Universidad Complutense de Madrid

Facultad de Ciencias Físicas

Tesis Doctoral

Diseño e Implementación de un Sistema de Distribución Cuántica de Clave en Variable Continua

Design and Implementation of a Continuous-Variable Quantum Key Distribution System

Memoria para optar al grado de Doctor

Presentada por:

Andrés Ruiz Chamorro

Directora:

Verónica Fernández Mármol

Universidad Complutense de Madrid

Facultad de Ciencias Físicas

Consejo Superior de Investigaciones Científicas

Instituto de Tecnologías Físicas y de la Información

Tesis Doctoral

Diseño e Implementación de un Sistema de Distribución Cuántica de Clave en Variable Continua

Design and Implementation of a Continuous-Variable Quantum Key Distribution System

---

Memoria para optar al título de:

Doctor en Física

Autor:

Andrés Ruiz Chamorro

Directora:

Verónica Fernández Mármol

Madrid, 2024

Abstract

Continuous-Variable Quantum Key Distribution (CV-QKD) is a quantum cryptography protocol that leverages continuous variables, such as the quadratures of the electromagnetic field, to encode and transmit information in a secure way, provable through the principles of quantum mechanics. This enables two remote parties to securely share a cryptographic key, even in the presence of an eavesdropper. This thesis addresses the design and implementation of an experimental CV-QKD system, including the conceptual design, numerical simulations, and experimental demonstrations that validate the methods introduced in this work.

The thesis covers system design and component characterization, including the development of realistic simulations to predict the impact of experimental imperfections on the protocol's security. The analysis concludes that the primary source of error hindering the experimental implementation of the protocol lies in the random frequency fluctuations of the lasers used both at the emitter and receiver sides. A method is presented to address this issue, which is then experimentally validated through CV-QKD transmissions over various distances using commercial optical fibers.

Finally, multiple experimental enhancements are introduced, demonstrating practical applications such as integrating the system into QKD networks and deploying encrypted connections secured by quantum keys distilled from the experimental system. This shows that the CV-QKD system presented can be effectively deployed in practical settings, providing high levels of security for critical data transmissions.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisor, Verónica Fernández, for her continuous support, guidance, and encouragement throughout my research. Her insights, expertise, and patience were invaluable. This work would have been impossible without her mentorship.

I am deeply grateful to my colleagues at the institute for their advice, assistance with everything I needed, and occasional breaks that provided much-needed relief during challenging times. Special thanks go to Alfonso Blanco and Natalia Denisenko for the countless hours we spent discussing various topics covered in this thesis and the training they provided when I joined the institute. Without them, this would not have been possible.

On a personal note, I would like to thank my family for their unconditional love and unwavering support. They were always there for me, making the workload more bearable during these years.

Finally, I would like to acknowledge the European Commission for their financial support, without which this research would not have been possible. I also appreciate the administrative staff at CSIC and UCM for their assistance and support during my studies.

Contents

List of Figures

List of Tables

Resumen

Esta tesis trata el diseño teórico e implementación experimental de un sistema de Distribución Cuántica de Claves de Variable Continua (CV-QKD), una tecnología dentro del campo de la criptografía cuántica, la cual en términos generales, emplea las leyes de la mecánica cuántica para garantizar la seguridad de la transmisión de claves criptográficas entre dos partes, de manera que cualquier intento de intercepción por parte de un tercero sea detectable.

La investigación se centra en el estudio, caracterización, simulación y desarrollo de un sistema experimental de CV-QKD con modulación gaussiana de estados coherentes (GMCS) y con oscilador local generado localmente (LLO). La tesis se organiza en varios capítulos que abordan desde los fundamentos teóricos hasta la implementación experimental y los resultados obtenidos.

El Capítulo 1 presenta los objetivos de la tesis y ofrece una primera introducción a la Distribución Cuántica de Claves, explicando los problemas que esta tecnología busca resolver. Se proporciona una motivación para este trabajo, y una visión general del campo de investigación, comentando los principales desafíos abordados.

En el Capítulo 2 se revisan las bases teóricas necesarias para comprender los conceptos utilizados en el resto de la tesis. El capítulo comienza con la Sección 2.1, donde se introducen genéricamente los principios fundamentales de la mecánica cuántica, enfocándose en los sistemas de variable continua, tales como las cuadraturas del campo electromagnético, y en la teoría de la información cuántica. Se explican conceptos clave como el formalismo matemático de la mecánica cuántica, los fotones y los estados coherentes, esenciales para entender el protocolo de CV-QKD. Posteriormente, se introducen los conceptos de entropía e información mutua, hasta llegar a la cota de Holevo, crucial para explicar las pruebas de seguridad en CV-QKD.

El capítulo continúa con la Sección 2.2 haciendo una revisión histórica y del estado del arte de los protocolos de Distribución Cuántica de Clave (QKD) más habituales, dividiéndolos en dos categorías principales: protocolos de Variable Discreta (DV-

QKD) y de Variable Continua (CV-QKD). Se explica brevemente el protocolo BB84, el cual es el primero y más conocido dentro de la categoría de DV-QKD, y el protocolo GG02, fundamental en CV-QKD. Esta revisión proporciona un contexto histórico y un estado del arte que resalta los avances más recientes en el campo de la QKD en general, mostrando los avances en diferentes implementaciones.

El capítulo finaliza con la Sección 2.3, donde se hace una revisión de las pruebas y análisis de seguridad de los protocolos de CV-QKD basados en GMCS. Se revisan las pruebas de seguridad, incluyendo el desarrollo de las expresiones matemáticas de la información mutua o la cota de Holevo, imprescindibles para estimar la tasa de clave segura (SKR), el factor que determina si una transmisión ha podido ser interceptada por un atacante.

El Capítulo 3 comienza describiendo el diseño experimental del sistema CV-QKD elegido en la Sección 3.1, explicando cómo se lleva a cabo la generación y detección de estados coherentes con dispositivos experimentales, tales como láseres, moduladores electro-ópticos y detectores coherentes.

Posteriormente, en la Sección 3.2, se resume todo el proceso de caracterización de todos los componentes necesarios para la implementación experimental, como los láseres, moduladores y detectores, y se identifican los rangos de trabajo óptimos para cada dispositivo y los desafíos experimentales más importantes, como la necesidad de estabilización de frecuencia debido a las fluctuaciones de los láseres.

Para finalizar el capítulo, en la Sección 3.3, se muestran las simulaciones realizadas para modelar el comportamiento de los dispositivos experimentales para estimar cómo distintas imperfecciones experimentales o *impairments* afectan a la tasa de clave segura. Las simulaciones y el modelado proporcionan una base que guía el desarrollo del sistema experimental, ya que permite predecir con precisión el comportamiento del sistema en condiciones reales.

El Capítulo 4 se centra en la implementación experimental del sistema CV-QKD y en el desarrollo del método de estabilización de frecuencias de los láseres. En la Sección 4.1, se presenta un método para corregir las fluctuaciones de frecuencia y fase de los láseres de manera eficaz utilizando técnicas de procesamiento digital de señales que se llevan a cabo tras la adquisición de la señal por parte del receptor. Este método se complementa con otros algoritmos de recuperación de fase y de reloj para corregir por completo la señal recibida hasta maximizar la correlación entre la señal enviada y la recibida.

Tras esto, en la Sección 4.2 se presentan diversas mejoras para aumentar la robustez y estabilidad del sistema, como los algoritmos de control automático de potencia, de búsqueda de la portadora y de corrección de la polarización. Estas mejoras

permitieron automatizar completamente el proceso de calibración del sistema antes de cada transmisión, facilitando y mejorando la precisión de los experimentos realizados.

Finalmente, en la Sección 4.3, se presenta la validación experimental del sistema completo, mostrando los resultados de distintas transmisiones experimentales realizadas en fibras ópticas comerciales de diferentes longitudes, siendo los resultados consistentes con las simulaciones previas.

Para concluir el capítulo, se describen varias demostraciones complementarias realizadas posteriormente, como la implementación del envío y detección de señales electrónicas en matrices de puertas programables en campo (FPGAs), la coexistencia en una fibra óptica comercial de canales clásicos y cuánticos mediante multiplexadores de longitud de onda (WDM), la provisión de claves destiladas a partir de las claves brutas distribuidas previamente por el sistema experimental a un administrador de una red cuántica, y el despliegue de una red privada virtual (VPN) cifrada con otra clave destilada del sistema.

Por último, tras la discusión sobre las conclusiones y los trabajos futuros del Capítulo 5, en los apéndices se complementa el contenido principal, proporcionando detalles adicionales sobre el sistema de unidades empleado durante toda la tesis y sobre los métodos utilizados en el postprocesado de las claves obtenidas en el sistema experimental. En el Apéndice A se introducen las unidades de ruido de disparo (SNU) utilizadas en CV-QKD, explicando cómo convertir las magnitudes medidas en unidades del SI a unidades de SNU en un entorno práctico. En el Apéndice B se detalla el protocolo de reconciliación utilizado para el post-procesado clásico de la clave, que incluye la corrección de errores y la amplificación de privacidad. Aunque el post-procesado clásico no es el objeto de estudio de esta tesis, es imprescindible para destilar las claves distribuidas por QKD, por lo que en este apéndice se presentan los distintos algoritmos utilizados para ello, como el de corrección de errores, basado en la comprobación de paridad de matrices de baja densidad (LDPC), o el algoritmo de hashing empleado para realizar la amplificación de privacidad, con el fin de minimizar la información que un atacante podría obtener sobre la clave.

Summary

This thesis addresses the theoretical design and experimental implementation of a Continuous-Variable Quantum Key Distribution (CV-QKD) system, a technology within the field of quantum cryptography, which uses the principles of quantum mechanics to ensure the secure transmission of cryptographic keys between two parties, making any eavesdropping attempts detectable.

The research focuses on the study, characterization, simulation, and development of an experimental CV-QKD system with Gaussian-Modulated Coherent States (GMCS) and a locally generated local oscillator (LLO). The thesis is organized into several chapters covering the theoretical foundations, experimental implementation, and results.

Chapter 1 presents the thesis objectives and offers an initial introduction to Quantum Key Distribution, explaining the problems this technology aims to solve. It provides a motivation for this work and an overview of the research field while reviewing the main challenges addressed.

In Chapter 2, the theoretical foundations necessary to understand the concepts used in the rest of the thesis are reviewed. The chapter begins with Section 2.1, which introduces the fundamental principles of quantum mechanics, focusing on continuous-variable systems, such as the quadratures of the electromagnetic field, and quantum information theory. Key concepts, such as the mathematical formalism of quantum mechanics, photons, and coherent states, essential for understanding CV-QKD protocols, are explained. Subsequently, entropy and mutual information are introduced, finishing with the Holevo bound, which is crucial for explaining the security proofs in CV-QKD.

The chapter continues with Section 2.2, providing a historical review and state of the art of the most common Quantum Key Distribution (QKD) protocols, dividing them into two main categories: Discrete-Variable (DV-QKD) and Continuous-Variable (CV-QKD) protocols. The BB84 protocol, the first and most well-known DV-QKD protocol, is briefly explained, as is the GG02 protocol, which is funda-

mental in CV-QKD. This review provides a historical context and state of the art that highlights the most recent advances in the field of QKD, showcasing developments across different protocols and implementations.

The chapter concludes with Section 2.3, where the security analysis of GMCS-based CV-QKD protocols is reviewed. This includes the derivation of mathematical expressions for the mutual information and the Holevo bound, which are essential for estimating the secret key rate (SKR). This parameter determines whether an attacker could have intercepted a transmission.

Chapter 3 begins by describing the experimental design of the selected CV-QKD system in Section 3.1, explaining how coherent states are generated and detected using experimental devices such as lasers, electro-optic modulators, and coherent detectors.

Subsequently, in Section 3.2, the process of characterizing all the components necessary for the experimental implementation, such as lasers, modulators, and detectors, is summarized, identifying the optimal working ranges for each device and the most significant experimental challenges, such as the need for frequency stabilization due to fluctuations in the lasers used.

To conclude the chapter, in Section 3.3, simulations are conducted to model the behavior of the experimental devices to estimate how different experimental imperfections or impairments affect the secret key rate. The simulations and modeling provide a foundation that guides the development of the experimental system, as they allow for precise prediction of the system's behavior under real-world conditions.

Chapter 4 focuses on the experimental implementation of the CV-QKD system and the development of the laser frequency-locking method. In Section 4.1, a method is presented to effectively correct frequency and phase fluctuations of the lasers using digital signal processing techniques after the receiver acquires the signal. This method is complemented by other phase and clock recovery algorithms to fully correct the received signal and maximize the correlation between the transmitted and received signals.

Following this, Section 4.2 presents improvements to increase the system's robustness and stability, such as automatic power control and polarization correction algorithms. These enhancements enabled the complete automation of the system calibration process before each transmission, facilitating and improving the experiments' precision.

Finally, in Section 4.3, the experimental validation of the complete system is presented, showing the results of various experimental transmissions carried out on

commercial optical fibers of different lengths, with results consistent with previous simulations.

To conclude the chapter, several additional demonstrations subsequently conducted are described, such as the implementation of signal transmission and detection using Field Programmable Gate Arrays (FPGAs), the coexistence of classical and quantum channels over a commercial optical fiber using wavelength-division multiplexing (WDM), the provision of distilled keys from raw keys previously distributed by the experimental system to a quantum network administrator, and the deployment of a Virtual Private Network (VPN) encrypted with another distilled key from the system.

Lastly, after discussing conclusions and future work in Chapter 5, the appendices complement the main content by providing additional details about the unit system used throughout the thesis and the methods employed in post-processing the keys obtained from the experimental system. Appendix A introduces the Shot Noise Units (SNU) used in CV-QKD, explaining how to convert the measured magnitudes from SI units to SNU in a practical setup. Appendix B details the reconciliation protocol used for the key classical post-processing, which includes error correction and privacy amplification. Although classical post-processing is not within the scope of this thesis, it is necessary for distilling the raw keys distributed by QKD. Therefore, this appendix presents the algorithms used, such as the error correction algorithm based on Low-Density Parity-Check (LDPC) matrices and the hashing algorithm for privacy amplification, to minimize the information an attacker could obtain about the key.

Abbreviations

AC Alternating Current

AES Advanced Encryption Standard

ADC Analog-to-Digital Converter

APC Angled Physical Contact

API Application Programming Interface

ARM Advanced RISC (Reduced Instruction Set Computer) Machine

AWG Arbitrary Waveform Generator

BD Balanced Detector

BPF Band-Pass Filter

BS Beam Splitter

CLI Command Line Interface

CS-SSB Carrier Suppressed Single Sideband

CV Continuous Variable

CV-QKD Continuous-Variable Quantum Key Distribution

CW Continuous Wave

CWL Continuous Wave Laser

DAC Digital-to-Analog Converter

DC Direct Current

DI-QKD Device-Independent Quantum Key Distribution

DSP Digital Signal Processing

DV Discrete Variable

DV-QKD Discrete-Variable Quantum Key Distribution

EB Entanglement-Based

EC Error Correction

EPR Einstein-Podolsky-Rosen

ETSI European Telecommunications Standards Institute

FC Fiber Connector

FER Frame Error Rate

FFT Fast Fourier Transform

FPGA Field-Programmable Gate Array

GF Galois Field

GMCS Gaussian-Modulated Coherent States

GS Group Specification

GUI Graphical User Interface

IP Internet Protocol

KMS Key Management System

LAN Local Area Network

LDPC Low-Density Parity-Check

LLO Locally generated Local Oscillator

LO Local Oscillator

LPF Low-Pass Filter

MBC Modulator Bias Controller

MDI Measurement-Device-Independent Quantum Key Distribution

MET Multi-Edge Type

MLE Maximum Likelihood Estimator

MP Moore-Penrose

MZM Mach-Zehnder Modulator

NEP Noise Equivalent Power

OPM Optical Power Meter

OSA Optical Spectrum Analyzer

PA Privacy Amplification

PANDA Polarization-maintaining AND Absorption-reducing

PC Polarization Controller

PDF Probability Density Function

PE Parameter Estimation

PID Proportional Integral Derivative

PM Prepare-and-Measure

PNS Photon Number Splitting

PSK Post Quantum Cryptography

PSK Phase Shift Keying

QAM Quadrature Amplitude Modulation

QBER Quantum Bit Error Rate

QKD Quantum Key Distribution

QPSK Quadrature Phase Shift Keying

RC Raised Cosine

RCF Raised Cosine Filter

RF Radio-Frequency

RFSoC Radio-Frequency System-on-Chip

RMS Root Mean Square

RRCF Root Raised Cosine Filter

RSA Rivest-Shamir-Adleman

SFP Small Form-factor Pluggable

SI International System of Units

SKR Secret Key Rate

SLSQP Sequential Least-Squares Quadratic Programming

SM Single-Mode

SMF Single-Mode Fiber

SMT Syndrome Matching Test

SNR Signal-to-Noise Ratio

SNU Shot Noise Units

TCP Transmission Control Protocol

TF-QKD Twin-Field Quantum Key Distribution

THD Total Harmonic Distortion

TTL Transistor-Transistor Logic

USB Universal Serial Bus

VHDL Very High-Speed Integrated Circuit Hardware Description Language

VOA Variable Optical Attenuator

VPN Virtual Private Network

WDM Wavelength Division Multiplexing

Chapter 1

Introduction

The recent development of quantum computing has introduced new threats to the security of modern communications, particularly concerning public-key cryptographic systems. These systems, which are currently the standard for key distribution between two remote parties, base their security on the computational difficulty of solving mathematical problems such as large number factorization. Currently, solving these problems would require nonexistent computational resources, which makes these schemes to be considered secure. However, with the introduction of quantum algorithms that can solve these problems in a reasonably short time using a quantum computer, the security of these systems is severely compromised.

This vulnerability raises the search for alternatives to current public-key distribution schemes. One possible solution is post-quantum cryptography (PQC), which involves developing classical cryptographic algorithms that are secure even against attacks from a quantum computer. These algorithms are also based on mathematical problems that, to date, cannot be efficiently solved by known quantum algorithms. While PQC may provide a smoother transition for classical cryptographic systems, as it does not require new infrastructure, it still faces significant challenges since it is also based on the complexity of solving mathematical problems. As it is also conditioned to the computing capacity of an adversary, it will always be exposed to future advances in both quantum and classical computing.

This is where Quantum Key Distribution (QKD) emerges as a robust theoretical solution to ensure communications security in a post-quantum world. Unlike classical key distribution methods, QKD guarantees that any attempt to intercept the cryptographic keys will introduce disturbances in the system that can be detected. This principle derives directly from the laws of quantum mechanics, specifically

the Heisenberg uncertainty principle and the no-cloning theorem, making it impossible to tamper the cryptographic key without being detected. In this context, the main problem QKD aims to solve is the secure distribution of cryptographic keys between two remote parties (Alice and Bob) in the presence of a potential eavesdropper (Eve). While in public key classical schemes, the security of this distribution is based on assumptions about Eve's computational inability to solve certain mathematical problems, in QKD, security is guaranteed by quantum principles. This means that the security of the key will not be compromised regardless of advances in an adversary's computational capabilities.

Most QKD protocols can be categorized into two families: Discrete Variables (DV-QKD) and Continuous Variables (CV-QKD). In DV protocols, information is encoded in discrete quantum states, such as the polarization of single photons. In contrast, in CV protocols, information is encoded in continuous variables, such as the quadratures of the electromagnetic field. This allows for the use of standard classical telecommunications technologies, such as coherent modulation and detection, which simplifies the experimental implementation and reduces costs.

Despite the practical advantages of CV-QKD, its experimental implementation presents several challenges that must be addressed to ensure its viability in real-world applications. Among the most significant challenges are the various experimental imperfections that can significantly affect the secret key rate (SKR), which determines how much secure information Alice and Bob can share in the presence of Eve. Regarding this, ensuring system stability and minimizing the impact of these experimental errors is crucial for successfully implementing CV-QKD.

While CV-QKD offers promising potential for secure key distribution, its current implementations encounter several challenges:

- **System complexity and integration**: Current CV-QKD systems require complex setups with multiple optical components, complicating scalability and integration into existing telecommunications networks.
- **Sensitivity to experimental imperfections**: CV-QKD systems are highly sensitive to imperfections in components, such as laser phase noise or detector inefficiencies, which can compromise both the secret key rate and overall security.
- **Lack of detailed simulation models**: CV-QKD simulations typically assume linear models that simulate noise and losses on coherent states. However, simulations that model the impact of specific experimental imperfections or provide step-by-step modeling of each component are lacking, complicating accurate predictions of system performance.

- **Integration in practical environments**: Implementing a fully operational CV-QKD system involves integrating multiple components and achieving stability in real-world conditions. Continuous monitoring and adaptive calibration are necessary to mitigate imperfections and environmental variability. Although recent demonstrations have shown the feasibility of practical CV-QKD implementations, each specific implementation requires customized control and stabilization algorithms for optimal performance.

To develop a low-complexity CV-QKD system suitable for integration in practical environments and to address the challenges mentioned above, this thesis establishes the following research objectives:

- **System design**: To address the challenge of system complexity and integration, this objective focuses on designing a CV-QKD system architecture with minimal component requirements. This will simplify integration with existing telecommunications infrastructure and enhance scalability. We adopt an implementation based on Gaussian-Modulated Coherent States (GMCS), which has been shown to be efficient for intermediate and long distances over optical fiber. This design requires a detailed plan of the necessary components, such as electro-optic modulators, coherent detectors, and lasers. This requires an analysis of the state of the art and scientific background, as well as a review of the recent advances in experimental CV-QKD implementations to ensure that the selected configuration is suitable for our purpose.

- **Component characterization**: Addressing the challenge of sensitivity to experimental imperfections, this objective involves detailed characterization of each system component under real experimental conditions. This includes characterizing lasers, modulators, detectors, and other optical devices necessary for transmitting and receiving quantum signals. Each of these components can introduce noise or fluctuations that affect the security and efficiency of the protocol. This characterization allows us to understand the practical limits of the devices, such as their optimal operating range and various imperfections, which is essential for modeling the system in simulations.

- **Theoretical modeling and simulation**: In parallel with the experimental characterization of the components, another key objective is to conduct detailed simulations that model the system's behavior under realistic experimental conditions, addressing the lack of detailed simulation models in existing literature. These simulations are based on mathematical models that consider experimental imperfections in detail, and the goal is to study the impact of these factors on the secret key rate. By conducting simulations prior to experimental implementation, it is possible to optimize system pa-

rameters and more accurately predict how the system will behave under real conditions. Additionally, the simulations provide guidance for adjusting the experimental components and mitigating the adverse effects of the observed imperfections.

- **Experimental implementation**: After characterizing the components and evaluating the impact of imperfections through simulations, the next objective is to assemble and configure the complete CV-QKD system. This involves integrating the different devices, including quantum state generation and detection systems, modulators, correction systems, and other electro-optic devices. By addressing different challenges related with the integration of CV-QKD systems in practical environments, we implement correction methods to mitigate the effects of different experimental imperfections.
- **Experimental demonstration**: Once the complete system is assembled, the next step is to perform experimental tests to evaluate the system's performance under real conditions. In this case, experimental transmissions are carried out through commercial optical fibers of different lengths to validate the system's stability and ability to generate secure keys in a realistic environment. The experimental results are analyzed, and the values obtained with the previous simulations are compared. The system's security is assessed by estimating the secret key rate for the different transmissions, ensuring the generated keys are completely secure against an attacker.
- **Real-world use case demonstration**: Finally, the last objective of this thesis is to demonstrate the applicability of the CV-QKD system in real-world use cases. This involves demonstrating the system's integrability into real-world scenarios, using the generated quantum keys to encrypt information in real-life applications. To do this, we use our system to deploy secure encrypted connections using keys distilled from it. This validates that the developed system is not only theoretically secure but also viable from a practical point of view.

With these objectives, this thesis aims to contribute to the development of quantum cryptography systems, specifically those based on continuous variables, that can offer a practical and secure solution for key distribution in real-world environments. Through the detailed study of the system and the presentation of solutions to the various challenges that arise during the completion of the different objectives, this work hopes to contribute to the state of the art of experimental CV-QKD implementations, paving the way for their large-scale deployment in global telecommunications networks.

Chapter 2

Scientific Background

This chapter aims to review the fundamental theory required for the rest of this thesis. Specifically, the chapter begins with a brief introduction to the basic concepts of Quantum Mechanics and Quantum Information necessary to understand the formalism and security proofs of Quantum Key Distribution (QKD) protocols. It then continues with a general review of the historical development and QKD's state of the art. Finally, it concludes with a review of the security analysis of the Continuous-Variable Quantum Key Distribution (CV-QKD) protocol implemented in this thesis.

2.1 Fundamentals of Quantum Information

This section quickly reviews the fundamental principles of quantum mechanics, focusing on continuous-variable systems and quantum information. We will begin with an overview of quantum mechanics, focusing on its core postulates, the formalism of state vectors, operators, observables, and the concept of quantum entanglement. This foundational knowledge is crucial for understanding continuous-variable quantum systems, which are characterized by observables with continuous spectra. We will discuss the classical mechanics analogs of these systems, followed by a review of Fock states, gaussian states, and coherent states.

Next, we will transition into quantum information theory, emphasizing the quantum extensions of classical information concepts such as entropy and mutual information. The section will also cover the von Neumann entropy, quantum mutual information, and the Holevo bound, which sets the limits of information extraction from quantum systems. These theoretical constructs are crucial for understanding the security framework in CV-QKD.

This section's contents are part of the academic literature, and the material can be found in numerous textbooks and reviews on quantum mechanics, information theory, quantum optics, etc. Thoroughly covering these topics would take much more than a thesis, so this section intends to briefly introduce the key concepts used in the subsequent sections.

2.1.1 Quantum Mechanics

Here, a basic introduction to quantum mechanics is presented, including the postulates of quantum mechanics theory and the uncertainty principle, which are the foundations of QKD. The contents of this subsection are drawn mainly from quantum mechanics textbooks [55, 114] that cover the main aspects of quantum mechanics and its mathematical formalism.

The first postulate of quantum mechanics states that for every isolated physical system, there is a Hilbert space (a complex vector space with an inner product) known as the system's state space. The system is completely defined by its state vector, which is a vector in the system's state space.

Following Dirac's notation, we refer to the state vector as the *ket*, $|\psi\rangle$, and its conjugate transpose as the *bra*, $\langle\psi|$. The inner product between two state vectors $|\psi\rangle$ and $|\phi\rangle$ in the system's state space is denoted by $\langle\psi|\phi\rangle$, and it is a scalar in the Hilbert space.

Within these Hilbert spaces, operators are defined as linear mappings that act on state vectors. If $\hat{O}$ is an operator and $|\psi\rangle$ is a state vector in the Hilbert space, then $\hat{O}\,|\psi\rangle$ is another state vector in the same Hilbert space. Operators can represent various transformations and operations performed on quantum states.

Observables are a special type of operator representing measurable physical quantities. An observable $\hat{A}$ is a Hermitian linear operator, meaning $\hat{A} = \hat{A}^\dagger$, where $\hat{A}^\dagger$ denotes the adjoint (conjugate transpose) of $\hat{A}$. Hermiticity ensures that the eigenvalues of observables are real numbers corresponding to possible measurement outcomes. The eigenvalue equation for an observable $\hat{A}$ is expressed as

$$\hat{A}\,|a_n\rangle = a_n\,|a_n\rangle\,, \tag{2.1}$$

where a_n is an eigenvalue and $|a_n\rangle$ is the corresponding eigenstate. The eigenvalues a_n represent the possible measurement results of the observable $\hat{A}$.

