulses interfere with each other due to their extending parts in the time-domain representation. For ISI suppression, a pulse-shaping filter is utilized to limit the pulse duration, which can be simultaneously used as an interpolator for the second stage of upsampling. The time-domain analog of the ideal LPF in Equation (3.44) will result in

a sinc function

$$\begin{aligned}
\mathcal{F}^{-1}\left\{H_{\text{LPF}}^{\text{ideal}}(\omega)\right\} &= \frac{1}{2\pi}\int_{-\pi}^{\pi} H_{\text{LPF}}^{\text{ideal}}(\omega)\, e^{j\omega n}\mathrm{d}\omega \\
&= \frac{1}{2\pi}\int_{-\omega_c}^{\omega_c} e^{j\omega n}\mathrm{d}\omega \\
&= \frac{1}{2\pi}\frac{e^{j\omega_c n} - e^{-j\omega_c n}}{jn} \\
&= \frac{\sin(\omega_c n)}{\pi n} \\
&= \frac{\omega_c}{\pi}\operatorname{sinc}(\omega_c n),
\end{aligned}$$

which is not absolutely summable since $\sum_{n=-\infty}^{\infty}\left|\frac{\omega_c}{\pi}\operatorname{sinc}(\omega_c n)\right| \not< \infty$.

ISI since the discrete-time Fourier transform (DTFT) of the ideal rectangular pulse is not absolutely summable [7]. Conversely, a rectangular pulse shape signal from an ideal pulse shaping filter, which does not cause any ISI, will result in ICI. A compromise between the two filter extremes is what is done in practice.

After the upsampling operation, each symbol is represented by L samples with a total duration of $T_{\text{sym}}^{\text{us}}$ as discussed in Section 3.2.2. The matched filter must correctly detect only a single sample on the receiver side where the ISI did not affect it. The remaining $L-1$ samples are permitted to be affected by ISI since they will be discarded [8]. Such filters, which tolerate ISI in specific regions, are said to satisfy the Nyquist ISI criterion. One widely used filter which satisfies the Nyquist ISI criterion is the raised-cosine (RC) filter. The following impulse response function defines the RC filter [60]

$$h_{\text{RC}}[n] = \begin{cases} 1, & \text{for } n = 0, \\ \frac{\pi}{4}\text{sinc}\left(\frac{\pi}{2\alpha}\right), & \text{for } |n| = \frac{L}{2\alpha}, \\ \text{sinc}\left(\frac{\pi n}{L}\right)\frac{\cos\left(\frac{\pi\alpha n}{L}\right)}{1-\left(\frac{2\alpha n}{L}\right)^2}, & \text{otherwise}, \end{cases} \tag{3.45}$$

[7] Similar to the previous analysis, the DTFT of the rectangular pulse violates the absolute summability condition

$$\begin{aligned} \mathcal{F}\{\Pi_N[n]\} &= \sum_{n=-\infty}^{\infty} \Pi_N[n]\, e^{-j\omega n} \\ &= \sum_{n=-N}^{N} e^{-j\omega n} \\ &= \frac{e^{j\omega N} - e^{-j\omega(N+1)}}{1-e^{-j\omega}} \\ &= \frac{\cancel{e^{-j\frac{\omega}{2}}}\left[e^{j\omega\left(N+\frac{1}{2}\right)} - e^{-j\omega\left(N+\frac{1}{2}\right)}\right]}{\cancel{e^{-j\frac{\omega}{2}}}\left(e^{j\frac{\omega}{2}} - e^{-j\frac{\omega}{2}}\right)} \\ &= \frac{\sin\left(\omega\left(N+\frac{1}{2}\right)\right)}{\sin\left(\frac{\omega}{2}\right)}, \end{aligned}$$

where the closed form of the geometric series was used

$$\sum_{n=n_{\text{i}}}^{n_{\text{f}}-1} r^n = \frac{r^{n_{\text{i}}} - r^{n_{\text{f}}}}{1-r}.$$

[8] The matched filter is discussed in Section 3.2.6.

where L'Hôpital's rule was used for the indeterminate cases and α is the roll-off factor (ROF), a measure of the excess bandwidth of the RC filter. In continuous-time representation, Equation (3.45) is expressed as

$$h_{\mathrm{RC}}(t) = \begin{cases} 1, & \text{for } t = 0, \\ \frac{\pi}{4}\mathrm{sinc}\left(\frac{\pi}{2\alpha}\right), & \text{for } |t| = \frac{T_{\mathrm{sym}}^{\mathrm{us}}}{2\alpha}, \\ \mathrm{sinc}\left(\frac{\pi t}{T_{\mathrm{sym}}^{\mathrm{us}}}\right) \frac{\cos\left(\frac{\pi \alpha t}{T_{\mathrm{sym}}^{\mathrm{us}}}\right)}{1-\left(\frac{2\alpha t}{T_{\mathrm{sym}}^{\mathrm{us}}}\right)^2}, & \text{otherwise.} \end{cases} \tag{3.46}$$

As evident from Figure 3.12, the RC filter satisfies the Nyquist ISI criterion. The output of the RC filter has a bandwidth of

$$B_{\mathrm{ps}} = (1 + \mathrm{ROF}) B_{\mathrm{orig}}. \tag{3.47}$$

In addition to the pulse shaping properties, the RC filter is simultaneously used as an LPF in the second stage of the upsampling operation. The frequency response of the RC filter is given by [60]

$$H_{\mathrm{RC}}(f) = \begin{cases} T_{\mathrm{sym}}^{\mathrm{us}}, & |f| \leq \frac{1-\alpha}{2T_{\mathrm{sym}}^{\mathrm{us}}}, \\ \frac{T_{\mathrm{sym}}^{\mathrm{us}}}{2}\left[1 + \cos\left(\frac{\pi T_{\mathrm{sym}}^{\mathrm{us}}}{\alpha}\left(|f| - \frac{1-\alpha}{2T_{\mathrm{sym}}^{\mathrm{us}}}\right)\right)\right], & \frac{1-\alpha}{2T_{\mathrm{sym}}^{\mathrm{us}}} < |f| \leq \frac{1+\alpha}{2T_{\mathrm{sym}}^{\mathrm{us}}}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.48}$$

The impulse and frequency responses for multiple ROF values is shown in Figure 3.13. At $\alpha = 0$, the RC filter becomes the ideal sinc filter of Equation (3.44). As will be explained in Section 3.2.6, in practice the RC filter is split into two equivalent filters known as root raised-cosine (RRC) filters. The RRC filter perform the functionality of the pulse shaping and matched filtering at the transmitter (Tx) and receiver (Rx), respectively. The result of passing the zero-padded signal through the RRC filter is

shown in Figure 3.14 which is obtained through the following convolution operation

$$\begin{aligned} x_{\text{ps}}[n] &= x_{\text{zp}}[n] * h_{\text{RRC}}[n] \\ &= \sum_{m=-\infty}^{\infty} x_{\text{zp}}[m]\, h_{\text{RRC}}[n-m]\,. \end{aligned} \tag{3.49}$$

3.2.4 Up-Conversion

Before converting the signal to the analog domain, a digital up-converter (DUC) is used to up-convert the signal from base-band to the IF, which serves two main purposes. First, the low-frequency noise of the electronics is avoided [61]. Moreover, it enables further multiplexing of the quantum signal and pilot tone in the frequency degree of freedom.

Considering a DAC with sampling frequency $f_{\text{s}}^{\text{Tx}} = 250$ MSa/s, the possible digital up-conversion is limited by the bandwidth of the pulse-shaped signal (B_{ps}) as following

$$\omega_{\text{uc}}^{\text{max}} = 1 - \frac{B_{\text{ps}}}{f_{\text{s}}^{\text{Tx}}} \quad \text{Rad/Sample.} \tag{3.50}$$

Evaluating for $f_{\text{s}}^{\text{Tx}} = 250$ MSa/s, $B_{\text{orig}} = 50$ MHz for a 50 MBd symbol rate, and 0.4 ROF gives

$$\begin{aligned} \omega_{\text{uc}}^{\text{max}} &= 1 - \frac{(1+0.4)\cdot 50}{250} \\ &= 0.72 \quad \text{Rad/Sample,} \end{aligned} \tag{3.51}$$

which corresponds to the following raw frequency value

$$\begin{aligned} \Omega_{\text{uc}}^{\text{max}} &= \frac{\omega_{\text{uc}}^{\text{max}}}{2} \cdot f_{\text{s}}^{\text{Tx}} \\ &= \frac{0.72}{2} \cdot 250 \times 10^{6} \\ &= 90 \quad \text{MHz.} \end{aligned} \tag{3.52}$$

Figure 3.15 shows the maximum possible frequency shift as a function of the ROF. To allow for the entire range of the ROF needed in its optimization procedure, the frequency up-conversion is set to $\Omega_{\text{uc}} = 75$ MHz, corresponding to a normalized frequency domain

value given by

$$\begin{aligned}\omega_{\text{uc}} &= 2\pi \cdot \frac{\Omega_{\text{uc}}}{f_{\text{s}}^{\text{Tx}}} \\ &= 2\pi \frac{75}{250} \\ &= 0.6\pi \quad \text{Rad/Sample},\end{aligned} \tag{3.53}$$

which defines the sinusoidal tones used to digitally shift the frequency of the pulse-shaped signal

$$x_{\text{uc}}[n] = \text{Re}\{x_{\text{ps}}[n]\} \cdot \cos(\omega_{\text{uc}} n) - \text{Im}\{x_{\text{ps}}[n]\} \cdot \sin(\omega_{\text{uc}} n). \tag{3.54}$$

The up-converted signal is shown in Figure 3.16 where the signal is also mirrored in the negative frequency half.

3.2.5 Down-Conversion

The digitized received signal ($x_{\text{rx}}[n]$) is down-converted to base-band frequency using a digital down-converter (DDC). The ADC sampling frequency (f_{s}^{Rx}) is set to 1.25 GSa/s, ten times the Nyquist frequency of the transmitted signal $f_{\text{N}}^{\text{Tx}} = f_{\text{s}}^{\text{Tx}}/2 = 125$ MHz, corresponding to the highest existing frequency component. To achieve a frequency down-conversion of $\Omega_{\text{dc}} = 75$ MHz, the needed normalized frequency shift differs from that of the Tx

$$\begin{aligned}\omega_{\text{dc}} &= 2\pi \cdot \frac{\Omega_{\text{dc}}}{f_{\text{s}}^{\text{Rx}}} \\ &= 2\pi \frac{75}{1.25 \times 10^3} \\ &= 0.12\pi \quad \text{Rad/Sample}.\end{aligned} \tag{3.55}$$

The down-converted signal shown in Figure 3.17 is given by

$$x_{\text{dc}}[n] = \text{Re}\{x_{\text{rx}}[n]\} \cdot \cos(\omega_{\text{dc}} n) - \text{Im}\{x_{\text{rx}}[n]\} \cdot \sin(\omega_{\text{dc}} n), \tag{3.56}$$

which results in two images centered at $\pm 2\Omega_{\text{dc}}$ that are omitted using an image-rejection LPF. Similar to the pulse-shaping filter being used for interpolation, the matched filter

performs the needed low-pass filtering.

3.2.6 Matched Filtering

An LPF is needed to suppress the high-frequency noise and interference from the incoming signal on the Rx side. However, the LPF should be matched to the pulse shaping filter at the Tx to prevent ISI. By splitting the RC filter into two equivalent sub-filters, the RRC filters, ISI suppression can be maintained while achieving the desired LPF functionalities at the Tx and Rx. The frequency response of the RRC filter is obtained by taking the square-root of the RC filter frequency response in Equation (3.48)

$$H_{\text{RRC}}(f) = \begin{cases} \sqrt{T_{\text{sym}}^{\text{us}}}, & |f| \leq \frac{1-\alpha}{2T_{\text{sym}}^{\text{us}}}, \\ \sqrt{T_{\text{sym}}^{\text{us}}} \cos\left(\frac{\pi T_{\text{sym}}^{\text{us}}}{2\alpha}\left(|f| - \frac{1-\alpha}{2T_{\text{sym}}^{\text{us}}}\right)\right), & \frac{1-\alpha}{2T_{\text{sym}}^{\text{us}}} < |f| \leq \frac{1+\alpha}{2T_{\text{sym}}^{\text{us}}}, \\ 0, & \text{otherwise}, \end{cases} \tag{3.57}$$

where the trigonometric identity $1 + \cos(2x) = 2\cos^2(x)$ was used. The corresponding impulse response of the RRC filter is given by [60]

$$h_{\text{RRC}}[n] = \begin{cases} \frac{1}{\sqrt{L}}\left[1 + \alpha\left(\frac{4}{\pi} - 1\right)\right], & \text{for } n = 0, \\ \frac{\alpha}{\sqrt{2L}}\left[\left(1 + \frac{2}{\pi}\right)\sin\left(\frac{\pi}{4\alpha}\right) + \left(1 - \frac{2}{\pi}\right)\cos\left(\frac{\pi}{4\alpha}\right)\right], & \text{for } |n| = \frac{L}{4\alpha}, \\ \frac{\sqrt{L}}{\pi n\left[1-\left(\frac{4\alpha n}{L}\right)^2\right]}\left[\sin\left(\frac{\pi n}{L}(1-\alpha)\right) + \frac{4\alpha n}{L}\cos\left(\frac{\pi n}{L}(1+\alpha)\right)\right], & \text{otherwise}, \end{cases} \tag{3.58}$$

where L'Hôpital's rule was used for the indeterminate cases. The continuous-time representation of Equation (3.58) is

$$h_{\text{RRC}}(t) = \begin{cases} \frac{1}{\sqrt{T_{\text{sym}}^{\text{us}}}}\left[1 + \alpha\left(\frac{4}{\pi} - 1\right)\right], & \text{for } t = 0, \\ \frac{\alpha}{\sqrt{2T_{\text{sym}}^{\text{us}}}}\left[\left(1 + \frac{2}{\pi}\right)\sin\left(\frac{\pi}{4\alpha}\right) + \left(1 - \frac{2}{\pi}\right)\cos\left(\frac{\pi}{4\alpha}\right)\right], & \text{for } |t| = \frac{T_{\text{sym}}^{\text{us}}}{4\alpha}, \\ \frac{\sqrt{T_{\text{sym}}^{\text{us}}}}{\pi t\left[1-\left(\frac{4\alpha t}{T_{\text{sym}}^{\text{us}}}\right)^2\right]}\left[\sin\left(\frac{\pi t}{T_{\text{sym}}^{\text{us}}}(1-\alpha)\right) + \frac{4\alpha t}{T_{\text{sym}}^{\text{us}}}\cos\left(\frac{\pi t}{T_{\text{sym}}^{\text{us}}}(1+\alpha)\right)\right], & \text{otherwise}. \end{cases} \tag{3.59}$$

Unlike for RC filters, RRC pulses do not display the zero crossings behavior at integer multiples of the symbol period ($T_{\text{sym}}^{\text{us}}$) as shown in Figure 3.18. Therefore, RRC filters do not satisfy the Nyquist no-ISI criterion except when using a pair of them, which is effectively an RC filter. The impulse and frequency responses for multiple ROF values is shown in Figure 3.19.

Similar to Equation (3.49), matched filtering is performed by convolving the RRC impulse response in Equation (3.58) with the down-converted signal ($x_{\text{dc}}[n]$)

$$\begin{aligned} x_{\text{mf}}[n] &= x_{\text{dc}}[n] * h_{\text{RRC}}[n] \\ &= \sum_{m=-\infty}^{\infty} x_{\text{dc}}[m]\, h_{\text{RRC}}[n-m]\,, \end{aligned} \tag{3.60}$$

where the corresponding outcome is shown in Figure 3.20.

3.2.7 Downsampling

Depending on the sampling rate of the ADC, there will be $M-1$ excess samples which need to be omitted. The downsampling by M operation is done by skipping samples as following

$$x_{\text{ds}}[n] = x_{\text{mf}}[Mn]\,. \tag{3.61}$$

For a receiver with sampling frequency $f_{\text{s}}^{\text{Rx}} = 1.25$ GSa/s and symbol period $T_{\text{sym}}^{\text{us}} = 20$ ns, M is given by

$$\begin{aligned} M &= \frac{T_{\text{sym}}^{\text{us}}}{T_{\text{s}}^{\text{Rx}}} \\ &= T_{\text{sym}}^{\text{us}} \cdot f_{\text{s}}^{\text{Rx}} \\ &= (20 \times 10^{-9}) \cdot (1.25 \times 10^{9}) \\ &= 25 \quad \text{Samples/Symbol.} \end{aligned} \tag{3.62}$$

The resulting downsampled by 25 signal is shown in Figure 3.21, where the sampling point which maximizes the variance was chosen. Figure 3.22 shows the phasor diagram

of the original ($x_{\text{orig}}[n]$) and retrieved symbols ($x_{\text{ds}}[n]$). Compared with the previously chosen ROF = 0.4, optimizing the ROF gave a better outcome for ROF = 0.416, as seen in Figure 3.23. The penalty in Figure 3.23 has been defined such that it is directly and linearly proportional to how far away the samples are from the ideal constellation points.

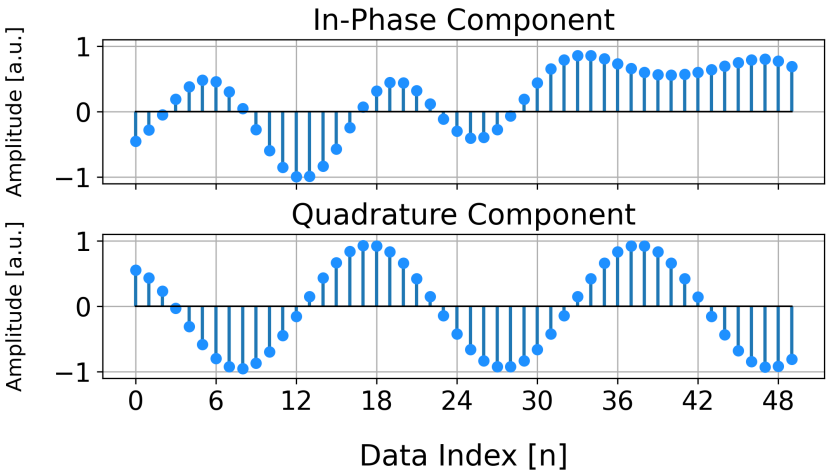
3.2.8 Demodulation

Each sample of the downsampled signal ($x_{\text{ds}}[n]$) represents a QPSK symbol, which is mapped back to the considered bits pair representation of Table 3.1.

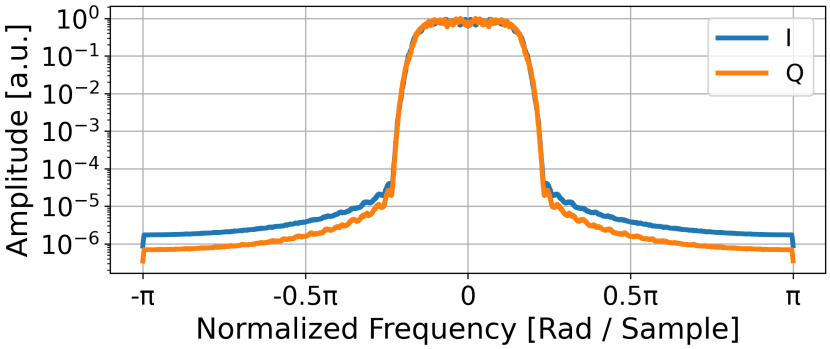
3.2.9 Practical Implementation

The required DSP algorithms for coherent communication and CV-QKD share many similarities, with the primary difference being their optimization objective. Both aim to maximize the mutual information between the Tx and Rx signals. However, in CV-QKD, the optimization objective also includes limiting the leaked information to Eve as defined by the Holevo bound.

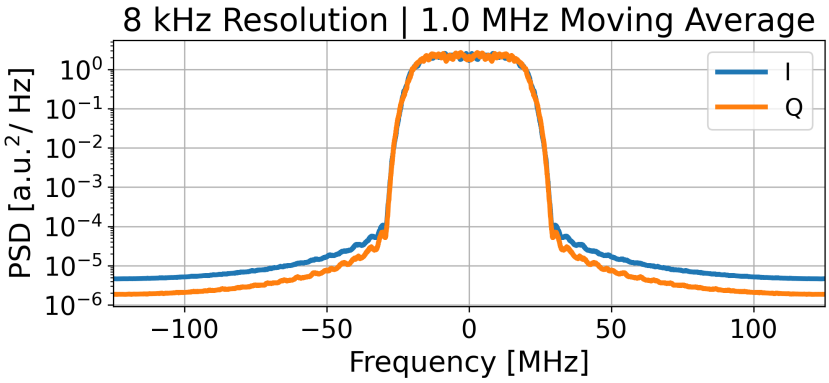
For CV-QKD, the DSP algorithms will be designed according to the following objectives. The upsampling factor will be set according to the desired baud rate and the DAC sampling frequency. A higher filter span is desirable for the pulse shaping filter because the ideal filter version is IIR. However, since the considered signals have a finite length, convolving them with a high-order filter will worsen the undesirable boundary effects. Therefore, an appropriate filter span must be selected to balance the ISI suppression and boundary effect mitigation properties. The pulse shaping filter ROF and the up-conversion frequency are optimized to enhance the system performance while being upper-limited by the Nyquist frequency of the utilized DAC.



(a)



(b)



(c)

Figure 3.11: The result of interpolating the zero-padded signal shown in Figure 3.9 is presented in (a), where the originally zero-valued samples have been replaced with interpolated values that are calculated based on the neighboring non-zero samples. This process effectively increases the sampling rate and improves the signal quality. The effect of the low-pass filtering, which is applied during the interpolation process, can be observed in the frequency domain representation shown in (b) and (c), where the higher frequency components are suppressed, leading to a smoother signal spectrum.