The second postulate states that the state space of a composite physical system is the tensor product of the state spaces of the component physical systems. If we have n systems, prepared in the state $|\psi_i\rangle$ for $i = 1, \ldots, n$, the total state of the complete system is the tensor product $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

The density operator, also known as the density matrix, provides a complete description of the state of a quantum system. For a pure state, which can be fully described by a single state vector $|\psi\rangle$, the density operator is defined as

$$\rho = |\psi\rangle\langle\psi| \,. \tag{2.2}$$

A pure state contains the maximum possible information about the quantum system, and its density operator satisfies $\rho^2 = \rho$ and $\mathrm{Tr}(\rho) = 1$. For a mixed state, which describes a situation where multiple different state vectors are needed to define the system's state, the density operator is a weighted combination of several pure states:

$$\hat{\rho} = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \,, \tag{2.3}$$

where p_i are positive probabilities that sum to one. This density operator is not idempotent, i.e., $\rho^2 \neq \rho$. Mixed states represent a statistical mixture of several pure states, and their trace is also one, $\mathrm{Tr}(\rho) = 1$. Assuming the system is in the state ρ, the expected value of an arbitrary observable $\hat{A}$ is calculated as

$$\langle \hat{A} \rangle = \mathrm{Tr}\,(\rho \hat{A}), \tag{2.4}$$

which in the case of ρ being a pure state defined by $|\psi\rangle\langle\psi|$ simplifies to

$$\langle \hat{A} \rangle = \langle\psi|\hat{A}|\psi\rangle \,. \tag{2.5}$$

The third postulate asserts that the time evolution of a quantum system is described by the Schrödinger equation [141], which states that the state vector's temporal evolution is governed by

$$i\frac{\mathrm{d}\,|\psi(t)\rangle}{\mathrm{d}t} = \hat{H}(t)\,|\psi(t)\rangle \,, \tag{2.6}$$

where $\hat{H}(t)$ is the Hamiltonian operator of the system associated with its total energy.

The fourth postulate states that quantum measurements are defined by a collection $\{\hat{M}_n\}$ of measurement operators. These operators act on the state space being measured, and m represents the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, the probability $p(m)$ of obtaining outcome m is given by

$$p(m) = \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle \,, \tag{2.7}$$

and the state of the system after the measurement is said to collapse to the measured outcome, and it then becomes

$$|\psi\rangle \to \frac{\hat{M}_m\,|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle}}. \tag{2.8}$$

Lastly, we introduce the uncertainty principle of quantum mechanics, which in its general form states that for two Hermitian operators $\hat{A}$ and $\hat{B}$, the uncertainty relation between them is expressed as

$$\Delta A \Delta B \geq \frac{1}{2} |\langle [\hat{A}, \hat{B}] \rangle| , \tag{2.9}$$

where $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ is the commutator of $\hat{A}$ and $\hat{B}$, and where ΔA and ΔB are the standard deviations of the observables $\hat{A}$ and $\hat{B}$. This means that the product of the standard deviations of both operators is greater than or equal to half the absolute value of the expected value of the commutator of the two operators. The standard deviation of an observable $\hat{A}$ in a state $|\psi\rangle$ is defined as

$$\Delta A = \sqrt{\langle \psi | \hat{A}^2 | \psi \rangle - \langle \psi | \hat{A} | \psi \rangle^2}. \tag{2.10}$$

Quantum Entanglement

Quantum entanglement is a fundamental phenomenon in quantum mechanics that describes a correlation between the properties of systems whose quantum states cannot be independently described. When two or more systems are entangled, the total quantum state of the ensemble must be considered as a whole, even if the systems are spatially separated. Mathematically, an entangled state cannot be factored as a tensor product of the individual states of each system. For example, for a system of two subsystems, an entangled state is represented as $|\psi\rangle_{AB}$ and it cannot be factored as a tensor product of two individual states,

$$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\phi\rangle_B . \tag{2.11}$$

Instead, the total quantum state is a superposition of tensor products, that is,

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij} |a_i\rangle_A \otimes |b_j\rangle_B , \tag{2.12}$$

where $|a_i\rangle_A$ and $|b_j\rangle_B$ are basis states of the Hilbert spaces of subsystems A and B, respectively, and c_{ij} are complex coefficients that describe the probability amplitude of finding the system in the combined states $|a_i\rangle_A$ and $|b_j\rangle_B$.

One of the most remarkable features of quantum entanglement is that measurements performed on one of the subsystems instantaneously influence the state of the other, regardless of the distance between them. This behavior was first described by Einstein, Podolsky, and Rosen [43] as "spooky action at a distance". However, in modern quantum theory, this non-locality is a natural consequence of quantum superposition and the coherence of entangled states.

2.1.2 Continuous-Variable Quantum Systems

Now, we introduce the concept of continuous-variable quantum systems, which are essential in quantum mechanics for describing systems where quantities like position and momentum can vary continuously. These systems are particularly important in the context of the electromagnetic field, where they are used to describe the quantum states of photons. The section will explore the mathematical representation of these systems, including the use of Fock states to describe systems of specific numbers of photons, as well as coherent states, which play a crucial role in encoding and transmitting information in CV-QKD. The contents of this section are drawn from various comprehensive textbooks and reviews [51, 24, 49, 84], which cover continuous-variable quantum systems with much more detail.

In quantum mechanics, a system is classified as a continuous-variable system when it is described by observables with continuous spectra in an infinite-dimensional Hilbert space.

In classical mechanics, the state of a particle is described by its position q and momentum p, known as canonically conjugate variables. In this formalism, the relationships between these variables are expressed using Poisson brackets. For two functions $f(q_i, p_i, t)$ and $g(q_i, p_i, t)$ for $i = 1, \ldots, N$ that describe N particles, the Poisson bracket is defined as

$$\{f, g\} = \sum_{i=1}^{N} \left(\frac{\partial f}{\partial q_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q_i} \right). \tag{2.13}$$

The canonical variables q_i and p_i satisfy the following fundamental relationships expressed in terms of the Poisson brackets:

$$\{q_i, q_j\} = 0, \quad \{q_i, p_j\} = \delta_{i,j}, \quad \{p_i, p_j\} = 0. \tag{2.14}$$

These relationships indicate that positions and momentum generally do not commute with each other, but the position and momentum corresponding to the same particle do. To translate this framework to quantum mechanics via canonical quantization, the classical variables are replaced by quantum operators $\hat{q}_i$ and $\hat{p}_i$, and the Poisson brackets by commutators:

$$[\hat{q}_i, \hat{q}_j] = 0, \quad [\hat{q}_i, \hat{p}_j] = i\delta_{i,j}, \quad [\hat{p}_i, \hat{p}_j] = 0. \tag{2.15}$$

These commutation relations lead to the famous Heisenberg uncertainty relation, which is derived from Equation (2.9) using these commutation relations,

$$\Delta\hat{q}\Delta\hat{p} \geq \frac{1}{2}. \tag{2.16}$$

This implies that it is not possible to measure a particle's position and momentum simultaneously with arbitrary precision.

Fock States

A typical example of a continuous-variable system consists of a system with multiple bosonic modes corresponding to quantum harmonic oscillators, such as the electromagnetic field, where each mode of the field corresponds to a photon state with a specific frequency. This infinite-dimensional Hilbert space is defined as

$$\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k, \tag{2.17}$$

where each $\mathcal{H}_k$ is called a *Fock space* and describes a specific mode of the system, and is constructed from a basis called the Fock basis, which consists of states such as $\{|0\rangle, |1\rangle, \ldots, |n\rangle\}$. A Fock space is a Hilbert space that describes quantum states of a variable number of identical particles, such as photons in the case of the electromagnetic field, allowing for the superposition and creation of states with different numbers of particles. The states in the Fock basis represent specific numbers of photons in each mode. Although this analysis generally applies to any system with multiple bosonic modes, we will focus on the electromagnetic field, and the particles in question will be photons.

With this, we can introduce the famous creation $\hat{a}^\dagger$ and annihilation $\hat{a}$ operators for photons for a mode i, defined by their actions on the Fock basis:

$$\hat{a}_i |n\rangle_i = \sqrt{n}\, |n-1\rangle_i, \quad \hat{a}_i^\dagger |n\rangle_i = \sqrt{n+1}\, |n+1\rangle_i. \tag{2.18}$$

These operators are related to the generic position and momentum operators $\hat{q}$ and $\hat{p}$, which in the case of the electromagnetic field are called *quadrature operators*, through the following expressions.

$$\hat{q} = \frac{1}{\sqrt{2}} \left(\hat{a} + \hat{a}^\dagger\right), \quad \hat{p} = \frac{-i}{\sqrt{2}} \left(\hat{a} - \hat{a}^\dagger\right), \tag{2.19}$$

The creation and annihilation operators are then expressed in terms of quadrature operators as

$$\hat{a} = \frac{1}{\sqrt{2}} \left(\hat{q} + i\hat{p}\right), \quad \hat{a}^\dagger = \frac{1}{\sqrt{2}} \left(\hat{q} - i\hat{p}\right), \tag{2.20}$$

Moreover, the vacuum state of the system, denoted by $|0\rangle$ and representing the state with no photons, is the ground state of the Hamiltonian of a system of N quantum harmonic oscillators, given by

$$\hat{H} = \sum_{i=1}^{N} \left(\hat{a}_i^\dagger \hat{a}_i + \frac{1}{2}\right). \tag{2.21}$$

In a quantum system with multiple modes, Fock states are formed by considering that each mode can contain a specific number of photons. For a global Hilbert space describing all the modes of the system, a Fock state is obtained by specifying the number of photons present in each mode. Mathematically, this is described by:

$$|n_1, \ldots, n_N\rangle = \frac{1}{\sqrt{n_1! n_2! \cdots n_N!}} \hat{a}_1^{\dagger n_1} \hat{a}_2^{\dagger n_2} \cdots \hat{a}_N^{\dagger n_N} |0\rangle . \tag{2.22}$$

Finally, it is important to mention that for multi-mode systems, the quadrature operators can be grouped into a single vector $\hat{r}$ defined by

$$\hat{r} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_N, \hat{p}_N)^T. \tag{2.23}$$

This allows the commutation relations to be expressed in a more compact form:

$$[\hat{r}_k, \hat{r}_l] = i\Omega_{kl}, \tag{2.24}$$

where Ω is known as the *symplectic matrix*, defined by

$$\Omega = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.25}$$

The term symplectic [176] refers to a mathematical structure that preserves the area in phase space during transformations. This means that the relationship between position and momentum coordinates, specifically how they combine to define the geometry of the system, remains unchanged.

Gaussian States

Gaussian states are a special type of quantum state in continuous-variable systems. A quantum state is said to be Gaussian when the probability distributions of its quadrature operators follow Gaussian distributions.

The main property of Gaussian states is that they are completely defined by what is known as their first and second statistical moments. The first statistical moments are the mean values of the quadrature operators, defined by

$$\langle \hat{r}_i \rangle = \mathrm{Tr}(\rho \hat{r}_i), \tag{2.26}$$

where ρ is a Gaussian state. The second statistical moment, which contains information about the variances of these operators, is defined by the *covariance matrix*. The covariance matrix is a fundamental tool in describing continuous-variable

quantum systems, as it captures the correlations and uncertainties between pairs of continuous variables. The covariance matrix Σ is defined by its elements

$$\Sigma_{ij} = \frac{1}{2} \langle \hat{r}_i \hat{r}_j + \hat{r}_j \hat{r}_i \rangle - \langle \hat{r}_i \rangle \langle \hat{r}_j \rangle . \tag{2.27}$$

This matrix provides a complete description of the quantum state in terms of the second-order correlations between the canonical variables. The covariance matrix must satisfy the Heisenberg uncertainty principle, expressed as

$$\Sigma + i\Omega \geq 0. \tag{2.28}$$

It can be shown [148] that for a covariance matrix Σ, there exists a non-unique symplectic transformation S, which is a linear map satisfying $S^T \Omega S = \Omega$, such that

$$S^T \Sigma S = \Lambda, \tag{2.29}$$

where Λ is a diagonal matrix defined by

$$\Lambda = \bigoplus_{k=1}^{N} \begin{pmatrix} \lambda_k & 0 \\ 0 & \lambda_k \end{pmatrix}, \tag{2.30}$$

where λ_k are known as the symplectic eigenvalues of the covariance matrix Σ, which corresponds with the positive eigenvalues of the operator $i\Omega\Sigma$.

As will be seen later, the covariance matrix is particularly useful in the security analysis of CV-QKD and the characterization of Gaussian quantum states.

Coherent States

Coherent states are of particular theoretical and experimental interest for several reasons. Theoretically, they provide an ideal representation of quantum states that minimize the Heisenberg uncertainty relation, making them useful for studying the limits of quantum mechanics and the transition between quantum and classical behaviors. Additionally, coherent states allow for a simple and elegant mathematical description of many physical situations, facilitating the resolution of complex problems in quantum optics and quantum information theory. Experimentally, coherent states are relatively easy to generate, especially in optical systems, as they can be produced using conventional attenuated lasers.

Coherent states, denoted by $|\alpha\rangle$, are defined as the eigenstates of the annihilation operator:

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle , \tag{2.31}$$

where α is a complex number. Coherent states are generated by displacing the vacuum state through the application of the displacement operator $\hat{D}(\alpha)$, which is defined as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}. \tag{2.32}$$

This operator is unitary and displaces the vacuum state $|0\rangle$ to the coherent state $|\alpha\rangle$, such that $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$. It is important to note that a coherent state $|\alpha\rangle$ can be expressed as a weighted superposition of Fock states as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{2.33}$$

Coherent states saturate the Heisenberg uncertainty principle, as they have the smallest possible uncertainty in their quadratures. For a coherent state, the variances of the quadrature operators $\hat{q}$ and $\hat{p}$ are minimal and satisfy

$$\Delta q^2 = \frac{1}{2}, \quad \Delta p^2 = \frac{1}{2}. \tag{2.34}$$

This means that coherent states have the smallest possible uncertainty in their quadratures and, therefore, approach classical behavior as closely as quantum mechanics allows.

2.1.3 Quantum Information Theory

To understand the basics of quantum information theory, it is essential to review fundamental concepts from classical information theory, such as entropy and mutual information. We thus begin reviewing the fundamental concepts of classical information theory and then introduce the necessary tools to understand the security analysis of CV-QKD, such as the quantum mutual information and the Holevo bound. A more detailed review of quantum information theory can be found in [114], covering the main topics of Quantum Computation and Quantum Information.

We begin by introducing Shannon entropy $H(X)$, which is a fundamental measure in classical information theory [142] that quantifies the uncertainty of a random variable X, and it is defined by

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x), \tag{2.35}$$

where $p(x)$ is the probability of obtaining x in the random variable X. For a binary variable X with possible outcomes 0 and 1, and probability p of being 1, the binary entropy simplifies to

$$H_2(X) = -p \log_2 p - (1-p) \log_2 (1-p). \tag{2.36}$$

The joint entropy of two random variables X and Y is defined by generalizing Equation (2.35) as

$$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log_2 p(x,y), \tag{2.37}$$

where $p(x,y)$ is the joint probability of obtaining x and y respectively. Lastly, the conditional entropy $H(Y|X)$, which measures the uncertainty of Y given X, is defined as

$$H(Y|X) = H(Y,X) - H(X) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log_2 \frac{p(x,y)}{p(x)}, \tag{2.38}$$

where $p(x,y)$ is the probability of measuring x and y, and $p(x)$ is the probability of measuring x regardless of the value of the variable Y.

The mutual information $I(X;Y)$ between two random variables X and Y measures the amount of information one variable contains about the other, and it is defined as

$$I(X;Y) = H(X) - H(X|Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log_2 \frac{p(x,y)}{p(x)p(y)}. \tag{2.39}$$

Mutual information has several key properties: Non-negativity implies that mutual information is always greater than or equal to zero. Symmetry establishes that $I(X;Y) = I(Y;X)$, meaning the information X has about Y is equal to the information Y has about X. Additivity refers to the fact that mutual information is additive for independent variables, i.e., $I(X;Y\cup Z) = I(X;Y) + I(X;Z)$.

Quantum Entropy and Mutual Information

The von Neumann entropy $S(\rho)$ measures the uncertainty of a quantum state represented by a density matrix ρ, and it is defined by

$$S(\rho) = -\operatorname{Tr}(\rho\log\rho). \tag{2.40}$$

If ρ is a mixed state that can be diagonalized as in Equation (2.3), then:

$$S(\rho) = -\sum_i \lambda_i \log\lambda_i, \tag{2.41}$$

where λ_i are the eigenvalues of ρ. Von Neumann entropy has several fundamental properties: Purity indicates that for a pure state $\rho = |\psi_i\rangle\langle\psi_i|$, the entropy is $S(\rho) = 0$. Invariance states that entropy is invariant under unitary transformations, i.e., $S(\hat{U}\rho\hat{U}^\dagger) = S(\rho)$, for $\hat{U}^\dagger = \hat{U}^{-1}$. The maximum value of entropy is reached for

a maximally mixed state in a Hilbert space of dimension d and is $S(\rho) = \log d$. Concavity indicates that $S(\eta\rho_1 + (1-\eta)\rho_2) \geq \eta S(\rho_1) + (1-\eta)S(\rho_2)$ for $0 \leq \eta \leq 1$. Finally, subadditivity means that the entropy of a composite quantum system can be less than the sum of the entropies of its parts, i.e., $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$.

Quantum mutual information measures the amount of information shared between two subsystems, A and B, of a composite quantum system. It is defined using von Neumann entropy and expressed as

$$I_{AB} = S(\rho_A) + S(\rho_B) - S(\rho_{AB}), \tag{2.42}$$

where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ are the reduced density matrices of subsystems A and B, respectively, and ρ_{AB} is the density matrix of the composite system. Similar to its classical counterpart, Quantum mutual information has several key properties, such as non-negativity and symmetry.

The Holevo Bound

The Holevo bound [63] sets an upper limit on the amount of classical information that can be extracted from a quantum system. This bound is fundamental in quantum information theory and has significant implications in the context of quantum cryptography, particularly in an attacker's ability to obtain information.

Consider a quantum system composed of three subsystems: A (the sender, typically Alice), B (the receiver, typically Bob), and E (the environment, which can represent an attacker, typically Eve). The Holevo bound provides a measure of the maximum amount of classical information that can be obtained by an attacker E about system A after measuring their part of the system.

For a set of mixed states $\{\rho_i^A\}$ with probabilities $\{p_i\}$, the Holevo information χ is defined as

$$\chi = S\left(\rho^A\right) - \sum_i p_i S(\rho_i^A), \tag{2.43}$$

where $\rho^A = \sum_i p_i \rho_i^A$ is the average density matrix of system A. The Holevo bound quantifies the average reduction in von Neumann entropy upon knowing the state preparation. It measures the amount of uncertainty eliminated when knowing in which specific state ρ_i^A the system A is.

In the context of quantum cryptography, suppose A and B are trying to share information securely, and E is trying to intercept that information. The Holevo bound imposes an upper limit on the amount of information that E can obtain. The quantum mutual information between A and E, denoted by I_{AE}, is bounded by χ:

$$I_{AE} \leq \chi. \tag{2.44}$$

This implies that the amount of classical information an attacker can obtain about system A cannot exceed χ, regardless of the measurement strategy employed.

For a composite system ρ_{ABE} that describes the correlations between A, B, and E, the Holevo bound can also be interpreted in terms of the information accessible to E after B performs a measurement. If B measures their part of the system, the resulting state in A and E can be used to evaluate how much E can learn about A through the relation:

$$\chi_{EB} = S(\rho_E) - S(\rho_{E|B}), \tag{2.45}$$

where $S(\rho_E)$ is the von Neumann entropy of system E and $S(\rho_{E|B})$ is the conditional entropy of system E given the measurement outcome of B.

It can be shown [37] that when ρ is a Gaussian state, the expression for the von Neumann entropy $S(\rho) = -\operatorname{Tr}(\rho \log \rho)$ simplifies to

$$S(\rho) = \sum_{k=1}^{N} G\left(\frac{\lambda_k - 1}{2}\right), \tag{2.46}$$

where N represents the number of modes in the system, λ_k are the symplectic eigenvalues of the covariance matrix associated with the Gaussian state ρ, and $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. This expression will be very useful for calculating the Holevo bound in the security analysis of CV-QKD.

2.2 Quantum Key Distribution

Quantum Key Distribution (QKD) is a technology that enables two parties to generate a shared and secret cryptographic key using the principles of quantum mechanics to ensure its security. Unlike traditional key distribution methods, QKD guarantees that any eavesdropping attempts are detected. This security is based on fundamental quantum principles such as the no-cloning theorem and Heisenberg's uncertainty principle, which ensure that any unwanted disturbance in a quantum system is detectable, alerting about the presence of a potential eavesdropper.

QKD is primarily used to generate cryptographic keys, ensuring that they cannot be intercepted without detection. These keys can then be employed in symmetric encryption systems, such as AES [111] to encrypt information. This is crucial for information security, as traditional public-key cryptography methods like RSA [133] or Diffie-Hellman [41] rely on the difficulty of solving mathematical problems that, over time, will become vulnerable to quantum computer attacks. Specifically, Shor's quantum algorithm [143] has the potential to break these cryptographic systems by efficiently solving these mathematical problems exponentially faster than classical algorithms.

In this section, we aim to briefly introduce different QKD protocols, focusing on the most common ones found in scientific literature. To do this, we first categorize the most important QKD protocols into two main families: Discrete-Variable (DV) and Continuous-Variable (CV) protocols. For the former, we introduce the BB84 protocol, which originally established the concept of QKD. For the latter, we present the GG02 protocol, which laid the foundation for CV-QKD. In both cases, we present a review of the state of the art, to highlight the latest advancements in all branches of QKD.

2.2.1 Discrete-Variable Quantum Key Distribution

DV-QKD introduces quantum cryptography by providing a secure method for distributing cryptographic keys between two parties, typically referred to as Alice and Bob. Its security is based on the principles of quantum mechanics rather than on the computational difficulty of solving a mathematical problem, as in classical cryptography. The distinctive feature of DV-QKD protocols is that they encode the key information in discrete quantum states, such as the polarization of single photons.

The first and most well-known DV-QKD protocol is the BB84 protocol, proposed by C. Bennett and G. Brassard in 1984 [19]. In BB84, Alice sends single photons to Bob, each prepared in one of four possible polarization states. Bob measures the incoming photons using randomly chosen polarization bases, either rectilinear or diagonal. The security of DV-QKD is based on the Heisenberg uncertainty principle and the no-cloning theorem, which states that an unknown quantum state cannot be copied perfectly. This implies that any eavesdropper attempting to intercept and measure the photons will inevitably introduce detectable disturbances. When Alice and Bob compare a subset of their measurement results over an authenticated public channel, they can detect the presence of Eve by studying the relationship between their shared results, which could indicate eavesdropping attempts.

Initially, the BB84 protocol was designed to emit optical pulses with a perfect single-photon source. However, due to the challenges in engineering such a source, an attenuated laser source was developed as an alternative. This approach made the protocol vulnerable to photon-number-splitting (PNS) attacks, significantly reducing the key rate. The decoy-state method [72] was later proposed to counter PNS attacks, resulting in a decoy-state-based BB84 protocol that closely approached the key rates of the original BB84. In addition to BB84, several other DV-QKD protocols have been developed, each with unique features and advantages. Here, some of the most known DV-QKD protocols are listed.

The E91 protocol [44] relies on entangled photon pairs that are shared between Alice and Bob. The entanglement ensures that the measurement outcomes are correlated, providing a robust method for key distribution that also enables security against more general types of attacks. However, implementing the E91 protocol is limited by the difficulty in engineering an entangled-photon source that outputs high-fidelity entangled photon pairs with a high repetition rate, making high-speed experimental implementations challenging.

Another notable DV-QKD protocol is the B92 protocol [17]. This protocol is a simplified version of the BB84 protocol, transmitting two non-orthogonal quantum states instead of four, and its security has been proven for an arbitrary non-orthogonality [154]. This implementation is very interesting due to its simplicity, which can make the implementation easier and more cost-effective. However, its security is limited, as the states can be deterministically distinguished by introducing losses, making it susceptible to side-channel attacks in which one channel is replaced by another with lower loss [155].

Device-Independent Quantum Key Distribution (DI-QKD) [12] guarantees security without requiring trust in the internal workings of the quantum devices used. It leverages the principles of quantum entanglement to ensure that the generated keys are secure, even if the devices are partially or fully untrusted or compromised. DI-QKD can be seen as a revised E91 protocol with different measurement settings and post-processing methods. Like the E91 protocol, DI-QKD detects information leakage by monitoring the violation of Bell inequalities, ensuring a high level of security even in the presence of device flaws.

Measurement-Device-Independent QKD (MDI-QKD) [97] is designed to eliminate security vulnerabilities associated with the detection process. In MDI-QKD, the measurement devices are placed in an untrusted or adversarial location. The security of the key distribution relies not on trusting the measurement devices but on the quantum correlations between the communicating parties, as the measurements are performed by an untrusted third party. This approach mitigates detector side-channel attacks and ensures that security is guaranteed even if the measurement devices are compromised.

Twin-Field Quantum Key Distribution (TF-QKD) [101] is a novel QKD protocol that enhances the distance over which secure quantum communication can be performed. TF-QKD leverages the concept of single-photon interference between two remote parties, facilitated by a central relay, without requiring direct transmission of quantum states over the entire communication distance. Using a twin-field setup effectively reduces the loss associated with the transmission, thereby significantly extending the secure communication range compared to traditional QKD

protocols. This improvement allows TF-QKD to break the fundamental point-to-point key rate bounds that apply to most QKD protocols, making it particularly promising for long-distance quantum communication networks.

Other important DV-QKD protocols include BBM92 [20], SARG04 [27], the Coherent One-Way Protocol [73], the Six-State Protocol [139], and the Differential-Phase-Shift Protocol [152]. A detailed review of DV-QKD, including its main concepts, protocols, technological challenges, and different attacks, can be found in [53].

The BB84 Protocol

The BB84 protocol [19] is a pioneering QKD protocol that allows two parties (Alice and Bob) to generate a shared secret key with provable security against an eavesdropper (Eve). First, Alice prepares a series of two-state quantum systems, known as *qubits*, in one of four possible states. These states are chosen from two orthogonal bases: the rectilinear basis with states $|0\rangle$ and $|1\rangle$, and the diagonal basis with states $|+\rangle$ $|-\rangle$, where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.47}$$

Alice then randomly selects the basis for each qubit and sends them to Bob over a quantum channel. Upon receiving the qubits, Bob measures each qubit on a randomly chosen basis (either rectilinear or diagonal). Due to the nature of quantum measurements, if Bob's basis matches Alice's basis, he will measure the correct state. However, if the bases do not match, the outcome is completely random. After the transmission, Alice and Bob communicate over a classical public channel to disclose their bases. This is known as *key sifting*, where they discard the results where their bases do not match, leaving them with a subset of correlated bits known as the raw key.

To distill an identical key and ensure its security, Alice and Bob perform *error correction* and *privacy amplification*. Error correction reconciles any discrepancies between their raw keys, likely caused by noise in the quantum channel. They use classical error correction codes and hash functions to detect and correct errors. Privacy amplification reduces the information that any potential eavesdropper, Eve, may have gained. They achieve this by applying a hash function to the reconciled key, resulting in a shorter but highly secure final key.

The Quantum Bit Error Rate (QBER) is a crucial parameter that quantifies the fraction of wrong bits after Alice and Bob have measured their qubits and compared their bases. It is defined as the fraction of the number of incorrect bits

divided by the total number of compared bits. To calculate QBER, Alice and Bob publicly compare a subset of their raw key bits. If they observe an error rate higher than expected due to channel noise alone, they can infer the presence of an eavesdropper and abort the protocol.

To ensure the security of the key, it is essential to understand the mutual information between the parties involved. The key rate, K, can be derived using the concept of mutual information and the Holevo bound [63], which is an upper bound to the information obtained by Eve. The mutual information between Alice and Bob, denoted as I_{AB}, represents the amount of shared information they have after the quantum communication process. If we denote the QBER by Q, the mutual information can be written as

$$I_{AB} = 1 - H_2(Q), \tag{2.48}$$

where $H_2(Q)$ is the binary entropy function, defined as

$$H_2(Q) = -Q \log_2 Q - (1 - Q) \log_2(1 - Q). \tag{2.49}$$

The mutual information between Alice and Eve quantifies the amount of information Eve has about Alice's key. According to quantum information theory, the maximum amount of information that Eve can extract from the quantum system is bounded by the Holevo bound, χ_{AE}. For the BB84 protocol, the Holevo bound can be expressed as

$$\chi_{AE} = S(\rho_E) - \sum_i p_i S(\rho_{E|i}), \tag{2.50}$$

where $S(\rho)$ is the von Neumann entropy of the density matrix ρ, calculated as in Equation (2.40), p_i are the probabilities of getting the outcome i, ρ_E is the density matrix representing the state of the quantum system accessible to Eve after she interacts with the quantum channel, which can be seen as Eve's description of her system if she knows nothing about the measurement results obtained by Alice after completing the protocol, and $\rho_{E|i}$ is the density matrix representing the quantum state of Eve, conditioned by a particular outcome i that Alice and Bob have measured. After a complex mathematical derivation [123], the bound simplifies to:

$$\chi_{AE} = H_2(Q). \tag{2.51}$$

This is because, in the presence of an eavesdropper, the maximum amount of information Eve can obtain about Alice's key is related to the errors she introduces, which is directly given by the binary entropy function. The asymptotic secret key rate K is the difference between the mutual information Alice and Bob share and Eve's information about Alice's key. Therefore, the secret key rate K is given by

$$K = I_{AB} - \chi_{AE} = 1 - 2H_2(Q). \tag{2.52}$$

This equation shows that the key rate K is positive if the QBER, Q, is below a certain threshold. For practical implementations of the BB84 protocol, the key remains secure if the QBER is below approximately 11 %, ensuring that Alice and Bob can generate a secure key, even in the presence of an eavesdropper [144].

State of the Art in DV-QKD

After the proposal of the BB84 protocol, it was experimentally demonstrated using optical fibers, showing that secure key distribution could be achieved over short distances of 32 cm using an optical table setup [18]. This experiment proved the feasibility of DV-QKD and laid the groundwork for future advancements. Subsequent experiments, both in fiber [71] and free-space [70], extended the transmission distance and improved the system's robustness, leading to the establishment of more sophisticated QKD networks. Notably, the DARPA Quantum Network [46] connected multiple nodes across Cambridge (Massachusetts), showcasing the potential of DV-QKD for secure communications in a metropolitan area.

Theoretically, after introducing the BB84 protocol, a rigorous proof of security was demonstrated [144]. Further developments introduced the concept of composable security [131], which guarantees that the security of DV-QKD remains intact even when integrated into larger cryptographic systems. More recently, different studies on realistic experimental devices have appeared, analyzing experimental imperfections in DV-QKD implementations from a theoretical point of view [178, 140, 172].

Regarding optical fiber demonstrations, notable implementations include the time-bin BB84 reaching 421 km [22], and multiple twin-field QKD implementations reaching 511 km [32], 830 km [165], and over 1000 km [95], all achieving positive secret key rates.

Regarding satellite-based implementations, the 1200 km satellite-to-ground transmission of the *Micius* satellite [92] is noteworthy. This was extended into a fully operational network of two satellites and 700 fiber QKD links, adding up to a total of 4600 km of QKD channel lengths [31].

Implementations of DV-QKD have also explored the integration of decoy-state protocols to enhance security and key generation rates. Decoy-state protocols [72] address the vulnerability of practical single-photon sources that occasionally emit multi-photon pulses, which can be exploited by eavesdroppers using photon-number-splitting (PNS) attacks. By randomly varying the intensity of the transmitted pulses and including decoy states with different mean photon numbers, these protocols can detect and mitigate these attacks, ensuring their security. Experimental demonstrations of decoy-state BB84 have significantly improved secure

key rates and transmission distances.

Advances in integrated photonic systems have provided significant improvements in terms of miniaturization, robustness, and scalability. A secret key rate of 866 b/s over a 150 km fiber [174] and 5 kb/s over a 250 km fiber [138] have been demonstrated using different integrated photonic implementations. MDI-QKD systems have also been miniaturized into a silicon photonics chip [175].

Finally, error correction and privacy amplification are essential components of experimental DV-QKD systems, ensuring the final shared key is identical and secure. Error correction algorithms such as the Cascade [23] and low-density parity-check (LDPC) codes [45] are implemented to correct discrepancies between Alice's and Bob's keys. Privacy amplification [21], typically performed using universal hash functions, reduces any partial information that an eavesdropper may have gained, resulting in a shorter but highly secure key.

2.2.2 Continuous-Variable Quantum Key Distribution

Continuous-Variable Quantum Key Distribution (CV-QKD) is an alternative type of QKD implementation to DV-QKD protocols, based on encoding information in continuous variables, such as the quadratures of quantum light states, rather than in discrete variables, such as the polarization states of single photons used in the BB84 protocol.

The main advantage of CV-QKD protocols over DV-QKD protocols is that the generation and detection of coherent states is simpler than the generation and detection of single photons [122], allowing the use of off-the-shelf components and making experimental implementations more cost-effective. Regarding the performance of each implementation, in a short-distance regime, CV-QKD shows greater tolerance to noise than DV-QKD. However, over long distances, DV-QKD shows greater tolerance to noise than CV-QKD [79]. In terms of the security of both protocols, DV-QKD generally offers a more straightforward and robust security framework due to its discrete nature and well-established theoretical foundations, while the continuous nature of CV-QKD complicates the security analysis due to the need for more complex mathematical tools and assumptions about the quantum channel and noise characteristics. Additionally, it is important to note that in CV-QKD, security proofs often require Gaussian assumptions and are more sensitive to imperfections in the system, making them less straightforward and potentially less robust against certain types of attacks.

The best-known CV-QKD protocol is the GG02 protocol [58], proposed by F. Grosshans and P. Grangier in 2002. In GG02, Alice generates random bit strings encoded onto Gaussian-modulated coherent states of light, which are sent to Bob

for homodyne detection to measure the quadrature components of the incoming states. The security proofs for GG02 rely on the optimality of Gaussian attacks, leveraging the fact that Gaussian states and operations are analytically tractable and experimentally feasible. The final key generation process involves classical post-processing consisting of the sifting of the keys where Alice and Bob communicate which basis or quadrature they used to encode and decode the information, followed by parameter estimation, where the two parties compare a randomly chosen subset of their data to analyze the channel and upper-bound the information stolen by an eavesdropper, followed by error correction where the two parties communicate the syndromes of the errors affecting their data to transform the raw keys into the same string of bits, and ending with privacy amplification, where the two parties generate a smaller but secret key, reducing Eve's knowledge of the key to a negligible amount. Apart from the GG02 protocol, there exist different CV-QKD protocols with various advantages. Here, some of them are listed and briefly described.

The no-switching protocol [171] is a variant of the GG02 protocol that simplifies the measurement process by allowing the receiver (Bob) to perform simultaneous measurements of both quadrature components (amplitude and phase) using heterodyne detection. This approach eliminates the need for the traditional switching between quadratures, thereby reducing implementation complexity and enhancing the overall efficiency of the key distribution process.

The discrete-modulated protocol is a variant of the GG02 protocol, in which Alice encodes information onto a set of discrete modulation of coherent states, which are then transmitted over a quantum channel to the receiver. Although discrete modulated CV-QKD appeared before the GG02 protocol [128], it was not widely used until its security was proven [88]. In this protocol, Bob measures the received states using homodyne or heterodyne detection to extract the quadrature components. Discrete modulation simplifies the implementation and reduces the complexity of the encoding process while still leveraging the high data rates and efficient error correction capabilities inherent to CV-QKD.

The reverse reconciliation protocol [145] appeared later to solve a significant problem. The classical post-processing phase involving error correction is typically known as reconciliation. Reconciliation is the procedure that allows Alice and Bob to align on the same data without an eavesdropper (Eve) obtaining information about the final key. Direct reconciliation is the traditional method where Bob tries to infer Alice's data. However, this becomes problematic when channel losses exceed 50 %, as Eve could obtain more information than Bob, putting the system's security at risk. This is known as the 3 dB limit, which is solved by reverse reconciliation. Unlike direct reconciliation, where Bob tries to infer Alice's data, reverse

reconciliation involves Alice guessing Bob's data. This approach allows the key distribution process to remain secure even when Eve intercepts more information than Bob. The primary advantage of reverse reconciliation is its ability to extend the range of CV-QKD protocols, making them more practical for real-world applications.

The squeezed state protocol [30] uses squeezed states of light to enhance security and key generation efficiency. In this protocol, Alice prepares squeezed states, which have reduced noise in one quadrature, and sends them to Bob, who performs homodyne or heterodyne detection. The reduced noise in squeezed states improves the signal-to-noise ratio, allowing for higher key rates and better resilience to eavesdropping. Squeezed states can be combined with homodyne or heterodyne detection, Gaussian or discrete modulation, and direct or reverse reconciliation. The only difference is the actual quantum states of light used to encode information.

Finally, among the remaining protocols, we highlight the Two-way protocol [125], which involves sending signals from Alice to Bob, who reflects them back with added modulation, increasing resilience against eavesdropping, and the Thermal state protocol [173], which uses thermal states of light, which are less sensitive to noise than coherent states, making the protocol robust in noisy environments. Both solutions are very promising but increase hardware complexity, and their security proofs are less studied.

The GG02 Protocol

The GG02 protocol, proposed by F. Grosshans and P. Grangier in 2002 [58], is one of the most well-known CV-QKD protocols. It is widely used in experimental implementations and, like the BB84 protocol, allows two parties (Alice and Bob) to generate a shared secret key with provable security against eavesdroppers based on the fundamental principles of quantum mechanics.

From now on, and throughout the rest of the thesis, all expressions will be expressed within the Shot Noise Units (SNU) framework. Hence, the equations presented here differ slightly from those presented in Section 2.1. For a more detailed explanation of the SNU framework, refer to Appendix A.

The protocol starts with Alice preparing displaced coherent states characterized by quadrature components q and p. These components are sampled from two independent and identically distributed random variables, $\mathcal{Q}$ and $\mathcal{P}$, both following a zero-mean normal distribution: $\mathcal{Q} \sim \mathcal{P} \sim \mathcal{N}(0, V_{\text{mod}})$, where V_{mod} represents the modulation variance of the quadrature components. Figure 2.1 illustrates these modulated coherent states in phase space and a modulated coherent state ensemble

using the two most common modulation schemes.

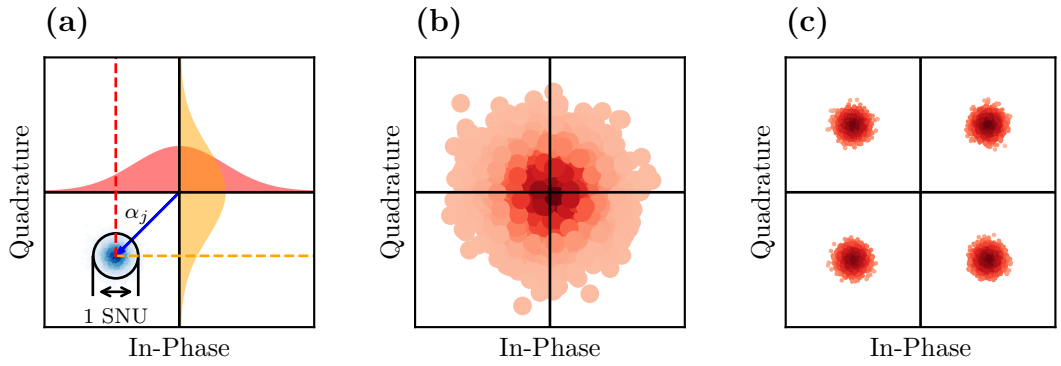

Figure 2.1: Representation of a Gaussian-modulated displaced coherent state and an ensemble of coherent states under different modulations. (a) shows the probability distribution functions of one Gaussian-modulated coherent state. As the variance of the modulation is V_{mod}, the position of the coherent state in the phase space is sampled from the two red Gaussian functions, both with variance V_{mod}. The variance of the coherent state itself is always 1 SNU as a consequence of the uncertainty principle. (b) shows an ensemble of 10,000 Gaussian-modulated coherent states in a density plot. (c) shows an ensemble of 10,000 discrete-modulated coherent states following a Quadrature Phase Shift Keying (QPSK) of four states in a density plot.

Each displaced coherent state is defined by $|\alpha_j\rangle = |q_j + ip_j\rangle$ and satisfies the eigenvalue equation:

$$\hat{a}\,|\alpha_j\rangle = \alpha_j\,|\alpha_j\rangle\,, \tag{2.53}$$

where the eigenvalues are $\alpha_j = q_j + ip_j$, and $\hat{a}$ is the annihilation operator, expressed in terms of the quadrature operators $\hat{q}$ and $\hat{p}$ in the SNU framework as

$$\hat{a} = \frac{1}{2}(\hat{q} + i\hat{p}). \tag{2.54}$$

Following [82], it can be shown that the variance of the $\hat{q}$ and $\hat{p}$ operators for the coherent state $|\alpha_j\rangle$ is given by the minimum possible uncertainty, which is 1 in the SNU framework:

$$\text{var}(\hat{q}_j) = \text{var}(\hat{p}_j) = \langle \hat{q}_j^2 \rangle - \langle \hat{q}_j \rangle^2 = \left(4q_j^2 + 1\right) - (2q_j)^2 = 1. \tag{2.55}$$

For the entire ensemble of coherent states prepared by Alice, the variance of the quadrature operators is calculated as follows, assuming $\langle \hat{q} \rangle = 0$ and that the expected value of $\mathcal{Q}^2$ is V_{mod}, both due to the zero-mean Gaussian distribution:

$$V := \text{var}_A(\hat{q}) = \text{var}_A(\hat{p}) = \langle \hat{q}^2 \rangle = 4q^2 + 1 = 4V_{\text{mod}} + 1 = V_A + 1, \tag{2.56}$$

where $V_A = 4V_{\text{mod}}$ is defined as the variance of the quadrature operators associated with Alice's modulation. This is commonly referred to as Alice's modulation variance, distinguishing it from V_{mod}, which is the variance of the quadrature components rather than the quadrature operators.

The mean photon number for the entire coherent state ensemble is given by the expected value of the photon number operator, also assuming $\langle \hat{q} \rangle = 0$:

$$\langle n \rangle = \langle \alpha | \hat{n} | \alpha \rangle = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = q^2 + p^2 = 2V_{\text{mod}} = \frac{V_A}{2}. \tag{2.57}$$

Alice then transmits the coherent state ensemble to Bob through a lossy and noisy channel, characterized by two key parameters: the transmittance T and the excess noise ξ. Upon arrival at Bob's location, the state ensemble is detected using a lossy and noisy detector, characterized by its efficiency η and electronic noise ν_{el}. The variance of Bob's quadrature operators, using the received state ensemble, is given by

$$V_B := \text{var}_B(\hat{q}) = \text{var}_B(\hat{p}) = T\eta(V + \chi_{\text{tot}}), \tag{2.58}$$

where χ_{tot} accounts for the total noise introduced by the channel and the detector, which is further discussed in the security analysis in Section 2.3.

After Bob measures the coherent states, Alice and Bob perform classical post-processing steps to transform Alice's modulation data and Bob's measurement results into a universally composable secure key. If Bob uses homodyne detection, he must perform the *sifting* stage. In homodyne detection, Bob randomly selects the quadrature to measure for each received coherent state and communicates this choice to Alice over a public classical channel to discard the states he did not measure. When Bob uses heterodyne detection, he measures both bases simultaneously, and no sifting is required.

Once Alice and Bob have two ensembles of coherent states of the same length, they reveal and compare a random subset of the transmitted and received data. This comparison allows them to estimate the total transmission and excess noise of the channel, enabling them to compute their mutual information and bound Eve's information. If Eve's information exceeds the mutual information, the protocol is aborted at this point.

If the protocol is not aborted, Alice and Bob proceed to information reconciliation. One-way information reconciliation, where one party sends information about the key to the other party, can be conducted in two ways: Bob can correct his bits based on Alice's data (*direct reconciliation*), or Alice can correct her bits based on Bob's data (*reverse reconciliation*).

In reverse reconciliation protocols, Alice attempts to infer what Bob received rather than Bob guessing what Alice sent [59]. In direct reconciliation, if the total transmittance T is less than 0.5 (equivalent to a 3 dB loss), Eve potentially has more information about what Alice prepared than Bob does, preventing the distillation of a secret key. The 3 dB loss limit can be overcome by reverse reconciliation, where Bob sends correction information to Alice, who adjusts her bit string according to Bob's data. In this scenario, Bob's data is primary, and since Alice's information about Bob's measurements always exceeds Eve's, the mutual information can remain greater than the Holevo bound for any transmittance.

For CV-QKD with Gaussian modulation, several reconciliation schemes have been proposed. Two significant schemes are slice reconciliation [159] and multidimensional reconciliation [86]. Both schemes use low-density parity-check (LDPC) codes [132] for error correction. In reverse reconciliation, one or several LDPC codes are used to calculate a compressed version of Bob's data, which is then transmitted over a classical channel to Alice and fed into her decoder.

Following information reconciliation, Alice and Bob conduct a confirmation step using a family of universal hash functions [29] to bind the probability of error correction failure. Alice or Bob uniformly selects a specific hash function from the family and communicates the choice to the other party. Both parties apply this hash function to their keys to obtain a hash value. They then exchange and compare these hash values; if they differ, the keys are not identical, and they abort the protocol. If the hash values match, they continue, knowing that they have bounded the probability that the keys are not identical.

Upon successful confirmation, Alice and Bob share the same bit string with very high probability. However, Eve may still possess some information about the key. To reduce Eve's likelihood of successfully guessing any part of the key to an acceptable level, Alice and Bob perform a privacy amplification protocol by applying a seeded randomness extractor algorithm to their bit strings. A family of universal hash functions is typically used for this purpose, which reduces the key length but ensures that Eve's information about the key is bounded to a negligible amount.

A simple schematic protocol diagram including all the steps and the channels involved up to the distilled key is shown in Figure 2.2.

State of the Art in CV-QKD

The foundational GG02 protocol [58] was crucial in demonstrating the feasibility of using Gaussian-modulated coherent states for secure key distribution. The first experimental implementation of Gaussian-modulated CV-QKD, achieved over

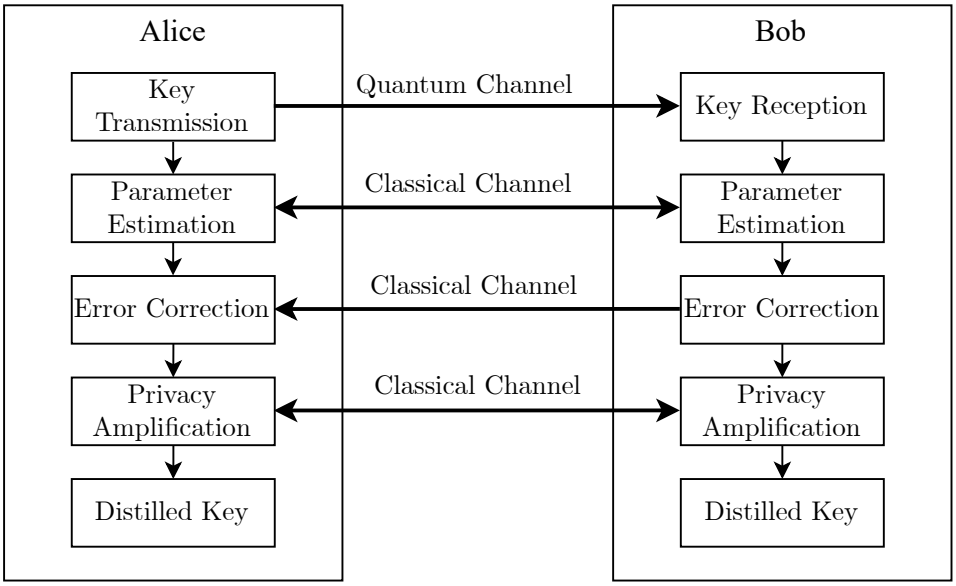

Figure 2.2: Diagram illustrating the CV-QKD protocol between Alice and Bob. The process involves key transmission over a quantum channel, followed by parameter estimation, error correction, and privacy amplification through classical channels, ultimately leading to the generation of a distilled key for secure communication.

a 25 km fiber [98], incorporated classical post-processing based on Low-Density Parity-Check (LDPC) codes for error correction. This milestone validated the viability of continuous-variable protocols under real-world conditions and laid the groundwork for subsequent advancements.

Modulation schemes are a crucial aspect of the development of CV-QKD protocols. While Gaussian modulation is easier for security analysis, its implementation over long distances is challenging due to its high noise sensitivity. To address these limitations, non-Gaussian modulation schemes that offer improved security and performance have also been explored. Discrete modulations, such as Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM), have been theoretically validated in the asymptotic limit [52, 38].

These schemes align closely with classical communication systems, simplifying integration. Among all the experimental advances using discrete modulation schemes for CV-QKD, one can highlight the experimental demonstration achieving a secret key rate of 21 Mb/s over a 25 km fiber using QAM modulation [161], the experiment employing Gaussian-like discrete modulation scheme with nearly 10 Mb/s over a 25 km fiber [135], or the successful implementation of QAM modulation over a 50 km fiber, highlighting the potential for high-rate secure communication [117].

A significant development in key reconciliation protocols is reverse reconciliation, which addresses the 3 dB loss limit issue. In traditional direct reconciliation, Bob attempts to infer Alice's data, which becomes problematic when channel losses exceed 50 %. Reverse reconciliation, however, allows Alice to infer Bob's data, thereby circumventing the loss limit and enhancing security [145]. Effective error correction and reconciliation are crucial for achieving high key rates, especially in high-loss or low signal-to-noise ratio (SNR) environments. Multi-edge-type (MET) LDPC codes have emerged as some of the most efficient solutions for error correction in continuous-variable systems [77, 169]. These codes enable robust error correction in challenging transmission conditions, thus extending the feasible range for secure communication.

Achieving longer distances and higher key rates remains a primary goal within the field. Recently, there has been remarkable progress, with several groundbreaking experimental implementations. Notably, the experimental transmission over a 100 km ultralow-loss fiber, achieving a distilled secret key rate of 25 kb/s using a true Local Oscillator setup with a Machine Learning-based carrier recovery algorithm to mitigate phase noise and laser fluctuations [60] stands out. It's important to note that this implementation also uses the same detection framework used in our implementations, known as low-complexity heterodyne detection, which has been a popular framework in the last years for implementing CV-QKD [61]. Another significant experiment estimated a secret key rate of 0.62 Mb/s over a 100 km fiber using a software-based frequency-locking technique with heterodyne detection [121]. The current distance record for CV-QKD is 202 km, achieving a 6 b/s key rate over a 32 dB loss ultralow-noise fiber channel [182].

Integrated photonics offers a promising pathway for scaling CV-QKD systems. Recent advancements include the demonstration of secure transmission using integrated tunable lasers, achieving a key rate of 0.75 Mb/s over a 50 km fiber [91]. Additionally, another experimental demonstration integrated all optical components except for the tunable lasers, achieving a key rate of 0.14 kb/s over a 100 km fiber [181]. These developments highlight the potential for compact and scalable solutions that align with existing telecommunications infrastructure.

Free-space implementations have also become viable solutions for secure communication in urban and remote areas. Notable achievements in this domain include atmospheric CV-QKD over 1.6 km horizontal links in urban environments using Gaussian-modulated coherent states [62] and squeezed states [120]. These experiments demonstrate the feasibility of secure communication under various environmental conditions, including adverse weather [160] and daylight [164].

Recent advancements in experimental demonstrations with squeezed states have

further expanded the field. For example, a 40 km fiber transmission using squeezed light with a LLO setup was successfully demonstrated [153].

Despite the significant progress, several challenges persisted unresolved for many years [40]. One critical issue was the finite-size effect in parameter estimation, which can lead to reduced secret key rates for small block sizes. This effect needs careful consideration in practical implementations. However, composable security through block-wise key generation has been theoretically validated [85], supported by simulations [109], and demonstrated experimentally [74].

2.3 Security Analysis of Gaussian CV-QKD

This section gathers information from various theoretical sources that address security analysis in CV-QKD. Many of the sources cited in this section are themselves reviews or compilations of the original works on CV-QKD security. Notably, the security analysis of CV-QKD by A. Leverrier [84] stands out, bringing to this field the security analysis previously proposed by R. Renner [131] for discrete variable protocols.

In Continuous Variable Quantum Key Distribution (CV-QKD), attacks by an adversary (Eve) are classified into individual and collective attacks, each with distinct strategies and capabilities. In individual attacks, Eve interacts independently with each quantum state sent from Alice to Bob, treating each state separately without considering information from other states. This type of attack limits the information Eve can obtain since each state is measured individually after the interaction. Although individual attacks are easier to analyze and defend against, as they do not exploit correlations between states, they provide an initial basis for evaluating the security of CV-QKD protocols.

On the other hand, in collective attacks, Eve also interacts individually with each state, but instead of measuring them immediately, she stores them in a quantum memory for later joint processing. This allows Eve to correlate information obtained from different states and optimize her measurements using the information revealed during the classical communication between Alice and Bob. Collective attacks are more powerful and harder to defend against, as they leverage state correlations to extract more information [57, 112]. Therefore, CV-QKD protocols must demonstrate security against these more advanced attacks to be considered robust and reliable.

Finally, general or coherent attacks are the most powerful eavesdropping strategy. In this approach, Eve interacts with multiple states simultaneously and performs a joint quantum measurement on all the intercepted states. This allows Eve to

maximize the information she can extract from the communication channel by leveraging the full quantum correlations and entanglement between the pulses. Coherent attacks are the most challenging to defend against and represent the ultimate test for the security of a CV-QKD protocol, as they take into account the most sophisticated analysis an eavesdropper can perform. Regarding this, it was proven by R. Renner and J.I. Cirac, using the de Finetti theorem, that using Gaussian modulation, collective attacks are the more general form of attack in the asymptotic limit [130]. Later, this was generalized to the finite-size regime by A. Leverrier *et al*, proving the security of Gaussian CV-QKD against arbitrary attacks [87]. For arbitrary modulation and detection, security against general attacks in the asymptotic regime was proven [38], but that proof in the finite-size regime is still an open task.

2.3.1 Mutual Information and Holevo Bound

In CV-QKD, two primary protocol descriptions are often employed: the prepare-and-measure (PM) scheme, which is the scheme employed in the original GG02 protocol [58], and the entanglement-based (EB) scheme, which was presented right after that [56] as an alternative scheme for analyzing the security of CV-QKD.