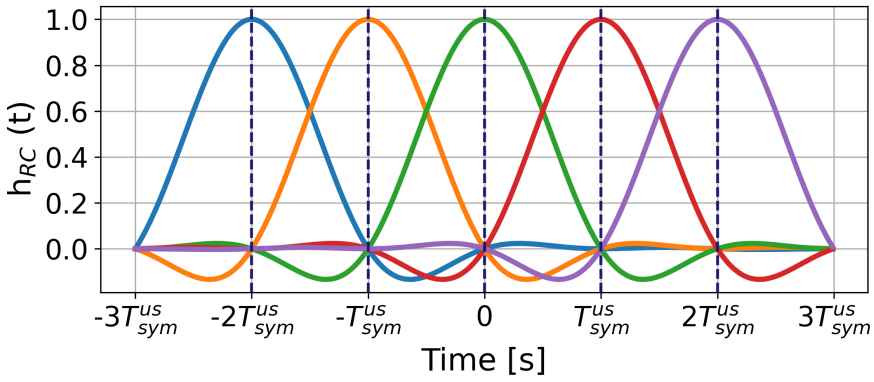
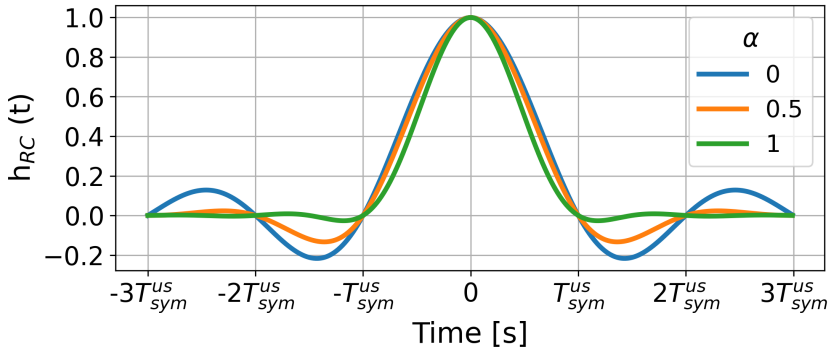
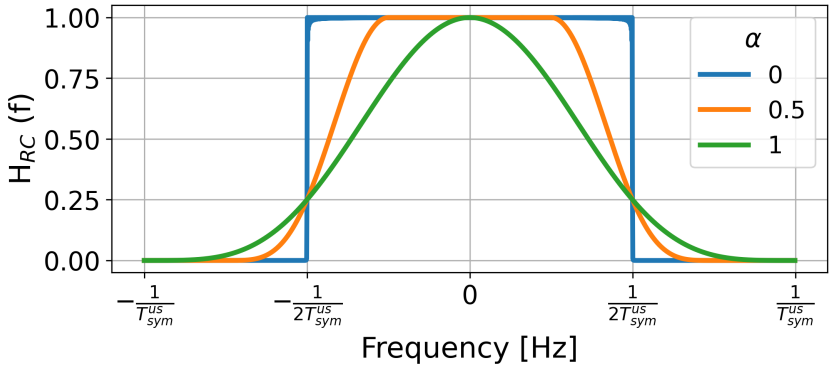


Figure 3.12: Consecutive raised-cosine (RC) pulses with roll-off factor (ROF) of 0.5 demonstrate the zero inter-symbol interference (ISI) criterion, where only a single one has a peak at multiples of the symbol period ($T_{\text{sym}}^{\text{us}}$), while the rest are zero.

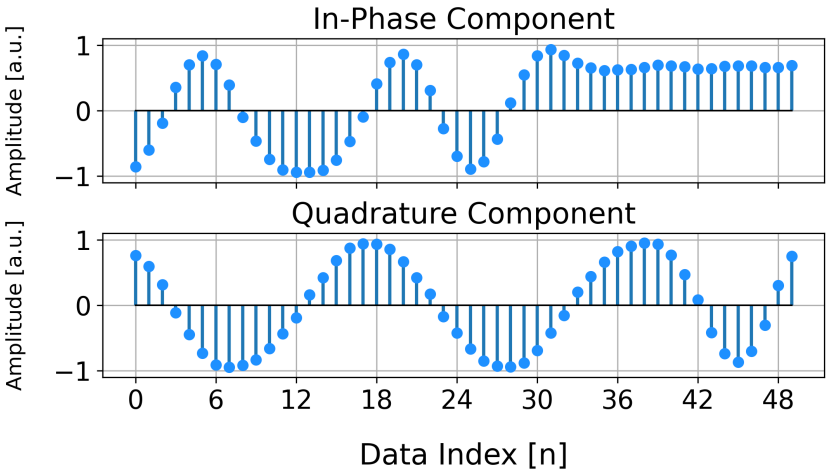


(a)

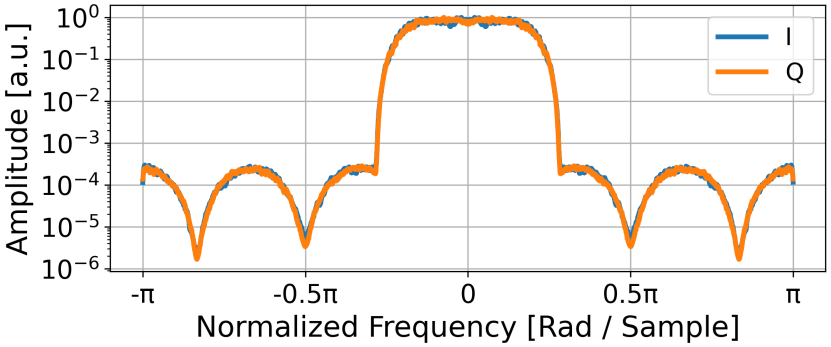


(b)

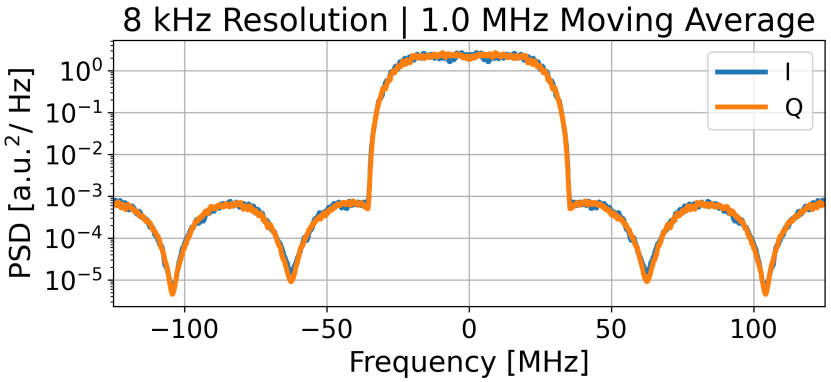
Figure 3.13: The (a) impulse and (b) frequency response of a raised-cosine (RC) filter for multiple roll-off factor (ROF) values.



(a)



(b)



(c)

Figure 3.14: The zero-padded QPSK symbols of Figure 3.9 after pulse shaping using a root raised-cosine (RRC) filter with 0.4 roll-off factor (ROF). The result is similar to Figure 3.11, where (a) the samples are interpolated in the time domain and (b-c) low-pass filtering is performed in the frequency domain.

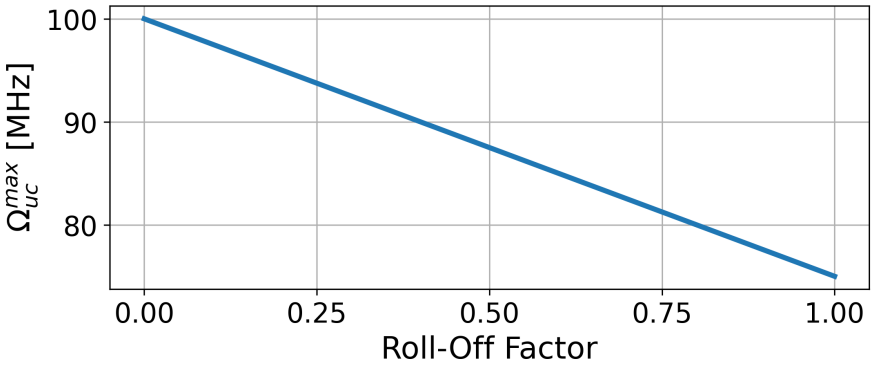
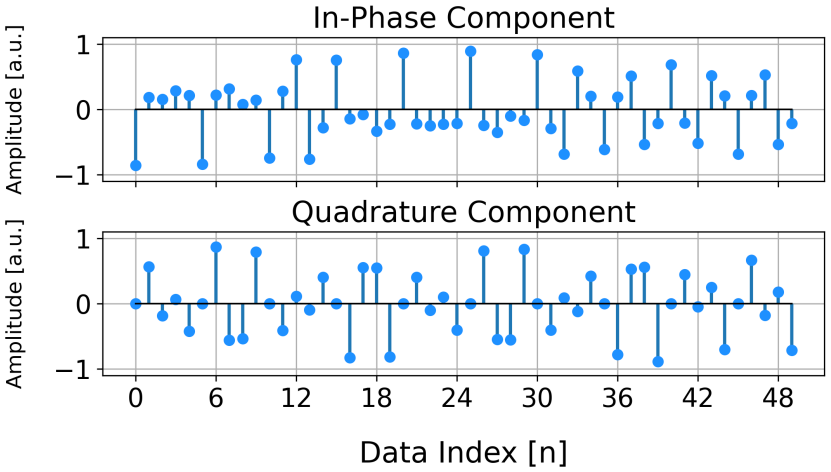
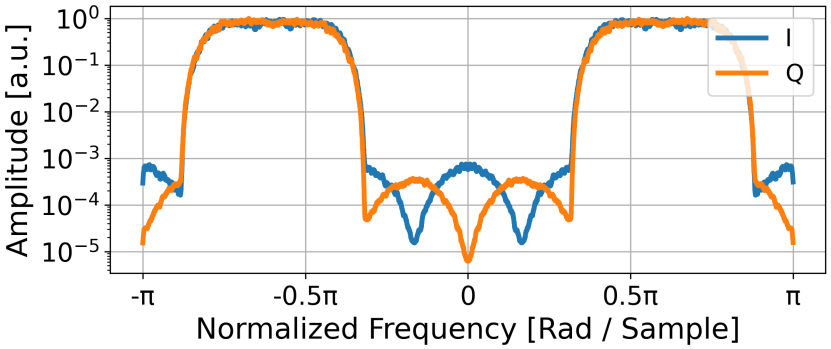


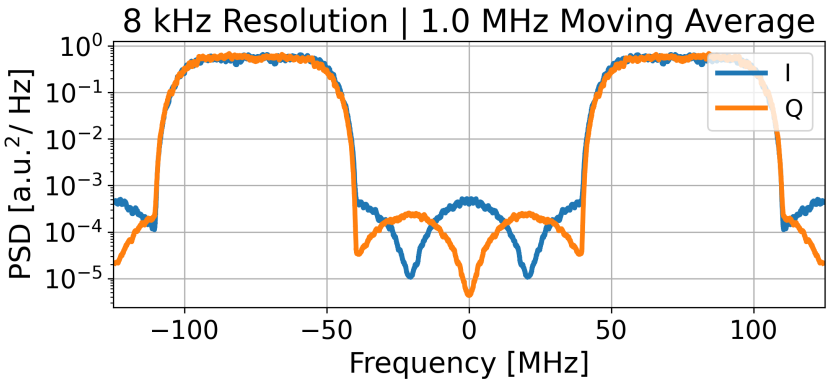
Figure 3.15: The maximum value for the up-conversion process limited by the sampling frequency of the digital-to-analog converter (DAC) $f_s^{\mathrm{Tx}} = 250$ MSa/s and the signal original bandwidth $B_{\mathrm{orig}} = 50$ MHz as a function of the root raised-cosine (RRC) filter roll-off factor (ROF).



(a)

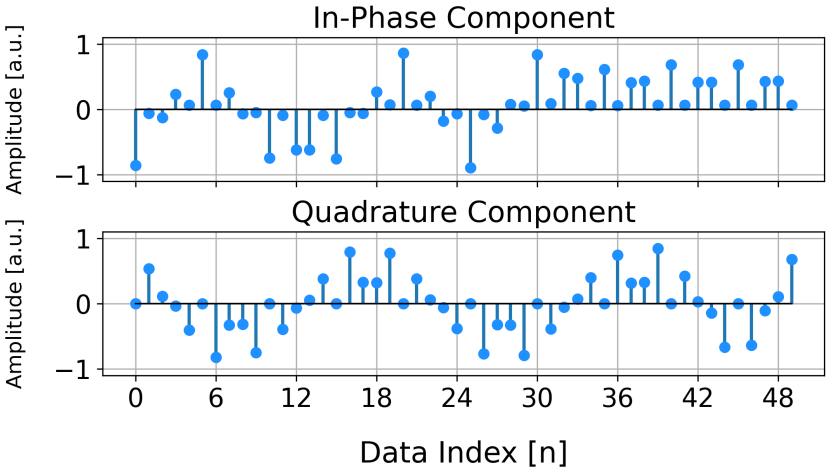


(b)

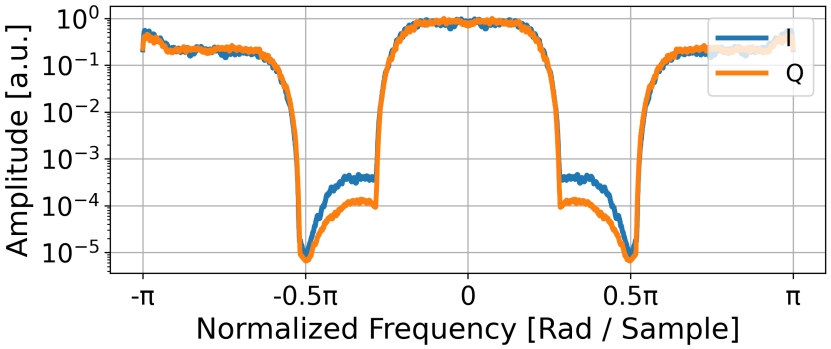


(c)

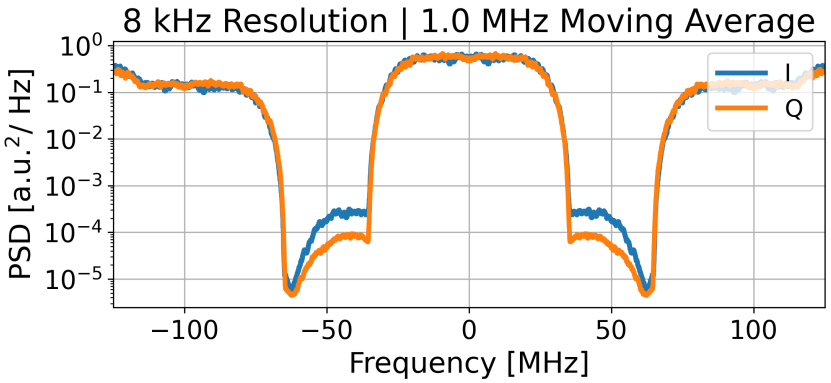
Figure 3.16: The pulse-shaped signal shown in Figure 3.14 is frequency up-converted, and the resulting signal exhibits sharp transitions in the discrete-time domain, as shown in (a). These transitions are caused by the high-frequency components, which were up-converted from the baseband. The frequency-domain representations shown in (b) and (c) illustrate the up-converted signal components, which contribute to the sharp transitions observed in (a).



(a)



(b)



(c)

Figure 3.17: The up-converted signal shown in Figure 3.16 is down-converted to a lower frequency range, resulting in a discrepant discrete-time signal as shown in (a), which does not match the pulse-shaped signal shown in Figure 3.14. This discrepancy is caused by the presence of two unwanted images centered at twice the down-conversion frequency, as illustrated in the frequency-domain representations shown in (b) and (c). These unwanted images should be filtered out by a low-pass filter (LPF).

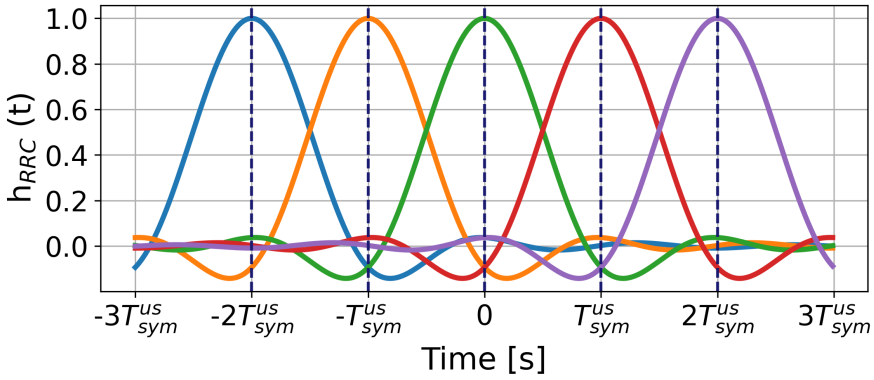
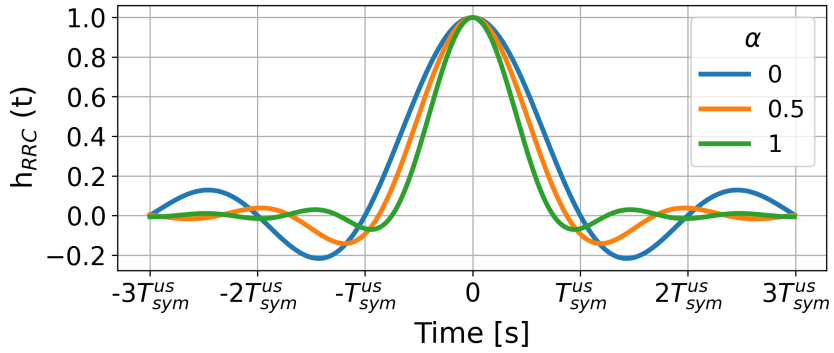
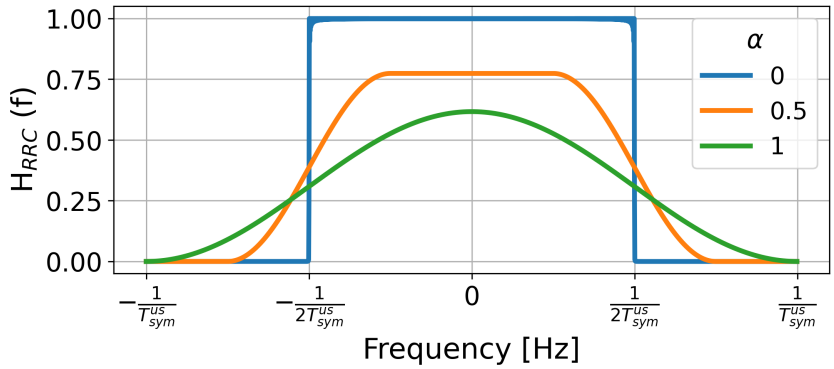


Figure 3.18: Consecutive RRC pulses do not satisfy the zero ISI criterion, where only a single one has a peak at multiples of the symbol period ($T_{\text{sym}}^{\text{us}}$), while the rest not necessarily equal to zero.

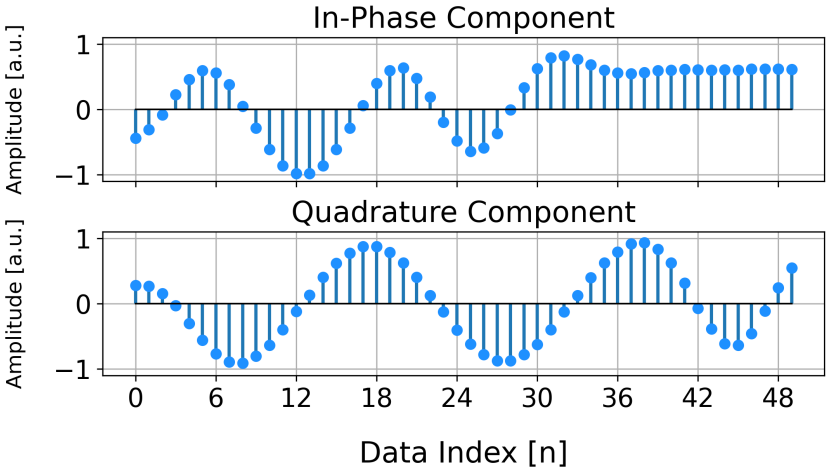


(a) Impulse Response

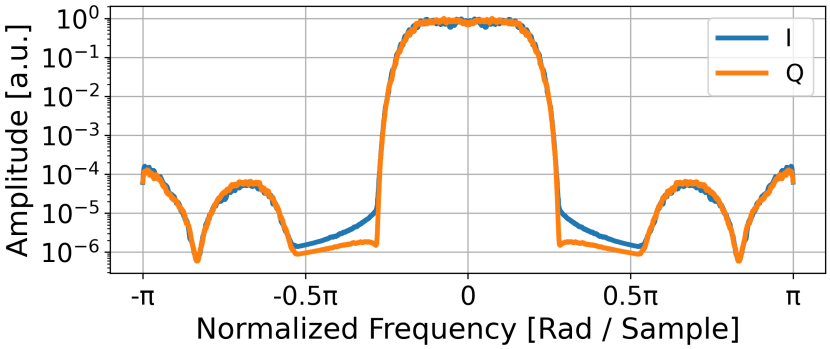


(b) Frequency Response

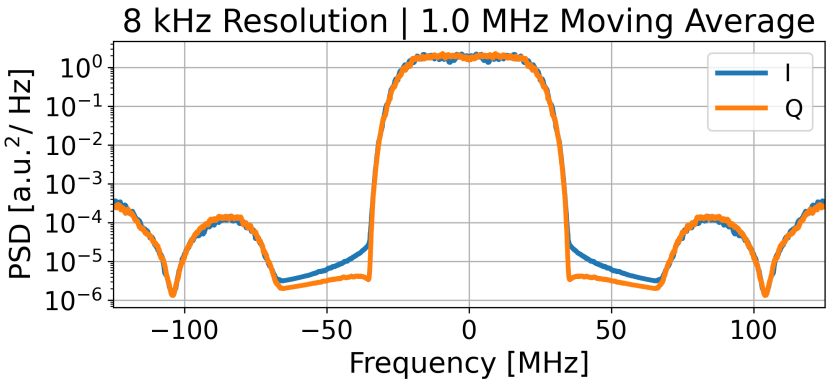
Figure 3.19: The (a) impulse and (b) frequency response of an RRC filter for multiple ROF values.



(a)

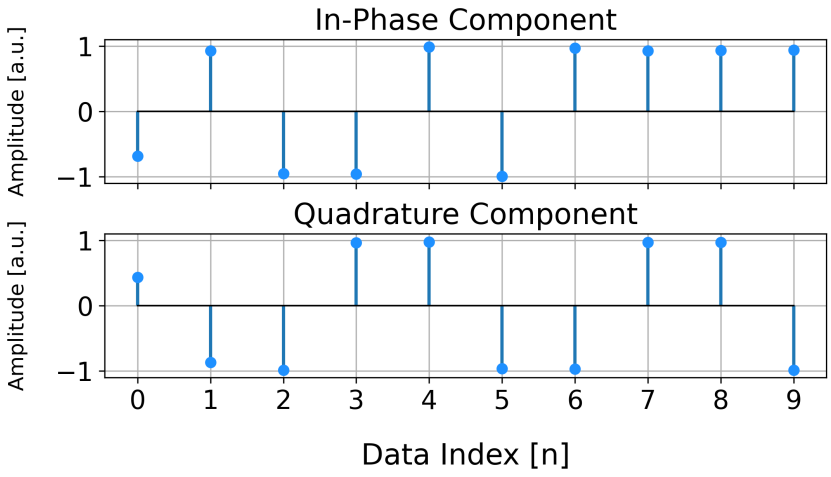


(b)

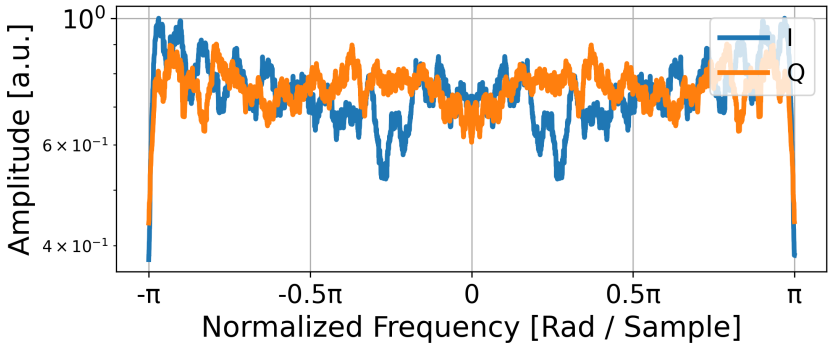


(c)

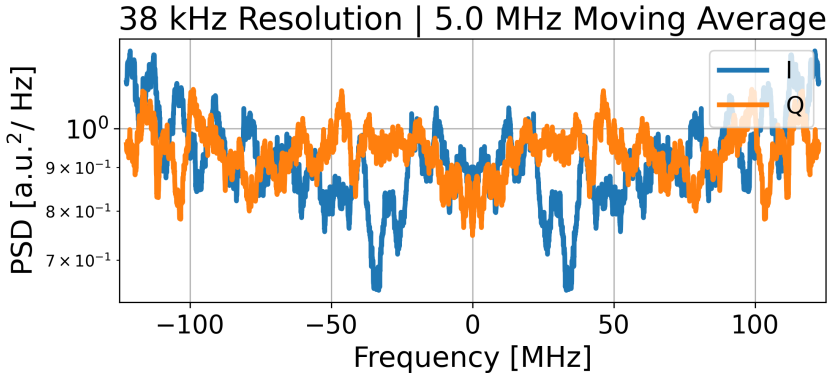
Figure 3.20: The frequency down-converted symbols of Figure 3.17 after being subjected to matched filtering using a root raised-cosine (RRC) filter. The time-domain representation of the resulting signal shown in (a) exhibits a smooth variation, which is due to the RRC filter's suppression of high-frequency components. The frequency-domain representations shown in (b) and (c) illustrate the limited spectrum of the signal after the matched filtering, with significant attenuation of the high-frequency components.



(a)



(b)



(c)

Figure 3.21: After downsampling the matched-filtered signal of Figure 3.20, the retrieved symbols. The time-domain representation of the resulting signal in (a) exhibits the QPSK nature of the symbols, with the signal occupying only two values (±1). The frequency-domain representations shown in (b) and (c) illustrate the baseband spectrum of the down-sampled signal, which occupies the entire frequency range due to the downsampling operation stretching the spectrum.

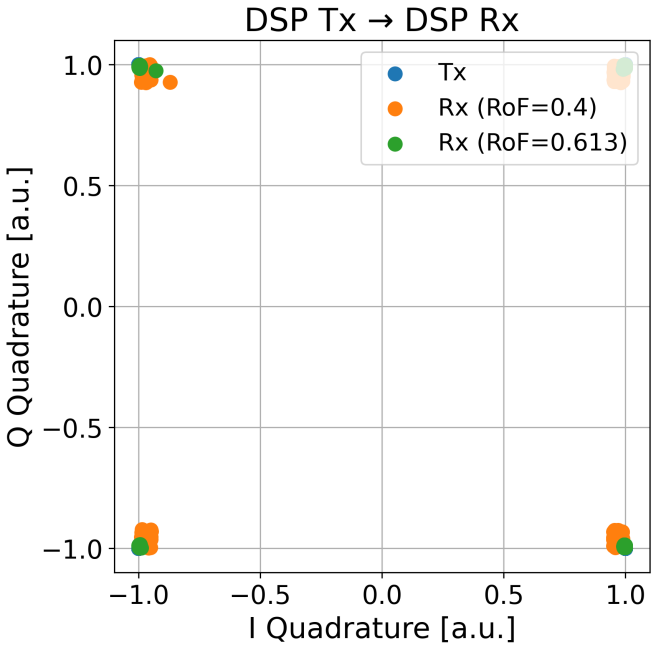


Figure 3.22: A phase diagram comparing the constellation points of the transmitted (Tx) and received (Rx) symbols for two roll-off factor (ROF) values. For the considered simulation, the higher ROF value results in a better performance.

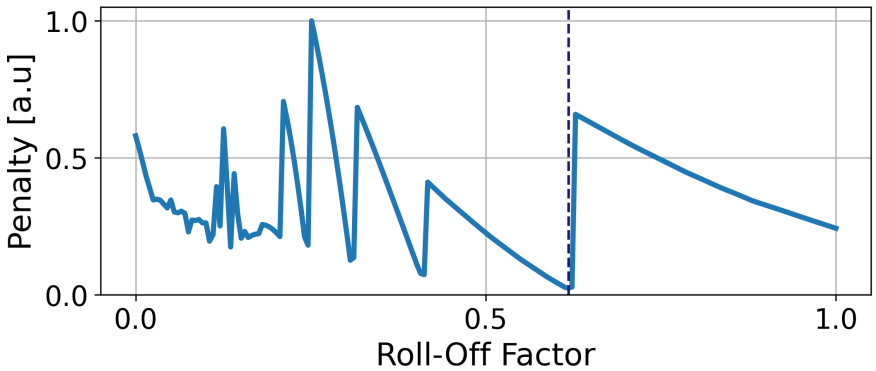


Figure 3.23: Optimizing the roll-off factor (ROF) value involves minimizing the penalty function, which is designed to have a small value for highly spread-out constellation points.

CHAPTER 4

CV-QKD NOISE SOURCES

One of the critical challenges to maintaining the operation in the quantum regime is that the shot noise of the system should dominate over all other sources of noise. Therefore, it is of interest to model the different sources of noise that will affect the performance of the system. Since measurements are given as a voltage in practice, Equation (2.54) is reexpressed as

$$\bar{\sigma}^2_{\hat{q}_\mathrm{B}} = T_\mathrm{tot}\bar{\sigma}^2_{\hat{\mathrm{A}}} + N_0 + \bar{\xi}_\mathrm{tot} \qquad [\mathrm{V}^2], \tag{4.1}$$

where N_0 is the shot noise variance (discussed in Section 4.1) and a total noise $\bar{\xi}_\mathrm{tot}$ that can be broken down into the following terms

$$\bar{\xi}_\mathrm{tot} = T_\mathrm{tot}\left(\bar{\xi}_\mathrm{A} + \bar{\xi}_\mathrm{exc}\right) + \bar{\xi}_\mathrm{B} \qquad [\mathrm{V}^2], \tag{4.2}$$

where the components $\bar{\xi}_\mathrm{A}$ and $\bar{\xi}_\mathrm{B}$ are due to Alice's and Bob's imperfect hardware, respectively, and $\bar{\xi}_\mathrm{exc}$ is excess noise attributed to the channel, Eve, and other unaccounted for sources. The excess noise is taken to be at the beginning of the channel since this is the optimal point of attack for Eve. The hardware imperfections result in the following noise

$$\bar{\xi}_\mathrm{A} = \bar{\xi}_{\mathrm{RIN_s}} + \bar{\xi}_\mathrm{DAC} \qquad [\mathrm{V}^2], \tag{4.3}$$

$$\bar{\xi}_\mathrm{B} = \bar{\xi}_{\mathrm{RIN_{LO}}} + \bar{\xi}_\mathrm{det} + \bar{\xi}_\mathrm{ADC} \qquad [\mathrm{V}^2], \tag{4.4}$$

where $\bar{\xi}_{\mathrm{RIN_s}}$ and $\bar{\xi}_{\mathrm{RIN_{LO}}}$ (discussed in Section 4.2) are the relative intensity noise (RIN) of the prepared signal and the utilized LO, respectively, $\bar{\xi}_\mathrm{det}$ is the detection noise (discussed in Section 4.3), while $\bar{\xi}_\mathrm{DAC}$ and $\bar{\xi}_\mathrm{ADC}$ (discussed in Section 4.4) are the quantization error due to the finite resolution of the DAC and ADC, respectively.

In the following sections, most of the excess noise analysis are based on [50], with a

slight variation in some of them.

4.1 SHOT NOISE

The shot noise variance, N_0, comes from the fundamental uncertainty in measuring the coherent state, where Poissonian statistics[1] govern photons' arrival time to the coherent detectors. In practice, all the system parameters are normalized with respect to the shot noise variance, giving it a unity value in the SNU formalism. The shot noise is manifested in the fluctuations of the generated photocurrent ($\Delta I_{\text{ph}}(t)$), which is expressed as

$$I_{\text{ph}}(t) = \langle I_{\text{ph}} \rangle + \Delta I_{\text{ph}}(t), \tag{4.5}$$

which is passed through a load of resistance R_{L}, giving a time-varying power component due to the fluctuating current

$$P_{\text{SN}}(t) = \left[\Delta I_{\text{ph}}(t)\right]^2 R_{\text{L}}. \tag{4.6}$$

The current fluctuation variance $\left[\Delta I_{\text{ph}}\right]^2$ is given by[2]

$$\left[\Delta I_{\text{ph}}(\omega)\right]^2 = 2eB\langle I_{\text{ph}} \rangle, \tag{4.7}$$

where e is the electron charge and $B \equiv \Delta\omega$ is the bandwidth of the fluctuating current. As expected from the Poisson statistics of the photocurrent, the photocurrent variance $\left[\Delta I_{\text{ph}}(\omega)\right]^2$ is directly proportional to its average value $\langle I_{\text{ph}} \rangle$. Plugging Equation (4.7) in Equation (4.6) gives

$$P_{\text{SN}}(\omega) = 2eBR_{\text{L}}\langle I_{\text{ph}} \rangle, \tag{4.8}$$

which is considered as white noise, since it is independent of the frequency. However, in

[1] The Poisson distribution gives the probability of n events occurring in a specific spatial or temporal interval given that N_{av} events happen on average as

$$P_n = \frac{N_{\text{av}}^n \cdot e^{-N_{\text{av}}}}{n!}.$$

[2] The derivation of Equation (4.7) is performed in Appendix A.

practice, the used detector is able to capture the shot noise statistics up to a maximum rate of about $B_D = 1/\tau_D$, where τ_D is the period between successive samples. A typical outcome when measuring a beam of light with a photodetector of bandwidth B_D is illustrated in Figure 4.1, where the frequency-dependent pink noise is due to the electronics driving the laser as well as the mechanical vibrations in the laser cavity mirror [38]. In order to suppress the low-frequency classical noise, a balanced detector can be used.

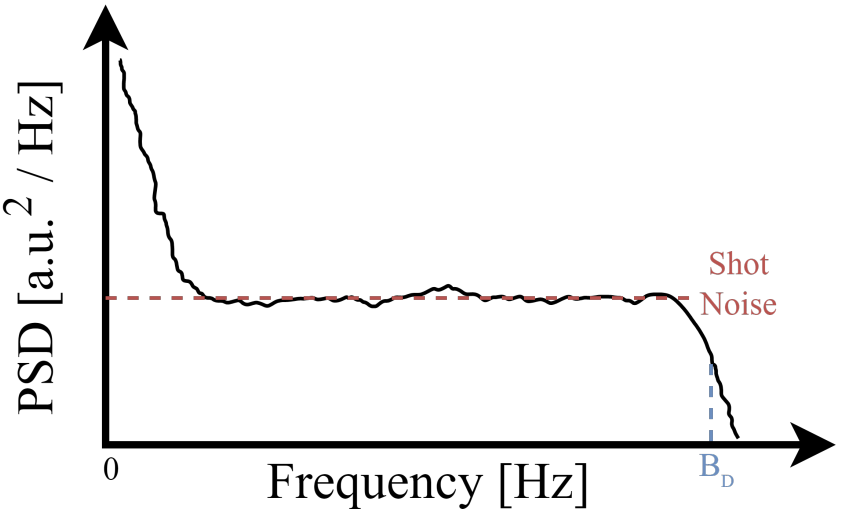


Figure 4.1: The power spectrum of the variance of the generated photocurrent due to a light source with low-frequency classical noise.

4.2 RELATIVE INTENSITY NOISE (RIN)

4.2.1 Signal

For a signal with power $P_s(t)$, the RIN is defined as [62]

$$\mathrm{RIN}_s \equiv \frac{S_{\sigma^2_{P_s}}}{\langle P_s \rangle^2}, \tag{4.9}$$

where $\langle P_s \rangle$ is the average power and $S_{\sigma^2_{P_s}}$ is the power spectral density (PSD)[3] of the power fluctuation. That is, $S_{\sigma^2_{P_s}}$ is the power variance per 1 Hz. For a signal of bandwidth

[3]The definition of the PSD is given by Equation (A.7) in Appendix A.

B_s, the power variance is

$$\begin{aligned}\sigma^2_{P_s} &= B_s \cdot S_{\sigma^2_{P_s}} \\ &= B_s \cdot \mathrm{RIN}_s \cdot \langle P_s \rangle^2,\end{aligned} \tag{4.10}$$

where Equation (4.9) was utilized. The average power of the signal can be expressed in terms of the average number of photons ($\langle n_s \rangle$) as following

$$\langle P_s \rangle = \frac{h f_s \cdot \langle n_s \rangle}{\tau_s}, \tag{4.11}$$

where h is Planck's constant, f_s is the frequency of the signal, and τ_s is the duration of the signal pulse. In terms of the creation ($\hat{a}^\dagger$) and annihilation ($\hat{a}$) operators, the photon number operator $\hat{n}$ is

$$\hat{n} = \hat{a}^\dagger \hat{a}. \tag{4.12}$$

As in Equation (2.34) and Equation (2.35), the creation ($\hat{a}^\dagger$) and annihilation ($\hat{a}$) operators can be expressed in terms of the quadrature operators $\hat{x}$ and $\hat{p}$ in SNU as following

$$\hat{a}_i^\dagger = \frac{1}{2}(\hat{x}_i - j\hat{p}_i) \qquad \text{[SNU]}, \tag{4.13}$$

$$\hat{a}_i = \frac{1}{2}(\hat{x}_i + j\hat{p}_i) \qquad \text{[SNU]}, \tag{4.14}$$

which when plugged into Equation (4.12) give[4]

$$\begin{aligned}\hat{n} &= \frac{1}{4}\left(\hat{x} - j\hat{p}\right)\left(\hat{x} + j\hat{p}\right) \\ &= \frac{1}{4}\left[\hat{x}^2 + \hat{p}^2 - j(\hat{p}\hat{x} - \hat{x}\hat{p})\right] \\ &= \frac{1}{4}\left[\hat{x}^2 + \hat{p}^2 - j[\hat{p}, \hat{x}]\right] \\ &= \frac{1}{4}\left[\hat{x}^2 + \hat{p}^2 - j \cdot 2j[\hat{a}, \hat{a}^\dagger]\right]^{-1} \\ &= \frac{1}{4}\left(\hat{x}^2 + \hat{p}^2 - 2\right).\end{aligned} \tag{4.15}$$

Thus, the variance in the average number of photons ($\sigma^2_{\langle n_s \rangle}$) is[5]

$$\begin{aligned}\sigma^2_{\langle n_s \rangle} = \sigma^2_{\hat{n}} &= \frac{1}{4^2}\sigma^2_{\hat{x}^2+\hat{p}^2} \\ &= \frac{1}{16}\left[\sigma^2_{\hat{x}^2} + \sigma^2_{\hat{p}^2}\right] \\ &= \frac{1}{8}\left[\sigma^4_{\hat{x}} + \sigma^4_{\hat{p}}\right] \\ &= \frac{1}{4}\sigma^4_{\hat{x}},\end{aligned} \tag{4.16}$$

where the variance of the two quadratures of the coherent state are assumed to be the same. Utilizing Equation (4.11) and Equation (4.16), the power variance ($\sigma^2_{P_s}$) is

$$\sigma^2_{P_s} = \left(\frac{hf_s}{\tau_s}\right)^2 \sigma^2_{\langle n_s \rangle} = \left(\frac{hf_s}{2\tau_s}\right)^2 \sigma^4_{\hat{x}}. \tag{4.17}$$

---

[4] Equation (2.32) and Equation (2.33) were used to derive the following relation

$$\begin{aligned}[\hat{p}, \hat{x}] = \hat{p}\hat{x} - \hat{x}\hat{p} &= j\left[(\hat{a}^\dagger - \hat{a})(\hat{a}^\dagger + \hat{a}) - (\hat{a}^\dagger + \hat{a})(\hat{a}^\dagger - \hat{a})\right] \\ &= j\left[\left(\cancel{\hat{a}^{\dagger 2}} - \cancel{\hat{a}^2} + \hat{a}^\dagger\hat{a} - \hat{a}\hat{a}^\dagger\right) - \left(\cancel{\hat{a}^{\dagger 2}} - \cancel{\hat{a}^2} - \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger\right)\right] \\ &= 2j[\hat{a}^\dagger, \hat{a}].\end{aligned}$$

[5] For a zero-mean random variable (X), its variance can be expressed as

$$\sigma^2_X = \langle X^2 \rangle - \langle X \rangle^2 = \langle X^2 \rangle,$$

and the variance of its square is

$$\sigma^2_{X^2} = \langle X^4 \rangle - \langle X^2 \rangle^2 = \langle X^4 \rangle - \left(\sigma^2_X\right)^2 = 2\left(\sigma^2_X\right)^2,$$

where $\langle X^4 \rangle = 3\left(\sigma^2_X\right)^2$ [63].

Therefore, the variance in the quadrature due to the RIN can be expressed as

$$\begin{aligned}\sigma^2_{\hat{x},\mathrm{RIN_s}} &= \frac{2\tau_\mathrm{s}}{hf_\mathrm{s}}\sigma_{P_\mathrm{s}} \\ &= \frac{2\tau_\mathrm{s}}{hf_\mathrm{s}}\sqrt{B_\mathrm{s}\cdot\mathrm{RIN_s}}\langle P_\mathrm{s}\rangle \\ &= \frac{2\cancel{\tau_\mathrm{s}}}{\cancel{hf_\mathrm{s}}}\sqrt{B_\mathrm{s}\cdot\mathrm{RIN_s}}\frac{\cancel{hf_\mathrm{s}}\cdot\langle n_\mathrm{s}\rangle}{\cancel{\tau_\mathrm{s}}} \\ &= 2\sqrt{B_\mathrm{s}\cdot\mathrm{RIN_s}}\langle n_\mathrm{s}\rangle.\end{aligned} \tag{4.18}$$

From Equation (2.42), the average number of photons ($\langle n_\mathrm{s}\rangle$) can be expressed in terms of the variance of the quadrature operators ($\sigma^2_{A'}$) as

$$\langle n_\mathrm{s}\rangle = \frac{\sigma^2_{A'}}{2} = 2\sigma^2_A, \tag{4.19}$$

which when plugged into Equation (4.18) gives the excess noise due to the RIN of the transmitted signal

$$\boxed{\sigma^2_{\hat{x},\mathrm{RIN_s}} \equiv \xi_{\mathrm{RIN_s}} = 4\sigma^2_A\sqrt{B_\mathrm{s}\cdot\mathrm{RIN_s}}}. \tag{4.20}$$

4.2.2 Local Oscillator (LO)

In balanced homodyne detection, the difference photon number operator ($\Delta\hat{n}$) for a coherent state is given by[6]

$$\Delta\hat{n} = |\alpha_\mathrm{LO}|\left[-\sin(\theta)\hat{x} + \cos(\theta)\hat{p}\right], \tag{4.21}$$

where θ is the phase of the LO. Taking the variance of Equation (4.21) gives

$$\begin{aligned}\sigma^2_{\Delta\hat{n}} &= \left\langle(\Delta\hat{n})^2\right\rangle - \langle\Delta\hat{n}\rangle^2 \\ &= \left\langle|\alpha_\mathrm{LO}|^2\right\rangle\left[\left\langle\hat{x}^2\right\rangle\sin^2\theta + \left\langle\hat{p}^2\right\rangle\cos^2\theta\right. \\ &\qquad\left. - \sin\theta\cos\theta\left(\langle\hat{x}\hat{p}\rangle + \langle\hat{p}\hat{x}\rangle\right)\right] \\ &\quad - \langle|\alpha_\mathrm{LO}|\rangle^2\left[\langle\hat{x}\rangle\sin\theta + \langle\hat{p}\rangle\cos\theta\right]^2.\end{aligned} \tag{4.22}$$

[6]The derivation of Equation (4.21) is performed in Appendix B.

since $\hat{x}$ and $\hat{p}$ are independent with respect to $|\alpha_{\mathrm{LO}}|$. Consider the phase of the LO to be $\theta = -\frac{\pi}{2}$, giving

$$\begin{aligned}
\sigma^2_{\Delta\hat{n}} &= \left\langle |\alpha_{\mathrm{LO}}|^2 \right\rangle \left\langle \hat{x}^2 \right\rangle - \langle |\alpha_{\mathrm{LO}}| \rangle^2 \langle \hat{x} \rangle^2 \\
&= \left(\sigma^2_{|\alpha_{\mathrm{LO}}|} + \langle |\alpha_{\mathrm{LO}}| \rangle^2 \right) \left\langle \hat{x}^2 \right\rangle - \langle |\alpha_{\mathrm{LO}}| \rangle^2 \langle \hat{x} \rangle^2 \\
&= \left(\sigma^2_{|\alpha_{\mathrm{LO}}|} + \langle |\alpha_{\mathrm{LO}}| \rangle^2 \right) \left\langle \hat{x}^2 \right\rangle \\
&= \left(\sigma^2_{|\alpha_{\mathrm{LO}}|} + \langle |\alpha_{\mathrm{LO}}| \rangle^2 \right) \sigma^2_{\hat{x}}.
\end{aligned} \tag{4.23}$$

where $\langle \hat{x} \rangle$ is set to zero [50]. Another way to express the variance of the photon number difference operator is by considering that the LO's RIN is contained in the variance of $\hat{x}$, such that $|\alpha_{\mathrm{LO}}|$ is constant which gives

$$\begin{aligned}
\sigma^2_{\Delta\hat{n}} &= |\alpha_{\mathrm{LO}}|^2 \sigma^2_{\hat{x}} \\
&= |\alpha_{\mathrm{LO}}|^2 \left(\sigma^2_{\hat{x},\mathrm{RIN_{LO}}} + \sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}} \right),
\end{aligned} \tag{4.24}$$

where $\sigma^2_{\hat{x},\mathrm{RIN_{LO}}}$ is due to the LO's RIN, while $\sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}}$ is caused by all other sources. Consequently, Equation (4.23) is reexpressed as

$$\sigma^2_{\Delta\hat{n}} = \left(\sigma^2_{|\alpha_{\mathrm{LO}}|} + \langle |\alpha_{\mathrm{LO}}| \rangle^2 \right) \sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}}. \tag{4.25}$$