In the PM scheme, Alice prepares a quantum state, typically a coherent or squeezed state, and sends it through a quantum channel to Bob, who then measures the received state using homodyne or heterodyne detection. In the EB scheme, a source located between the two parties generates entangled states, which are shared between Alice and Bob. Both parties measure their respective parts of the entangled state, and their measurement outcomes are correlated, allowing them to establish a shared key.

It's important to note that these two schemes are fundamentally equivalent under certain conditions. Specifically, this equivalence holds when Alice's states in the PM scheme are Gaussian-modulated coherent or squeezed states, and Bob uses homodyne or heterodyne detection. Additionally, the equivalence is robust when reverse reconciliation is employed. This equivalence allows the more rigorous and well-established security arguments from the EB approach to be used to prove the security of the PM protocol, providing a strong foundation for secure quantum communication in CV-QKD.

In this subsection, the security analysis presented in [50] for the EB scheme, which proves the security of the PM scheme used in the experimental implementations, is depicted step by step, showcasing the principal results.

In the prepare-and-measure framework, for each state transmitted through the channel, Alice randomly selects values for the in-phase quadrature q_A and the

orthogonal quadrature p_A from two independent zero-mean Gaussian distributions. She then generates a coherent state centered at (q_A, p_A) and sends it to Bob via the quantum channel. This channel has a transmittance T and an excess noise ξ. The total noise introduced by the channel in shot noise units is defined as

$$\chi_{\text{ch}} = \frac{1}{T} - 1 + \xi, \tag{2.59}$$

which is derived from the equation $T(\chi_{\text{ch}} + 1) = 1 + T\xi$, equating the noise at the channel output (comprising shot noise and channel noise, attenuated by transmittance) with the noise at the receiver input (shot noise and excess noise ξ scaled by the channel losses T).

Upon receiving the coherent state, Bob measures either one of the quadratures randomly (homodyne detection) or both quadratures simultaneously (heterodyne detection). A detector's efficiency η and electronic noise ν_{el} characterize it. Analogous to the channel, the noise at Bob's input is defined as

$$\chi_{\text{hom}} = \frac{(1-\eta) + \nu_{\text{el}}}{\eta}, \quad \chi_{\text{het}} = \frac{1 + (1-\eta) + 2\nu_{\text{el}}}{\eta}, \tag{2.60}$$

derived from summing the electronic noise and the noise due to the undetected part, $1 - \eta$. In the heterodyne detection case, an additional shot noise term is added because of an extra vacuum noise term from two detections. The total noise, combining channel and detector noise, is expressed as

$$\chi_{\text{tot}} = \chi_{\text{ch}} + \frac{\chi_{\text{hom}}}{T}, \quad \chi_{\text{tot}} = \chi_{\text{ch}} + \frac{\chi_{\text{het}}}{T}. \tag{2.61}$$

A more detailed review of the CV-QKD noise model analysis separating different noise sources can be found in [81], although such a level of detail in noise components is not taken into account during this work.

In the entanglement-based setup, which is depicted in Figure 2.3, Alice's preparation of a coherent state is modeled by a heterodyne measurement on one half of a two-mode squeezed vacuum state (a quantum state where two separate modes or beams of light are entangled), commonly referred to as an Einstein-Podolsky-Rosen (EPR) state, with variance $V = V_A + 1$, while the other half is sent to Bob via the quantum channel.

Bob's detector inefficiency is modeled using a beam splitter with transmission η, and its electronic noise ν_{el} is modeled by an EPR state of variance v. The variance v is chosen such that the total detector noise equals $\eta\chi_{\text{hom}}$ or $\eta\chi_{\text{het}}$. For homodyne detection, we have

$$v = \frac{\eta\chi_{\text{hom}}}{1-\eta} = 1 + \frac{\nu_{\text{el}}}{1-\eta}, \tag{2.62}$$

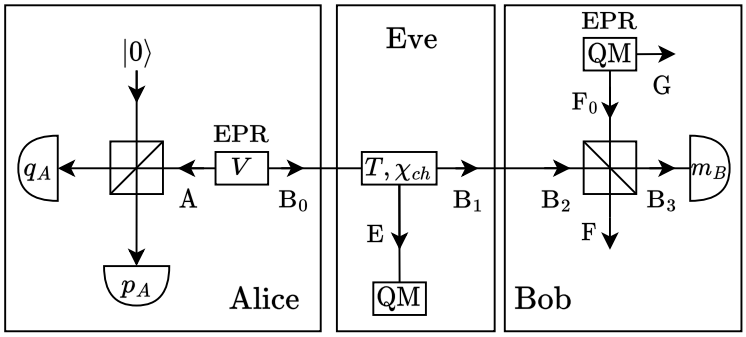

Figure 2.3: Schematic of an entanglement-based CV-QKD protocol. Alice generates an entangled two-mode squeezed vacuum (EPR) state, measures one mode using heterodyne detection to produce q_A and p_A, and sends the other mode, B_0, to Bob through a quantum channel characterized by transmission T and noise χ_{ch}. Eve may intercept the signal in the channel, measure the mode E, and send the mode B_1 to Bob. Bob receives the mode B_2, processes it using a beam splitter, and performs homodyne (or heterodyne) detection to measure m_B on the resulting mode B_3 to complete the protocol.

and for heterodyne detection,

$$v = \frac{\eta\chi_{\text{het}}}{1-\eta} = 1 + \frac{2\nu_{\text{el}}}{1-\eta}. \tag{2.63}$$

After the quantum transmission phase, Alice and Bob use classical data processing, including a reconciliation algorithm to extract a consistent bit string from their correlated continuous data and a privacy amplification process to derive a final secret key. Reconciliation is direct when Alice's data serve as a reference and reverse when Bob's data are the reference. Reverse reconciliation significantly benefits QKD system performance, so the calculations are performed for this scenario. Direct reconciliation expressions can be similarly derived [39].

The goal is to calculate the secret key generation rates for the Gaussian coherent-state CV-QKD protocol with homodyne and heterodyne detection, considering both individual and collective eavesdropping attacks, assumed to be Gaussian and optimal. In individual attacks, Eve interacts with each coherent state Alice sends, stores her ancillary states in a quantum memory, and measures them after sifting but before reconciliation. In collective attacks, Eve interacts with each state but waits until the entire classical procedure concludes before performing the optimal collective measurement on her stored ancillary states.

The maximum information Eve can obtain about Bob's key is bounded by the Holevo bound χ_{BE} for collective attacks [63]. The secret key information that Alice and Bob can distill is defined, for reverse reconciliation, as $K = I_{AB} - \chi_{BE}$

for collective attacks, where I_{AB} represents the information shared between Alice and Bob.

It is essential to note that the security of CV-QKD protocols against coherent attacks has been established. Coherent attacks enable Eve to collectively interact with all pulses sent by Alice and perform joint measurements on her ancillary states after the complete quantum and classical communication. Security proofs indicate that the bounds for the secret key generation rate in collective attacks remain asymptotically valid for arbitrary coherent attacks. Therefore, the results derived for collective attacks also ensure the unconditional security of the corresponding QKD systems against coherent attacks.

The mutual information between Alice and Bob is derived from Bob's measured variance $V_B = \eta T(V + \chi_{\text{tot}})/\mu$ and its conditional variance $V_{B|A} = \eta T(1 + \chi_{\text{tot}})/\mu$, where $\mu = 1$ for homodyne detection and $\mu = 2$ for heterodyne detection, using Shannon's equation:

$$I_{AB} = \frac{\mu}{2} \log_2 \frac{V_B}{V_{B|A}} = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}. \tag{2.64}$$

The Holevo quantity bounds the maximum information available to Eve about Bob's key:

$$\chi_{BE} = S(\rho_E) - \int p(m_B) S(\rho_E^{m_B}) \mathrm{d}m_B, \tag{2.65}$$

where m_B represents Bob's measurement, which could be $m_B = q_B$ for homodyne detection or $m_B = q_B, p_B$ for heterodyne detection. Also, $p(m_B)$ is the probability density of the measurement, $\rho_E^{m_B}$ is the eavesdropper's state conditional on Bob's measurement result, and $S(\rho)$ is the Von Neumann entropy of the state ρ.

Considering that Eve's system purifies the system AB_1 and Bob's measurement purifies the system AEFG, and noting that $S(\rho_{AFG}^{m_B})$ is independent of m_B for Gaussian modulation, χ_{BE} can be expressed as

$$\chi_{BE} = S(\rho_{AB_1}) - S(\rho_{AFG}^{m_B}). \tag{2.66}$$

Given that Gaussian attacks are optimal for collective attacks and assuming the states are prepared using Gaussian modulation, it is valid to consider that both ρ_{AB_1} and $\rho_{AFG}^{m_B}$ are Gaussian states [113]. Thus, with this assumption and using Equation (2.46), the entropy expression simplifies to

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{2.67}$$

where $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix Σ_{AB_1} characterizing the state ρ_{AB_1}, where $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrix $\Sigma_{AFG}^{m_B}$ characterizing the state $\rho_{AFG}^{m_B}$ after Bob's projective measurement, and where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

The covariance matrix Σ_{AB_1} depends only on Alice's system and the quantum channel, so the first part of Equation (2.67) is the same for both homodyne and heterodyne cases. The matrix is written as

$$\Sigma_{AB_1} = \begin{pmatrix} V \cdot \mathbb{I}_2 & \sqrt{T(V^2-1)} \cdot \sigma_z \\ \sqrt{T(V^2-1)} \cdot \sigma_z & T(V+\chi_{\text{ch}}) \cdot \mathbb{I}_2 \end{pmatrix}, \tag{2.68}$$

where $\mathbb{I}_2$ is the 2×2 identity matrix and σ_z is the third Pauli matrix:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.69}$$

The symplectic eigenvalues $\lambda_{1,2} \geq 1$ of the above matrix are given by

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{2.70}$$

where A and B are given by

$$A = V^2(1-2T) + 2T + T^2(V+\chi_{\text{ch}})^2, \quad B = T^2(V\chi_{\text{ch}}+1)^2. \tag{2.71}$$

To find the second part of Equation (2.67), we need the symplectic eigenvalues of the covariance matrix $\Sigma_{AFG}^{m_B}$, which can be written as

$$\Sigma_{AFG}^{m_B} = \Sigma_{AFG} - \Sigma_{AFGB_3}^T H \Sigma_{AFGB_3}, \tag{2.72}$$

where H is the matrix representing the homodyne or heterodyne measurement on mode B_3. For homodyne detection, $H_{\text{hom}} = (X\Sigma_{B_3}X)^{\text{MP}}$, where X is

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{2.73}$$

and MP stands for the Moore-Penrose pseudo-inverse of a matrix. For heterodyne detection, $H_{\text{het}} = (\Sigma_{B_3} + \mathbb{I}_2)^{-1}$. The matrices Σ_{B_3}, Σ_{AFG}, and Σ_{AFGB_3} can be derived from the decomposition of the covariance matrix given by

$$\Sigma_{AFGB_3} = \begin{pmatrix} \Sigma_{AFG} & \Sigma_{AFGB_3}^T \\ \Sigma_{AFGB_3} & \Sigma_{B_3} \end{pmatrix}. \tag{2.74}$$

This matrix can be derived with appropriate rearrangement from the matrix describing the system AB_3FG, as seen in Figure 2.3:

$$\Sigma_{AB_3FG} = Y^T(\Sigma_{AB_1} \oplus \Sigma_{F_0G})Y. \tag{2.75}$$

Here, Σ_{AB_1} is given in Equation (2.68), while Σ_{F_0G} describes the EPR state of variance v used to model the detector's electronic noise:

$$\Sigma_{F_0G} = \begin{pmatrix} v \cdot \mathbb{I}_2 & \sqrt{(v^2-1)} \cdot \sigma_z \\ \sqrt{(v^2-1)} \cdot \sigma_z & v \cdot \mathbb{I}_2 \end{pmatrix}, \tag{2.76}$$

where v takes the appropriate value for homodyne or heterodyne detection. Finally, the matrix Y represents the beam splitter transformation modeling the detector's inefficiency, acting on modes B_2 and F_0:

$$Y = \mathbb{I}_A \oplus Y_{B_2F_0} \oplus \mathbb{I}_G, \tag{2.77}$$

where

$$Y_{B_2F_0} = \begin{pmatrix} \sqrt{\eta} \cdot \mathbb{I}_2 & \sqrt{1-\eta} \cdot \mathbb{I}_2 \\ -\sqrt{1-\eta} \cdot \mathbb{I}_2 & \sqrt{\eta} \cdot \mathbb{I}_2 \end{pmatrix}. \tag{2.78}$$

With these elements, we can compute the symplectic eigenvalues $\lambda_{3,4,5}$. For both homodyne and heterodyne cases, $\lambda_{3,4} \geq 1$ are given by

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right], \tag{2.79}$$

where for the homodyne case, the values of C and D are given by the following expressions:

$$\begin{aligned} C_{\text{hom}} &= \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(V + \chi_{\text{ch}})}{T(V + \chi_{\text{tot}})}, \\ D_{\text{hom}} &= \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}, \end{aligned} \tag{2.80}$$

while in the case of heterodyne detection, they are given by two slightly longer expressions:

$$\begin{aligned} C_{\text{het}} &= \frac{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}(V\sqrt{B} + T(V + \chi_{\text{ch}})) + 2T(V^2 - 1)}{(T(V + \chi_{\text{tot}}))^2}, \\ D_{\text{het}} &= \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \end{aligned} \tag{2.81}$$

where A and B are as given in Equation (2.70). The last symplectic eigenvalue is $\lambda_5 = 1$ for both cases. Based on Equations (2.67), (2.70) and (2.79) to (2.81), we compute the Holevo information bound χ_{BE} and thereby determine the secret key rate,

$$K = I_{AB} - \chi_{BE}, \tag{2.82}$$

with χ_{BE} calculated by using the appropriate symplectic eigenvalues expression for homodyne or heterodyne detection.

2.3.2 Parameter Estimation

As seen in the previous section, to estimate the secret key rate K, the only requirements are knowledge of the modulation variance V_A, the efficiency η, the electronic noise ν_{el}, the channel transmittance T, and the excess noise ξ.

In practice, a random substring of the key is used for parameter estimation while the rest is kept for the key. If Alice sends a total of N symbols, Alice and Bob will share a string of N real or imaginary numbers, depending on whether Bob uses homodyne or heterodyne detection. In both cases, after Alice randomly chooses what m indices will be used for Parameter Estimation, they will share a string of length m for the parameter estimation symbols and a string of length $n = N - m$ for the key symbols. This procedure is shown in Figure 2.4.

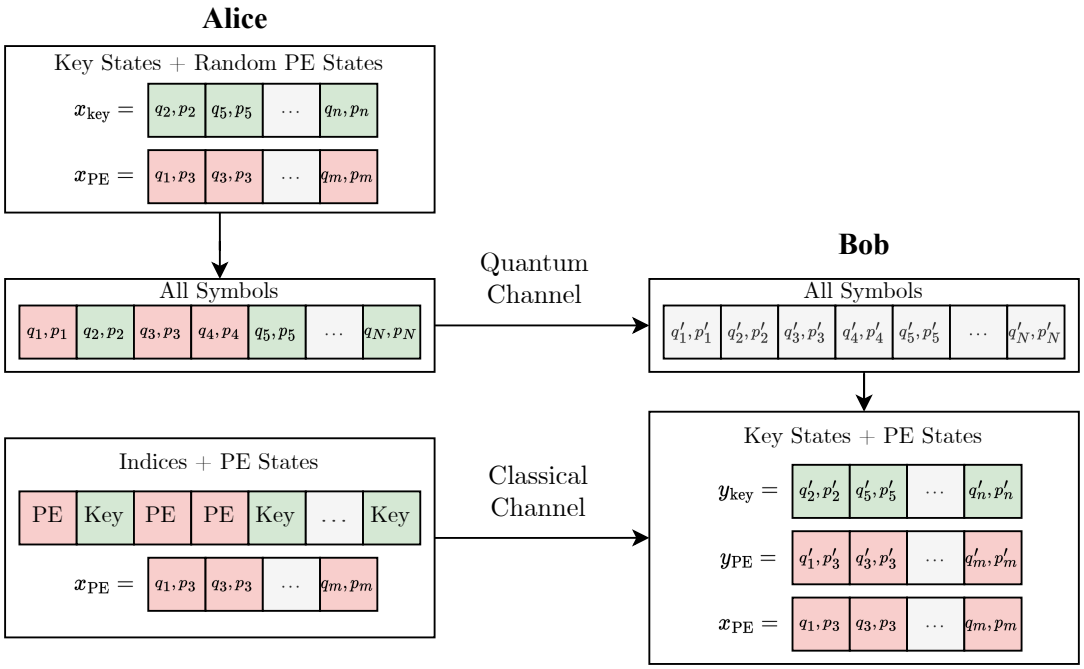

Figure 2.4: All steps of the Parameter Estimation symbol selection and public sharing. Alice randomly chooses which indices of the total raw key will be used for PE and for the key, and then she communicates both the indices and her values to Bob through a classical channel. Based on these values, Bob performs Parameter Estimation to estimate the secret key rate and discards the key if necessary.

Once they have the substring for parameter estimation, they proceed as follows. The variance V_A is known by Alice, who can measure it by measuring the output optical power for calculating the average photon number per pulse, as later shown in Equation (3.9). The detector efficiency is determined by performing an onsite calibration transmission and equating the variance of the measurement of N states

with the sum of the scaled modulation variance and the electronic noise [185],

$$\eta V_A + 1 + \nu_{\text{el}} = \frac{1}{\mu N} \sum_{k=1}^{\mu N} x_k, \tag{2.83}$$

from which η can be easily calculated, as the electronic noise is measured as described in Appendix A. Finally, the channel transmittance T and the excess noise ξ need to be statistically estimated. To correctly estimate these two parameters, the analysis of [170] is followed, starting from the maximum-likelihood estimators $\hat{t}$ and $\hat{\sigma}^2$ for the standard linear model [89, 85]. Defining $t = \sqrt{\eta T}$ and $\sigma^2 = 1 + \eta T \xi + \nu_{\text{el}}$, the maximum-likelihood estimators for the transmittance and the excess noise are given by

$$\hat{t} = \frac{\sum_{i=1}^{\mu N} x_i y_i}{\sum_{i=1}^{\mu N} x_i^2}, \quad \hat{\sigma}^2 = \frac{1}{\mu N} \sum_{i=1}^{\mu N} \left(y_i - \hat{t} x_i\right)^2. \tag{2.84}$$

The random distributions of these MLEs are given by

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^{\mu N} x_i^2}\right), \quad \frac{N\hat{\sigma}^2}{\sigma^2} \sim \chi^2(\mu N - \mu), \tag{2.85}$$

where t and σ^2 are the actual parameter values, $\mathcal{N}$ is the normal distribution, and χ^2 is the chi-squared distribution. To ensure the system's security, a secret key rate is estimated with a probability of $1 - \varepsilon_{\text{PE}}$ when t is at its minimum and σ^2 is at its maximum, from their respective confidence intervals:

$$t_{min} = \hat{t} - \Delta t, \quad \sigma^2_{max} = \hat{\sigma}^2 + \Delta\sigma^2, \tag{2.86}$$

where the confidence intervals [78] are defined by

$$\Delta t = z_{\text{PE}} \sqrt{\frac{\hat{\sigma}^2}{\mu N V_A}}, \quad \Delta\sigma^2 = z_{\text{PE}} \frac{\hat{\sigma}^2 \sqrt{2}}{\sqrt{\mu N}}, \tag{2.87}$$

and where z_{PE} is such that $1 - \text{erf}(z_{\text{PE}}/\sqrt{2})/2 = \varepsilon_{\text{PE}}/2$, so

$$z_{\text{PE}} = \sqrt{2}\, \text{erf}^{-1}(2 - \varepsilon_{\text{PE}}), \tag{2.88}$$

and the error function $\text{erf}(x)$ is defined as

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2}\, \mathrm{d}t\,. \tag{2.89}$$

Once t_{min} and σ^2_{max} values are computed, we can deduce the parameters T^* and ξ^* known as the worst-case scenario transmittance and excess noise,

$$T^* = \frac{t^2_{min}}{\eta}, \quad \xi^* = \frac{\sigma^*_{max} - 1 - \nu_{\text{el}}}{\eta T^*}. \tag{2.90}$$

With these estimated parameters, we repeat all the calculations from the previous subsection for calculating the SKR, using these two worst-case estimation values to calculate it. Furthermore, the expression for the SKR can be generalized to account for the reconciliation efficiency β in the classical post-processing and the finite-size effects, giving the expression

$$K^* = \frac{n}{N}(\beta I_{AB} - \chi_{EB}), \tag{2.91}$$

where $n = N - m$ is the number of states sent for the key, and m is the number of states sent for parameter estimation. The procedure to evaluate I_{AB} and χ_{EB} follows the previous section but uses the estimators T^* and ξ^*. This way, we estimate the SKR in the finite-size regime, assuming a reconciliation efficiency β. This measure will determine whether the transmission can be secure after all the classical post-processing or if it might have been attacked.

Chapter 3

Design and Characterization

This chapter details the previous process leading up to the experimental transmissions described in the next chapter. This begins with the conceptual design of the experimental system to implement a CV-QKD protocol, specifically a protocol based on Gaussian-Modulated Coherent States (GMCS) with a locally generated local oscillator (LLO), using low-complexity heterodyne detection. Therefore, the chapter explains this implementation, emphasizing how coherent states are generated and detected in experimental setups and the common challenges encountered when using real devices with imperfections to conduct the experiments.

It continues with the characterization of all components selected to build the experimental system, studying their behavior, limitations, and imperfections to determine the optimal operating range for each device and minimize errors caused by experimental imperfections in the final implementation.

The chapter ends with the results of the first publication [1] related to this thesis, which involves the theoretical modeling of different experimental devices considering their imperfections and the detailed numerical simulation of coherent state transmissions and parameter estimation using these models to study the relationship between the impairments present in the experimental devices and the SKR losses. This allows for determining the maximum allowed impairments for each experimental device and enables studying the effects of potential corrections applied to them.

3.1 Design of the CV-QKD system

This section starts by detailing the process of generating coherent states in practice. It starts from the simple wave equation of the electric field of a laser and then shows

the mathematical models that describe the field's behavior in an electro-optic modulator. Then, it explains the process of optical power calibration to achieve coherent states at the quantum level. This content can be found in textbooks and lecture notes on coherent optical systems [134].

The section continues by explaining how coherent states are detected using balanced detectors and the different detection schemes that can be used for this purpose. Subsequently, the implementation chosen for the experiments is explained. Finally, the section concludes by reviewing potential challenges in creating and detecting coherent states within the experimental setup, which will be considered in the following sections on characterization and simulation.

3.1.1 Generation of Coherent States

For generating coherent states in real-life experiments, we start with the electric field of a light wave produced by a Continuous-Wave (CW) laser diode. Theoretically, these laser diodes emit a stable and continuous optical field with a well-defined amplitude E_A, frequency ω_A, and phase ϕ_A. The electric field of this laser can be represented as

$$E(t) = E_A e^{i(\omega_A t + \phi_A)}. \tag{3.1}$$

This light wave can be modulated by using a Mach-Zehnder electro-optic Modulator (MZM), described in Figure 3.1a, which consists of one beam splitter with a 1:1 splitting ratio, two branches made of electro-optic materials, such as LiNbO3, which changes the optical length by varying the refractive index of each path by applying different voltages to them, and finally another 1:1 beam splitter which combines both paths.

At the output of the first beam splitter, we have two electric fields in each branch:

$$E_1(t) = \frac{E_{\text{in}}(t)}{\sqrt{2}}, \quad E_2(t) = \frac{E_{\text{in}}(t)}{\sqrt{2}}. \tag{3.2}$$

Then, the phase shift applied to each field is proportional to the voltage applied to each branch:

$$\phi_1(t) = \pi \frac{V_1(t)}{V_\pi}, \quad \phi_2(t) = \pi \frac{V_2(t)}{V_\pi}, \tag{3.3}$$

where V_π is known as the half-wave voltage and represents the voltage required to produce a π phase shift. Then, after the second beam splitter, the output of the MZM is given by

$$E_{\text{out}}(t) = \frac{E_{\text{in}}(t)}{2} \left(e^{i\phi_1(t)} + e^{i\phi_2(t)} \right). \tag{3.4}$$

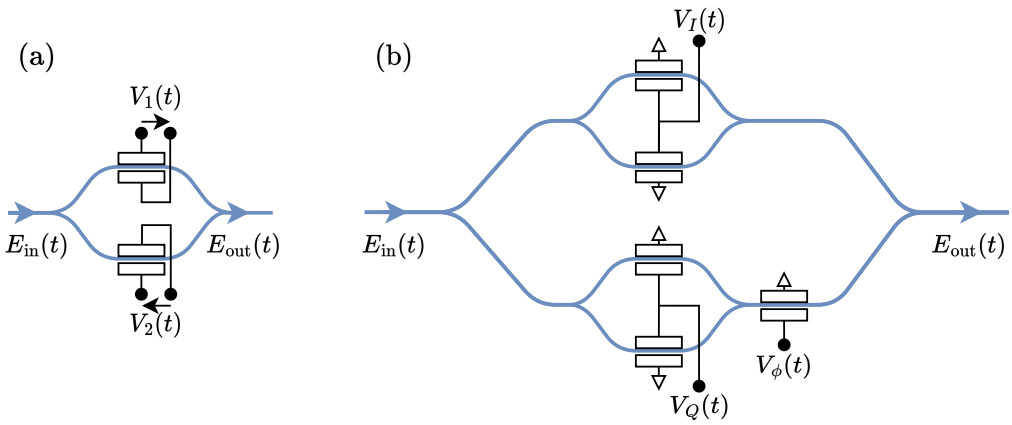

Figure 3.1: Representation of different electro-optic modulators. (a) shows a single Mach-Zehnder interferometer with variable phase modulators controlled by voltages $V_1(t)$ and $V_2(t)$ to modulate the output field $E_{\text{out}}(t)$. (b) shows a double-nested Mach-Zehnder interferometer or IQ modulator, where both amplitude and phase modulators, controlled by $V_I(t)$, $V_Q(t)$ and $V_\phi(t)$, are used for complex modulation of the output field $E_{\text{out}}(t)$, based on the input field $E_{\text{in}}(t)$.

In a particular case in which $V_1(t) = -V_2(t) = V(t)/2$ (known as Push-Pull operation), the output becomes

$$E_{\text{out}}(t) = E_{\text{in}}(t) \cos\left(\frac{V(t)}{2V_\pi}\pi\right). \tag{3.5}$$

This principle can be combined into a dual-nested MZM, known as IQ (In-Phase and Quadrature) optical modulator, as shown in Figure 3.1b, which gives out the following output by naming $V_I(t)$ to the $V(t)$ applied in the upper MZM, $V_Q(t)$ to the $V(t)$ applied to the lower MZM, and $V_\phi(t)$ to the $V(t)$ applied to the main MZM:

$$E_{\text{out}}(t) = \frac{E_{\text{in}}(t)}{2}\left[\cos\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right) + e^{i\pi\frac{V_\phi(t)}{V_\pi}}\cos\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right)\right]. \tag{3.6}$$

We can achieve a linear output by adding three bias voltages to each MZM. Also, we consider the main MZM to be only modulated by a constant bias voltage V_{b3} as we only need it to produce a $\pi/2$ phase shift. In this case, for any bias voltages added to the other two MZM voltages, we have

$$E_{\text{out}}(t) = \frac{E_{\text{in}}(t)}{2}\left[\cos\left(\frac{\pi}{2}\frac{(V_I(t)+V_{b1})}{V_\pi}\right) + e^{i\pi\frac{V_{b3}}{V_\pi}}\cos\left(\frac{\pi}{2}\frac{(V_Q(t)+V_{b2})}{V_\pi}\right)\right]. \tag{3.7}$$

Then we tune the bias voltages V_{b1}, V_{b2} and V_{b3} so that $V_{b1} = -V_\pi$, $V_{b2} = -V_\pi$ and $V_{b3} = V_\pi/2$, which is known as the minimum transmission operating point and is explained in Figure 3.2.

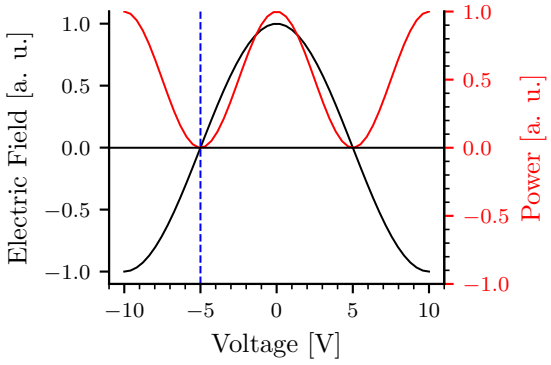

Figure 3.2: Transfer function of a Mach-Zehnder Modulator showing the relationship between the input voltage and the resulting electric field (black curve) and output power (red curve). The blue dashed line shows the voltage where the electric field is zero, corresponding to the modulator's half-wave voltage. When no modulating signal is applied, the input voltage corresponds to the bias voltage, and thus setting the bias voltage at $\pm V_\pi$ is called setting the modulator at the minimum transmission operating point, resulting in minimum output power when no modulation is applied.

Then, we finally have the transfer function for an IQ modulator operating at the minimum transmission operating point:

$$E_{\text{out}}(t) = \frac{E_{\text{in}}(t)}{2}\left[\sin\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right) + i\sin\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right)\right]. \tag{3.8}$$

Then, by varying $V_I(t)$ and $V_Q(t)$, we can directly modulate the real and imaginary parts of the laser light wave, achieving a complex modulation. We must apply small voltages to keep the relation between the applied voltages and the output electric field linear, and we must always satisfy $-V_\pi < V_I(t) < V_\pi$ and $-V_\pi < V_Q(t) < V_\pi$ to remain within the linear region as seen in Figure 3.2. With this method, we can modulate the amplitude and phase of a light wave, for example, by assigning values following a Gaussian distribution in the phase space, so when the amplitude is attenuated, we get pulses of coherent states.

For attenuating the light to the desired quantum level, we need to evaluate the power of the light at the output of the IQ modulator with any photodiode and apply a straightforward mathematical expression for estimating the number of photons per pulse [26],

$$\langle \hat{n} \rangle = \frac{P\lambda}{f_s hc}, \tag{3.9}$$

where P is the measured power of the light wave, λ is the wavelength of the light wave, f_s is the symbol frequency or pulse frequency, h is the Planck constant and c is the speed of light constant. Note that as hc/λ is just the energy of a single

photon, and P/f_s is the energy of each symbol or pulse of our light wave, $\langle\hat{n}\rangle$ is just the relation between them. Thus, by reading the power at the output of the IQ modulator, we can precisely calibrate the mean number of photons per pulse, which, as seen in Section 2.2.2, is directly related to the variance of the Gaussian modulation in coherent states.

This can be achieved by adding a beam splitter of 99:1 splitting ratio at the output of the IQ modulator to measure the 99 % output in an optical power meter while attenuating the signal until the required power is achieved by using a Variable Optical Attenuator (VOA). The 1 % output is then sent into the channel.

3.1.2 Detection of Coherent States

To measure coherent states in real experiments, the receiver must measure the amplitude and phase of each pulse. The optical signal must be converted into an electrical signal, so the frequency must be down-converted from the THz domain to the MHz domain. The received signal, which can be assumed to be just $E_{\text{out}}(t)$ from Equation (3.8) for this purpose, is mixed in a 2x2 1:1 beam splitter with another light wave of amplitude E_B, frequency ω_B and phase ϕ_B produced by another laser known as the local oscillator, which in this case is called the locally generated local oscillator (LLO). The result fields at each of the two outputs of the beam splitter are then given by

$$\begin{aligned} E_1(t) &= \frac{1}{\sqrt{2}}\left[E_{\text{out}}(t) + E_B e^{i(\omega_B t+\phi_B)}\right], \\ E_2(t) &= \frac{1}{\sqrt{2}}\left[E_{\text{out}}(t) - E_B e^{i(\omega_B t+\phi_B)}\right]. \end{aligned} \tag{3.10}$$

The two outputs are then measured in a balanced detector, which consists of two photodiodes that measure the optical power of light, each followed by a transimpedance gain amplifier and then an operational device that outputs the difference between both photodiode readings. The power measured by each photodiode is given by $P_i(t) \propto |E_i(t)|^2$, and thus the voltage at the output of the balanced detector is given by $V(t) = \rho(P_1(t) - P_2(t))$, where ρ is a constant that accounts for the area and sensitivity of the photodetectors as well as the gain of the amplifiers. From this point, as we are constantly measuring the balanced detector output, we can assume $P_i(t) = |E_i(t)|^2$ without loss of generality.

After calculating the expression for each optical power and after substituting Equation (3.10) with Equation (3.8), the voltage at the output of the balanced detector becomes

$$V(t) = \rho E_A E_B \left[\cos(\delta(t)) \sin\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right) - \sin(\delta(t)) \sin\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right)\right], \tag{3.11}$$

where $\delta(t) = \Delta\omega t + \Delta\phi$, where $\Delta\omega = \omega_A - \omega_B$ and where $\Delta\phi = \phi_A - \phi_B$. We can see that $V(t)$ depends on $\Delta\omega$, which should be in the MHz domain, instead of depending on ω_A or ω_B which are in the THz domain.

Let's now suppose that we achieve that $\Delta\omega = 0$ and $\Delta\phi = 0$, which is done by sending Alice's laser to Bob or by phase-locking Bob's laser to Alice's laser. In this case, Equation (3.11) becomes

$$V(t) = \rho E_A E_B \sin\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right), \tag{3.12}$$

so we can directly measure $V_I(t)$, which has the I-quadrature information modulated by Alice. On the other hand, if $\Delta\phi = \pi/2$ we'd have

$$V(t) = -\rho E_A E_B \sin\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right), \tag{3.13}$$

so by switching the phase difference between the local oscillator and the signal laser, Bob can measure either the I-quadrature value or the Q-quadrature value. This is called homodyne detection, and by measuring one of these two quadratures each time, they have to perform key sifting as in the BB84 protocol and discard all the non-measured pulses.

There is another approach to homodyne detection in CV-QKD known as heterodyne detection, in which Bob can measure both quadratures in all pulses, so they don't need to perform key sifting at all. This is done just by splitting the received signal and the local oscillator with two 1:1 beam splitters, phase-shift by 90° one of the outputs of the split LO, and then duplicating the 1:1 beam splitter and balanced detector setup of the homodyne detection method to measure both quadratures at the same time with different $\Delta\phi$ in each detector. This setup is later shown in Figure 3.5.

3.1.3 Chosen CV-QKD implementation

Among all possible implementations of CV-QKD [122], we can group them depending on what kind of quantum states are used for encoding information. Typically, coherent states are employed, which are quantum states with minimum noise uncertainty, symmetrically distributed in both quadratures. On the other hand, one could use squeezed states, where the noise is less than the vacuum noise in one of the two quadratures while greater in the other [54]. We choose the coherent states implementation as it is typically easier to implement in experimental setups, as we can use standard telecom lasers to generate coherent states. Then, regarding the modulation of the coherent states, there are mainly two groups of modulation schemes: Gaussian and Discrete modulation. Gaussian modulation involves

encoding information using continuous distributions, typically Gaussian, on the quadratures of quantum states [82]. As discussed in Section 2.2.2, this method is easier to implement due to its security analysis. Discrete modulation, on the other hand, uses a limited set of states [88]. While it may be experimentally simpler to implement, it usually offers lower secret key rates compared to Gaussian modulation [163] and requires a more complex security analysis. These different modulation schemes were shown in Figure 2.1.

Regarding the location of the local oscillator, there are two possible implementations of the coherent detector. The local oscillator could be generated by Alice and be sent alongside the signal through the channel or can be generated by Bob independently. The latter is typically known as the locally generated local oscillator (LLO). Figure 3.3 shows the experimental setup for the first implementation, where the local oscillator is sent from Alice to Bob through a separate optical channel. Note that we have not implemented this experimental setup in our system.

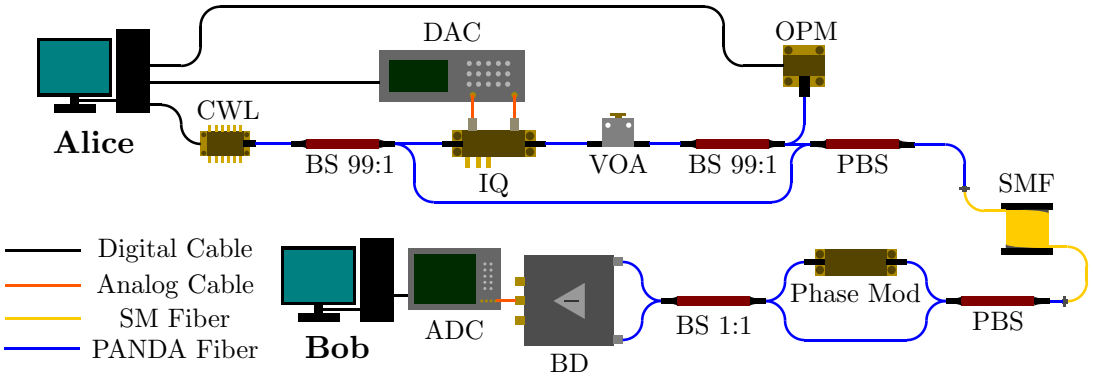

Figure 3.3: CV-QKD setup using the same laser for the quantum signal and the Local Oscillator and homodyne detection. The optical setup consists of a Continuous-Wave Laser (CWL), three Beam Splitters (BS) with different splitting ratios, two Polarized Beam Splitters (PBS) to combine the quantum signal and the LO in orthogonal polarization components, a Phase Modulator to perform homodyne detection, an IQ modulator, a Balanced Detector (BD), a Variable Optical Attenuator (VOA), and an Optical Power Meter (OPM). The electronics include a Digital-to-Analog Converter (DAC) and an Analog-to-Digital Converter (ADC). The entire system is controlled by two computers. Please note that the cable and fiber color code remains consistent throughout all the following figures.

The main advantage of this implementation is that there is no phase drift in the laser as both signal and Local Oscillator signals are ideally always in phase. Hence, the demodulation is perfect, and the symbol band can be as large as the detector bandwidth. The problem is that it has been proven that sending the Local Oscillator from Alice is not secure due to the wavelength attack [103, 68]. This attack allows an eavesdropper to alter the splitting ratio of Bob's beam splitter by changing the wavelength of Alice's laser in the channel. As a result, the attacker

can modify the proportion of the signal reaching Bob's detectors, affecting the measurement process and compromising the system's security. Another problem of this implementation is that Eve can simulate LO fluctuations to hide her Gaussian collective attack by reducing the intensity of the LO, and if Bob does not monitor the LO intensity and does not scale his measurements with the instantaneous intensity values of the LO, the secret key rate will be compromised severely [102].

The pilot tone was consequently introduced [127, 150] to be able to use an LLO implementation in a practical setup and solve this problem: Instead of transmitting the local oscillator directly from the transmitter, the approach involves sending a reference pulse (pilot tone) that is frequency-multiplexed with the quantum data signal. This reference tone has a much lower amplitude than the local oscillator. However, it is still greater than the quantum signal and is used by Bob to calibrate his laser's frequency and phase to match those of Alice's laser, thus enabling the demodulation of the quantum signal.

The pilot tone has been widely tested in experimental implementations, including discrete modulation implementations [80, 83] or gaussian modulation implementations [162] both with frequency-multiplexed pilots. Time-multiplexed techniques have also been used for calibration purposes since the first experimental demonstrations [78], and a time-multiplexed pilot tone used for placing the local oscillator at Bob's side was subsequently demonstrated [126, 167]. Also a polarization-multiplexed pilot has also been tested [166] and proved to be secure in transmissions over long distances.

Regarding our implementation, we chose to use a frequency-multiplexed pilot in order to use a locally generated local oscillator (LLO). The advantage of using a frequency-multiplexed pilot instead of a time-multiplexed pilot is that both the quantum signal and the reference signal travel simultaneously, allowing for real-time calibrations and corrections, and eliminating issues related to rapid fluctuations in the frequency or phase of the lasers. Therefore, the experimental setup we have chosen to implement the CV-QKD system is based on an LLO, with one laser located at Alice and another at Bob, as shown in Figure 3.4.

Finally, depending on the detector, Gaussian modulation-based CV-QKD is also typically classified in Homodyne and Heterodyne detection. Homodyne detection consists of measuring one of the quadratures of the quantum state using a local oscillator with a matching phase while discarding the non-matching phase measurements, similar to BB84's key sifting. Heterodyne detection simultaneously measures both quadratures by using two local oscillators with a 90° phase difference, which provides more information at the cost of additional 3 dB noise compared to homodyne detection due to the extra beam splitter [82].

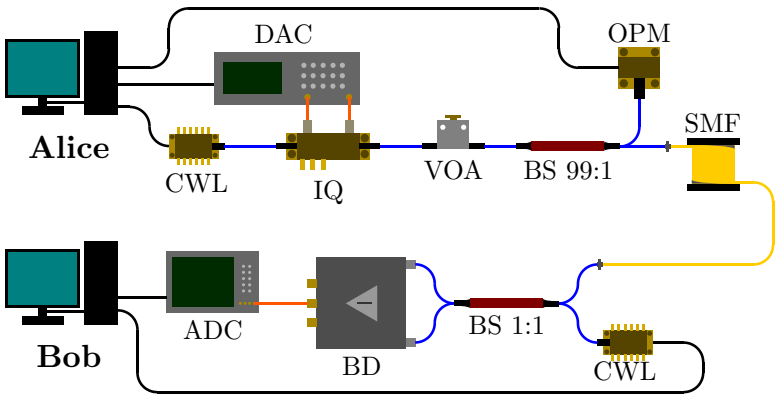

Figure 3.4: CV-QKD setup using separate lasers for the quantum signal and the local oscillator, referred to as the locally generated local oscillator (LLO) implementation.

There is another type of quadrature detection method called *low-complexity* heterodyne detection, which consists of displacing the symbol band to an intermediate frequency and then obtaining both quadratures at the same time by using only one balanced detector and digital signal processing techniques [26]. This may seem to violate the quantum uncertainty principle as the 3 dB extra loss of the additional beam splitter in the heterodyne detection is removed, and there is no key-sifting or symbols discarded, but when the signal is displaced to an intermediate frequency, the noise bandwidth is doubled so the noise level is also doubled, as in the heterodyne detection. These three detection schemes are compared in Figure 3.5.

It is important to clarify the equivalence in terminology used in optical communications and classical telecommunications domains. What is known as heterodyne detection in optical communications is referred to as dual homodyne detection or intradyne detection in classical telecommunications. On the other hand, the term heterodyne detection in classical telecommunications typically refers to what is called low-complexity heterodyne detection in the context of CV-QKD. This distinction helps align the terms used in both fields for a clearer understanding.

The three options are similar in noise levels and thus have the same potential to recover information, while the latter is possibly the simplest hardware implementation, sifting a great part of the process to software processing.

In practical setups, the phase drift on both lasers appearing when using an LLO implementation makes it very difficult to implement the homodyne or heterodyne detection schemes, as the signal can't be kept stable at any frequency, so it moves to an undesired intermediate frequency, increasing the phase noise, and making it much more convenient to implement the low-complexity option. For this reason, we chose the low-complexity heterodyne detection method to implement our coherent

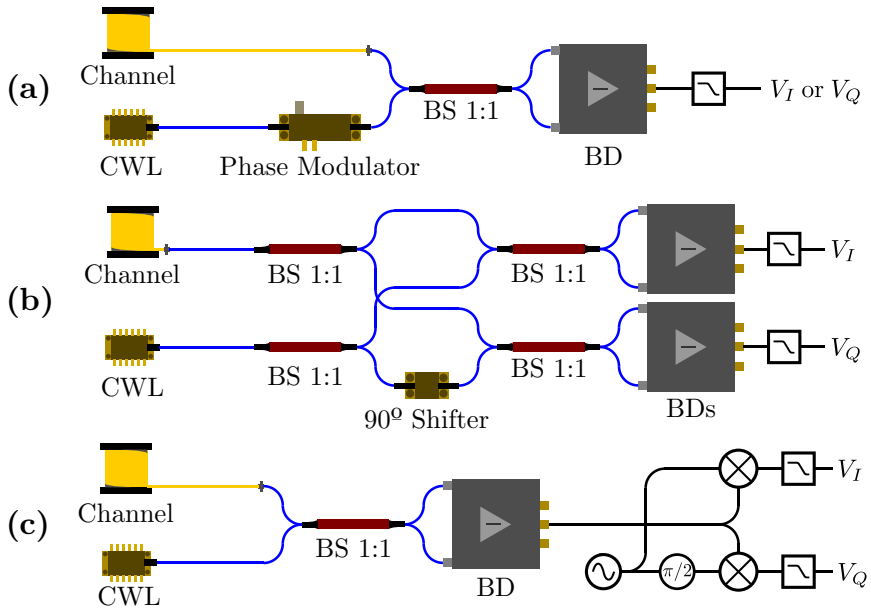

Figure 3.5: Schematics of different detection schemes: (a) homodyne detection with a phase modulator in the LO for switching quadratures, (b) heterodyne detection using a fixed $\pi/2$ phase shifter for simultaneous quadrature detection, and (c) low-complexity heterodyne detection without a phase modulator or shifter, capable of recovering both quadratures after signal acquisition using digital signal processing (DSP) techniques.

detection scheme.

3.1.4 Experimental Challenges

Due to imperfections in real experimental devices, the generation and detection of coherent states have many problems. Mitigating these effects or taking them into account in the security analysis is key to achieving a secure CV-QKD implementation.

Lasers fluctuate in phase, frequency, and even power when using real devices. These fluctuations are greater as long as the lasers are simpler and easier to acquire, for example, in telecom standard tunable C-Band lasers. This makes the detection of coherent states nearly impossible at first sight if using two separate lasers for Alice and Bob, as being unable to lock the frequency and phase difference of two lasers means that one can't measure either $V_I(t)$ or $V_Q(t)$ directly. To solve this, it's possible to use locking electronics or digital signal processing algorithms to remove the effect of the frequency and phase drifts. The fluctuations in power can also lead to errors in characterizing the Shot Noise Units, giving wrong security estimations, so fast power stabilization loops and a fast SNU estimation algorithm

must also be implemented to solve this issue.

The electro-optic modulator also presents many problems in real setups. First, the transfer function's non-linearity must be considered when performing the detection, as Bob is not directly measuring $V_I(t)$. This can be easily solved by filtering the signal. Another problem is that typically, V_π is not the same for all three Mach Zehnder Modulators. They are slightly different and drift over time, and this means that an electronic loop for locking the modulator to the minimum transmission operating point must be implemented in all of the three interferometers independently. This is solved with an electronic device that implements this loop, known as the Modulator Bias Controller. The difference in V_π also implies correctly scaling the amplitude of $V_I(t)$ and $V_Q(t)$ accordingly to compensate for the differences between different half-wave voltages.

There is also a problem due to both lasers having different polarizations. If Alice's laser have an arbitrary polarization $\vec{E_A} = (E_{Ax}, E_{Ay})$, and Bob's laser another polarization $\vec{E_B} = (E_{Bx}, E_{By})$, the outputs of Bob's beam splitter are given by

$$\begin{aligned} \vec{E_1} &= \frac{1}{\sqrt{2}} \begin{pmatrix} E_{Ax} + E_{Bx} \\ E_{Ay} + E_{By} \end{pmatrix}, \\ \vec{E_2} &= \frac{1}{\sqrt{2}} \begin{pmatrix} E_{Ax} - E_{Bx} \\ E_{Ay} - E_{By} \end{pmatrix}, \end{aligned} \tag{3.14}$$

and then we calculate the power of each field using $P = |E_x|^2 + |E_y|^2$, so we then calculate the voltage of the signal at the balanced detector output as $V(t) = \rho(P_1(t) - P_2(t))$, which after simplification is reduced to

$$V(t) = \rho(E_{Ax}E_{Bx}^* + E_{Ay}E_{By}^*). \tag{3.15}$$

In this equation, it's easy to see that if $\vec{E_A}$ and $\vec{E_B}$ have orthogonal polarizations, $V(t) = 0$, and on the other hand, if they have the same polarization, $V(t)$ will maximize. As we receive weak signals attenuated near to shot noise level, we must ensure that both polarizations are equal to maximize the detected signal. Otherwise we are unable to recover the pulses sent by Alice. This is accomplished using a polarization controller at Bob's input and polarization-maintaining fibers in the rest of the setup. An algorithm that maximizes the balanced detector amplitude reading should control the polarization controller.

Another common problem is the optical fiber backscattering [110], which consists of some of the power back-reflected into the fiber. This is important in the long-distance fibers used in the channel as if a small portion of the high-power local oscillator laser gets reflected into the channel due to imperfections in the beam

splitter or the detector it can be back-reflected into the beam splitter again, adding noise to the balanced detector output.

This problem is typically solved by adding optical isolators or circulators, which are devices that only let light with a specific direction pass through them. Although this may introduce some losses, these devices are required to prevent problems and even attacks.

3.2 Experimental Characterizations

One of the main goals of this work is to use commercially available optical and electronic components for the experimental setup, which is typical among CV-QKD implementations [34]. Thus, all the different off-the-shelf devices presented in this section are used to implement the experimental setup. The first characterized devices are the lasers, specifically, their frequency stability. Then, the IQ modulator is characterized, including the amplifiers and bias controller used with it, mainly focusing on the linearity and on the response of all the components to identify the best settings to use with them. The variable attenuator is then characterized to understand how it responds to voltage. And finally, all the detector is characterized, specifically, the saturation and linearity of both photodiodes in the balanced detector, and the polarization-dependent losses.

3.2.1 Lasers

For all experiments, from characterization to the CV-QKD transmission, we acquired two tunable lasers in frequency and power that operate in the C-band (191.5 to 196.25 THz) and are delivered with a PANDA (Polarization-maintaining AND Absorption-reducing) fiber output with FC/APC (Ferrule Connector / Angled Physical Contact) connectors.

Among the characteristics of the laser in the datasheet, it is worth noting that it has a linewidth of 10 kHz, a frequency range of 191.5 THz to 196.25 THz (equivalent to a wavelength range of 1527.6 nm to 1565.5 nm), a power range of 6 dBm to 13.5 dBm (equivalent to a range of 3.98 mW to 22.39 mW). The datasheet mentions a frequency setpoint resolution (not accuracy) of 1 MHz.

The laser connects via USB 2.0 to the computer and can be controlled directly through an RS-232 interface [48]. A CLI or GUI can also be used, but to integrate it with the rest of the components in the same software, we chose the RS-232 option, consisting of sending 4 B packets indicating a checksum to verify the integrity of the packet, the register (for example, the frequency or the power) to be modified, and the data to modify the register.

It is important to note that the laser has two operating modes (*dither* and *whisper* modes) that determine its frequency stability. The *dither* mode prioritizes long-term frequency stability, always keeping the 10 kHz band between an allowed frequency window despite having rapid frequency vibration, while the *whisper* mode prioritizes short-term frequency stability, causing the 10 kHz wide band to fluctuate much less over short periods of time, but drifting away slowly over time. This is the best choice for our purpose, as the narrow bandwidth of the detectors requires minimizing fast fluctuations to fit within the detector's range. Therefore, both lasers are always configured to operate in whisper mode.

Characterization of Frequency Stability.

For the rest of this work, characterizing the frequency stability of the lasers is strongly needed. To study the frequency stability of the two lasers separately, we would need a high-resolution and high-speed acquisition Optical Spectrum Analyzer (OSA) to analyze how a 10 kHz line fluctuates. This is not feasible with an OSA since there are no commercially-available OSAs with that resolution and speed because those with higher resolution tend to have a higher acquisition time. The solution to this is simply to study the beat signal of the two lasers, which is the signal at the output of an interferometer consisting of a beam splitter with two inputs and two outputs with a 1:1 splitting ratio. Subsequently, the two outputs of the interferometer are measured with a balanced detector. In this way, we can characterize the frequency difference between the two lasers, which drifts over time with sufficient resolution and speed, using a balanced detector instead of an OSA. The experimental setup for this characterization is shown in Figure 3.6.

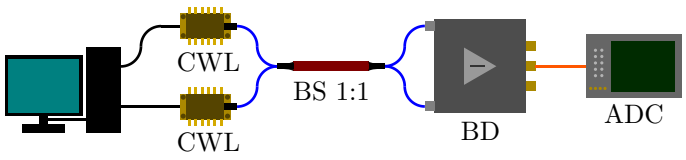

Figure 3.6: Experimental setup for characterizing the frequency drift of the beat signal between two lasers, using a balanced beam splitter and a balanced detector.

The electric field at the output of laser k is defined by

$$E_k(t) = \sqrt{P_k} e^{i(\omega_k t + \phi_k)}, \tag{3.16}$$

where P_k is the laser power, $\omega_k = 2\pi f_k$ its frequency, and ϕ_k its phase. If the fields of lasers A and B, i.e., $E_A(t)$ and $E_B(t)$, are at the two inputs of the 1:1 beam splitter, the electric fields at the two outputs of the beam splitter can be calculated as

$$E_1(t) = \frac{1}{\sqrt{2}}(E_A(t) + E_B(t)), \quad E_2(t) = \frac{1}{\sqrt{2}}(E_A(t) - E_B(t)). \tag{3.17}$$

These two electric fields hit the photodiodes of the balanced detector. Each photodiode measures the power of each field as a function of time, and since the power of an electric field can be calculated as $P(t) = |E(t)|^2$, the powers of the two fields $E_1(t)$ and $E_2(t)$ are given by

$$\begin{aligned} P_1(t) &= \frac{1}{2}\left(P_A + P_B + 2\sqrt{P_A P_B}\cos(\Delta\omega t + \Delta\phi)\right), \\ P_2(t) &= \frac{1}{2}\left(P_A + P_B - 2\sqrt{P_A P_B}\cos(\Delta\omega t + \Delta\phi)\right), \end{aligned} \tag{3.18}$$

where $\Delta\omega = \omega_A - \omega_B$ and $\Delta\phi = \phi_A - \phi_B$. The voltage output of the balanced detector is described by $V(t) = \rho(P_1(t) - P_2(t))$, with ρ being the detector's conversion factor in V/W, usually constant. Thus, the signal we measure on the oscilloscope is given by

$$V(t) = 2\rho\sqrt{P_A P_B}\cos(\Delta\omega t + \Delta\phi). \tag{3.19}$$

With this technique, although we cannot characterize the frequency stability of the two lasers separately, we can characterize the stability of the frequency difference between them, which is the only factor affecting coherent detection. In this way, we can measure $\Delta\omega$ with sufficient precision and speed using very simple hardware, since measuring $\Delta\omega$ (on the order of MHz) instead of ω_A or ω_B (on the order of THz), requires a considerably lower bandwidth, which can be resolved with simple optics and electronics, such as the balanced detector.