Equating Equation (4.24) and Equation (4.25) gives

$$\begin{aligned}
|\alpha_{\mathrm{LO}}|^2 \left(\sigma^2_{\hat{x},\mathrm{RIN_{LO}}} + \cancel{\sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}}} \right) &= \left(\sigma^2_{|\alpha_{\mathrm{LO}}|} + \cancel{\langle |\alpha_{\mathrm{LO}}| \rangle^2} \right) \sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}} \\
\longrightarrow \sigma^2_{\hat{x},\mathrm{RIN_{LO}}} &= \frac{\sigma^2_{|\alpha_{\mathrm{LO}}|}}{|\alpha_{\mathrm{LO}}|^2} \sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}}.
\end{aligned} \tag{4.26}$$

To find the effect of the LO amplitude fluctuation on the number of photons, the relationship between their variances needs to be derived. As already established, the expectation value of the photon number is the magnitude squared of the coherent state amplitude

$$\langle n_{\mathrm{LO}} \rangle = |\alpha_{\mathrm{LO}}|^2. \tag{4.27}$$

Taking the partial derivative of Equation (4.27) gives

$$\frac{\partial \langle n_{\mathrm{LO}} \rangle}{\partial |\alpha_{\mathrm{LO}}|} = 2|\alpha_{\mathrm{LO}}|, \tag{4.28}$$

resulting in the following relation between small differences of the coherent state amplitude and the photon number expectation

$$\delta \langle n_{\mathrm{LO}} \rangle = 2|\alpha_{\mathrm{LO}}| \cdot \delta |\alpha_{\mathrm{LO}}|, \tag{4.29}$$

which when squared gives the variances relation as

$$\sigma^2_{\langle n_{\mathrm{LO}} \rangle} = 4|\alpha_{\mathrm{LO}}|^2 \sigma^2_{|\alpha_{\mathrm{LO}}|}. \tag{4.30}$$

From Equation (4.11), the average number of photons is

$$\langle n_{\mathrm{LO}} \rangle = \frac{\tau_{\mathrm{LO}} \langle P_{\mathrm{LO}} \rangle}{h f_{\mathrm{LO}}} = |\alpha_{\mathrm{LO}}|^2, \tag{4.31}$$

with the variance being

$$\begin{aligned} \sigma^2_{\langle n_{\mathrm{LO}} \rangle} &= \left(\frac{\tau_{\mathrm{LO}}}{h f_{\mathrm{LO}}} \right)^2 \sigma^2_{P_{\mathrm{LO}}} \\ &= \left(\frac{\tau_{\mathrm{LO}}}{h f_{\mathrm{LO}}} \right)^2 B_{\mathrm{LO}} \langle P_{\mathrm{LO}} \rangle^2 \, \mathrm{RIN}_{\mathrm{LO}}, \end{aligned} \tag{4.32}$$

where Equation (4.10) was utilized. Plugging Equation (4.31) and Equation (4.32) in Equation (4.30) gives

$$\begin{aligned} \sigma^2_{|\alpha_{\mathrm{LO}}|} &= \frac{\sigma^2_{\langle n_{\mathrm{LO}} \rangle}}{4|\alpha_{\mathrm{LO}}|^2} \\ &= \frac{1}{4} \left(\frac{\tau_{\mathrm{LO}}}{h f_{\mathrm{LO}}} \right)^{\cancel{2}} B_{\mathrm{LO}} \langle P_{\mathrm{LO}} \rangle^{\cancel{2}} \, \mathrm{RIN}_{\mathrm{LO}} \frac{h f_{\mathrm{LO}}}{\cancel{\tau_{\mathrm{LO}} \langle P_{\mathrm{LO}} \rangle}} \\ &= \frac{\tau_{\mathrm{LO}} B_{\mathrm{LO}} \langle P_{\mathrm{LO}} \rangle}{4 h f_{\mathrm{LO}}} \mathrm{RIN}_{\mathrm{LO}}. \end{aligned} \tag{4.33}$$

Plugging Equation (4.33) in Equation (4.26) results in

$$\sigma^2_{\hat{x},\mathrm{RIN}_{\mathrm{LO}}} = \frac{\tau_{\mathrm{LO}} B_{\mathrm{LO}} \langle P_{\mathrm{LO}} \rangle}{4 h f_{\mathrm{LO}} |\alpha_{\mathrm{LO}}|^2} \cdot \mathrm{RIN}_{\mathrm{LO}} \cdot \sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}}, \tag{4.34}$$

which when plugging Equation (4.31) gives

$$\boxed{\sigma^2_{\hat{x},\mathrm{RIN_{LO}}} \equiv \xi_{\mathrm{RIN_{LO}}} = \frac{B_{\mathrm{LO}}}{4} \cdot \mathrm{RIN_{LO}} \cdot \sigma^2_{\hat{x},\overline{\mathrm{RIN}}_{\mathrm{LO}}}}. \tag{4.35}$$

4.3 DETECTION NOISE

In a balanced homodyne detector, the difference photon number operator ($\Delta\hat{n}$) for a coherent state is given by Equation (4.21) as

$$\Delta\hat{n} = |\alpha_{\mathrm{LO}}| \left[-\sin(\theta)\hat{x} + \cos(\theta)\hat{p}\right]. \tag{4.36}$$

Without loss of generality (WLOG), let the phase of the LO be $\theta = -\frac{\pi}{2}$, giving

$$\Delta\hat{n} = |\alpha_{\mathrm{LO}}|\hat{x}, \tag{4.37}$$

where

$$|\alpha_{\mathrm{LO}}| = \sqrt{\langle n_{\mathrm{LO}}\rangle} = \sqrt{\frac{P_{\mathrm{LO}}\tau_{\mathrm{LO}}}{h f_{\mathrm{LO}}}}, \tag{4.38}$$

giving the following expression for the variance of the difference photon number operator

$$\sigma^2_{\Delta\hat{n}} = \frac{P_{\mathrm{LO}}\tau_{\mathrm{LO}}}{h f_{\mathrm{LO}}}\sigma^2_{\hat{x}}. \tag{4.39}$$

The electronic noise of the balanced homodyne detector is represented by the noise-equivalent power (NEP), in units of $\mathrm{W}/\sqrt{\mathrm{Hz}}$, that is present at the photodiode input. To express the voltage noise (V_{Det}) at the receiver output in terms of the NEP, Equation (3.10) is utilized

$$P_{\mathrm{inc}} = \frac{I_{\mathrm{ph}}}{R}, \tag{4.40}$$

where I_{ph} and R are the photodiode generated current and its responsivity, respectively. In practice, the generated photocurrent (I_{ph}) is passed through a transimpedance amplifier (TIA), which converts the input current (I_{ph}) to a voltage (V_{Det}) with a gain factor of g_{TIA}

$$V_{\mathrm{Det}} = g_{\mathrm{TIA}} I_{\mathrm{ph}} = g_{\mathrm{TIA}} P_{\mathrm{inc}} R = g_{\mathrm{TIA}} R \cdot \mathrm{NEP}\sqrt{B_{\mathrm{el}}}, \tag{4.41}$$

where B_{el} is the electronic bandwidth. The effect of the electronic noise can be modelled as an ideal receiver with an excess signal power difference (ΔP_{inc}) at its inputs, which gives rise to an extra current difference (ΔI_{ph}) at the photodiodes output

$$\delta(\Delta P_{\text{inc}}) = \frac{\delta I_{\text{ph}}}{R} = \text{NEP}\sqrt{B_{\text{el}}}, \tag{4.42}$$

with the variance being

$$\sigma^2_{\Delta P_{\text{inc}}} = \text{NEP}^2 B_{\text{el}}. \tag{4.43}$$

From Equation (4.11), the LO's power uncertainty is related to the uncertainty in the detected photon number by

$$\Delta n = \frac{\Delta P_{\text{LO}} \tau_{\text{LO}}}{h f_{\text{LO}}}, \tag{4.44}$$

where h is Planck's constant, f_{LO} is the LO frequency, and τ_{LO} is the pulse duration of the LO. Therefore, the variance of the photon number difference is

$$\begin{aligned} \sigma^2_{\Delta n} &= \left(\frac{\tau_{\text{LO}}}{h f_{\text{LO}}}\right)^2 \sigma^2_{\Delta P_{\text{inc}}} \\ &= \left(\frac{\tau_{\text{LO}} \text{NEP}}{h f_{\text{LO}}}\right)^2 B_{\text{el}}. \end{aligned} \tag{4.45}$$

Equalizing Equation (4.39) and Equation (4.45) gives

$$\begin{aligned} \sigma^2_{\hat{x}} &= \sigma^2_{\Delta n} \frac{h f_{\text{LO}}}{P_{\text{LO}} \tau_{\text{LO}}} \\ &= \left(\frac{\tau_{\text{LO}} \text{NEP}}{h f_{\text{LO}}}\right)^2 B_{\text{el}} \frac{h f_{\text{LO}}}{P_{\text{LO}} \tau_{\text{LO}}} \\ &= \frac{\tau_{\text{LO}} \text{NEP}^2 B_{\text{el}}}{h f_{\text{LO}} P_{\text{LO}}}. \end{aligned} \tag{4.46}$$

Therefore,

$$\boxed{\sigma^2_{\hat{x}} \equiv \xi_{\text{det}} = 2\frac{\tau_{\text{LO}} \text{NEP}^2 B_{\text{el}}}{h f_{\text{LO}} P_{\text{LO}}}}, \tag{4.47}$$

where the factor of two is due to having two detectors.

4.4 QUANTIZATION NOISE

4.4.1 Bob

After the signal is detected using Bob's receiver, the output is quantized using an ADC. The limited resolution of the ADC results in a quantization error, which can be modelled using an ideal ADC with excess voltage δV_{Det} at its input, resulting in an uncertainty in the detected photon number given by Equation (4.44). Utilizing Equation (4.41), Equation (4.44) can be expressed as

$$\begin{aligned} \Delta n &= \frac{\Delta I_{\text{ph}} \tau_{\text{LO}}}{h f_{\text{LO}} R} \\ &= \frac{\delta V_{\text{Det}} \tau_{\text{LO}}}{h f_{\text{LO}} R g_{\text{TIA}}}, \end{aligned} \tag{4.48}$$

with the variance being

$$\sigma^2_{\Delta n} = \sigma^2_{\delta V_{\text{Det}}} \left(\frac{\tau_{\text{LO}}}{h f_{\text{LO}} R g_{\text{TIA}}} \right)^2, \tag{4.49}$$

which when equated to Equation (4.39) gives

$$\begin{aligned} \sigma^2_{\hat{x}} &= \frac{h f_{\text{LO}}}{P_{\text{LO}} \tau_{\text{LO}}} \left(\frac{\tau_{\text{LO}}}{h f_{\text{LO}} R g_{\text{TIA}}} \right)^2 \sigma^2_{\delta V_{\text{ADC}}} \\ &= \frac{\tau_{\text{LO}}}{P_{\text{LO}} h f_{\text{LO}} R^2 g^2_{\text{TIA}}} \sigma^2_{\delta V_{\text{ADC}}}. \end{aligned} \tag{4.50}$$

The finite resolution of an ADC results in a voltage variance of [64]

$$\begin{aligned} \sigma^2_{\delta V_{\text{ADC}}} &= \frac{Q^2}{12} \\ &= \frac{V^2_{\text{FS}}}{12 \cdot 2^{2\lfloor B_{\text{th}} \rfloor}}, \end{aligned} \tag{4.51}$$

where Q is the quantization step size, V_{FS} is the full-scale voltage range, and B_{th} is the maximum resolution in SNR-bits, which is given by [64]

$$B_{\text{th}} = \frac{1}{2} \log_2 \left(\frac{V^2_{\text{FS}}}{6 k T R_{\text{eff}} f_{\text{s}}} \right) - 1, \tag{4.52}$$

where k is Boltzmann's constant, T is the absolute temperature, R_{eff} is the effective thermal resistance, and f_{s} is the sampling frequency. A floor function is applied on B_{th} to round it to the greatest integer less than it since a bit can only assume integer

values by definition. Given that $B_{\text{th}} \propto f_{\text{s}}^{-1}$, it can be deduced that $\sigma^2_{\delta V_{\text{ADC}}} \propto f_{\text{s}}$. Thus, the quantization noise of Bob is directly proportional to the sampling rate (f_{s}). Finally, plugging Equation (4.51) in Equation (4.50) and considering two ADCs gives the desired final expression

$$\boxed{\sigma^2_{\hat{x}} \equiv \xi_{\text{ADC}} = \frac{2\tau_{\text{LO}}}{P_{\text{LO}} h f_{\text{LO}} R^2 g^2_{\text{TIA}}} \frac{V^2_{\text{FS}}}{12 \cdot 2^{2\lfloor B_{\text{th}} \rfloor}}}. \tag{4.53}$$

4.4.2 Alice

During the modulation of the initial coherent state ($|\alpha_i\rangle$), the finite resolution of the used DAC contributes to the excess noise. Assuming the desired and the excess outputs of the DAC to be V_{DAC} and δV_{DAC}, respectively, the output voltage is represented as

$$V_a = g(V_{\text{DAC}} + \delta V_{\text{DAC}}), \tag{4.54}$$

where g is the amplification factor of the amplifier following the DAC that is required to drive the I/Q modulator. The eigenvalue of the I/Q modulator output state ($|\alpha_m\rangle$) is[7]

$$\alpha_m = \frac{\alpha_i}{2} (\sin\phi_2 + j \sin\phi_1), \tag{4.55}$$

where α_i is the eigenvalue of the input state ($|\alpha_i\rangle$). Assuming that $\alpha_i \in \mathbb{R}$, the corresponding quadratures for the output state ($|\alpha_m\rangle$) are

$$x_m = \frac{\alpha_i \sin\phi_2}{2}, \tag{4.56}$$

$$p_m = \frac{\alpha_i \sin\phi_1}{2}. \tag{4.57}$$

The obtained phase shift is related to the applied voltage (V_a) as following

$$\phi = \pi \frac{V_a}{V_\pi}, \tag{4.58}$$

where V_a is given by Equation (4.54) and V_π is the voltage required to achieve a π phase shift. The effect of the excess voltage (δV_{DAC}) is that it adds an extra term to the

[7] The derivation of Equation (4.55) is performed in Appendix C.

quadrature x_m as follows[8]

$$
\begin{aligned}
x_m + \delta x_m =& \frac{\alpha_i}{2} \sin\left(\pi \frac{V_a}{V_\pi}\right) \\
=& \frac{\alpha_i}{2} \sin\left(\pi \frac{g[V_{\mathrm{DAC}} + \delta V_{\mathrm{DAC}}]}{V_\pi}\right) \\
=& \frac{\alpha_i}{2} \sin\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi} + \pi \frac{g \delta V_{\mathrm{DAC}}}{V_\pi}\right) \\
=& \frac{\alpha_i}{2} \sum_{n=0}^{\infty} \frac{\mathrm{d}^n \sin\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)}{\mathrm{d}\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)^n} \frac{(\pi \frac{g \delta V_{\mathrm{DAC}}}{V_\pi})^n}{n!} \\
=& \frac{\alpha_i}{2} \sin\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right) \\
&+ \frac{\alpha_i}{2} \sum_{n=1}^{\infty} \frac{\mathrm{d}^n \sin\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)}{\mathrm{d}\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)^n} \frac{(\pi \frac{g \delta V_{\mathrm{DAC}}}{V_\pi})^n}{n!}, \\
\longrightarrow \delta x_m =& \frac{\alpha_i}{2} \sum_{n=1}^{\infty} \frac{\mathrm{d}^n \sin\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)}{\mathrm{d}\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)^n} \frac{(\pi \frac{g \delta V_{\mathrm{DAC}}}{V_\pi})^n}{n!} \\
\approx& \frac{\alpha_i}{2} \left[\left(\pi \frac{g \delta V_{\mathrm{DAC}}}{V_\pi}\right) \cos\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)\right. \\
&\left. - \frac{1}{2}\left(\pi \frac{g \delta V_{\mathrm{DAC}}}{V_\pi}\right)^2 \sin\left(\pi \frac{g V_{\mathrm{DAC}}}{V_\pi}\right)\right] \\
=& \frac{\alpha_i \gamma \delta V_{\mathrm{DAC}}}{2} \left[\cos\left(\gamma V_{\mathrm{DAC}}\right)\right. \\
&\left. - \frac{\gamma \delta V_{\mathrm{DAC}}}{2} \sin\left(\gamma V_{\mathrm{DAC}}\right)\right],
\end{aligned}
\tag{4.59}
$$

where $\gamma \equiv \pi g / V_\pi$. Therefore, the magnitude of the excess quadrature modulation (δx_m)

[8] The Taylor series expansion of a function $f(x)$ in the neighborhood of a point δ is

$$
f(x + \delta) = \sum_{n=0}^{\infty} \frac{\mathrm{d}^n f(x)}{\mathrm{d}x^n} \frac{\delta^n}{n!}.
$$

is

$$
\begin{aligned}
|\delta x_m| &= \frac{\gamma\alpha_i|\delta V_{\mathrm{DAC}}|}{2}\left|\cos\left(\gamma V_{\mathrm{DAC}}\right)\right. \\
&\qquad\left. - \frac{\gamma\delta V_{\mathrm{DAC}}}{2}\sin\left(\gamma V_{\mathrm{DAC}}\right)\right| \\
&\leq \frac{\gamma\alpha_i|\delta V_{\mathrm{DAC}}|}{2}\left[\left|\cos\left(\gamma V_{\mathrm{DAC}}\right)\right|\right. \\
&\qquad\left. + \left|-\frac{\gamma\delta V_{\mathrm{DAC}}}{2}\sin\left(\gamma V_{\mathrm{DAC}}\right)\right|\right] \\
&\leq \frac{\gamma\alpha_i|\delta V_{\mathrm{DAC}}|}{2}\left[\left|\cos\left(\gamma V_{\mathrm{DAC}}\right)\right|\right. \\
&\qquad\left. + \frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\left|\sin\left(\gamma V_{\mathrm{DAC}}\right)\right|\right] \\
&\leq \frac{\gamma\alpha_i|\delta V_{\mathrm{DAC}}|}{2}\left(1 + \frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\right).
\end{aligned}
\tag{4.60}
$$

In order to satisfy Equation (4.19), the I/Q modulator output ($|\alpha_m\rangle$) is attenuated by a factor of $\sqrt{t}$, giving

$$
|\alpha_A\rangle = \left|\sqrt{t}\alpha_m\right\rangle. \tag{4.61}
$$

Thus, the excess quadrature modulation transmitted by Alice (δx_A) is upper bounded by

$$
\delta x_A \leq \frac{\gamma\sqrt{t}\alpha_i|\delta V_{\mathrm{DAC}}|}{2}\left(1 + \frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\right), \tag{4.62}
$$

$$
\longrightarrow \sigma^2_{x_A} \leq \frac{\gamma^2 t\alpha_i^2|\delta V_{\mathrm{DAC}}|^2}{4}\left(1 + \frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\right)^2, \tag{4.63}
$$

Considering the magnitude-squared of Equation (4.55) gives

$$
\begin{aligned}
|\alpha_m|^2 &= \left|\frac{\alpha_i}{2}\left(\sin\phi_2 + j\sin\phi_1\right)\right|^2 \\
&= \frac{\alpha_i^2}{4}\left(\sin^2\phi_2 + \sin^2\phi_1\right),
\end{aligned}
\tag{4.64}
$$

$$
\begin{aligned}
\longrightarrow \alpha_i^2 &= \frac{4|\alpha_m|^2}{\sin^2\phi_2 + \sin^2\phi_1} \\
&= \frac{4|\alpha_A|^2}{t\left(\sin^2\phi_2 + \sin^2\phi_1\right)},
\end{aligned}
\tag{4.65}
$$

which when plugged in Equation (4.63) gives

$$\begin{aligned}\sigma_{x_A}^2 &\leq \frac{\gamma^2|\alpha_A|^2|\delta V_{\mathrm{DAC}}|^2}{\sin^2\phi_2+\sin^2\phi_1}\left(1+\frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\right)^2 \\ &= \frac{\gamma^2\sigma_{A'}^2|\delta V_{\mathrm{DAC}}|^2}{2\left(\sin^2\phi_2+\sin^2\phi_1\right)}\left(1+\frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\right)^2,\end{aligned} \tag{4.66}$$

where the fact that $|\alpha_A|^2 = \langle n_{\mathrm{s}}\rangle = \sigma_{A'}^2/2$ from Equation (4.19) was used. The variances of the quadrature operator ($\sigma_{A'}^2$) and variable (σ_A^2) are related by $\sigma_{A'}^2 = 4\sigma_A^2$, which gives

$$\boxed{\sigma_{x_A}^2 \equiv \xi_{\mathrm{DAC}} \leq \frac{T_{\mathrm{tot}}\gamma^2 2\sigma_A^2|\delta V_{\mathrm{DAC}}|^2}{\sin^2\phi_2+\sin^2\phi_1}\left(1+\frac{\gamma|\delta V_{\mathrm{DAC}}|}{2}\right)^2}, \tag{4.67}$$

where $|\delta V_{\mathrm{DAC}}|$ is given by the square root of Equation (4.51). For QPSK modulation, the RF amplifier gain factor (g) is given by

$$g = \frac{V_\pi}{V_{\mathrm{DAC}}}, \tag{4.68}$$

giving $\gamma = \frac{\pi}{V_{\mathrm{DAC}}}$. Also, since $\phi_1, \phi_2 \in \left\{\pm\frac{\pi}{2}\right\}$ for QPSK modulation, $\sin^2\phi_2 + \sin^2\phi_1 = 2$, resulting in

$$\boxed{\xi_{\mathrm{DAC}}^{\mathrm{QPSK}} \leq \frac{T_{\mathrm{tot}}\pi^2\sigma_A^2|\delta V_{\mathrm{DAC}}|^2}{V_{\mathrm{DAC}}^2}\left(1+\frac{\pi|\delta V_{\mathrm{DAC}}|}{2V_{\mathrm{DAC}}}\right)^2}. \tag{4.69}$$

4.5 NOISE ANALYSIS

In order to approximate the effect of noise sources in a practical experiment, noise models are utilized using hardware-specific parameters that match the experiment described in Chapter 5. This helps optimize system performance and identify potential sources of error, improving experimental accuracy and reliability.

- Laser:
  - Wavelength ($\lambda_{\mathrm{s,\,LO}}$) = 1550 nm
  - LO Power (P_{LO}) = 5 mW
  - Linewidth ($B_{\mathrm{s,\,LO}}$) = 100 kHz
  - Modulation Variance (σ_A^2) = 40.5 SNU
  - $\mathrm{RIN}_{\mathrm{s,\,LO}} = 3.16 \times 10^{-14}\ \mathrm{Hz}^{-1}$
- DAC:

- Full-Scale Voltage ($V_{\text{FS}}^{\text{DAC}}$) = 2 V
- Maximum Voltage (V_{DAC}) = 12 mV
- Resolution ($n_{\text{bits}}^{\text{DAC}}$) = 16 Bits

- ADC:
  - Full-Scale Voltage ($V_{\text{FS}}^{\text{ADC}}$) = 2.5 V
  - Sampling Frequency ($f_{\text{s}}^{\text{ADC}}$) = 2.5 GSa/s
  - Resolution ($n_{\text{bits}}^{\text{ADC}}$) = 12 Bits

- Detector:
  - NEP = 5 pW/$\sqrt{\text{Hz}}$
  - Responsivity (R) = 1.05 A/W
  - Bandwidth (B_{el}) = 400 MHz
  - TIA Gain (g_{TIA}) = 4.76 kV/A

- Channel:
  - Length (L_{ch}) = 50 km
  - Attenuation Rate (α_{ch}) = 0.2 dB/km

The simulated noises along with their parameters dependence and anticipated values are outlined below:

- $\xi_{\text{RIN}_\text{s}}\left(\sigma_A^2, B_\text{s}, \text{RIN}_\text{s}\right) = 0.009$ SNU,
- $\xi_{\text{det}}\left(\tau_{\text{LO}}, \text{NEP}, B_{\text{el}}, f_{\text{LO}}, P_{\text{LO}}\right) = 0.078$ SNU,
- $\xi_{\text{ADC}}\left(\tau_{\text{LO}}, f_{\text{LO}}, P_{\text{LO}}, R, g_{\text{TIA}}, V_{\text{FS}}^{\text{ADC}}, n_{\text{bits}}^{\text{ADC}}\right) = 0.01$ SNU,
- $\xi_{\text{DAC}}^{\text{QPSK}}\left(L_{\text{ch}}, \sigma_A^2, V_{\text{FS}}^{\text{DAC}}, n_{\text{bits}}^{\text{DAC}}, V_{\text{DAC}}^{\text{max}}\right) = 0$ SNU,

where $\tau_{\text{LO}} = 1/B_{\text{el}}$ for a CW laser. Figure 4.2 shows the dependence of ξ_{RINs} on the modulation variance (σ_A^2), exhibiting a linear relationship as the signal power increases. In Figure 4.3, the anticipated values of ξ_{det} and ξ_{ADC} as a function of the LO power (P_{LO}) are presented, following an exponential decay behavior. For ξ_{ADC}, its contribution can be safely ignored.

Among all the noise sources, the detector noise (ξ_{det}) has the most adverse effect on the system performance, as evident from Figure 4.3. Although increasing the LO power will diminish it, other noise sources, like ξ_{RINs} from Figure 4.2 and the thermal noise, start becoming significant.

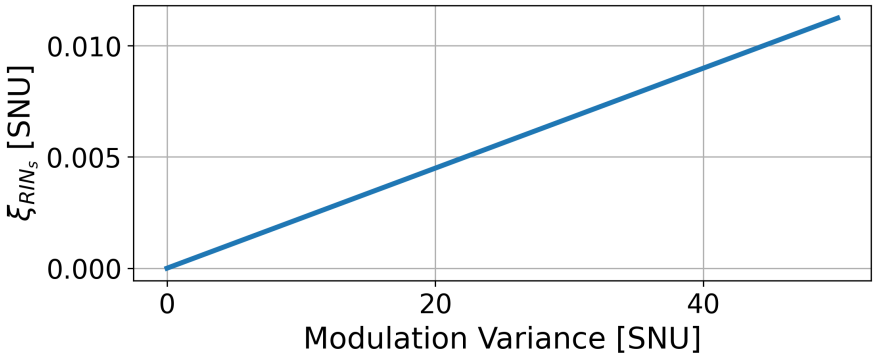


Figure 4.2: Dependence of excess noise due to the relative intensity noise (RIN) on signal power, quantified by modulation variance (σ_A^2). A linear relationship is observed with relatively small noise levels (< 0.01 SNU) for practical values of σ_A^2.

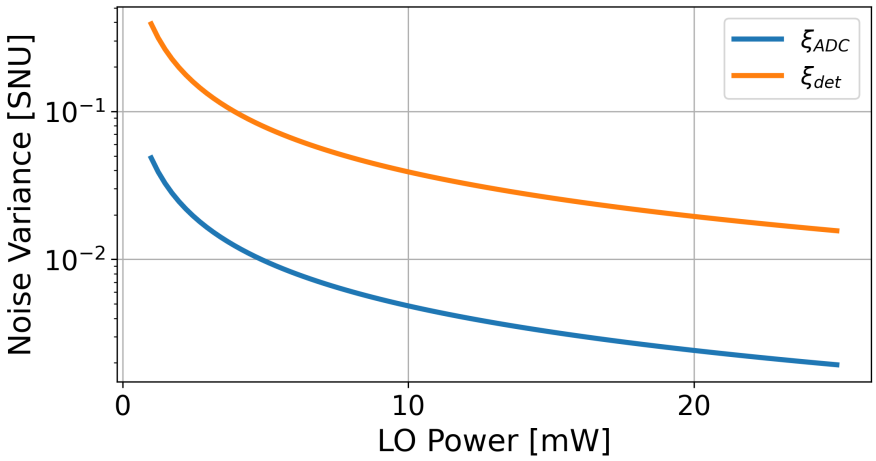


Figure 4.3: The effect of varying the local oscillator (LO) power on the detection noise (ξ_{det}) and analog-to-digital converter (ADC) quantization noise (ξ_{ADC}). An exponential decay dependence is observed, where ξ_{det} is consistently an order of magnitude higher than ξ_{ADC}.

CHAPTER 5

HARDWARE IMPLEMENTATION

5.1 SYSTEM DESIGN

The major advantage of CV-QKD comes from the ability to detect the transmitted quantum signal using coherent receivers, originally developed for coherent telecommunication systems. In the coherent receiver, the quantum signal is mixed with an LO characterized by a high power. In order to correctly interpret the coherent receiver output, the relative phase shift between the incoming quantum signal and the LO should be known. Some implementations of CV-QKD relied on sending the original LO used for the quantum signal [65], known as the transmitted local oscillator (TLO) scheme. However, transmitting the LO poses a security threat as it enables side-channel attacks [66]–[70]. Moreover, in TLO, the channel loss limits the available power of the LO at the receiver side, which degrades the performance of the coherent receiver. As discussed in Appendix B, in shot-noise limited coherent detection, the LO power is assumed to be high such that it is treated classically. Experimentally, it was shown that the typical photons per pulse difference between the LO and the quantum signal is around $n_\gamma = 10^8$ [65]. At a wavelength of 1550 nm, pulse repetition rate of $f_{\text{sym}} = 100$ MBd, and 25 dB channel loss[1], this corresponds to a power difference of

$$\begin{aligned}\Delta P &= \frac{hc}{\lambda} \cdot n_\gamma \cdot f_{\text{sym}} \cdot 10^{\frac{\text{Loss}_{\text{dB}}}{10}} \\ &= \frac{\left(6.626 \times 10^{-34}\right)\left(2.998 \times 10^{8}\right)}{1550 \times 10^{-9}} \cdot 10^8 \cdot 10^8 \cdot 10^{2.5} \\ &\approx 400 \text{ mW}.\end{aligned}$$

Moreover, transmitting the LO with high power, besides being energy inefficient, will disturb the transmitted quantum signals. Therefore, the LLO is the chosen scheme in the

[1] This is the typical loss for a 100 km single-mode fiber at 1550 nm.

design.

In LLO, the carrier signal and the LO are independently generated and carrier recovery is needed to estimate and compensate for the frequency and phase mismatch. Since the quantum signal is extremely weak, resulting in a low transmission rate, it is not reliable to establish a phase reference. Therefore, a strong pilot tone is utilized as a reference signal. The pilot tone is also used for clock synchronization between Alice and Bob. Different multiplexing schemes of the quantum signal and pilot tone have been investigated in the literature. In [71], the time and polarization degrees of freedom are simultaneously utilized for multiplexing. For [31], frequency multiplexing is performed, while a combination of frequency and polarization multiplexing are used in [33], [35]. The opted multiplexing scheme is in the polarization degree of freedom, known as polarization-division multiplexing (PDM). PDM offers several advantages over other multiplexing schemes. First, the power of the pilot tone and quantum signal can be more conveniently adjusted. Moreover, PDM of the pilot tone and quantum signal offers better performance due to the reduction of crosstalk, as shown by [72].

5.2 EXPERIMENTAL SETUP

For system verification, the initial implementation will utilize the TLO scheme along with time-division multiplexing (TDM). The devised experimental setup and DSP algorithms are shown in Figure 5.1. Initially, a 90:10 optical coupler is utilized to split the light from a 1550 nm laser with 100 kHz linewidth. The optical isolator serves to prevent decoherence and damage to the laser. The higher power output is transmitted directly to the receiver to be used as an LO. In reality, the LO could be generated at Bob's side, with appropriate signal processing to correct the frequency offset between the transmitted laser and LO [30]. Nevertheless, the configuration discussed here suffices for the current scope of work. The signal is transmitted through a one km standard single-mode fiber with 0.2 dB/km attenuation rate. At the receiver, a 90° optical hybrid is used, followed by two 400

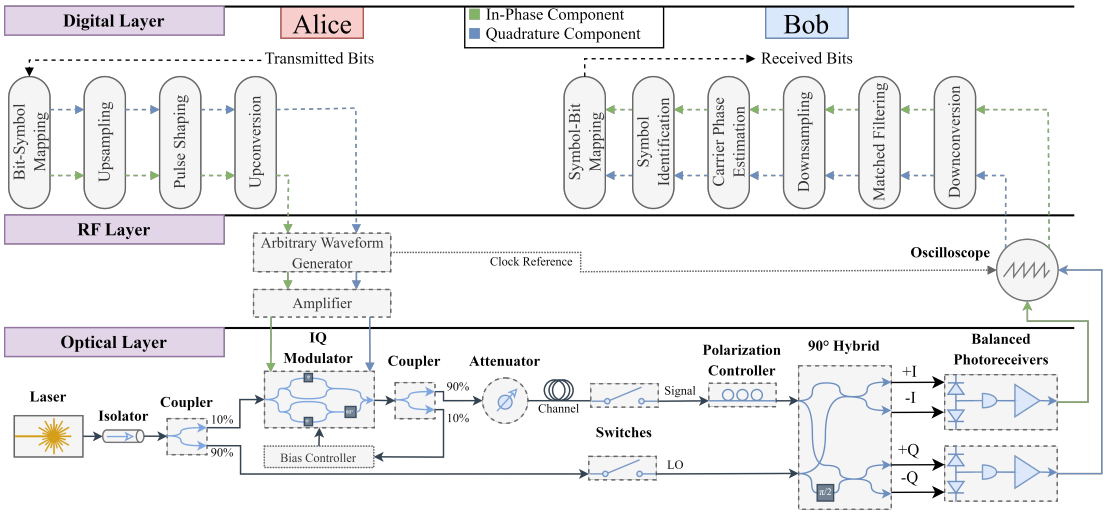


Figure 5.1: System architecture showcasing the utilized signal processing algorithms and hardware setup. The pulse-shaped and frequency-up-converted data are modulated into the optical signal via an RF waveform. The signal and local oscillator (LO) polarizations are matched at the receiver before being mixed in the 90° hybrid. The 90° hybrid generates a pair of signals for each quadrature, which is detected using a balanced receiver. An oscilloscope subsequently samples the output of the balanced receiver.

MHz bandwidth and DC-coupled balanced photoreceivers with a 25 dB common-mode rejection ratio (CMRR)[2]. The low 5 pW/$\sqrt{\text{Hz}}$ NEP makes this receiver applicable for operation in the shot-noise-dominated regime, which is required in CV-QKD. Finally, the analog output is sampled at 2.5 GSa/s with a 390 μV resolution enabled by the high-resolution 12-bit oscilloscope. In order to eliminate the need for DC offsetting, which degrades the oscilloscope resolution, DC blocks are placed after the balanced receivers. Even though the photoreceiver DC component is blocked, there is a significant low-frequency pink noise due to the electronics, which needs to be eliminated to obtain positive key rates. This is achieved by matched filtering, an LPF that captures the signal band after shifting the low-frequency electronic noise away from the baseband through frequency downconversion.

[2]The CMRR is a metric that quantifies an electronic circuit's ability to reject undesired common-mode signals in both the input signal and the ground reference. A higher value indicates that the circuit can more effectively reject common-mode signals, thus preserving the integrity of the differential signal.

5.3 RESULTS

5.3.1 Shot-Noise Calibration[3]

For the following result, a different balanced receiver than the one used in Section 5.3.2 and discussed previously is utilized. The experimental stages are outlined in Table 5.1. At first, the detector noise ($\bar{\xi}_{\text{det}}$) is measured by blocking both switches. Then, the LO switch is turned ON to estimate the shot noise variance (N_0). High clearance between the shot and detector noises is desired, quantified by the logarithmic difference of their powers as following

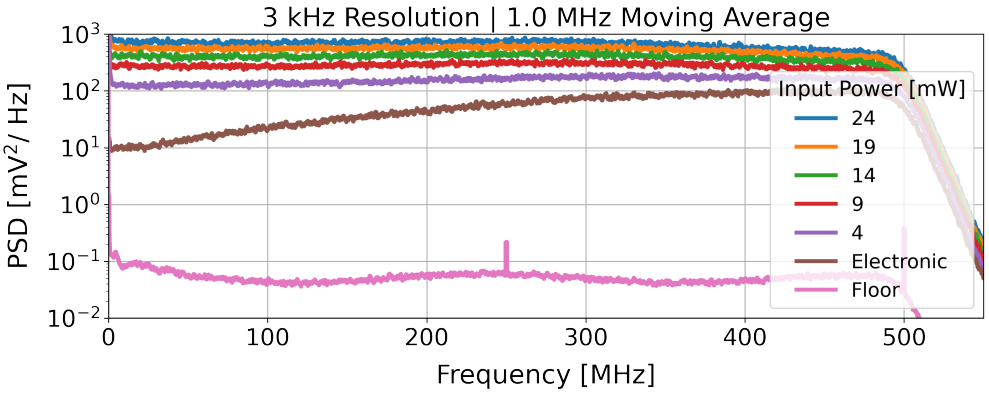
$$\text{Clearance} \equiv 10 \cdot \log_{10}\left(\frac{\bar{\xi}_{\text{sn}}}{\bar{\xi}_{\text{det}}}\right) \qquad [\text{dB}]. \tag{5.1}$$

Table 5.1: The followed steps needed to evaluate the detector (electronic noise $\bar{\xi}_{\text{det}}$), shot-noise (N_0), and excess noise ($\bar{\xi}_{\text{A}}$) different sources of variance.

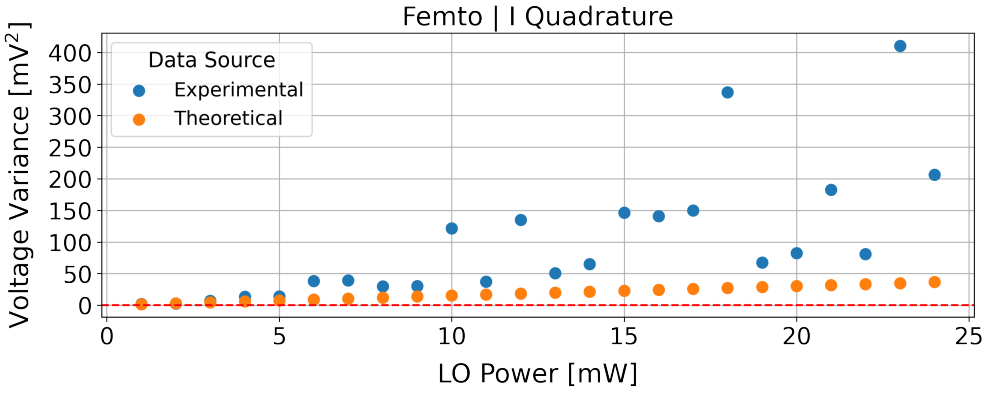
	LO Switch	**Signal Switch**	**Measured Variance [V^2]**
Stage I	OFF	OFF	$\bar{\xi}_{\text{det}}$
Stage II	ON	OFF	$N_0 + \bar{\xi}_{\text{det}}$
Stage III	ON	ON	$N_0 + \bar{\xi}_{\text{det}} + T_{\text{tot}} \cdot \bar{\sigma}_{\text{A}}^2 + \bar{\xi}_{\text{tot}}$

An optical attenuator was used to vary the LO power to maximize the clearance while ensuring the linear power dependence, corresponding to the quantum regime where the shot noise is dominant over other classical noises (e.g., thermal and laser intensity fluctuation). As Figure 5.2 shows, the low-frequency noise has a detrimental effect on calibrating the receiver in the shot-noise limit. When this noise is blocked using a LPF, the expected linear-dependence is obtained as shown in Figure 5.3. The frequency response plots shown in 5.2 and 5.3 reveal that the high-frequency components have significantly higher electronic noise levels, resulting in a smaller Clearance, as illustrated in 5.4. Limiting the high-frequency components can increase the Clearance, but this also reduces the maximum possible symbol rate, highlighting the need to optimize between these two factors.

[3] A. Alsaui, Y. Alwehaibi, A. Prabhakar, and D. Venkitesh, "Digital filter design for experimental continuous-variable quantum key distribution", in 2023 Optical Fiber Communications Conference and Exhibition (OFC), IEEE, 2023, pp. 1–3.



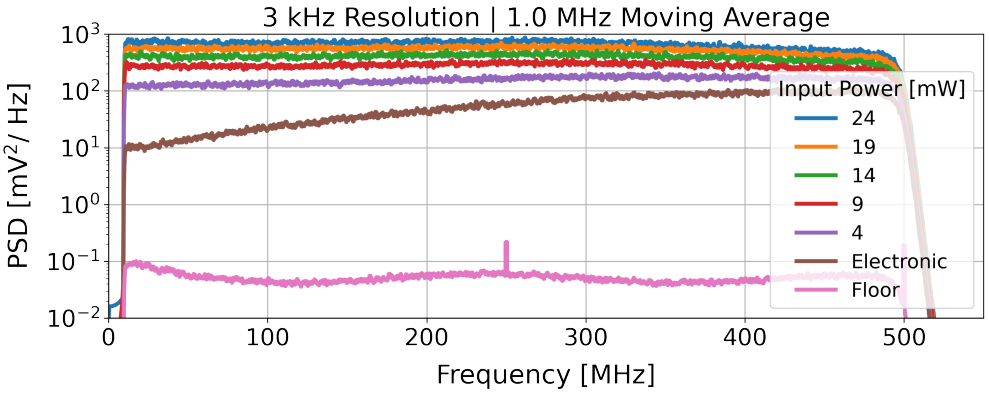
(a)



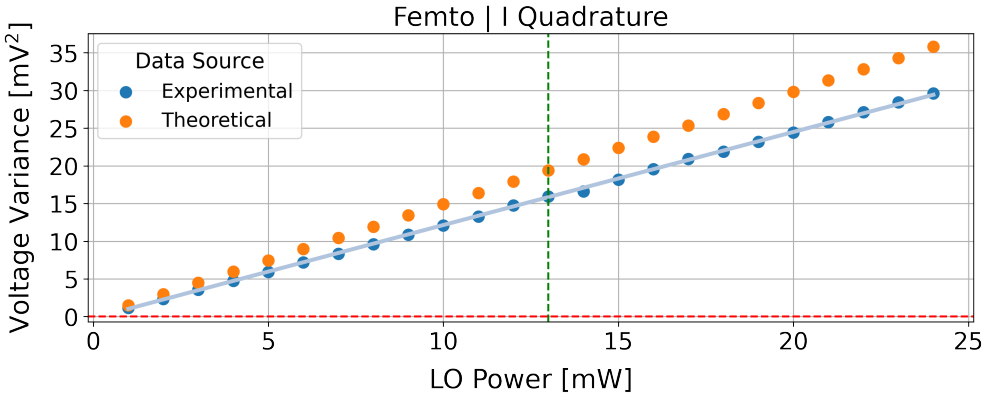
(b)

Figure 5.2: (a) Magnitude of frequency components and (b) corresponding voltage variance behavior for the different local oscillator (LO) powers. Although a linear relationship with LO power is expected in (b), it is not observed due to the influence of low-frequency noise depicted in (a).

For the optimized LO power, we capture the variance at the output (σ_B^2) for different values of input signal power levels. We also vary the first stage band-pass filter (BPF)'s lower and upper cutoff frequencies. The secret key rate (SKR) for each case is shown in the heat map in Figure 5.5. In case of low signal powers, irrespective of the filter used, SKR is close to zero because the electronic noise dominates. At very high signal power levels, the system moves to classical operation. In the optimal range of optical powers, the filters' cutoff frequencies are found to significantly influence the maximal achievable key rates, shown in Figure 5.5. Note that the filter bandwidths change with a change in the shot noise (optical power). Figure 5.6 shows the achievable transmission lengths and the corresponding SKR for the possible combination of the lower and upper



(a)



(b)

Figure 5.3: Low-pass filtered version of Figure 5.2, where (a) shows the magnitude of frequency components and (b) the corresponding voltage variance behavior for the different local oscillator (LO) powers. The low-pass filter removes the effect of high-frequency noise, revealing a clear linear dependence on LO power in (b).

cutoff frequencies indicated in the legend. At 20 km, around 20 MBd is possible for $\sigma_A^2 = 12.5\ \mu$W. Note that the possible symbol rate for modulation gets limited as the bandwidth decreases. These plots highlight the importance of the correct choice of filter cutoff frequencies in the BPF used as a first post-processing step to achieve a positive SKR in a practical experiment.