Results of Frequency Stability Characterization.

After building the previously described experimental setup, the first task is to measure the frequency difference Δf over time. To do this, we acquire a signal of an arbitrary but sufficient duration, which in our case is 10 ms, from the balanced detector while both lasers are activated. We then calculate the Fast Fourier Transform (FFT) of that signal, and once calculated, we search for the value where the FFT maximizes, which corresponds to the main frequency component of the signal, Δf. After repeating this for 3 min, we obtain the results of Figure 3.7.

It can be seen that the frequency difference fluctuates randomly around a value close to 250 MHz. We see that there are a fast deviation and a slow deviation. The fast one depends mainly on the laser working principle itself, mainly on the cavity mirrors vibrating inside the lasers, and the slow deviation depends mainly on much slower temperature fluctuations. These two deviations require us to implement two different frequency stabilization algorithms. There must be a slow active frequency stabilization algorithm which should vary the frequency of one laser until the signal enters the detection bandwidth of the balanced detector. Once

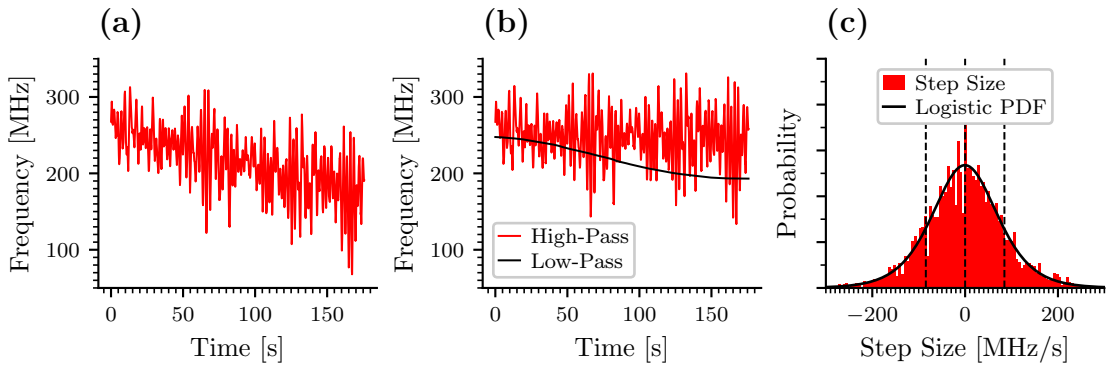

Figure 3.7: Measurements of the characterization of frequency drift between two lasers. (a) shows the evolution of the frequency of the beat signal $\Delta f(t)$ over time. (b) shows the same, but high-pass and low-pass filtered to isolate the fast and slow drift components, respectively. (c) shows the histogram of the random drift step sizes, calculated as the frequency difference between two subsequent points and normalized to one second. This histogram has been fitted to the probability density functions (PDF) of common random distributions, with the logistic distribution providing the closest fit to the experimental data, specifically a logistic distribution with mean zero and standard deviation near 80 MHz/s.

located, the frequency will fluctuate quickly and slowly, as shown in the red curve of Figure 3.7b. These fast and slow algorithms will be discussed in Section 4.1 and Section 4.2, respectively.

Note that in Figure 3.7c, the step sizes (frequency difference between two subsequent points) have been time-normalized by dividing them by the sample time, which in our case was 10 ms. This normalization for any step time would only be possible if the dependence between the magnitude of the frequency fluctuations and the step time were linear, which turns out to be the case, as shown in Figure 3.8.

As we can see, as long as the chosen step time is below 100 ms, the assumption of linearity will be correct, and we can work with normalized step size's standard deviations. In practice, we will always be below this time, as typical sampling times are smaller than 100 ms.

3.2.2 Transmitter Devices

Among the devices used in the transmitter, we employ a commercial IQ modulator, which is a 1550 nm high extinction ratio modulator, meaning it features CS-SSB (carrier and subcarrier suppressions), attenuating the optical carrier signal by 40 dB, leaving only the modulated signal.

According to the technical datasheet, it has a bandwidth of 25 GHz, and the half-

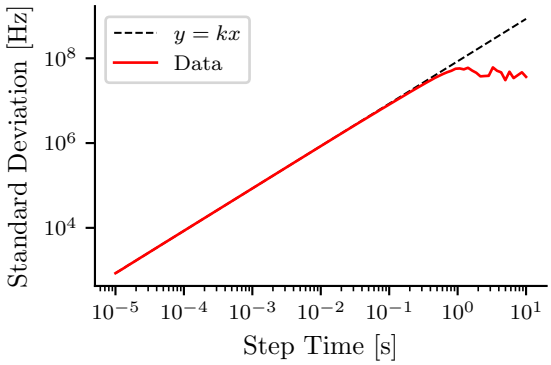

Figure 3.8: Linear relationship between frequency step sizes and step times. The standard deviation of the step sizes for different sampling or step times is compared, showing a linear relationship for step times below 100 ms.

wave voltages for the I and Q electrodes are around 6 V, while the half-wave voltage for the main electrode is around 9 V. The technology is based on a Lithium Niobate X-Cut Y-Prop crystal, with an insertion loss of 5 dB, and can handle signals up to 630 mW, far exceeding the laser power.

At each of the two RF inputs of the IQ modulator, we use an amplifier with a bandwidth of 10 GHz, a maximum output voltage of 15.9 V, and a gain of 27 dB. Additionally, the IQ modulator's operating point is controlled with a Modulator Bias Controller (MBC), a device that connects via USB to the computer and can operate in manual mode with three voltage outputs ranging from −12 V to 12 V, or in automatic mode, locking the modulator to the minimum transmission operating point.

Following the MBC, we use a variable optical attenuator which operates at 1550 nm and attenuates up to 50 dB by manually adjusting a screw. The output is divided into two paths with a 99:1 beam splitter, and the higher power output is measured with an optical power meter. To generate the analog modulating signals, we use a 12-bit resolution and 12 GSa/s arbitrary waveform generator (AWG).

The use of an amplifier at the IQ modulator inputs is necessary because if the half-wave voltage is around 6 V, the input signals should have an amplitude below this value but of the same order, and high-speed arbitrary generators, such as the AWG we use, typically do not have high voltage output signals. Specifically, our generator produces signals up to a maximum amplitude of 350 mV. Therefore, this signal must be amplified to cover the full voltage range of the IQ modulator.

After all these considerations, the experimental setup of Figure 3.4 is complemented with an MBC, an attenuator, a power meter, and a 99:1 beam splitter to

measure the power before the channel. The new setup is represented in Figure 3.9.

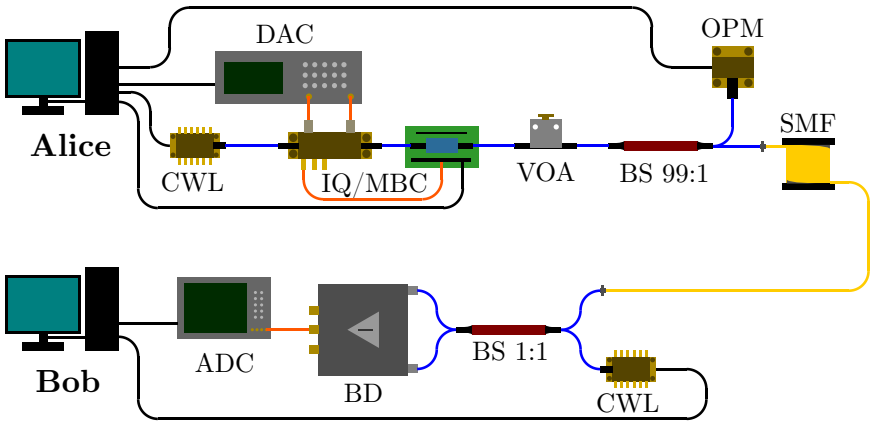

Figure 3.9: Experimental setup of the CV-QKD with LLO implementation including a Modulator Bias Controller (MBC) to lock the modulator to the minimum transmission operating point, a Variable Optical Attenuator (VOA), and an Optical Power Meter (OPM), both to calibrate the modulation variance, related with the output optical power.

IQ Modulator and Amplifier Characterization

We have characterized the response of the IQ modulator, the signal amplifiers connected to the IQ modulator, and the Modulator Bias Controller (MBC). The IQ modulator and the amplifiers have a range of input voltages where the output is linear and less distorted, and we must accurately characterize both components to know the voltage ranges the signal should be in. To characterize both components, we use the experimental setup shown in Figure 3.10.

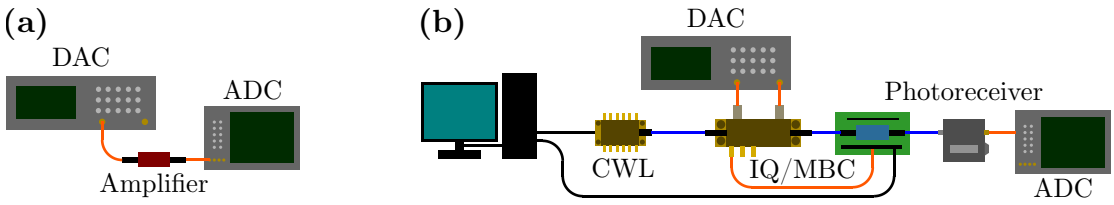

Figure 3.10: Setups for characterizing the response of the IQ modulator and its amplifiers. (a) shows the simple setup used to characterize the response of the amplifiers separately from the IQ modulator. Typically, both amplifiers are connected to both modulator inputs by default, so they are not shown as separate components in other figures. However, they can be separated to characterize each one individually. (b) shows the setup used to characterize the behavior of the IQ modulator, including the amplifiers, using a photodetector connected to the ADC to measure the power of the electric field.

Once this setup is done, we proceed to input sine signals to analyze the output of the amplifiers and the optical output of the IQ modulator combined with the

amplifiers. We aim to find the region where the relationship between input and output in both devices is as linear as possible while the signal is as undistorted as possible. To study the signal distortion, we use the Total Harmonic Distortion (THD) measure, defined as the ratio between the sum of the powers of all harmonics in the spectrum and the power of the fundamental harmonic. This ratio is typically expressed in dB.

The signal at the amplifier output, according to the setup in Figure 3.10a, will simply be the same input signal but multiplied by a certain gain. It should have the same frequency and shape. On the other hand, the signal measured by the photodetector (InGaAs detector with a 1.2 GHz bandwidth and 5.5 mW saturation power) in Figure 3.10b will be more complex than proportional to the input signal. We can analyze this in Equation (3.7), as the IQ modulator output for the case $V_I(t) = \sin(\omega t)$ and $V_Q(t) = \cos(\omega t)$, assuming the operating point is reached and that the three half-wave voltages are different, would result in an electric field at the IQ modulator output whose power is given by

$$P(t) = \frac{E_A^2}{8}\left[2 - \cos\left(\frac{\pi \sin(\omega t)}{2V_{\pi 1}}\right) - \cos\left(\frac{\pi \cos(\omega t)}{2V_{\pi 2}}\right)\right]. \tag{3.20}$$

We can see in Figure 3.11 that the measured power of the field at the IQ modulator output matches the simulation following Equation (3.20), when modulating with $V_I(t) = \sin(\omega t)$ and $V_Q(t) = \cos(\omega t)$, and setting $V_{\pi 1} = -V_{b1}$ and $V_{\pi 2} = -V_{b2}$, being V_{b1} and V_{b2} the bias voltages applied by the MBC when locked into the minimum transmission operating point. Once it is verified that the modulator response is as expected, we check the limits and the ideal amplitude range for working with the amplifiers, specifically with the amplifier and IQ modulator set.

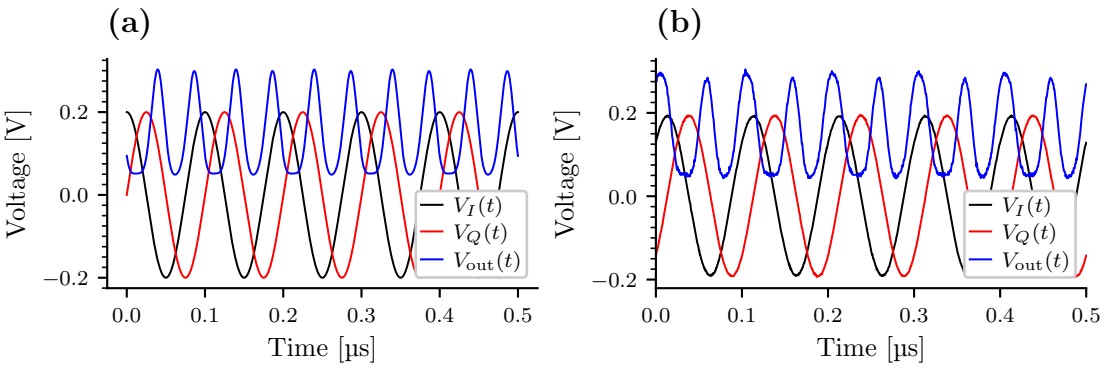

Figure 3.11: Response of the IQ modulator. (a) shows simulations of the IQ modulator response for two sinusoidal input signals based on Equation (3.20). (b) shows experimental data collected from the oscilloscope for the same input signals generated with the arbitrary waveform generator.

To achieve this, we measure both the amplitude and THD at the amplifier output,

as shown in Figure 3.10a, and the voltage (which is proportional to optical power) measured by the photodetector in Figure 3.10b for different input voltages. We generate two 90° shifted sine waves of varying amplitudes using the AWG, which are then sent to both amplifiers. In the first case, we measure the amplitude and THD of the signal at the output of one of the amplifiers. In the second case, we connect both amplifiers to the RF inputs of the IQ modulator again, and after reaching the locked operating point status in the bias controller, we measure the modulator's output with a photodetector, which provides a voltage output proportional to the measured power. The amplitude and THD of this photodetector output are then measured, and the results of both sets of measurements are presented in Figure 3.12.

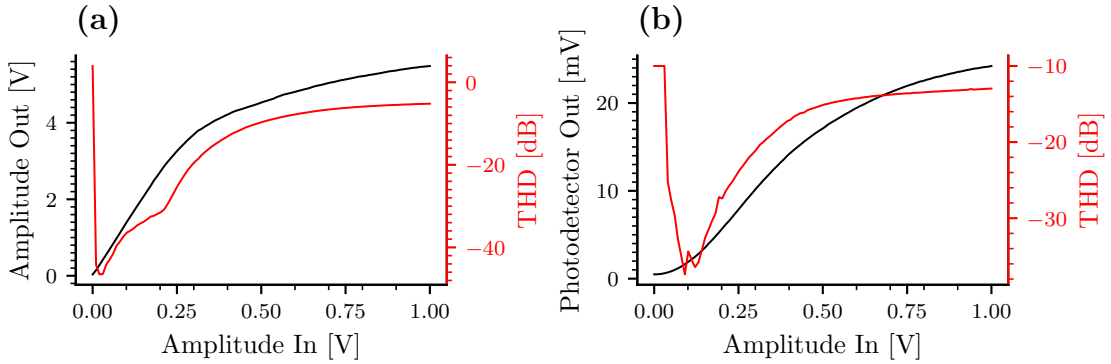

Figure 3.12: Characterization of the output response and Total Harmonic Distortion (THD) for different input amplitudes. (a) shows the output amplitude (black curve) and THD (red curve) of the amplifier as a function of the input amplitude. (b) shows the corresponding output amplitude and THD for the IQ modulator. The output amplitude is plotted on the left vertical axis, while the THD is shown on the right vertical axis in decibels (dB).

It can be observed that to maintain linearity in the amplifier, input signals should have an amplitude of less than 200 mV, while to maintain linearity at the IQ modulator output, input signals should have an amplitude from 200 mV to 400 mV. However, in both the amplifier and the modulator, it is recommended to input signals with an amplitude below 200 mV (ideally 100 mV) to minimize distortion, ensuring that the output signal has a high correlation with the input signal.

While our primary focus is on the second setup, which consists of the modulator, amplifiers, and MBC, characterizing the amplifier separately was also of interest. As observed from the similarities between Figure 3.12a and Figure 3.12b, we can assume that a great part of the behavior of the full modulator setup is influenced by the limitations of the amplifier.

Given that, we consider the optimal working range to be near an amplitude of 250 mV (500 mV peak-to-peak) for the input signal, as this is where non-linearity is

minimized. It is important to note that the remaining non-linearity and harmonic distortion could be further corrected through digital signal processing at Bob, although this has not been necessary for the present work.

MBC and Attenuator Characterization

As shown in the previous setup, when the signal exits the IQ modulator, it enters the MBC, where it is split with a 99:1 beam splitter. The 1 % power output is measured to adjust the bias voltages to set the modulator at the minimum transmission operating point. Subsequently, after exiting the MBC, the variable attenuator attenuates the signal to reach the desired power equivalent to a specific number of photons per pulse. To characterize the response of the MBC, we use the same setup of Figure 3.12b. For the variable attenuator, we replace the manual VOA with an electronic one, which operates at 1550 nm and attenuates up to 25 dB using voltages from 0 V to 5 V. To characterize its response, we use the setup shown in Figure 3.13.

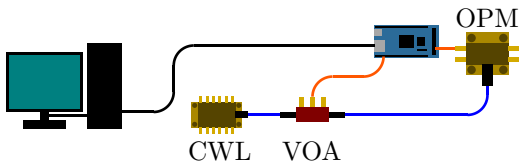

Figure 3.13: Setup for characterizing the attenuation response of the electronic Variable Optical Attenuator (VOA) to the input voltage.

The MBC implements a control algorithm to minimize the output power when no modulation signal is applied (minimum transmission operating point), ensuring that when $V_I(t) = 0$ and $V_Q(t) = 0$, the output power is zero. When $V_I(t) \neq 0$ and $V_Q(t) \neq 0$, the electric field at the output is as linear as possible (although the power is not), as shown in Figure 3.2. The response of varying each of the three bias voltages while leaving the two other voltages at the operating point value can be seen in Figure 3.14a, and the transfer function of the electronic variable attenuator can be seen in Figure 3.14b.

From Figure 3.14a, we can obtain the real values of each half-wave voltage, $V_{\pi 1}$, $V_{\pi 2}$, and $V_{\pi 3}$, which are 5.45 V, 5.65 V and 6.76 V, and we can see that they are different, which means there will be a slight imperfection compared to the ideal model in Section 3.1.1. This will be studied further in the simulations of Section 3.3.

3.2.3 Receiver Devices

Among the receiver devices, there are a polarization controller, a beam splitter, and a balanced detector. The balanced detector has a bandwidth from DC to 400 MHz,

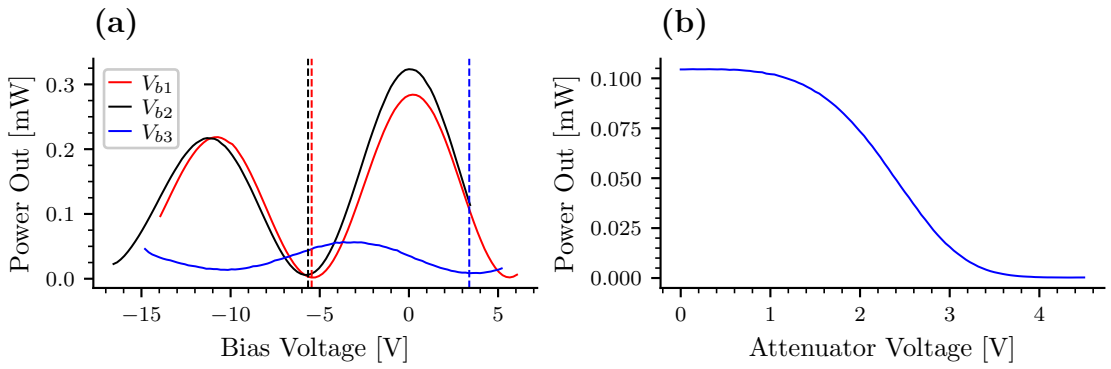

Figure 3.14: Characterization measurements of the MBC and the attenuator. (a) shows the output power of the IQ modulator while manually varying one bias voltage, with the other two biases automatically maintained at their minimum transmission operating point. The minimum power points correspond to these operating points. (b) shows the optical power at the output of the electronic VOA when using a 0.1 mW input for different voltages.

a sensitivity of 5 V/mW or 10 V/mW, and a sufficiently low noise value, characterized by the NEP (Noise Equivalent Power), which in this case is $5\,\mathrm{pW}/\sqrt{\mathrm{Hz}}$. The output of the balanced detector is digitalized in a 2 GHz bandwidth oscilloscope.

The beam splitter used is a 2x2 coupler with a splitting ratio of 1:1 for 1550 nm with PANDA-type polarization-maintaining fibers, and according to the datasheet, it has a tolerance of 1.5 % in the splitting ratio.

The polarization controller is composed of a development board equipped with high-voltage drivers, which interact with the controller's piezoelectrics to modify the polarization of the light by applying pressure to the SM fiber along different axes. Moreover, we also tested a manual 3-paddle polarization controller, which adjusts the polarization in the SM fiber by using stress-induced birefringence. This manual method provides a simple and effective alternative for controlling polarization without additional electronic components.

By incorporating the polarization controller into the experimental setup, we finally arrive at the most fundamental experimental setup, which is capable of achieving CV-QKD transmissions. This setup includes all the essential components necessary for transmitting and receiving modulated light, ensuring a complete basic implementation. The configuration, which represents the minimal hardware requirements, is depicted in Figure 3.15.

After presenting the experimental setup for the receiver side, the characterization procedure for these three devices (the beam splitter, the balanced detector, and the polarization controller) is described in detail.

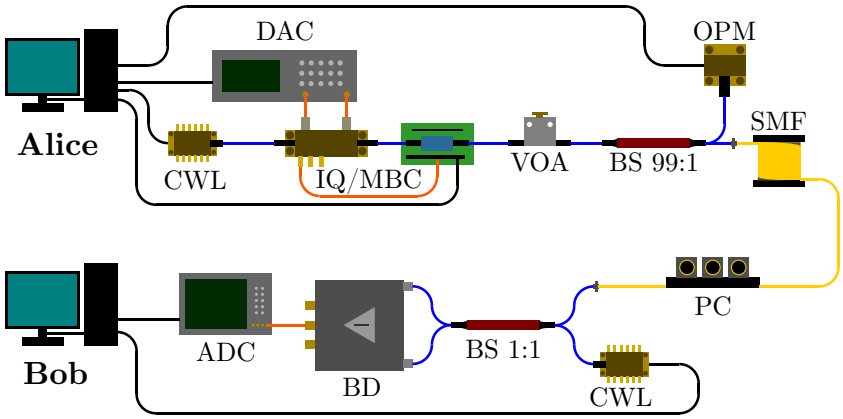

Figure 3.15: Experimental setup of the CV-QKD with LLO implementation including a Polarization Controller (PC) to align the polarization of the incoming quantum signal to the local oscillator. This setup includes all the minimum necessary components to perform a CV-QKD transmission

Beam Splitter

To characterize the beam splitter, we introduce a laser beam of power P_{in} through input 1 and measure the power at outputs 1 and 2, P_1 and P_2. Then, we introduce the same beam of power P_{in} through input 2 and measure the power at outputs 1 and 2, P_1' and P_2'. In this way, we can characterize the reflectance and transmittance indices as

$$|r_1|^2 = \frac{P_1}{P_{\text{in}}}, \quad |t_1|^2 = \frac{P_2}{P_{\text{in}}}, \quad |r_2|^2 = \frac{P_2'}{P_{\text{in}}}, \quad |t_2|^2 = \frac{P_1'}{P_{\text{in}}}, \tag{3.21}$$

After performing these measurements by calibrating the input power P_{in} and measuring the four different output powers, we obtained $|r_1|^2 = 0.4948$, $|r_2|^2 = 0.4983$, $|t_1|^2 = 0.5052$, and $|t_2|^2 = 0.5017$, which falls within the tolerance margins specified by the manufacturer, as we found deviations between 0.3 % and 1 %.

Balanced Detector

To characterize the balanced detector, the approach is to characterize its two photodetectors separately. For this, we generate an optical signal with a laser and modulate it with the IQ modulator, with signals $V_I(t) = \cos(\omega t)$ and $V_Q(t) = \sin(\omega t)$, using a frequency $\omega = 2\pi f$, with $f = 10\,\text{MHz}$. Then, this modulated signal passes through a variable attenuator, and the output of the attenuator is split with a 1x2 beam splitter with a coupling ratio of 1:1 so that one output is measured with a power meter and the other goes directly to the balanced detector. The characterization setup is shown in Figure 3.16.

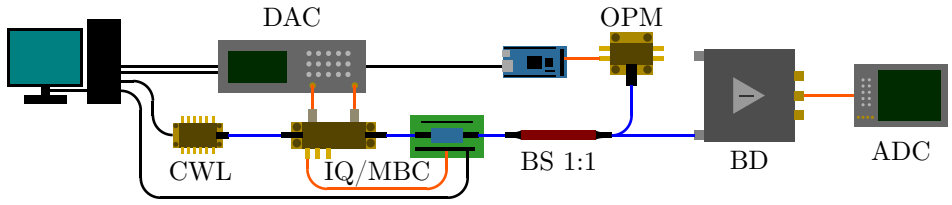

Figure 3.16: Setup for characterizing the two photodiodes of the balanced detector, consisting of a laser and the IQ modulator, to generate optical signals of different powers, which are then measured in each photodiode while the optical power is monitored.

The results of these measurements are shown in Figure 3.17, where it can be concluded that balanced detector output saturates above 400 µW (as stated in the datasheet) but it becomes to be distorted above 250 µW, as this is where the amplitude does not increase linearly with power. It can also be concluded that the gain is very similar in the two photodetectors, as the difference in signal offsets is practically zero for any input power.

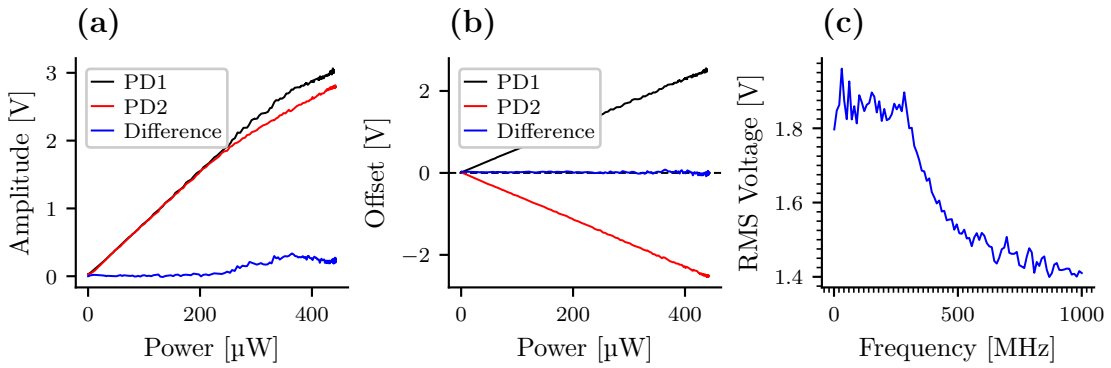

Figure 3.17: Measurements from the characterization of the balanced detector. (a) shows the amplitude of a detected sinusoidal signal as a function of input power for the two photodiodes and their difference. (b) shows the offset or mean voltage of the detected sinusoidal signal as a function of input power for the two photodiodes and their difference. (c) shows the RMS voltage of the detected sinusoidal signal for different input signal frequencies, showing its frequency response, which lets us estimate the bandwidth of the detector.