5.3.2 Symbols Exchange

The shot-noise calibration procedure is redone for the initially described balanced receiver.Figure 5.7 shows the measured noise variance as a function of LO power after

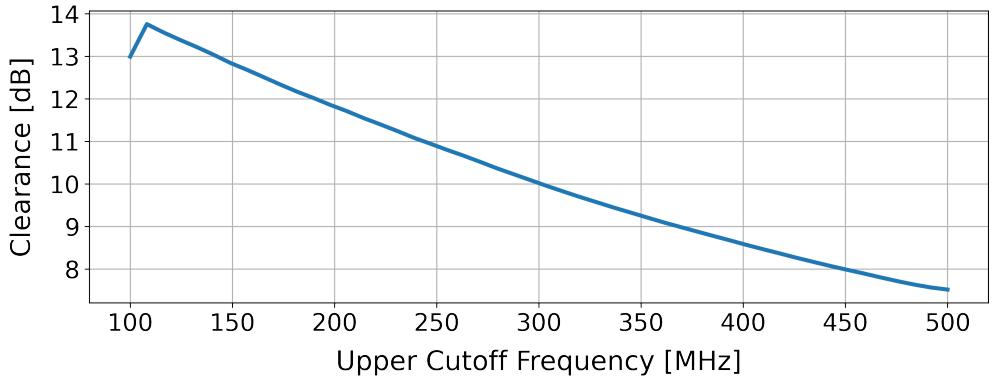


Figure 5.4: The effect of band-pass filtering on the achieved Clearance, with the lower cutoff frequency set to 100 MHz. The achieved Clearance exhibits an inverse relationship with the upper cutoff frequency, as the filter blocks the higher-power components of the electronic noise.

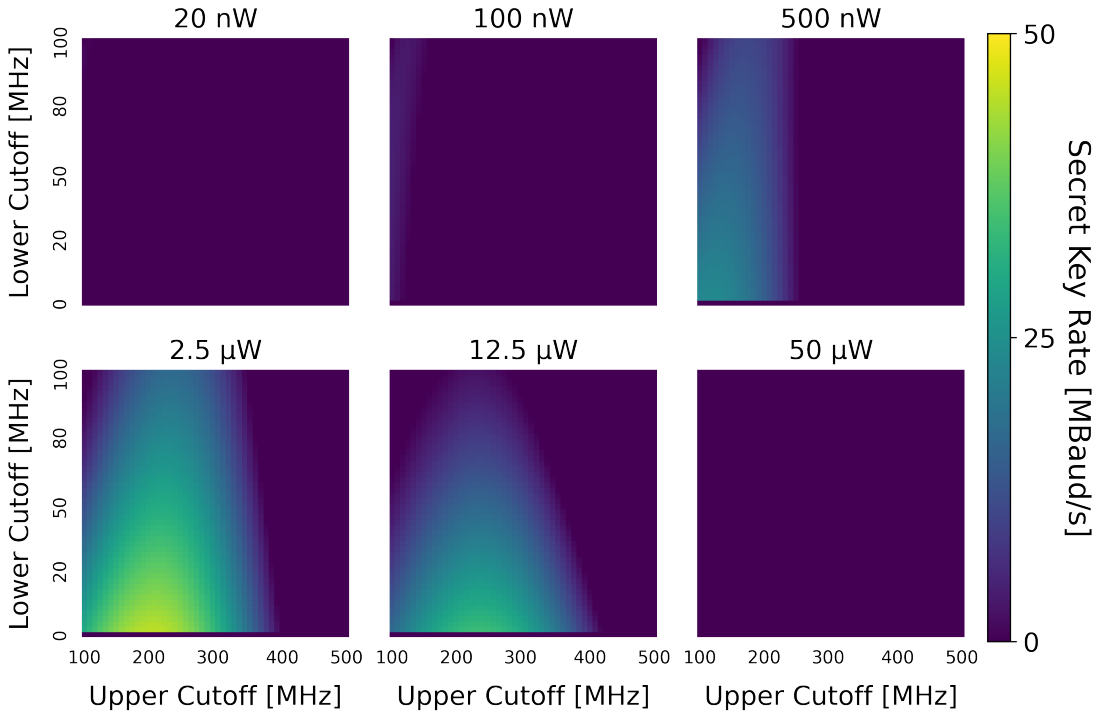


Figure 5.5: Heat map of secret key rate (SKR) for different input signal power levels with optimized local oscillator (LO) power and various band-pass filter (BPF) cutoff frequencies. The filters' cutoff frequencies significantly influence the maximal achievable key rates in the optimal range of optical powers.

applying a BPF with cutoff frequencies $[32.5, 92.5]$ MHz, corresponding to a 50 Mbd signal with a 0.2 ROF and up-converted to 62.5 MHz. The achieved clearance is 19.4

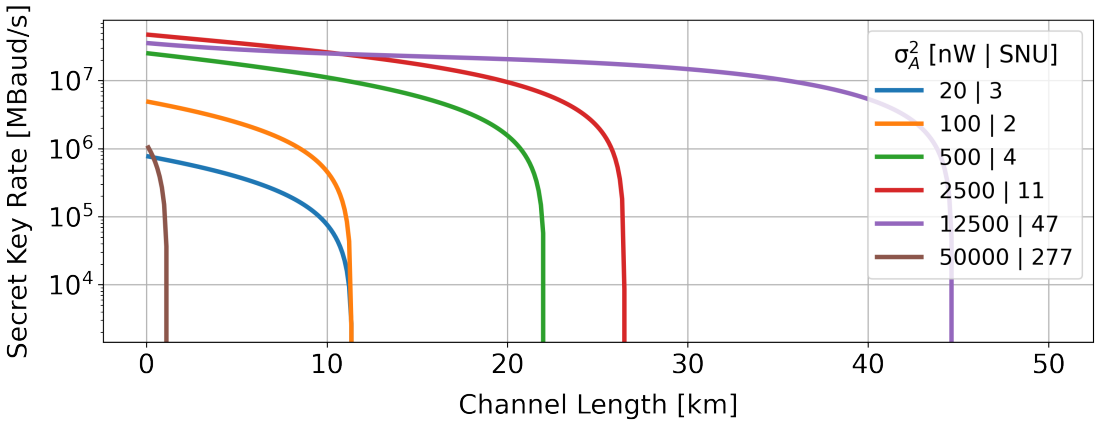


Figure 5.6: Extrapolated secret key rate (SKR) for the optimum cutoff frequencies at each modulation power from Figure 5.5.

dB at around 5 mW LO power. We use this optimized LO power for further experiments.

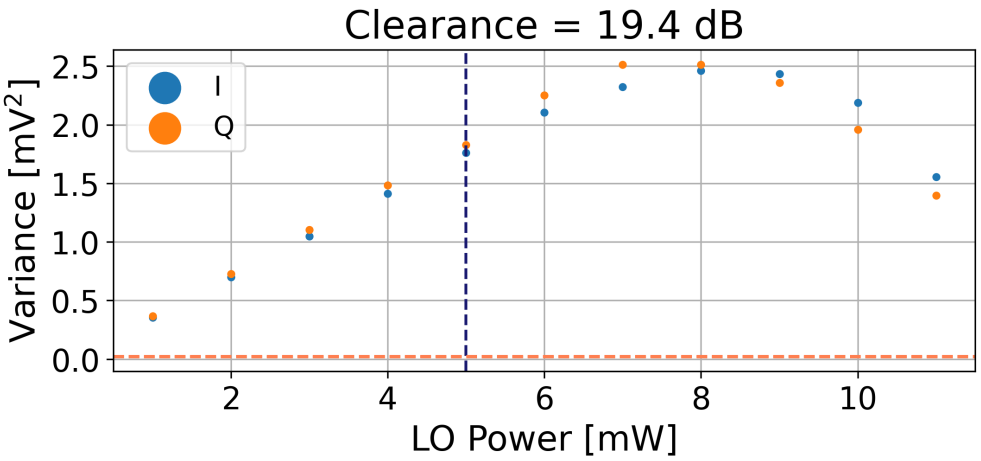


Figure 5.7: Shot-noise calibration procedure: voltage variance is measured as a function of the LO power. The dashed orange line indicates the detector noise, and the purple line shows the optimal operating point.

6,558 QPSK symbols are exchanged at a 50 MBd rate, where the first half is dedicated to pilot symbols for phase correction. The symbols obtained after the Rx DSP are shown in Figure 5.9, where the pilot symbols' high power compared to the quantum symbols is apparent. Moreover, the obtained phase is smudged all over the phasor plane, caused by the linear phase shift depicted in Figure 5.10. The retrieved quantum symbols after phase correction are shown in Figure 5.11 with 4% BER, where the amplitude has been

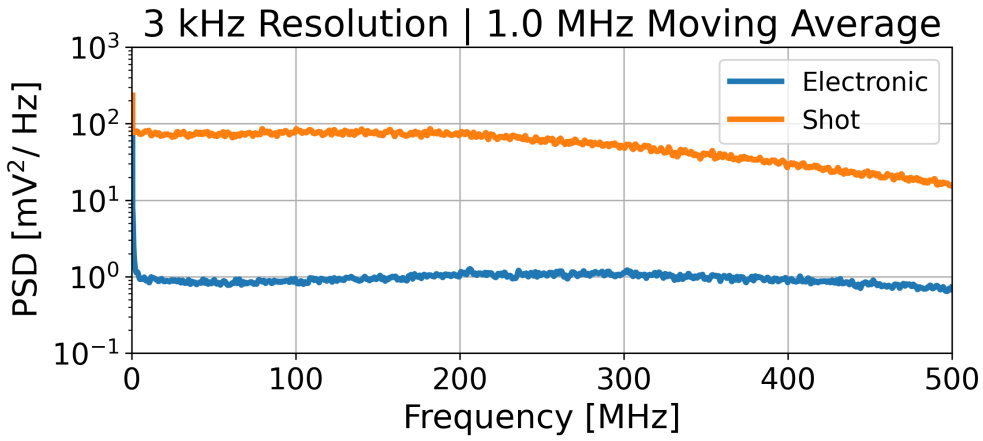


Figure 5.8: Power spectral density contributions of the detector and Shot noises at the chosen 5 mW LO operation point. The bandwidth considered affects the clearance between the shot and electronic noise, where the higher frequency band reduces clearance.

normalized to SNU after dividing the voltage by the square root of the shot noise (N_0). The modulation variance (σ_A^2) is estimated as following

$$\begin{aligned} \sigma_A^2 &= 2\langle n \rangle \\ &= 2\frac{E_{sym}}{E_\gamma} \\ &= 2\frac{P_{sym} \cdot T_{sym}}{\frac{hc}{\lambda}}. \end{aligned} \tag{5.2}$$

Since the symbol power (P_{sym}) is too weak to be measured by the optical power meter (OPM), the pilot signal power (P_{pilot}) and the quantum to pilot signals amplitude ratio (R_{sym}) are utilized to compute it as follows

$$\begin{aligned} P_{sym} &= P_{pilot} \cdot R_{sym}^2 \\ &= (900\ \text{nW}) \cdot (0.012)^2 \\ &= 130\ \text{pW}, \end{aligned} \tag{5.3}$$

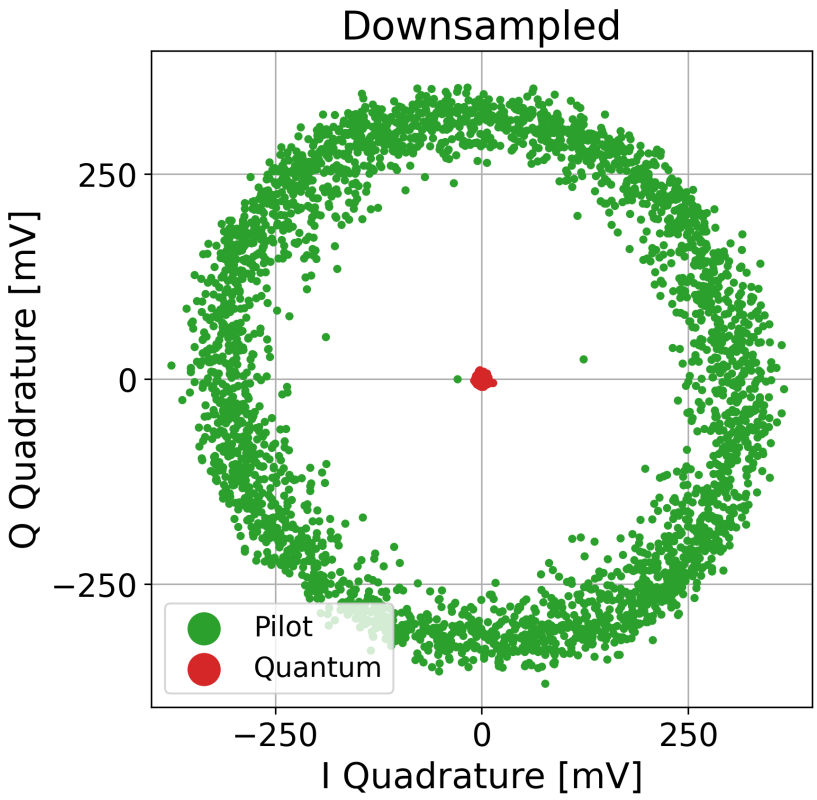


Figure 5.9: Phasor representation of the pilot and quantum symbols before phase correction, showing the spread of constellation points around the phase space due to linear phase noise.

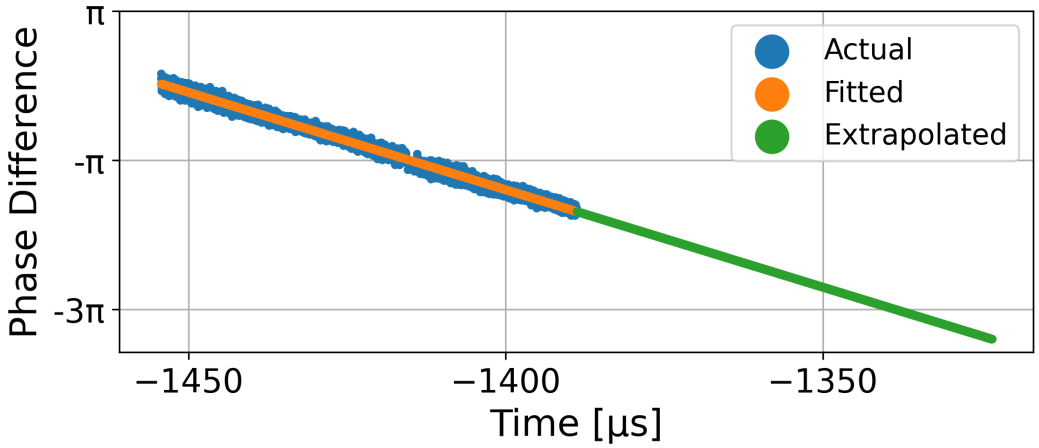


Figure 5.10: The extrapolated quantum symbols correction phase from the linearly fitted pilot tone phase offset.

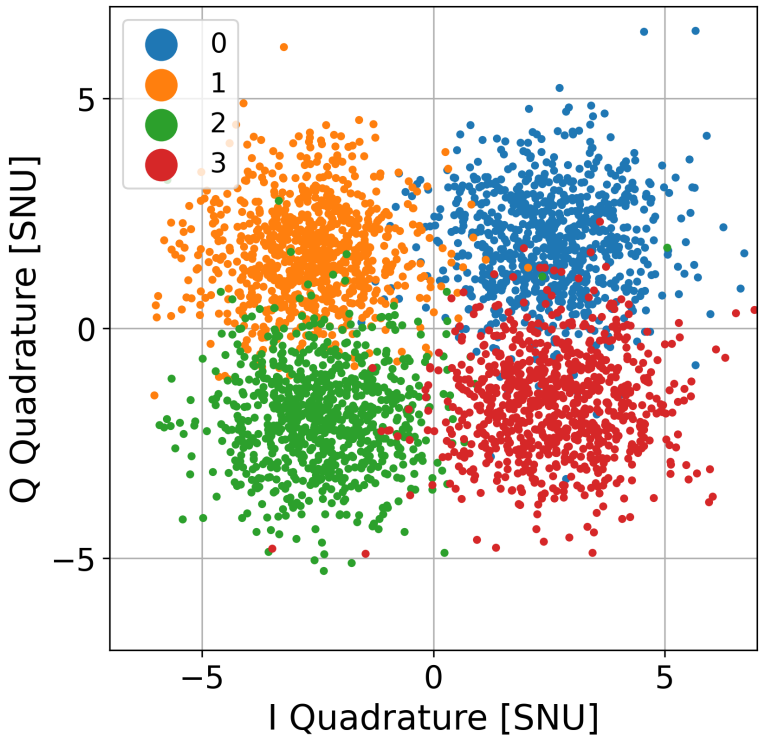


Figure 5.11: The phasor representation of the retrieved quantum symbols shows each symbol represented as a vector in the complex plane. The length of the vector indicates the symbol's amplitude, while the angle represents the phase. As intended, the symbols are clustered around the origin, indicating a high degree of uncertainty in distinguishing them, resulting in a high bit error rate (BER) of 4%.

which gives

$$\begin{aligned}\sigma_{\mathrm{A}}^2 &= 2\frac{\left(152\times10^{-12}\right)\cdot\left(20\times10^{-9}\right)}{\left(6.63\times10^{-34}\right)\left(3.00\times10^{8}\right)}\cdot\left(1550\times10^{-9}\right)\\ &= 40.5\ \text{SNU},\end{aligned} \tag{5.4}$$

corresponding to around 20 photons per symbol. For a back-to-back configuration with a channel length of a couple of meters, the obtained excess noise (ξ_{exc}) was 0.0002 SNU, which permits system operation with positive SKR for high distances as shown in Figure 5.12.

The system performance for different signal powers is investigated. Figure 5.13 shows the effect of the signal power on the achieved BER. The investigated trials had a photon

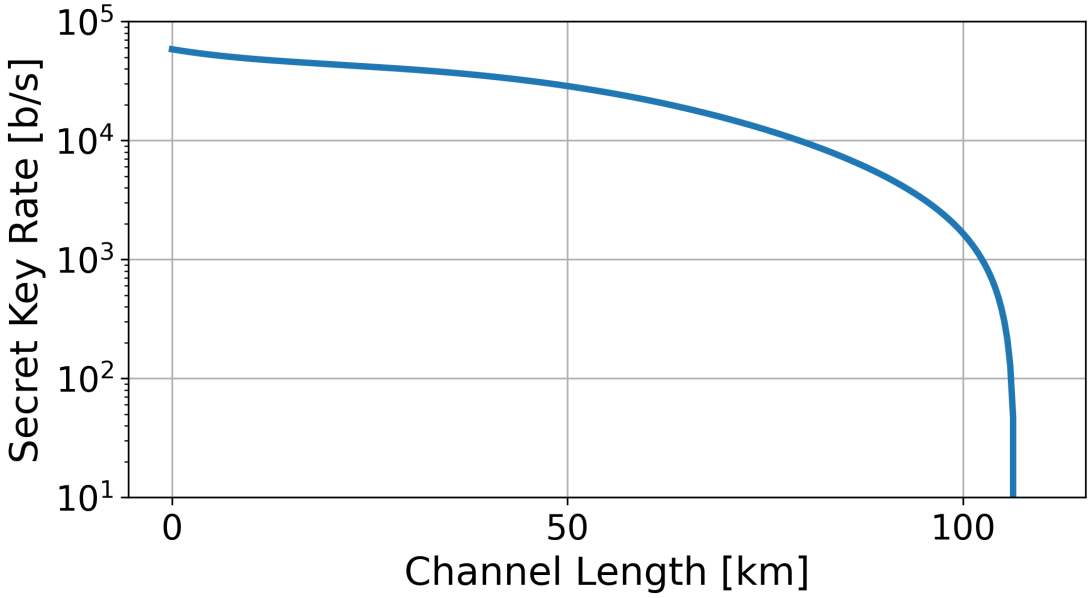


Figure 5.12: The extrapolated SKR for $\xi_{\text{exc}} = 0.0002$ SNU and $\sigma_{\text{A}}^2 = 40.5$ SNU.

per symbol of 0.3, 1.1, 4.4, and 17.8, corresponding to the powers 1.8, 7.1, 28.5, and 114 pW, respectively. As expected, higher modulation variances decrease the BER. On the other hand, as highlighted in Figure 2.8, the SKR diminishes for a higher signal power. Therefore, the optimal power range should be carefully chosen to maximize the SKR without increasing the BER beyond what the ECC algorithm can correct.

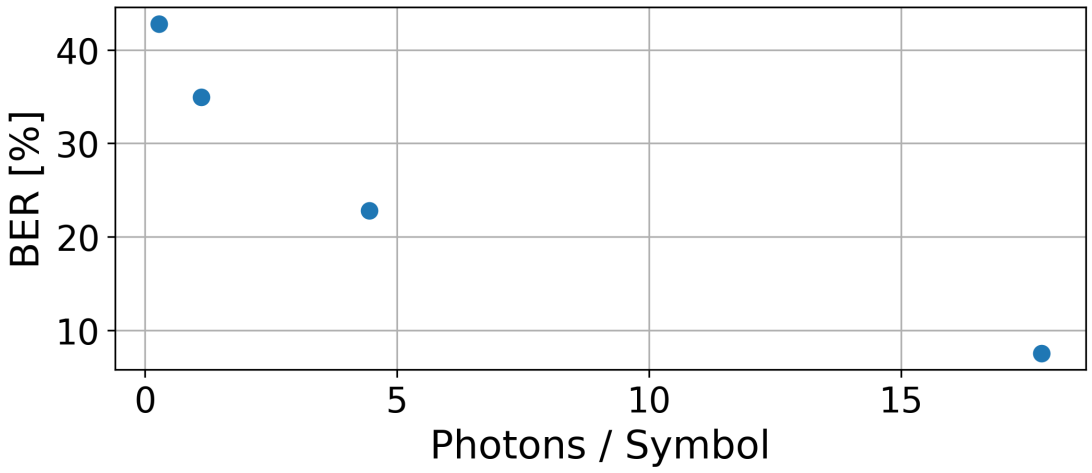


Figure 5.13: Effect of varying the signal power, represented by photons per symbol, on the achieved bit error rate (BER). As expected, a low modulation variance gives rise to a higher error.

CHAPTER 6

CONCLUSION

6.1 MAIN CONTRIBUTION

The work extensively covered all the practical CV-QKD implementation elements. Initially, the theoretical background of CV-QKD was discussed and analyzed, including mathematical formalism, system representation, and state evolution. Moreover, the post-processing stages for the protocol were detailed. The security proofs of CV-QKD systems were rigorously derived and examined.

Techniques from coherent optical communication were utilized as the enabling platform for implementing CV-QKD systems. The operation principle of the coherent receiver was reviewed, and the appropriate operation regime was determined. DSP algorithms relevant to the desired system functionality were first theoretically defined. Then, Python-based implementation of the DSP techniques was built from scratch, including resampling, modulation, filtering, and phase correction algorithms. The practical aspects of deploying the devised DSP algorithms were also considered.

The physical effect from which the system security is derived, the quantum shot noise, was examined, and its mathematical description was meticulously derived. Concerning the anticipated system nonidealities, prominent sources of classical noise were investigated, and their expected effect on the system performance was simulated. Although the final expressions are identical to [50], the derivations performed in this work are more detailed and elaborate.

The experimental system architecture is presented with a rationale for the software and hardware design choices. Optimization of the digital filtering procedure demonstrated the capability of enhancing the system performance, which was published at the Optical

Fiber Communication (OFC) conference [73]. Finally, quantum symbols were exchanged with low excess noise, demonstrating the system's capability of transferring secure keys over large distances.

All the utilized hardware components (e.g., IQ modulator, hybrid, and balanced receiver) are typically used in coherent optical communications. The novel aspect is picking the correct components with the needed characteristics to enable quantum communication applications. Below are some of the significant hardware characteristics that has been considered:

- High voltage resolution, sample rate, and bandwidth arbitrary waveform generator (i.e., DAC) and oscilloscope (i.e., ADC).
- Small linewidth laser.
- Low dark noise and high bandwidth balanced photoreceiver.

One novel aspect is the implemented time-multiplexing scheme of the pilot tone (to track the laser phase) and quantum symbols. Other works have utilized time-multiplexing but in a different way than what was done in this work [74], although both approaches result in an equivalent outcome.

Overall, this work contributes to the field of QKD by demonstrating the capability of a discrete-modulated CV-QKD system using state-of-the-art components. Developing robust DSP algorithms further enhance the achievable SKR, and investigating various noise sources and their effects on system performance led to the development of methods to mitigate these effects. The main contributions of this Master's thesis are listed below.

- Operation of an optical QPSK-modulated CV-QKD system through:
  1. Robust DSP algorithms.
  2. Thorough security analysis.
  3. Appropriate system design.
  4. Careful experimental implementation.
- System performance enhancing through:

1. Digital filter optimization [73]. 2. Utilization of machine learning.[1]

6.2 FUTURE WORK

The proof-of-principle CV-QKD system has successfully demonstrated its capability to achieve high key rates over long distances. However, future work should incorporate finite-size analysis to ensure its practical applicability, considering the effect of finite data samples on the system's security. This will result in a more realistic assessment of the achievable key rates, which will be lower than the asymptotic limit presented in Figure 5.12. Additionally, the system's quantum symbol power can be optimized for each channel length to further increase the achievable key rates. Moreover, Gaussian security proofs are known to overestimate the SKR of QPSK modulation in the high-power regime of greater than five photons per symbol [51]. In order to address this limitation, two approaches could be considered: reducing the power of the quantum symbols or utilizing the ready-made MATLAB model for QPSK modulation by [44]. On the experimental front, potential areas for improvement in CV-QKD systems include multiplexing the pilot tone in both the frequency and polarization degrees of freedom, which has been shown to reduce crosstalk between the classical and quantum channels and increase the SKR [72]. This would require a dual-polarization I/Q modulator and a polarization-diverse coherent receiver. Also, utilizing a local LO at Bob's side can enhance security against side-channel attacks [66]. By exploring these potential improvements, CV-QKD systems could achieve higher SKRs and enhanced security.

[1] A. Alsaui, Y. Alghofaili, and D. Venkitesh, "Machine Learning Modeling and Time-Series Decomposition Analysis for Continuous-Variable Quantum Key Distribution", European Conference on Optical Communication (ECOC), 2023 [Submitted Paper]

APPENDIX A

SHOT NOISE CURRENT

In order to derive an expression for the variance of the shot noise current fluctuation, $\left[\Delta I_{\text{ph}}(t)\right]^2$, consider the configuration illustrated in Figure A.1a, where a potential difference is applied across two electrodes separated by a distance d. Since the potential difference is kept small, electrons are emitted from electrode A to electrode B in a random manner, generating a current ($i(t)$) for each impinging electron. An exchanged electron can be modelled as a large and thin sheet of charge $-e$ which moves towards electrode B with speed v. Utilizing Figure A.1b, the induced charge on electrodes A and B are [75]

$$Q_A = \frac{e(d-x)}{d}, \tag{A.1}$$

$$Q_B = \frac{ex}{d}, \tag{A.2}$$

where the varying charge (Q_B) gives rise to the current generated in electrode B as follows

$$i(t) = \frac{\mathrm{d}Q_B}{\mathrm{d}t} = \frac{e}{d}\frac{\mathrm{d}x}{\mathrm{d}t} = \frac{e}{d}v(t), \tag{A.3}$$

for a velocity $v(t)$ of the moving sheet. For an aperiodic signal $x(t)$, its Fourier transform can be expressed as

$$X(\omega) = \mathcal{F}\left[x(t)\right] = \int_{-\infty}^{\infty} x(t)e^{-j\omega t}\mathrm{d}t. \tag{A.4}$$

Now, letting the time of emission and absorption of the electron be 0 and t_a, respectively, the Fourier transform of $i(t)$ is

$$I(\omega) = \frac{e}{d}\int_0^{t_a}\frac{\mathrm{d}x}{\mathrm{d}t}e^{-j\omega t}\mathrm{d}t = \frac{e}{d}\int_0^{t_a} e^{-j\omega t}\mathrm{d}x. \tag{A.5}$$

Since the transition time of the electron, t_a, is extremely small, $\omega t_a \ll 1$ and thus

$$I(\omega) \approx \frac{e}{d} \int_0^{t_a} \mathrm{d}x = e. \tag{A.6}$$

The PSD of a signal $x(t)$ with a Fourier transform $X(\omega)$ is defined as

$$S_x(\omega) = \lim_{T \to \infty} \frac{|X_T(\omega)|^2}{T}, \tag{A.7}$$

where $S_x(\omega)\mathrm{d}\omega$ is the average power from the frequency components ω to $\omega + \mathrm{d}\omega$ of the signal $x(t)$. For a Poissonian distribution, the PSD can be approximated as [75]

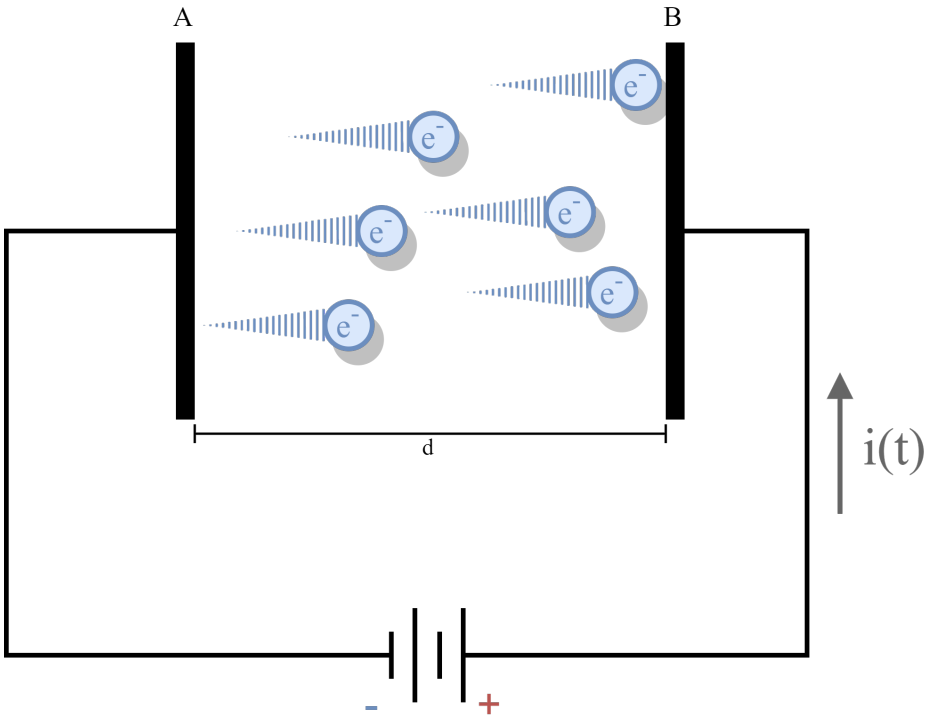
$$S_x(\omega) \approx 2\langle N \rangle |X(\omega)|^2, \tag{A.8}$$

where $\langle N \rangle$ is the average rate of impinging electrons. For $i(t)$, the PSD is

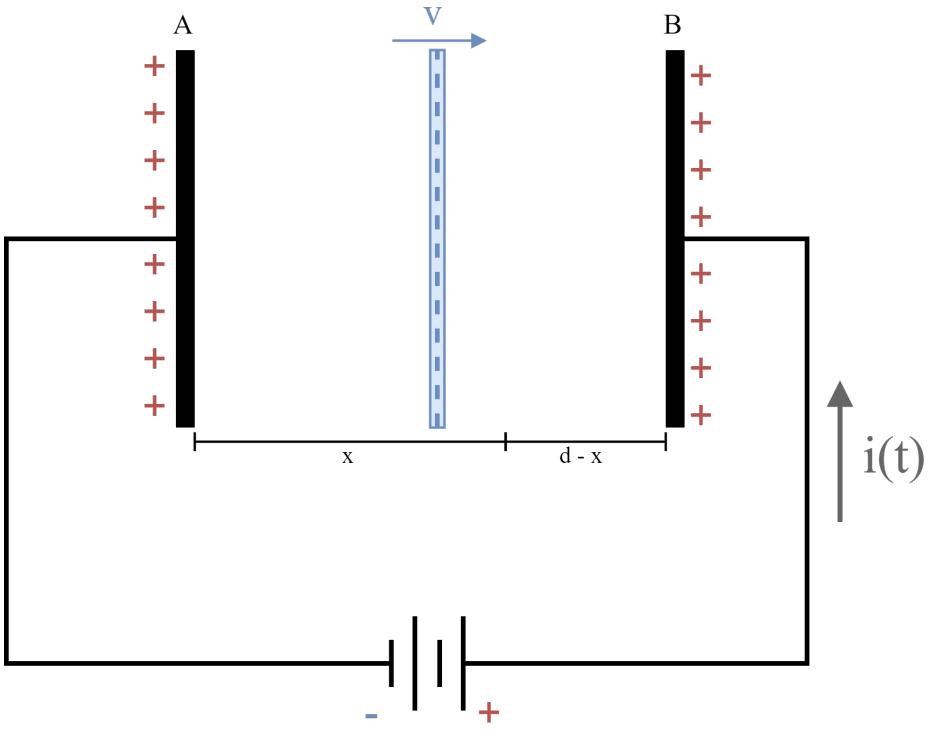
$$S_i(\omega) = 2\langle N \rangle |I(\omega)|^2 = 2\langle N \rangle e^2 = 2\langle I \rangle e. \tag{A.9}$$

Given a bandwidth $\Delta\omega$, the sought-after form of the shot noise current variance is

$$\boxed{\langle i_{\mathrm{SN}}^2 \rangle = 2\langle I \rangle e \Delta\omega}. \tag{A.10}$$



(a)



(b)

Figure A.1: The considered configuration utilized for the derivation of an expression for $\left[\Delta I_{\text{ph}}(t)\right]^2$.

APPENDIX B

BALANCED HOMODYNE DETECTION

The balanced homodyne detector (BHD) is the quantum analogue of the 180° hybrid. In principle, the signal of interest is mixed with a LO using a 50:50 beam splitter (BS) as shown in Figure B.1. For an ideal phase-free (balanced) 50:50 BS, the scattering matrix is given by [52]

$$T_{BS} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & j \\ j & 1 \end{bmatrix}. \tag{B.1}$$

For the input coherent state ($|\alpha\rangle$), the corresponding annihilation operator ($\hat{a}$) in SNU is given by Equation (2.35). The LO field is treated classically since it has a high power with respect to the signal, which is given by

$$\alpha_{\mathrm{LO}} = |\alpha_{\mathrm{LO}}| e^{j\theta} = x_{\mathrm{LO}} + j p_{\mathrm{LO}}. \tag{B.2}$$

Applying the BS to the two input signals give rise to the outputs represented by the operators $\hat{O}_1$ and $\hat{O}_2$ as following

$$\begin{aligned} \begin{bmatrix} \hat{O}_1 \\ \hat{O}_2 \end{bmatrix} &= T_{BS} \begin{bmatrix} \hat{a} \\ \alpha_{\mathrm{LO}} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & j \\ j & 1 \end{bmatrix} \begin{bmatrix} \hat{a} \\ \alpha_{\mathrm{LO}} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} \hat{a} + j\alpha_{\mathrm{LO}} \\ j\hat{a} + \alpha_{\mathrm{LO}} \end{bmatrix}. \end{aligned} \tag{B.3}$$

The photocurrents generated from the BS outputs are proportional to the number of photons, which is represented by the photon number operators $\hat{n}_1$ and $\hat{n}_2$ for the outputs

$\hat{O}_1$ and $\hat{O}_2$, respectively, where they are given by

$$\begin{aligned}\hat{n}_1 = \hat{O}_1^\dagger \hat{O}_1 &= \frac{1}{2}\left(\hat{a}^\dagger - j\alpha_{\mathrm{LO}}^*\right)\left(\hat{a} + j\alpha_{\mathrm{LO}}\right) \\ &= \frac{1}{2}\left(\hat{a}^\dagger\hat{a} + j\hat{a}^\dagger\alpha_{\mathrm{LO}} - j\alpha_{\mathrm{LO}}^*\hat{a} + |\alpha_{\mathrm{LO}}|^2\right),\end{aligned} \tag{B.4}$$

$$\begin{aligned}\hat{n}_2 = \hat{O}_2^\dagger \hat{O}_2 &= \frac{1}{2}\left(-j\hat{a}^\dagger + \alpha_{\mathrm{LO}}^*\right)\left(j\hat{a} + \alpha_{\mathrm{LO}}\right) \\ &= \frac{1}{2}\left(\hat{a}^\dagger\hat{a} - j\hat{a}^\dagger\alpha_{\mathrm{LO}} + j\alpha_{\mathrm{LO}}^*\hat{a} + |\alpha_{\mathrm{LO}}|^2\right).\end{aligned} \tag{B.5}$$

Thus, the difference between the generated photocurrent should be proportional to the difference photon number operator ($\Delta\hat{n}$) given by

$$\Delta\hat{n} \equiv \hat{n}_1 - \hat{n}_2 = j\left(\alpha_{\mathrm{LO}}\hat{a}^\dagger - \alpha_{\mathrm{LO}}^*\hat{a}\right). \tag{B.6}$$

Utilizing Equation (2.34) and Equation (2.35) along with Equation (B.2) in Equation (B.6) gives

$$\begin{aligned}\Delta\hat{n} &= j\left(\alpha_{\mathrm{LO}}\hat{a}^\dagger - \alpha_{\mathrm{LO}}^*\hat{a}\right) \\ &= |\alpha_{\mathrm{LO}}|e^{j\theta}\frac{j}{2}(\hat{x} - j\hat{p}) - |\alpha_{\mathrm{LO}}|e^{-j\theta}\frac{j}{2}(\hat{x} + j\hat{p}) \\ &= \frac{|\alpha_{\mathrm{LO}}|}{2}\left[j\left(e^{j\theta} - e^{-j\theta}\right)\hat{x} + \left(e^{j\theta} + e^{-j\theta}\right)\hat{p}\right] \\ &\longrightarrow \boxed{\Delta\hat{n} = |\alpha_{\mathrm{LO}}|\left[-\sin(\theta)\hat{x} + \cos(\theta)\hat{p}\right]}.\end{aligned} \tag{B.7}$$

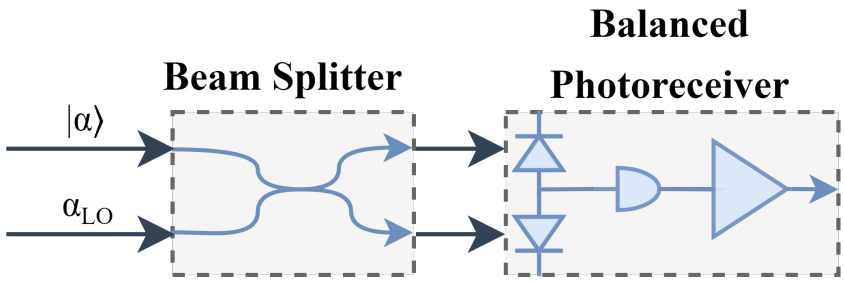


Figure B.1: A diagram representing a balanced homodyne detector (BHD), where $|\alpha\rangle$ and LO represents the incoming coherent state and the local oscillator signals, respectively.

APPENDIX C

MODULATOR

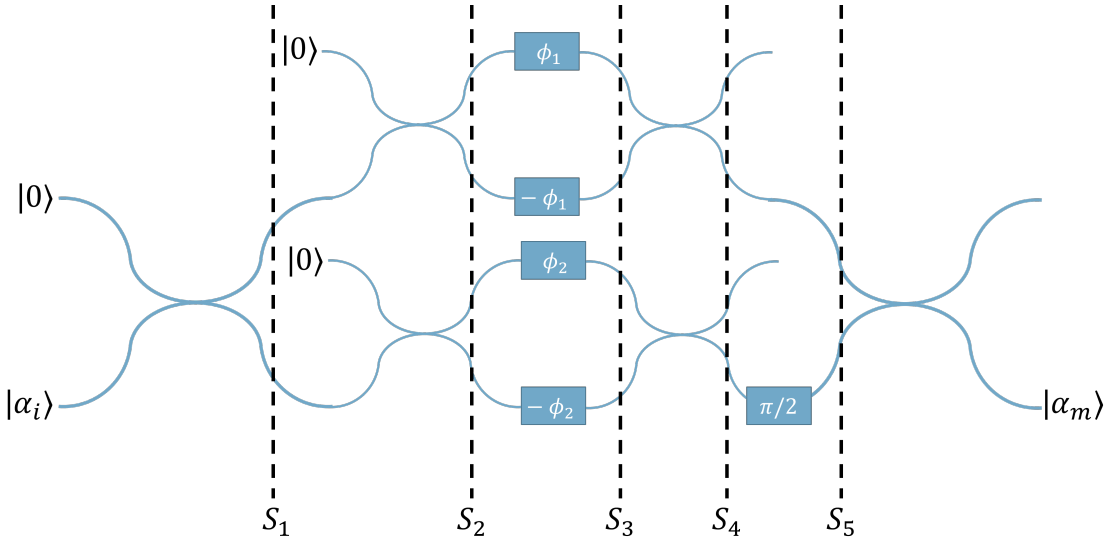


Figure C.1: Configuration for the I/Q modulator made up of two directional couplers, two MZIs, and a phase shifter.

The considered I/Q modulator is depicted in Figure C.1 which starts with a directional coupler, followed by two MZIs along with a phase shifter for one of them, then a directional coupler in the final stage. The output of the first stage is

$$\begin{aligned}\begin{bmatrix} S_1^1 \\ S_1^2 \end{bmatrix} &= T_{\text{BS}} \begin{bmatrix} 0 \\ \alpha_i \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & j \\ j & 1 \end{bmatrix} \begin{bmatrix} 0 \\ \alpha_i \end{bmatrix} \\ &= \frac{\alpha_i}{\sqrt{2}} \begin{bmatrix} j \\ 1 \end{bmatrix}.\end{aligned} \tag{C.1}$$

In the second stage, the corresponding outputs are

$$\begin{aligned}\begin{bmatrix} S_2^1 \\ S_2^2 \end{bmatrix} &= T_{\mathrm{BS}} \begin{bmatrix} 0 \\ S_1^1 \end{bmatrix} \\ &= \frac{S_1^1}{\sqrt{2}} \begin{bmatrix} j \\ 1 \end{bmatrix} \\ &= \frac{\alpha_i}{2} \begin{bmatrix} -1 \\ j \end{bmatrix},\end{aligned} \tag{C.2}$$

and

$$\begin{aligned}\begin{bmatrix} S_2^3 \\ S_2^4 \end{bmatrix} &= T_{\mathrm{BS}} \begin{bmatrix} 0 \\ S_1^2 \end{bmatrix} \\ &= \frac{S_1^2}{\sqrt{2}} \begin{bmatrix} j \\ 1 \end{bmatrix} \\ &= \frac{\alpha_i}{2} \begin{bmatrix} j \\ 1 \end{bmatrix}.\end{aligned} \tag{C.3}$$

After applying the phase shifts in the third stage, the states are transformed to

$$\begin{aligned}\begin{bmatrix} S_3^1 \\ S_3^2 \\ S_3^3 \\ S_3^4 \end{bmatrix} &= \begin{bmatrix} e^{j\phi_1} S_2^1 \\ e^{-j\phi_1} S_2^2 \\ e^{j\phi_2} S_2^3 \\ e^{-j\phi_2} S_2^4 \end{bmatrix} \\ &= \frac{\alpha_i}{2} \begin{bmatrix} -e^{j\phi_1} \\ j e^{-j\phi_1} \\ j e^{j\phi_2} \\ e^{-j\phi_2} \end{bmatrix}.\end{aligned} \tag{C.4}$$

In the fourth stage, directional couplers are applied, giving

$$\begin{aligned}\begin{bmatrix} S_4^1 \\ S_4^2 \end{bmatrix} &= T_{\text{BS}} \begin{bmatrix} S_3^1 \\ S_3^2 \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} S_3^1 + jS_3^2 \\ jS_3^1 + S_3^2 \end{bmatrix} \\ &= \frac{\alpha_i}{2\sqrt{2}} \begin{bmatrix} -e^{j\phi_1} - e^{-j\phi_1} \\ -je^{j\phi_1} + je^{-j\phi_1} \end{bmatrix} \\ &= \frac{-\alpha_i}{\sqrt{2}} \begin{bmatrix} \cos\phi_1 \\ -\sin\phi_1 \end{bmatrix},\end{aligned} \tag{C.5}$$

and

$$\begin{aligned}\begin{bmatrix} S_4^3 \\ S_4^4 \end{bmatrix} &= T_{\text{BS}} \begin{bmatrix} S_3^3 \\ S_3^4 \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} S_3^3 + jS_3^4 \\ jS_3^3 + S_3^4 \end{bmatrix} \\ &= \frac{\alpha_i}{2\sqrt{2}} \begin{bmatrix} je^{j\phi_2} + je^{-j\phi_2} \\ -e^{j\phi_2} + e^{-j\phi_2} \end{bmatrix} \\ &= \frac{j\alpha_i}{\sqrt{2}} \begin{bmatrix} \cos\phi_2 \\ -\sin\phi_2 \end{bmatrix}.\end{aligned} \tag{C.6}$$

Considering only two outputs where one is phase shifted gives

$$\begin{aligned}\begin{bmatrix} S_5^1 \\ S_5^2 \end{bmatrix} &= \begin{bmatrix} S_4^2 \\ \cancel{e^{j\frac{\pi}{2}}} \cdot S_4^4 \end{bmatrix} \\ &= \frac{\alpha_i}{\sqrt{2}} \begin{bmatrix} \sin\phi_1 \\ \sin\phi_2 \end{bmatrix}.\end{aligned} \tag{C.7}$$

Finally, after passing through the last optical element,

$$\alpha_m = \frac{1}{\sqrt{2}} \left(j S_5^1 + S_5^2 \right),$$

$$\longrightarrow \boxed{\alpha_m = \frac{\alpha_i}{2} \left(j \sin \phi_1 + \sin \phi_2 \right)}. \tag{C.8}$$

APPENDIX D

NORMAL DISTRIBUTION SAMPLING

In order to obtain a truthful representation for the normal distribution, a certain number of samples is needed. The fidelity of the sampled distribution is measured through the width of the confidence interval (CI) containing the actual value of a parameter from the actual population with certain desired confidence $(1 - \alpha)$. For example, $\alpha = 0.05$ defines the 95% CI, where the parameter's actual value falls within the CI with a 0.95 probability. For N samples, the degrees of freedom (DoF) is

$$\text{DoF} = N - 1, \tag{D.1}$$

which is used to compute the CI in the standard deviation σ as following [76]

$$\frac{\sigma_s\sqrt{\text{DoF}}}{\chi_{1-\alpha/2}} \leq \sigma \leq \frac{\sigma_s\sqrt{\text{DoF}}}{\chi_{\alpha/2}}, \tag{D.2}$$

where σ_s is the standard deviation of the sampled distribution and χ^2_x is the position in the chi-squared distribution where a fraction x of the area falls to the left of it. That is, χ^2_x is the point marking the beginning of the chi-squared distribution left-tail to be excluded. Some of the critical values for the chi-squared distribution are tabulated in Table D.1 [76]. As an example, let DoF = 50 and $\alpha = 0.1$, which gives

$$\begin{aligned} &\frac{\sigma_s\sqrt{50}}{\chi_{0.95}} \leq \sigma \leq \frac{\sigma_s\sqrt{50}}{\chi_{0.05}}, \\ \longrightarrow\ &\frac{\sigma_s\sqrt{50}}{\sqrt{67.505}} \leq \sigma \leq \frac{\sigma_s\sqrt{50}}{\sqrt{34.764}}, \\ \longrightarrow\ &0.861\sigma_s \leq \sigma \leq 1.199\sigma_s. \end{aligned} \tag{D.3}$$

For $\sigma = 10$, 50 trials are performed where the sampled standard deviation (σ_s) is computed from 51 data points that are sampled from a normal distribution. The result of the experiment is tabulated in Table D.2, where it is expected that about 45 trials (90%)

will satisfy Equation (D.3). 44 trials (88%) give a standard deviation within the CI.