On the other hand, in Figure 3.17c, we see that the bandwidth is close to 400 MHz as stated in the datasheet, as this is the frequency where the input amplitude is attenuated by −3 dB.

It is important to note that, in addition to the balanced detector used in the experimental design, two other balanced detectors were tested and subsequently discarded. These models had interesting features such as AC coupling, which allows for high-pass filtering of the detected signal to eliminate the undesired DC component produced by different detector gains, or a potentiometer for offset com-

pensation, which allowed fine-tuning of the gain of each photodetector to eliminate any impairments. However, despite these features, after transmitting a block of Gaussian symbols for subsequent detection, it was found that both detectors resulted in a lower correlation between transmitted and received symbols, as shown in Table 3.1.

Detector	Bandwidth (MHz)	NEP ($pW/\sqrt{Hz}$)	Correlation (%)
Detector 1	400	5	91.8
Detector 2	200	8.7	88.9
Detector 3	400	2.5	84.6

Table 3.1: Results for the comparisons of the three balanced detectors tested. The correlation measurements were performed after transmitting 10^6 Gaussian symbols and subsequently demodulating them using the methods described in Section 3.3 and Section 4.1. The bandwidth and NEP values were taken from the technical datasheet of each device.

As can be seen, according to the technical datasheet of the different detectors, the third detector has the lowest NEP and would seem to be the best option, while the second detector, having the lowest bandwidth and the highest noise, seems to be the worst option. However, in a real setup applied to our specific implementation, the first detector shows a higher correlation between sent and received symbols, which is ultimately what we are most concerned with for conducting CV-QKD experiments. Therefore, we decided to discard the other two detectors.

Polarization Controller

In this case, to study how differences in polarization in the two fields interfering in the beam splitter affect the amplitude measured in the balanced detector, we use the setup proposed in Figure 3.18.

We use two polarimeters to measure the power, azimuth, and ellipticity of infrared light in the 900 nm to 1700 nm range. These polarimeters have a power range from 1 µW to 10 mW and a sampling speed of 30 Sa/s, with an accuracy of 0.25° in both azimuth and ellipticity. To take measurements, we constantly monitor the azimuth and ellipticity on the two polarimeters and the amplitude at the output of the balanced detector for 10 min while randomly varying the polarization of one of the paths using a polarization controller to represent how the amplitude depends on these two variables. This is shown in Figure 3.19.

The ellipticity and azimuth of the path without the polarization controller hardly change over the 10 min of the experiment since we are using a PANDA fiber both in the laser and in the beam splitter. The path with the polarization controller

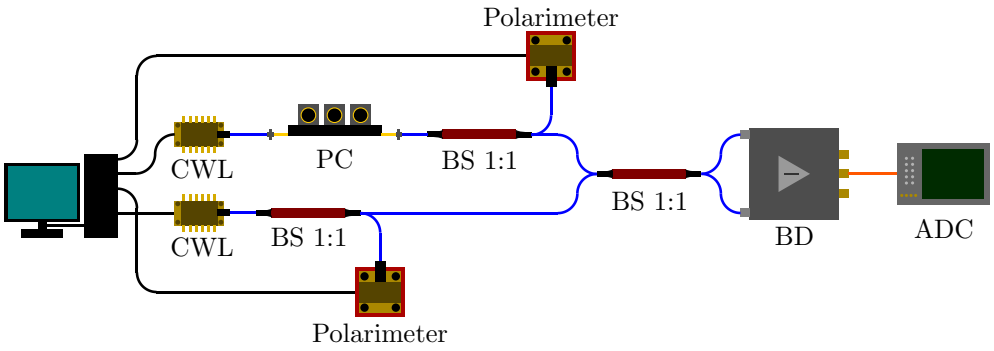

Figure 3.18: Setup for characterizing the impact of polarization on detector efficiency by interfering two signals. The polarization of both signals is monitored using two polarimeters, while the polarization of one signal is varied using a polarization controller.

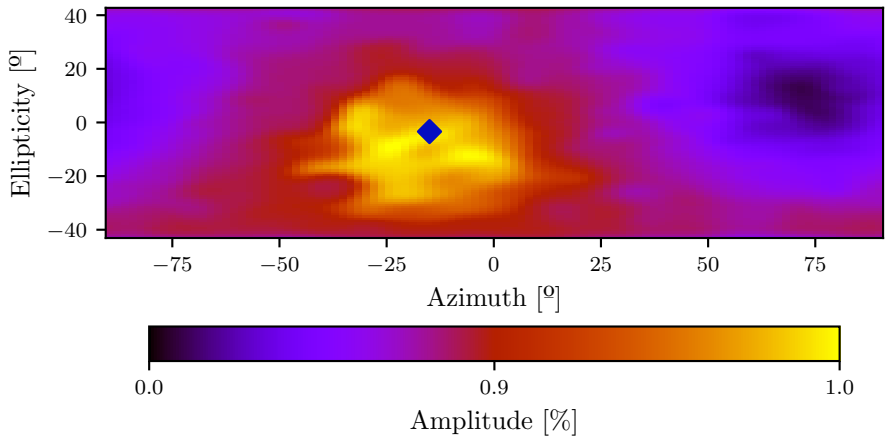

Figure 3.19: Heatmap showing the detection efficiency as a function of azimuth and ellipticity angles for one of the two interfering signals. The point in the center, marked by the blue diamond, represents the fixed polarization of the path that does not vary during the experiment.

varies, as during the 10 min of the experiment, we randomly move the three axes of the polarization controller to collect data. We see a clear dependence of the amplitude at the output of the balanced detector on the polarization, and we can completely attenuate the signal if the polarization does not match. We also see that the area where the amplitude of the balanced detector output is maximized is where the polarization of both paths is similar.

3.3 Simulation of the CV-QKD system

In this section, detailed numerical simulations of the two first stages of the CV-QKD protocol are run, specifically signal transmission and parameter estimation,

to analyze how experimental imperfections or impairments affect the secret key rate. We start by introducing a generalized mathematical model that describes these impairments, deriving an expression for the analog signal at the detector output, and then we conclude by showing the simulation results, studying how the secret key rate decreases in response to different experimental impairments.

There exist studies on noise models for different sources in a CV-QKD system [81, 82] that separate different noise sources theoretically to divide the total excess noise depending on the source. There are also studies on particular components of the experimental setup, such as impairments in coherent detectors [119, 147, 146], intensity fluctuations in laser sources [90], imperfect modulation [94], imperfect basis choice in homodyne detection [93], or studying the discrete effects in real modulation [76], which demonstrates that a non-ideal Gaussian modulation can be sufficient to perform CV-QKD.

In this work, we don't study a particular noise independently and theoretically. By running simulations of the whole transmission, we numerically analyze the effect of a specific impairment in the total excess noise and, thus, in the final estimated secret key rate without trying to divide the excess noise into different noise sources. In this section, we follow the methods and results that led to the first publication related to this thesis [1].

3.3.1 Simulation of the Protocol

The GG02 protocol, described in Section 2.2.2, consists of 4 steps: the transmission of coherent states from Alice to Bob, the security estimation or parameter estimation, the error correction, and the privacy amplification. In this section, we focus on the first two steps, as we will study how the estimation of the secret key rate depends on various experimental imperfections of the system.

To achieve this, we will focus on mathematically simulating the CV-QKD system in detail. The idea is to simulate at the electric field level what happens to the signals under different system imperfections and how parameter estimation would be in each case.

State Preparation

We start by simulating the generation of the signal at Alice. The first step in a Gaussian modulation protocol [82] is the sampling of random symbols following a Gaussian distribution centered at zero with modulation variance V_A so that Alice's symbols to modulate in each quadrature are given by $q_n \in \mathcal{N}(0, V_A)$ for the I quadrature and $p_n \in \mathcal{N}(0, V_A)$ for the Q quadrature, for $n = 1, \ldots, N$, for a total

number of N symbols sent by Alice. Subsequently, for correct digital processing of the signal, these symbols must be convolved with a root-raised cosine filter [26].

The Raised Cosine Filter (RCF) is used in classical telecommunications [136] to shape the pulses sent by the transmitter to minimize inter-symbol interference and to smooth the transmitted signal. The impulse response of the raised cosine filter is defined as a function that smoothly transitions from the passband (the part of the spectrum that is allowed to pass) to the stopband (the part of the spectrum that is filtered out), reducing the bandwidth of the filtered signal while maintaining data integrity. This impulse response is defined by

$$h(t) = \begin{cases} \dfrac{\pi}{4T_s}\,\mathrm{sinc}\left(\dfrac{1}{2\beta}\right), & t = \pm\dfrac{T_s}{2\beta}, \\ \dfrac{1}{T_s}\,\mathrm{sinc}\left(\dfrac{t}{T_s}\right)\dfrac{\cos\left(\dfrac{\pi\beta t}{T_s}\right)}{1-\left(\dfrac{2\beta t}{T_s}\right)^2}, & \text{otherwise.} \end{cases} \tag{3.22}$$

where β is the roll-off factor related to the smoothness of the filter, $T_s = 1/f_{\mathrm{sym}}$ is the symbol period, and $\mathrm{sinc}(x) = \sin(x)/x$. On the other hand, the Root Raised Cosine Filter (RRCF) is also widely used to split the pulse shaping equally between the transmitter and the receiver. When an RRCF is used at the transmitter and another at the receiver, the combined effect is equivalent to a single RCF at the emitter. The impulse response of the RRCF is defined by

$$r(t) = \begin{cases} \dfrac{1}{T_s}\left(1+\beta\left(\dfrac{4}{\pi}-1\right)\right), & t = 0, \\ \dfrac{\beta}{T_s\sqrt{2}}\left[\left(1+\dfrac{2}{\pi}\right)\sin\left(\dfrac{\pi}{4\beta}\right)+\left(1-\dfrac{2}{\pi}\right)\cos\left(\dfrac{\pi}{4\beta}\right)\right], & t = \pm\dfrac{T_s}{4\beta}, \\ \dfrac{1}{T_s}\dfrac{\sin\left[\pi\dfrac{t}{T_s}(1-\beta)\right]+4\beta\dfrac{t}{T_s}\cos\left[\pi\dfrac{t}{T_s}(1+\beta)\right]}{\pi\dfrac{t}{T_s}\left[1-\left(4\beta\dfrac{t}{T_s}\right)^2\right]}, & \text{otherwise.} \end{cases} \tag{3.23}$$

Typically, in standard implementations of classical telecommunications, the RRCF is more commonly used as the filtering effort is split between the transmitter and the receiver, making the filtering process more efficient. However, for simplicity and ease of calculation, we implement the RCF only once at the emitter. To apply this filter to the symbols generated by Alice, we first need to define the raw symbol

signal as

$$R_{\mathrm{IQ}}(t) = \begin{cases} x_n \in \mathcal{CN}(0, 2V_A), & t = nT_s, \text{ for all } n \in \mathbb{Z}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.24}$$

That is, a signal that is always zero at all times except at each symbol period, where it has the value of the symbol, which is sampled from a complex Gaussian distribution with mean 0 and variance $2V_A$ (equivalent to the real and imaginary parts following two Gaussian distributions with mean 0 and variance V_A respectively). This signal is convolved with the impulse response of the filter, $h(t)$, to produce the symbol band signal sent by Alice,

$$S_{\mathrm{IQ}}(t) = (R_{\mathrm{IQ}} * h)(t) = \int_{-\infty}^{\infty} R_{\mathrm{IQ}}(\tau) h(t-\tau)\, \mathrm{d}\tau. \tag{3.25}$$

Since the function $R_{\mathrm{IQ}}(t)$ is zero at all points except at the sampling times, it can be represented as a sum of Dirac deltas,

$$R_{\mathrm{IQ}}(t) = \sum_{n=1}^{N} (q_n + ip_n)\delta(t - nT_s), \tag{3.26}$$

where N is the total number of symbols sent. Therefore, the expression of the convolution between $R_{\mathrm{IQ}}(t)$ and $h(t)$ can be discretized as

$$S_{\mathrm{IQ}}(t) = \sum_{n=1}^{N} (q_n + ip_n) h(t - nT_s). \tag{3.27}$$

In Figure 3.20, the signals $R_{\mathrm{IQ}}(t)$ and $S_{\mathrm{IQ}}(t)$ are represented, where the effect of the RCF on the symbol signals can be observed.

We can see in the frequency spectrum that applying this filter to the signal reduces the signal's bandwidth from infinity to f_{sym}. On the other hand, we see that in the time domain, the function $R_{\mathrm{IQ}}(t) = S_{\mathrm{IQ}}(t)$ when $t = nT_s$, so by sending $R_{\mathrm{IQ}}(t)$, Alice is sending the information of the symbols obtained randomly following a Gaussian distribution, so it should be enough to send this signal to Bob so he can recover the sent symbols.

However, for the experimental implementation with an LLO at Bob, it is necessary to send a pilot tone that serves as a reference to measure the frequency and demodulate the signal correctly. In addition to adding a pilot tone to the symbol signal, we must shift the result of this sum to a higher frequency to move away from the optical carrier and prevent the beat signal of the two lasers from appearing within the bandwidth of the balanced detector when detection is performed.

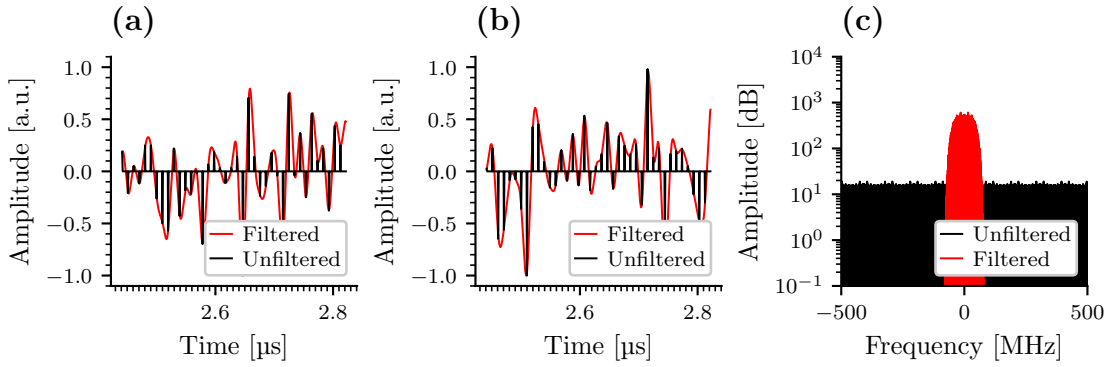

Figure 3.20: Symbol signals before and after filtering with a Raised Cosine (RC) filter. (a) shows the real part of the random symbols and the filtered signals. (b) shows the imaginary part of the random symbols and the filtered signals. (c) shows the Fourier Transform of both $R_{\mathrm{IQ}}(t)$ and $S_{\mathrm{IQ}}(t)$ signals.

To do this, we have to multiply the sum of the symbol signal and pilot tone by a high-frequency intermediate frequency ω_u to perform the up-conversion,

$$V_{\mathrm{IQ}}(t) = e^{i\omega_u t}\left[S_{\mathrm{IQ}}(t) + V_p e^{i\omega_p t}\right], \tag{3.28}$$

where V_p is the pilot tone amplitude. The real part of $V_{\mathrm{IQ}}(t)$ corresponds to the signal $V_I(t)$ acting on the first MZM of the IQ modulator, and the imaginary part corresponds to the signal $V_Q(t)$ acting on the second MZM of the IQ modulator. Therefore, These signals are finally generated in the two Digital-Analog Converters (DAC) of the AWG and sent to the two inputs of the IQ modulator to modulate the laser electric field. The complete expression for the modulating signal, separating their real and imaginary parts, is thus calculated by introducing Equation (3.27) into Equation (3.28) and expanding,

$$\begin{aligned} V_I(t) &= \left(\sum_{n=1}^{N} q_n h(\tau_n)\right)\cos(\omega_u t) - \left(\sum_{n=1}^{N} p_n h(\tau_n)\right)\sin(\omega_u t) + V_p\cos\left(\omega_p' t\right), \\ V_Q(t) &= \left(\sum_{n=1}^{N} q_n h(\tau_n)\right)\sin(\omega_u t) + \left(\sum_{n=1}^{N} p_n h(\tau_n)\right)\cos(\omega_u t) + V_p\sin\left(\omega_p' t\right). \end{aligned} \tag{3.29}$$

where $\tau_n = t - nT_s$, and where $\omega_p' = \omega_u + \omega_p$. The field's expression at the IQ modulator's output would be the expression of Equation (3.8), introducing these two signals respectively. If we add the effect of the attenuator and the 1:99 beam splitter, we finally have the optical signal at the output of Alice,

$$E_{\mathrm{out}}(t) = \left(0.01 \times 10^{-\kappa/10}\right)\frac{E_A e^{i\omega_A t}}{2}\left[\sin\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right) + i\sin\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right)\right], \tag{3.30}$$

where κ is the attenuation in dB of the variable attenuator. This electric field is the one that finally goes into the channel.

State Measurement

Once the electric field of Equation (3.30) leaves the channel, we have to simulate its effect. This is the simplest part, as we only need to simulate the losses due to the attenuation of the optical fiber. Normally in commercial fibers, losses are indicated as dB/km, α, which in the case of single-mode fibers for 1550 nm is usually around 0.2 dB/km. Therefore, the field that Bob receives coming from the channel is given by

$$E_R(t) = (0.01 \times 10^{-(\kappa+\alpha L)/10}) \frac{E_A e^{i\omega_A t}}{2} \left[\sin\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right) + i \sin\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right)\right], \quad (3.31)$$

where L is the length of the channel. This field interferes in the 1:1 beam splitter with Bob's local oscillator. Using the results from Equations (3.10) and (3.11), assuming $\Delta\phi = 0$ for simplicity, and expressing the field amplitudes as the square root of their optical power, the analog signal at the output of the balanced detector can be expressed as

$$V(t) = k \left[\cos(\Delta\omega t) \sin\left(\frac{\pi}{2}\frac{V_I(t)}{V_\pi}\right) - \sin(\Delta\omega t) \sin\left(\frac{\pi}{2}\frac{V_Q(t)}{V_\pi}\right)\right], \quad (3.32)$$

where k is defined as a scaling factor taking into account Alice's attenuator, channel losses, balanced detector gain factor, and the optical powers of both lasers. It is defined by

$$k = (0.01 \times 10^{-(\kappa+\alpha L)/10}) \rho \sqrt{P_A P_B}. \quad (3.33)$$

Then, after acquiring $V(t)$, the low-complexity heterodyne detection demodulation method is performed. To do this, the symbol band must be centered at the intermediate frequency ω_{IF}. This is achieved by setting the laser frequencies such that $\Delta\omega = \omega_{\text{IF}} - \omega_u$, since multiplying a sinusoidal signal of frequency ω_1 by one of frequency ω_2 results in two signals of frequency $\omega_1 \pm \omega_2$, so $V(t)$ will have the symbol band centered at ω_{IF} after filtering out the other component.

Once we have set $\Delta\omega = \omega_{\text{IF}} - \omega_u$, we follow the demodulation procedure of Figure 3.5c, and multiply $V(t)$ by a sinusoidal signal of frequency ω_{IF} and then filter the result with a Butterworth low-pass filter h_l with a cutoff frequency equal to the symbol band, f_{sym}, to demodulate the symbols,

$$V_{\text{IQ}}(t) = \left(h_l * V(t) e^{-i\omega_{\text{IF}} t}\right)(t) \propto S_{\text{IQ}}(t). \quad (3.34)$$

It means that the signal Bob recovers after demodulation is similar to Alice's symbol signal. This result derives from introducing the signals of Equation (3.29)

into Equation (3.32) and expanding all the terms, approximating the sine terms via the Jacobi-Anger expansion,

$$\begin{aligned}\sin(z\cos\theta) &= -2\sum_{n=1}^{\infty}(-1)^n J_{2n-1}(z)\cos[(2n-1)\theta] \approx 2J_1(z)\cos\theta,\\ \sin(z\sin\theta) &= 2\sum_{n=1}^{\infty} J_{2n-1}(z)\sin[(2n-1)\theta] \approx 2J_1(z)\sin\theta,\end{aligned} \tag{3.35}$$

where in this case $z = \pi V_p/2V_\pi < 1$. For the typical values used for V_p and V_π, we have $J_n(z) \ll J_1(z)$ for $n > 1$, so we can approximate them only to the first term.

After obtaining the demodulated signal V_{IQ}, the next step is to sample the symbols p' and q', which will be compared with the symbols p and q generated by Alice. To do this, it is enough to sample the signal $V_{\mathrm{IQ}}(t)$ at times $t = nT_s$ for $n = 1, \ldots, N$. To include the effect of noise (including shot noise, excess noise, and electronic noise), a Gaussian noise with mean 0 and variance σ_z must be added to the symbols measured by Bob,

$$\begin{aligned}p' &= \{\mathrm{Re}\,[V_{\mathrm{IQ}}(nT_s)] + p_z \text{ for } n \text{ in } 1,\ldots N \text{ and } p_z \in \mathcal{N}(0,\sigma_z)\},\\ q' &= \{\mathrm{Im}\,[V_{\mathrm{IQ}}(nT_s)] + q_z \text{ for } n \text{ in } 1,\ldots N \text{ and } q_z \in \mathcal{N}(0,\sigma_z)\}.\end{aligned} \tag{3.36}$$

With all this, we can form the concatenated vectors $x = \{p, q\}$ and $y = \{p', q'\}$ and estimate the channel transmittance and excess noise to calculate the mutual information, the Holevo bound, and thus estimate the secret key rate as presented in Section 2.3.

3.3.2 Modeling Experimental Devices

The next step is to generalize the described model to include the experimental imperfections characterized in Section 3.2. The goal is to simulate an experimental transmission by modifying the impairment values and comparing them with actual experimental devices. By having a realistic twin model of the experimental system, many tests can be performed without physically conducting experiments. Therefore, the idea is to simulate the entire transmission using the mathematical models from the previous section, generalized to include experimental imperfections, extract the symbols x and y from Alice and Bob, and estimate the security of the transmission using the security analyses from Section 2.3.

Laser Drift

We start by modifying the mathematical model to include the most critical part, which is the random frequency drift of the lasers. As seen in Section 3.2.1, the

random frequency drift can be described as a random walk where the step size follows a random distribution. In other words, the frequency $\omega(t)$ of the laser at time t can be modeled as

$$\omega(t + \Delta t) = \omega(t) + \Delta\omega(t)\Delta t, \tag{3.37}$$

where Δt is the time increment during which the variation occurs and $\Delta\omega(t)$ is the random step size per second at time t. We assume that $\Delta\omega(t)$ is a random variable following a random distribution $\mathcal{D}$, which, as shown in Figure 3.7c, is a zero-mean logistic distribution. Note that, as shown in Figure 3.8, the step size is time-normalized and needs to be multiplied by Δt. This normalization is valid for step times within the linear region of the plot ($\Delta t < 1\,\mathrm{s}$) and is useful for performing simulations with different step times while maintaining consistent random drift amplitudes. Therefore, the frequency at discretized time $t_k = k\Delta t$ will be the sum of the initial frequency and the cumulative sum of the frequency steps from the initial time to t_k,

$$\omega(t_k) = \omega(t_0) + \sum_{j=0}^{k-1} \Delta\omega(t_j)\Delta t. \tag{3.38}$$

The phase of the angular frequency is its integral over time, which can be expressed discretely as

$$\phi(t_k) = \sum_{j=0}^{k-1} \omega(t_j)\Delta t, \tag{3.39}$$

which, after substituting the expression for $\omega(t_k)$ and simplifying, gives us the electric field of the laser at time t_k, defined by $E(t) = E_0 e^{i\phi(t)}$, as

$$E(t_k) = E_0 \exp\left[i\left(\omega(t_0)t_k + \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} \Delta\omega(t_i)\Delta t^2\right)\right]. \tag{3.40}$$

To conduct realistic simulations, we use this equation to model the electric fields of Alice's and Bob's lasers, respectively, as

$$\begin{aligned} E_A(t_k) &= \sqrt{P_A}\exp\left[i\left(\omega_A(t_0)t_k + \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} \Delta\omega_A(t_i)\Delta t^2\right)\right], \\ E_B(t_k) &= \sqrt{P_B}\exp\left[i\left(\omega_B(t_0)t_k + \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} \Delta\omega_B(t_i)\Delta t^2\right)\right], \end{aligned} \tag{3.41}$$

where P_A and P_B are the optical powers of the lasers, $\omega_A(t_0)$ and $\omega_B(t_0)$ are the initial frequencies before the laser drift for Alice and Bob, and $\Delta\omega_A(t)$ and $\Delta\omega_B(t)$

are elements of the random distribution $\mathcal{D}$, which, as characterized in Section 3.2.1, corresponds to a zero-mean logistic distribution. By modifying the variance, we can simulate the frequency drift intensity of the lasers, thus studying its effect on the final key security.

IQ Modulator

Next, we need to generalize the field at the output of the IQ modulator. As seen in Section 3.2.2, the minimum transmission operating point is not always ideally achieved, as there is an electronic control loop responsible for it. Like any electronic control loop, it has an error that, although very small, is not zero. Additionally, Figure 3.14a shows that this power is never zero, making it practically impossible to reach the operating point ideally. The figure also shows that the half-wave voltages of the three interferometers forming the dual-nested MZM are different. Therefore, we cannot use Equation (3.8) to derive the output of the balanced detector. Instead, we need to generalize Equation (3.7) for a drifting frequency and for different bias and half-wave voltages to calculate the field at the modulator output. Combined with the effect of the attenuator, the channel losses, and the 99:1 beam splitter for the power monitoring, the general expression for the electric field received by Bob becomes

$$E_R(t) = k' \frac{E_A(t)}{2} \left[\cos\left(\frac{\pi}{2} \frac{(V_I(t) + V_{b1})}{V_{\pi 1}} \right) + e^{i\pi \frac{V_{b3}}{V_{\pi 3}}} \cos\left(\frac{\pi}{2} \frac{(V_Q(t) + V_{b2})}{V_{\pi 2}} \right) \right], \quad (3.42)$$

where $E_A(t)$ is given by Equation (3.41), $V_I(t)$ and $V_Q(t)$ are the modulating signals defined in Equation (3.29), and the scaling factor k' is given by

$$k' = (0.01 \times 10^{-(\kappa + \alpha L)/10}). \quad (3.43)$$

Note that the half-wave and bias voltages are distinguished in this equation to allow simulations with different values. These values will be different in practice, and the operating point will not be ideally locked. Therefore, we must use this equation to simulate the effects of impairments in the modulator and bias controller.