A different and crude approach to approximate the needed number of samples is illustrated in Figure D.1. The number of samples is swept for different values for the standard deviation. As evident by Equation (D.2), for higher standard deviation (σ) values, the uncertainty of the sampled standard deviation (σ_s) grows wider.

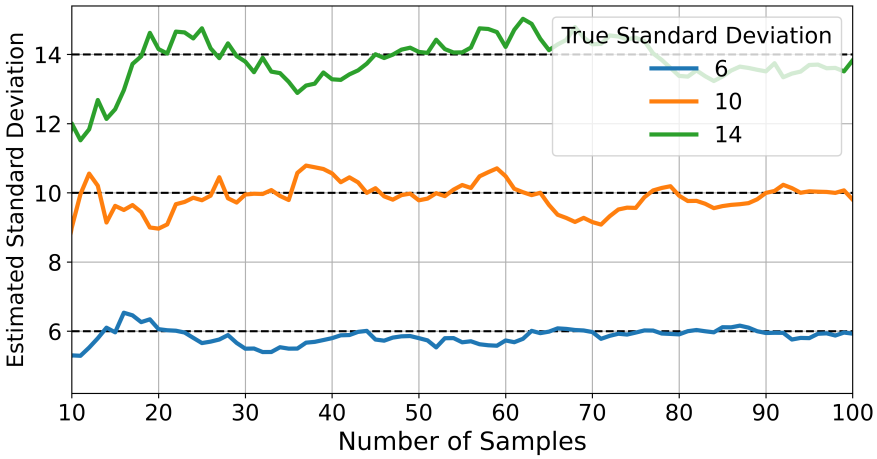


Figure D.1: The sampled standard distribution as a function of the number of samples for different standard distributions. A moving average that is eight samples wide is used to smoothen the plot.

Table D.1: Tabulated values for the one-tailed chi-squared distribution values.

x	0.01	0.05	0.2	0.5	0.9	0.95	0.99
DoF							
1	0.000157	0.00393	0.0158	0.455	2.706	3.841	6.635
2	0.020	0.103	0.211	1.386	4.605	5.991	9.210
3	0.115	0.352	0.584	2.366	6.251	7.815	11.345
4	0.297	0.711	1.064	3.357	7.779	9.488	13.277
5	0.554	1.145	1.610	4.351	9.236	11.070	15.086
6	0.872	1.635	2.204	5.348	10.645	12.592	16.812
7	1.239	2.167	2.833	6.346	12.017	14.067	18.475
8	1.646	2.733	3.490	7.344	13.362	15.507	20.090
9	2.088	3.325	4.168	8.343	14.684	16.919	21.666
10	2.558	3.940	4.865	9.342	15.987	18.307	23.209
11	3.053	4.575	5.578	10.341	17.275	19.675	24.725
12	3.571	5.226	6.304	11.340	18.549	21.026	26.217
13	4.107	5.892	7.042	12.340	19.812	22.362	27.688
14	4.660	6.571	7.790	13.339	21.064	23.685	29.141
15	5.229	7.261	8.547	14.339	22.307	24.996	30.578
16	5.812	7.962	9.312	15.338	23.542	26.296	32.000
17	6.408	8.672	10.085	16.338	24.769	27.587	33.409
18	7.015	9.390	10.865	17.338	25.989	28.869	34.805
19	7.633	10.117	11.651	18.338	27.204	30.144	36.191
20	8.260	10.851	12.443	19.337	28.412	31.410	37.566
21	8.897	11.591	13.240	20.337	29.615	32.671	38.932
22	9.542	12.338	14.041	21.337	30.813	33.924	40.289
23	10.196	13.091	14.848	22.337	32.007	35.172	41.638
24	10.856	13.848	15.659	23.337	33.196	36.415	42.980
25	11.524	14.611	16.473	24.337	34.382	37.652	44.314
26	12.198	15.379	17.292	25.336	35.563	38.885	45.642
27	12.879	16.151	18.114	26.336	36.741	40.113	46.963
28	13.565	16.928	18.939	27.336	37.916	41.337	48.278
29	14.256	17.708	19.768	28.336	39.087	42.557	49.588
30	14.953	18.493	20.599	29.336	40.256	43.773	50.892
31	15.655	19.281	21.434	30.336	41.422	44.985	52.191
32	16.362	20.072	22.271	31.336	42.585	46.194	53.486
33	17.074	20.867	23.110	32.336	43.745	47.400	54.776
34	17.789	21.664	23.952	33.336	44.903	48.602	56.061
35	18.509	22.465	24.797	34.336	46.059	49.802	57.342
36	19.233	23.269	25.643	35.336	47.212	50.998	58.619
37	19.960	24.075	26.492	36.336	48.363	52.192	59.892
38	20.691	24.884	27.343	37.335	49.513	53.384	61.162
39	21.426	25.695	28.196	38.335	50.660	54.572	62.428
40	22.164	26.509	29.051	39.335	51.805	55.758	63.691
41	22.906	27.326	29.907	40.335	52.949	56.942	64.950
42	23.650	28.144	30.765	41.335	54.090	58.124	66.206
43	24.398	28.965	31.625	42.335	55.230	59.304	67.459
44	25.148	29.787	32.487	43.335	56.369	60.481	68.710
45	25.901	30.612	33.350	44.335	57.505	61.656	69.957
46	26.657	31.439	34.215	45.335	58.641	62.830	71.201
47	27.416	32.268	35.081	46.335	59.774	64.001	72.443
48	28.177	33.098	35.949	47.335	60.907	65.171	73.683
49	28.941	33.930	36.818	48.335	62.038	66.339	74.919
50	29.707	34.764	37.689	49.335	63.167	67.505	76.154

Table D.2: Trials performed to check the validity of the computed confidence interval (CI) in Equation (D.3).

Trial #	Samp Std Dev	90% CI Min.	90% CI Max.	Within CI
1	10.324	8.889	12.379	✓
2	9.262	7.975	11.106	✓
3	10.779	9.280	12.923	✓
4	10.915	9.398	13.087	✓
5	9.841	8.473	11.800	✓
6	9.833	8.466	11.790	✓
7	8.988	7.739	10.777	✓
8	10.350	8.912	12.410	✓
9	9.156	7.884	10.978	✓
10	11.104	9.561	13.314	✓
11	9.268	7.979	11.112	✓
12	11.214	9.655	13.445	✓
13	11.094	9.552	13.302	✓
14	10.425	8.976	12.500	✓
15	11.167	9.615	13.390	✓
16	9.879	8.506	11.845	✓
17	8.138	7.007	9.758	✗
18	10.025	8.631	12.020	✓
19	10.659	9.177	12.780	✓
20	10.244	8.820	12.283	✓
21	12.486	10.751	14.971	✗
22	11.078	9.539	13.283	✓
23	8.805	7.581	10.557	✓
24	7.993	6.882	9.584	✗
25	9.457	8.142	11.339	✓
26	8.309	7.154	9.963	✗
27	10.006	8.615	11.997	✓
28	9.846	8.477	11.805	✓
29	9.555	8.227	11.456	✓
30	11.132	9.585	13.347	✓
31	9.407	8.099	11.278	✓
32	11.828	10.184	14.181	✗
33	10.793	9.293	12.941	✓
34	10.622	9.145	12.736	✓
35	10.374	8.932	12.439	✓
36	11.108	9.564	13.318	✓
37	9.709	8.360	11.642	✓
38	10.306	8.873	12.357	✓
39	8.362	7.199	10.026	✓
40	10.328	8.892	12.383	✓
41	11.807	10.166	14.156	✗
42	10.565	9.097	12.668	✓
43	9.577	8.246	11.483	✓
44	10.057	8.659	12.058	✓
45	9.926	8.546	11.901	✓
46	9.844	8.476	11.803	✓
47	9.437	8.125	11.315	✓
48	8.429	7.257	10.106	✓
49	9.790	8.429	11.738	✓
50	11.142	9.593	13.359	✓

BIBLIOGRAPHY

[1] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[2] K. Scarfone, W. Jansen, M. Tracy, *et al.*, "Guide to general server security," *NIST Special Publication*, vol. 800, no. 123, 2008.

[3] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.

[5] R. C. Merkle, "Secure communications over insecure channels," *Communications of the ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[6] W. Diffie, "New direction in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, pp. 472–492, 1976.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[8] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, Ieee, 1994, pp. 124–134.

[9] R. Renner and R. Wolf, "Quantum advantage in cryptography," *arXiv preprint arXiv:2206.04078*, 2022.

[10] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[11] J. L. Park, "The concept of transition in quantum mechanics," *Foundations of physics*, vol. 1, no. 1, pp. 23–33, 1970.

[12] B.-Y. Tang, B. Liu, Y.-P. Zhai, C.-Q. Wu, and W.-R. Yu, "High-speed and large-scale privacy amplification scheme for quantum key distribution," *Scientific reports*, vol. 9, no. 1, pp. 1–8, 2019.

[13] C. H. Bennet, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, Dec. 1984*, 1984, pp. 175–179.

[14] J. Li, N. Li, Y. Zhang, *et al.*, "A survey on quantum cryptography," *Chinese Journal of Electronics*, vol. 27, no. 2, pp. 223–228, 2018.

[15] C. Weedbrook, S. Pirandola, R. García-Patrón, *et al.*, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, p. 621, 2012.

[16] F. Roumestan, A. Ghazisaeidi, H. Mardoyan, J. Renaudier, E. Diamanti, and P. Grangier, "6 Mb/s secret key rate transmission over 13.5 km SMF using PCS-256QAM super-channel continuous variable quantum key distribution," in *Optical Fiber Communication Conference*, Optica Publishing Group, 2022, Tu3I–4.

[17] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[18] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, *et al.*, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Opt. Express*, vol. 20, no. 13, pp. 14 030–14 041, Jun. 2012. DOI: 10.1364/OE.20.014030. [Online]. Available: http://opg.optica.org/oe/abstract.cfm?URI=oe-20-13-14030.

[19] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[20] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Optics letters*, vol. 40, no. 16, pp. 3695–3698, 2015.

[21] D. Huang, D. Lin, C. Wang, *et al.*, "Continuous-variable quantum key distribution with 1 mbps secure key rate," *Optics express*, vol. 23, no. 13, pp. 17 511–17 519, 2015.

[22] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable qkd with intense dwdm classical channels," *New Journal of Physics*, vol. 17, no. 4, p. 043 027, 2015.

[23] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific reports*, vol. 6, no. 1, pp. 1–9, 2016.

[24] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," *Optics letters*, vol. 41, no. 15, pp. 3511–3514, 2016.

[25] T. Hirano, T. Ichikawa, T. Matsubara, *et al.*, "Implementation of continuous-variable quantum key distribution with discrete modulation," *Quantum Science and Technology*, vol. 2, no. 2, p. 024 010, 2017.

[26] S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," *Optics letters*, vol. 42, no. 8, pp. 1588–1591, 2017.

[27] T. A. Eriksson, T. Hirano, G. Rademacher, *et al.*, "Joint propagation of continuous variable quantum key distribution and 18×24.5 gbaud pm-16qam channels," in *2018 European Conference on Optical Communication (ECOC)*, IEEE, 2018, pp. 1–3.

[28] T. Wang, P. Huang, Y. Zhou, *et al.*, "High key rate continuous-variable quantum key distribution with a real local oscillator," *Optics express*, vol. 26, no. 3, pp. 2794–2806, 2018.

[29] F. Karinou, H. H. Brunner, C.-H. F. Fung, *et al.*, "Toward the integration of cv quantum key distribution in deployed optical networks," *IEEE Photonics Technology Letters*, vol. 30, no. 7, pp. 650–653, 2018.

[30] F. Laudenbach, B. Schrenk, C. Pacher, *et al.*, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum*, vol. 3, p. 193, 2019.

[31] S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, "Experimental investigation of heterodyne quantum key distribution in the s-band embedded in a commercial dwdm system," in *Optical Fiber Communication Conference*, Optical Society of America, 2019, Th1J–3.

[32] T. A. Eriksson, T. Hirano, B. J. Puttnam, *et al.*, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels," *Communications Physics*, vol. 2, no. 1, pp. 1–8, 2019.

[33] T. A. Eriksson, R. S. Lu'ıs, B. J. Puttnam, *et al.*, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," *Journal of Lightwave Technology*, vol. 38, no. 8, pp. 2214–2218, 2020.

[34] S. Ren, S. Yang, A. Wonfor, R. Penty, and I. White, "Experimental demonstration of high key rate and low complexity cvqkd system with local local oscillator," in *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, IEEE, 2020, pp. 1–3.

[35] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "Spectrally-shaped continuous-variable qkd operating at 500 mhz over an optical pipe lit by 11 dwdm channels," in *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, IEEE, 2020, pp. 1–3.

[36] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," *Optics Express*, vol. 28, no. 10, pp. 14 547–14 559, 2020.

[37] A. Leverrier, "Theoretical study of continuous-variable quantum key distribution," Ph.D. dissertation, Télécom ParisTech, 2009.

[38] M. Fox, *Quantum optics: an introduction*. OUP Oxford, 2006, vol. 15.

[39] G. Adesso, S. Ragy, and A. R. Lee, "Continuous variable quantum information: Gaussian states and beyond," *Open Systems & Information Dynamics*, vol. 21, no. 01n02, p. 1 440 001, 2014.

[40] E. Parzen, *Modern probability theory and its applications*. Wiley, 1960.

[41] R. Bhatia, "Positive definite matrices, princeton ser," *Appl. Math., Princeton University Press, Princeton, NJ*, 2007.

[42] R. Gilmore, "Baker-campbell-hausdorff formulas," *Journal of Mathematical Physics*, vol. 15, no. 12, pp. 2090–2092, 1974.

[43] U. Leonhardt, *Measuring the quantum state of light*. Cambridge university press, 1997, vol. 22.

[44] F. P. Kanitschar, "Finite-size security proof for discrete-modulated continuous-variable quantum key distribution," 2022.

[45] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, 2021.

[46] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057 902, 2002.

[47] Z. Bai, S. Yang, and Y. Li, "High-efficiency reconciliation for continuous variable quantum key distribution," *Japanese Journal of Applied Physics*, vol. 56, no. 4, p. 044 401, 2017.

[48] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0306141*, 2003.

[49] L. P. Hughston, R. Jozsa, and W. K. Wootters, "A complete classification of quantum ensembles having a given density matrix," *Physics Letters A*, vol. 183, no. 1, pp. 14–18, 1993.

[50] F. Laudenbach, C. Pacher, C.-H. F. Fung, *et al.*, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1 800 011, 2018.

[51] L. Trigo Vidarte, "Design and implementation of high-performance devices for continuous-variable quantum key distribution," Ph.D. dissertation, Université Paris-Saclay (ComUE), 2019.

[52] R. Hui, *Introduction to fiber-optic communications*. Academic Press, 2019.

[53] V. Ferrero and S. Camatel, "Optical phase locking techniques: An overview and a novel method based on single side sub-carrier modulation," *Optics express*, vol. 16, no. 2, pp. 818–828, 2008.

[54] F. Roumestan, "Advanced signal processing techniques for continuous variable quantum key distribution over optical fiber.," Ph.D. dissertation, Sorbonne Université, 2022.

[55] K. Kikuchi, "Coherent optical communications: Historical perspectives and future directions," in *High Spectral Density Optical Communication Technologies*, Springer, 2010, pp. 11–49.

[56] A. Ghazisaeidi, I. F. de Jauregui Ruiz, R. Rios-Müller, *et al.*, "Advanced c+ l-band transoceanic transmission systems based on probabilistically shaped pdm-64qam," *Journal of Lightwave Technology*, vol. 35, no. 7, pp. 1291–1299, 2017.

[57] G. Smith, D. Novak, and Z. Ahmed, "Technique for optical ssb generation to overcome dispersion penalties in fibre-radio systems," *Electronics letters*, vol. 33, no. 1, pp. 74–75, 1997.

[58] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "High rate cv-qkd secured mobile wdm fronthaul for dense 5g radio networks," *Journal of Lightwave Technology*, vol. 39, no. 11, pp. 3445–3457, 2021.

[59] N. Jain, I. Derkach, H.-M. Chin, *et al.*, "Modulation leakage vulnerability in continuous-variable quantum key distribution," *Quantum Science and Technology*, vol. 6, no. 4, p. 045 001, 2021.

[60] Q. Chaudhari, *Wireless Communications from the Ground Up - An SDR Perspective*. CreateSpace, 2018. [Online]. Available: https://wirelesspi.com/book.

[61] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, "High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam," in *2021 European Conference on Optical Communication (ECOC)*, IEEE, 2021, pp. 1–4.

[62] M. Henini, *Dilute nitride semiconductors*. Elsevier, 2004.

[63] S. Miller and D. Childers, *Probability and random processes: With applications to signal processing and communications*. Academic Press, 2012.

[64] R. H. Walden, "Analog-to-digital converter survey and analysis," *IEEE Journal on selected areas in communications*, vol. 17, no. 4, pp. 539–550, 1999.

[65] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Physical Review A*, vol. 76, no. 5, p. 052 323, 2007.

[66] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Physical Review A*, vol. 87, no. 6, p. 062 313, 2013.

[67] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, *et al.*, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Physical Review A*, vol. 87, no. 6, p. 062 329, 2013.

[68] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," *Physical Review A*, vol. 87, no. 5, p. 052 309, 2013.

[69] ——, "Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems," *Physical Review A*, vol. 88, no. 2, p. 022 339, 2013.

[70] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, *et al.*, "Quantum hacking on quantum key distribution using homodyne detection," *Physical Review A*, vol. 89, no. 3, p. 032 304, 2014.

[71] D. B. Soh, C. Brif, P. J. Coles, *et al.*, "Self-referenced continuous-variable quantum key distribution protocol," *Physical Review X*, vol. 5, no. 4, p. 041 010, 2015.

[72] M. Rückmann and C. G. Schaeffer, "Cv-qkd system using a commercial coherent transceiver module," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, IEEE, 2021, pp. 1–3.

[73] A. Alsaui, Y. Alwehaibi, A. Prabhakar, and D. Venkitesh, "Digital filter design for experimental continuous-variable quantum key distribution," in *2023 Optical Fiber Communications Conference and Exhibition (OFC)*, IEEE, 2023, pp. 1–3.

[74] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," *Physical Review X*, vol. 5, no. 4, p. 041 009, 2015.

[75] A. Yariv and P. Yeh, *Photonics: optical electronics in modern communications*. Oxford university press, 2007.

[76] D. J. Sheskin, *Handbook of parametric and nonparametric statistical procedures*. Chapman and Hall/CRC, 2003.

CURRICULUM VITAE

NAME Abdulmohsen Alsaui

DATE OF BIRTH 04 March 1997

EDUCATION QUALIFICATIONS

2020 **Bachelor of Science**

Institution	King Fahd University of Petroleum and Minerals
Specialization	Electrical Engineering

2020 **Bachelor of Science**

Institution	King Fahd University of Petroleum and Minerals
Specialization	Physics

Master of Science

Institution	Indian Institute of Technology Madras
Specialization	Electrical Engineering
Registration Date	01 February 2021

GENERAL TEST COMMITTEE

Chairperson	Dr. Balaji Srinivasan Professor Department of Electrical Engineering
Guide	Dr. Deepa Venkitesh Professor Department of Electrical Engineering
Members	Dr. Anil Prabhakar Professor Department of Electrical Engineering
	Dr. Prabha Mandayam Professor Department of Physics