Coherent Detector

For the detector, we have Bob's laser, a 1:1 beam splitter, and a balanced detector with gain ρ. All three components exhibit imperfections in real experiments. Bob's laser, like Alice's, has random frequency deviations, the beam splitter is not exactly 1:1, and the two photodetectors in the balanced detector do not have identical gains. Therefore, the first step is to replace the expression for the fields at the 1:1 beam splitter output in Equation (3.10) with the more general expression [99] for

a classical lossless beam splitter,

$$E_1(t) = r_1 E_R(t) + t_1 E_B(t), \quad E_2(t) = t_2 E_R(t) - r_2 E_B(t), \tag{3.44}$$

where r_1 and r_2 are the reflectance coefficients, and t_1 and t_2 are the transmittance coefficients. $E_R(t)$ is the field defined in Equation (3.42), and $E_B(t)$ is the field defined in Equation (3.41). Note that in the case of an ideal 1:1 beam splitter, Equation (3.44) would become

$$E_1(t) = \frac{1}{\sqrt{2}} \left(E_{\text{out}}(t) + E_B(t) \right), \quad E_2(t) = \frac{1}{\sqrt{2}} \left(E_{\text{out}}(t) - E_B(t) \right). \tag{3.45}$$

But in the realistic case, once we have the fields from Equation (3.44), we calculate the power of each field with $P_i = |E_i|^2$, obtaining

$$\begin{aligned} P_1(t) &= r_1^2 |E_R(t)|^2 + r_1 t_1 E_R(t) E_B^*(t) + t_1 r_1 E_B(t) E_R^*(t) + t_1^2 |E_B(t)|^2, \\ P_2(t) &= t_2^2 |E_R(t)|^2 + r_2 t_2 E_R(t) E_B^*(t) + t_2 r_2 E_B(t) E_R^*(t) + r_2^2 |E_B(t)|^2. \end{aligned} \tag{3.46}$$

Generalizing the balanced detector output to the case where the two photodetectors have different gain factors ρ_1 and ρ_2, it becomes

$$V(t) = \kappa_p (\rho_1 P_1(t) - \rho_2 P_2(t)), \tag{3.47}$$

where $P_1(t)$ and $P_2(t)$ are the powers defined in Equation (3.46). The term κ_p represents a value between 0 and 1 and is introduced to simulate the effect of non-matching polarization between Alice and Bob. Simulating the polarization states entirely would be very complex, and as seen in Section 3.2.3, polarization calibration errors result in amplitude reduction, which can reach 0, as shown in Figure 3.19. Therefore, introducing this term simulates its effect.

3.3.3 Parameter Estimation Simulations

Once we have all the equations for the simulations, we proceed with them. For simplicity, we study the effect of each imperfection or experimental parameter separately, keeping the rest ideal. For the simulations, we generate 10^6 random symbols $x_n = q_n + ip_n$ following a Gaussian distribution with variance $0.001 V_p$, where V_p is the pilot tone amplitude, taken as $V_p = 0.5 V_\pi$. These symbols are filtered with the RCF, the pilot tone is added, and then both are up-converted to ω_u to obtain $V_I(t)$ and $V_Q(t)$.

Then, we simulate the generation and modulation of the electric field, its transmission through the channel, and Bob's subsequent detection and demodulation. Once we have the signal $V(t)$ detected by Bob, we perform the demodulation

using low-complexity heterodyne detection and then sample the data to obtain $y_n = q'_n + ip'_n$. Once we have x and y, we perform the parameter estimation process to obtain the secret key rate in the worst-case scenario within the trusted noise model, as described in Section 2.3. Table 3.2 shows the ideal values of all simulation parameters.

Parameter	Value
Number of symbols (N)	10^6
Symbol frequency (f_s)	100 MHz
Pilot tone frequency (f_p)	100 MHz
Alice Laser frequency ($\omega_A/2\pi$)	10.75 GHz
Bob Laser frequency ($\omega_B/2\pi$)	10 GHz
Local oscillator power (P_B)	10 dBm
Detector gain (ρ)	5 V/mW
Electronic noise (ν_{el})	0.1 SNU
Detector efficiency (η)	0.55
Reconciliation efficiency (β)	0.95
Confidence intervals (ε_{PE})	10^{-10}

Table 3.2: Parameters used in the simulated transmission and secret key rate estimation. All values closely match those experimentally characterized. The chosen modulation variance V_A is the one that maximizes the SKR for each length, ranging between 2 SNU to 10 SNU, depending on the channel length.

To simulate the detector efficiency and determine the variance of the Gaussian noise to be added to the symbols, we perform simulations for two different distances, L_1 and L_2, obtain $\sigma_1^2 = \text{var}(y)_1$ and $\sigma_2^2 = \text{var}(y)_2$ respectively, and solve the following system of equations relating the variances of the transmitted and received states,

$$\begin{cases} k^2\sigma_1^2 + \sigma_z^2 = \eta T_1 V_A + \eta T_1 \xi + 1 + \nu_{\text{el}}, \\ k^2\sigma_2^2 + \sigma_z^2 = \eta T_2 V_A + \eta T_2 \xi + 1 + \nu_{\text{el}}, \end{cases} \tag{3.48}$$

where $T_i = 10^{\alpha L_i/10}$ is the transmittance for distance L_i, and k is the scaling factor applied to Bob's symbols to simulate the detection efficiency η, and σ_z^2 is the variance of the Gaussian noise added to Bob's symbols to simulate the shot noise, electronic noise, and excess noise. The solution to these equations is

$$\begin{cases} k = \sqrt{\dfrac{\eta(T_1 - T_2)(V_A + \xi)}{\sigma_1^2 - \sigma_2^2}}, \\ \sigma_z^2 = \eta T_1 V_A + \eta T_1 \xi + 1 + \nu_{\text{el}} - \dfrac{\eta(T_1 - T_2)(V_A + \xi)\sigma_1^2}{\sigma_1^2 - \sigma_2^2}, \end{cases} \tag{3.49}$$

Once Bob's symbols are correctly scaled and the noise is added to the demodulated symbols, we can study the effect of the experimental impairments on the SKR.

We start by running 1000 simulated experiments with the entire process described above, leaving all values ideal except for V_{b1} and V_{b2}, which will vary between $-40\,\%$ and $40\,\%$ of their ideal values. For each bias voltage value of the bias controller, we simulate the entire transmission and calculate the SKR. We then do the same but varying the value of $V_{\pi 1}$ and $V_{\pi 2}$ between $-40\,\%$ and $40\,\%$ of their ideal values. For these two sets of simulations, each run for four different distances, simulation results are shown in Figure 3.21.

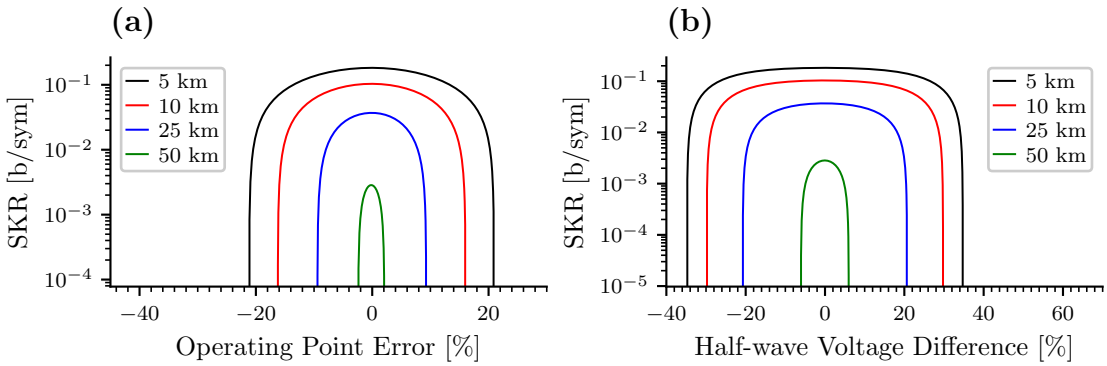

Figure 3.21: Effects of impairments in the IQ modulator on SKR. (a) shows the impact of incorrect operating point locking in the modulator bias controller on the SKR. (b) illustrates the effects of differing half-wave voltages in the I and Q arms of the modulator on the SKR.

It can be seen that the security of the transmission is more sensitive to errors in the bias controller when finding the minimum transmission operating point than to differences in the half-wave voltage. It is evident that the system has less margin for error over longer distances, so reducing the impact of impairments is essential. To eliminate the effect of the impairment shown in Figure 3.21a, the only solution is to improve the electronic control algorithm. In our case, the commercial MBC employed has an error of less than $1\,\%$, so no further action is required. To eliminate the effect of the impairment shown in Figure 3.21b, it is sufficient to scale $V_I(t)$ and $V_Q(t)$ differently so that $V_I(t)/V_{\pi 1}$ is similar to $V_Q(t)/V_{\pi 2}$ in Equation (3.42).

On the receiver side, we can simulate the two main impairments (differences in the beam splitter's splitting ratio and the gains of the photodetectors of the balanced detector). For the first case, we perform four sets of 1000 simulations for various distances, as before, but varying the reflection and transmission indices in Equation (3.44). We assume that $r_1 = -r_2 := r$ and $t_1 = t_2 := t$ with $r + t = 1$, but we vary the value of r around the ideal value of $\sqrt{1/2}$. In the second case,

we perform the same simulations while varying the value of ρ_1 in Equation (3.47) while assuming $\rho_1 + \rho_2$ is constant in all measurements to prevent an increased symbol correlation as a consequence of a higher detector gain. The results of these simulations are shown in Figure 3.22.

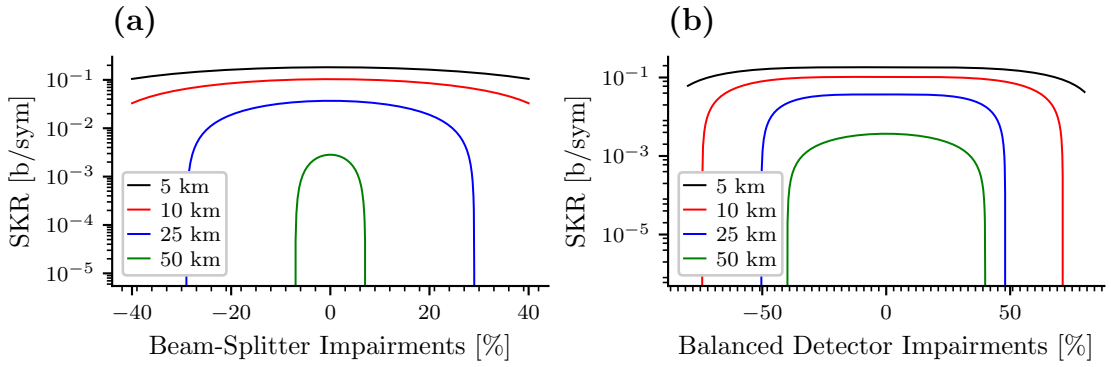

Figure 3.22: Effects of impairments in the coherent detector on SKR. (a) shows the impact of an unbalanced splitting ratio in the detector's beam splitter on the SKR. (b) illustrates the effects of different gains in the two photodiodes of the balanced detector on the SKR.

It can be seen that the system allows for considerable error in the reflection and transmission indices of the beam splitter, and given that our experimental system has a beam splitter with a tolerance of 1.5 % in the splitting ratio, this is not a concern. With the balanced detector, it is the same; the experimental system is well below the values that would prevent an experimental transmission, so it is not a concern. However, to maximize the SKR, eliminating the effect of these impairments is preferable. Both can be addressed by calibrating the gains of the photodetectors in the balanced detector to compensate for differences in the detector and the beam splitter. Some commercial balanced detectors include a potentiometer to adjust the gain offset between the photodetectors, and correctly calibrating this offset can eliminate the effect of these two impairments to maximize the SKR.

Regarding the lasers, they fluctuate in power and frequency. The power fluctuations of real lasers depend on temperature, so they are slow and do not affect detection. Implementing a control loop to calibrate the power before each transmission is sufficient. However, frequency fluctuations of the lasers severely impact key transmission. If we perform several simulations as before, but this time leaving all values ideal except for the laser frequencies, defined by the fields in Equation (3.41), for different drift amplitudes determined by the time-normalized standard deviation of the random walk step size distribution modeling the lasers' behavior, we can see how laser stability affects key transmission. We have performed these simulations using the standard direct demodulation procedure explained in Sec-

tion 3.3.1. On the other hand, we have also realized the same simulations using the pilot-aided demodulation method described in the next chapter to verify it with simulated transmissions. The results are shown in Figure 3.23.

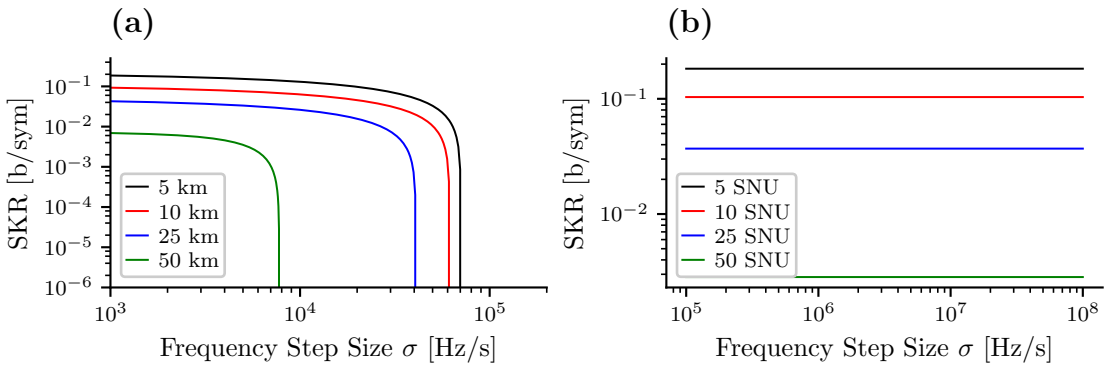

Figure 3.23: Effect of frequency drift in both lasers on the SKR. (a) shows the impact of frequency drift magnitude on the SKR using direct demodulation. (b) shows the impact of frequency drift magnitude on the SKR using the frequency-locking algorithm presented later in Chapter 4.

Given that the time-normalized standard deviation of the frequency drift step size of the commercial lasers we use is around 80 MHz/s, it would be impossible to perform any CV-QKD transmission at any distance solely because of this. Using the frequency-locking algorithm proposed in Section 4.1 completely eliminates this problem at any distance.

Finally, it is interesting to study the effect of poor polarization correction in the detector or the impact of Bob's laser power on transmission security. We perform the same previous simulations under ideal conditions for the first case but vary κ_p in Equation (3.47) between 0 and 1. For the second, we vary the value of P_B in Equation (3.46). The results are shown in Figure 3.24.

We see that as long as Bob's laser power is greater than 1 mW, there are no issues, and with our laser at 10 mW, it is sufficient. Clearly, the higher the local oscillator power, the better the signal-to-noise ratio, as the signal will be amplified more in the beam splitter, the shot noise as well, but the electronic noise will remain constant, reducing the ratio between electronic noise and shot noise as power increases. On the other hand, we see that if κ_p drops below a certain value for each distance, the SKR drops drastically. This, as seen in Figure 3.19, does not seem to be a significant issue, as there is a wide range of azimuth and ellipticity values where $\kappa_p > 0.9$, so as long as we have an automated polarization controller calibrated before sending the signal, there should be no problems.

In addition to the previous figures, we can also use the simulation model to study the dependence on arbitrary system parameters, not necessarily impairments. For

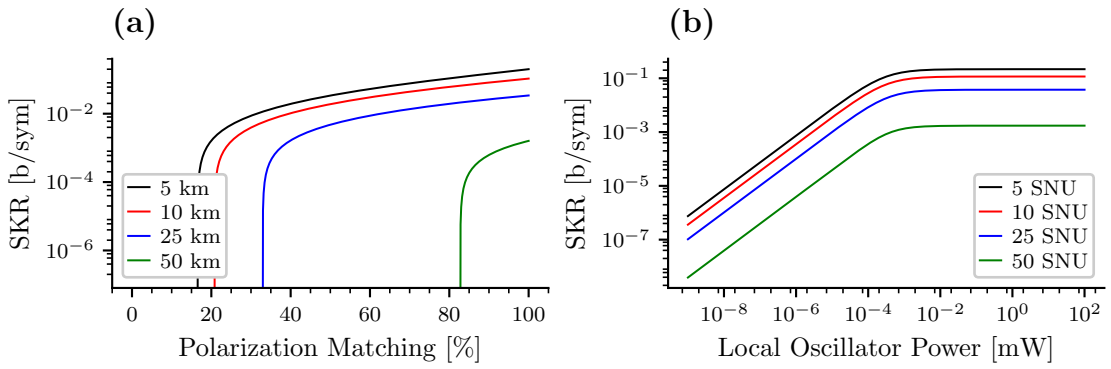

Figure 3.24: Additional simulations. (a) shows the effect on the SKR of incorrect polarization matching between Alice and Bob's lasers. (b) shows the effect on the SKR of varying power levels in the local oscillator laser.

instance, we can explore how the SKR depends on modulation variance and channel length, as shown in Figure 3.25.

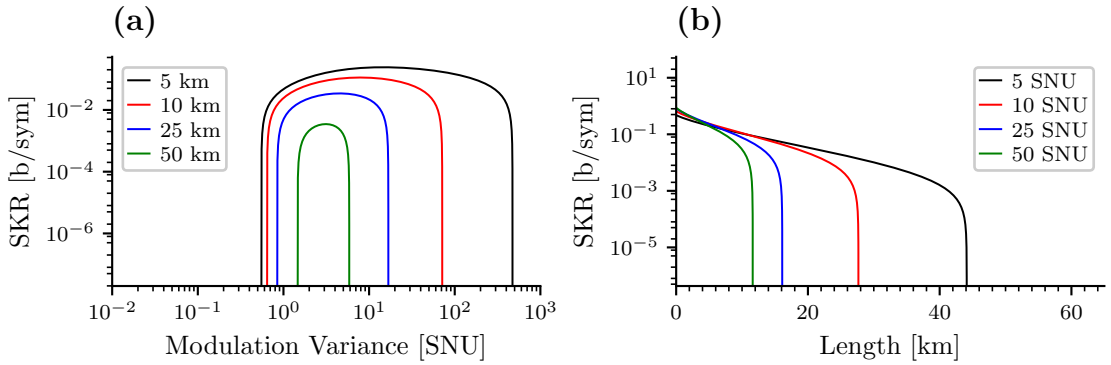

Figure 3.25: Simulations of various system variables. (a) shows the SKR for different modulation variances across various distances. (b) shows the SKR for different channel lengths at different modulation variances.

Another set of important parameters we can analyze are correlation and excess noise. Excess noise directly affects the SKR; as excess noise increases, the Holevo bound increases, leading to a decrease in the SKR. The dependence of SKR on both excess noise and correlation is illustrated in Figure 3.26.

As we can see, there is a narrow range of permissible correlation values. This indicates that to ensure secure transmissions, the system must operate within a specific region. A high correlation implies that the Holevo bound will increase, allowing Eve to gain too much information about the key. Conversely, too little correlation means Bob does not have sufficient information to recover the key. Understanding this dependence allows us to assess the correlation after signal

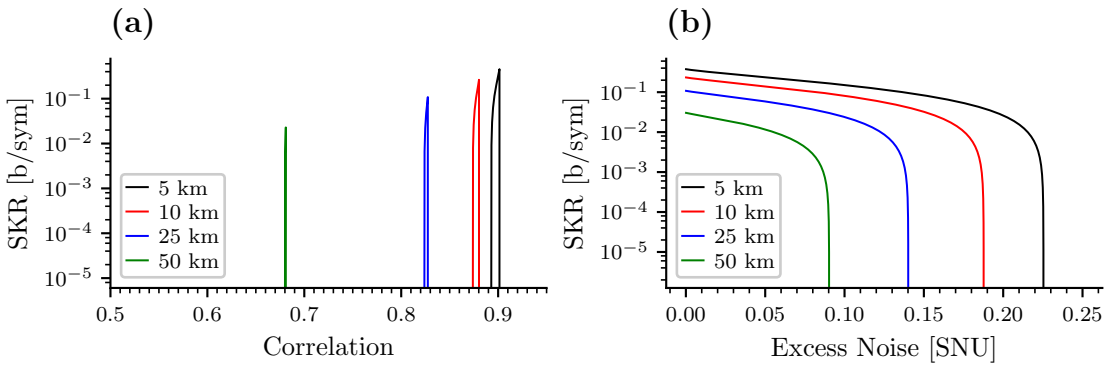

Figure 3.26: Simulations of various system variables. (a) shows the dependence of the SKR on symbol correlation. (b) shows the direct dependence of the SKR on excess noise.

demodulation, which is a straightforward step that can provide valuable insights into the key's security even before parameter estimation.

3.4 Conclusions

This chapter has outlined the entire process of designing, characterizing, and simulating the experimental system required to implement a CV-QKD protocol based on Gaussian-Modulated Coherent States (GMCS) with a locally generated local oscillator (LLO) and low-complexity heterodyne detection. After conceptualizing the system, we proceeded with the characterization of various components, including lasers, modulators, amplifiers, attenuators, and detectors.

For the electro-optic modulator, its amplifiers, and the bias controller, we identified no significant limitations, aside from the fact that certain input voltage ranges yield a more linear output response. Additionally, we observed that the half-wave voltage of the three Mach-Zehnder modulators in the IQ modulator differ slightly. Simulations indicated that this variation could potentially reduce the secret key rate in an experimental transmission. However, the deviation required to significantly impact the key rate is much larger than what is typically observed in the experimental devices. A potential solution would be to appropriately scale $V_I(t)$ and $V_Q(t)$ so that the arguments of the cosines in Equation (3.7) have similar magnitudes. For the attenuator, we characterized its response to determine how it attenuates based on the input voltage, allowing us to set a precise output power and, thus, a precise modulation variance.

Regarding the receiver, we characterized the reflection and transmission indices of the beam splitter, finding them close to ideal values. Simulations showed a high tolerance in this aspect, requiring a significantly deviated beam splitter to

notably affect the secret key rate. The balanced detector was also characterized, revealing deviations much smaller than those needed to lower the secret key rate. We also measured the detector's bandwidth, which is crucial for keeping the signal within the detection window to maximize efficiency. Additionally, we studied the dependence of the secret key rate on the polarization mismatch between the incoming signal and the LO, highlighting the necessity of implementing a polarization stabilization system to optimize detection efficiency and minimize unnecessary information loss.

For the lasers, we investigated the challenges caused by the LLO implementation, specifically the presence of two free-running lasers with different drifting frequencies and phases. We characterized these random fluctuations and simulated a similar deviation to analyze the effect on key transmission. From this, we concluded that the CV-QKD protocol with LLO could not be effectively implemented without some frequency-locking technique. Simulations demonstrated that without frequency stabilization, the allowed limits for the random frequency drifts of the lasers were several orders of magnitude smaller than the actual deviations. This issue can be addressed using more stable lasers, implementing an electronic frequency stabilization circuit, or correcting the frequency drift effect after signal acquisition using digital signal processing techniques. We ultimately chose the latter, developing our own frequency-locking algorithm, as detailed in the following chapter.

In summary, this chapter used modeling and numerical simulation of experimental devices to study the impact of real-world impairments on the protocol's performance, laying the groundwork for the experimental transmissions described in the next chapter. The necessity of implementing a frequency-locking system to enable these transmissions is also established and will be further discussed in the following chapter.

Chapter 4

Experimental Implementation

In this chapter, we introduce the pilot-assisted frequency-locking method, which represents the main result of this thesis and has led to the second publication related to this work [2]. The first section describes the methods presented in [2, 3] regarding the pilot-assisted frequency-locking method. The chapter ends with the last section showing the results presented in [2].

The pilot-assisted frequency-locking method addresses the challenge of frequency stabilization in LLO implementations through digital signal processing. After presenting this method, we review various improvements implemented in our experimental system to enhance its robustness and stability, including the development of automatic calibration and stabilization algorithms. The chapter concludes with the results of experimental transmissions conducted using the frequency-locking algorithm, as well as real-world use cases executed with our experimental setup.

4.1 Pilot-Assisted Frequency-Locking Algorithm

This section provides a step-by-step introduction to the digital signal processing algorithms used to correct the local oscillator's frequency and phase drifts relative to the detector's incoming signal. We begin by analyzing the issue of phase and frequency fluctuations in lasers, followed by the presentation of the pilot-assisted frequency-locking algorithm that addresses this problem. The section concludes by introducing two additional phase and clock recovery algorithms that refine the initial solution, completing the necessary digital signal processing techniques for stabilizing lasers after signal acquisition.

Since CV-QKD with LLO implementations began, maintaining the same frequency in two independent lasers separated from each other has been challenging for all

experimental implementations. There are several complex solutions to address this problem before the development of CV-QKD [64]. Typically, the solution was locking the frequency of both lasers to a precise spectral line given by the emission or absorption of a gas cell [16]. Also, it's been shown that a laser can be stabilized to a fixed optical cavity resonance with an adjustable offset, providing a wide tuning range for the central frequency [156]. Another proposed method is the Optical Injection Locking [96], which is a technique used to synchronize the frequency and phase of a slave laser to that from a master laser through the injection of a small portion of the master laser's light into the slave laser's cavity. All of these solutions require specialized hardware designed for this purpose, which increases the system's complexity and cost.

Focusing on software solutions developed explicitly for CV-QKD systems that appeared a few years later with the rise of experimental demonstrations, one of them is the use of time-interleaved reference pulses, which consists of introducing reference signals that are time-multiplexed with the quantum signal to perform the carrier recovery and solve the frequency-locking problem [129, 65]. Similar to what happened with the time-multiplexed pilot, these techniques imply slight delays between the calibration and correction stages, which may result in deficient corrections.

If discrete modulation is used instead of Gaussian, standard carrier recovery algorithm used in classical communications such as the feedforward algorithm [115] or the Costas loop [118] can also be used to mitigate the frequency drift effects.

Additionally, algorithms based on Machine Learning for carrier recovery have been developed recently [100, 33], and have been recently used in record-breaking experimental transmissions [60] to resolve the frequency-locking problem with software solutions.

Similar to what we present here, there are also frequency-locking algorithms based on phase characterization and compensation based on correlation implemented after signal acquisition [66].

Between all the possibilities presented for implementing frequency-locking, we have tried to choose the lowest complexity option, prioritizing digital signal processing techniques over hardware-based active correction techniques to reduce the system's cost and increase its robustness. This is why our proposed frequency-locking method is entirely based on digital signal processing and does not depend on any hardware component.

Aside from the frequency-locking problem, the clock recovery problem has usually been solved by sending a clock reference signal by a different channel or recovering

it from the LO when it is sent from Alice. However, software-defined clock recovery techniques based on digital signal processing have been used in real experimental systems too [168]. Thus, we also implement a phase and clock recovery technique based on digital signal processing performed after signal acquisition.

4.1.1 The Problem of Frequency and Phase Fluctuations

Starting with the basic experimental setup for implementing CV-QKD shown in Figure 3.15, we send a key from Alice to Bob by continuously generating 100-symbol random Gaussian-modulated signals, which are added to a frequency-shifted pilot tone, as described in Section 3.3.1. We use the same signals from the simulations without modification. These digital signals are sent to the AWG, which generates them through its two analog outputs connected to the IQ modulator. The MBC locks the modulator at the minimum transmission operating point, and the attenuator is manually adjusted until the power read on the power meter corresponds to the desired modulation variance (see Figure 3.25a).

Subsequently, when the signal reaches Bob, we manually calibrate the polarization controller until we find an area where the signal at the output of the balanced detector, which is monitored in real-time on the oscilloscope, is maximized. Once everything is correctly calibrated, we pause the transmission and generate another random sequence as before, but this time of 10^6 symbols. This time, we send it once and acquire it completely on the oscilloscope, and then we transfer it to the computer for digital signal processing. The signal acquired by the oscilloscope is shown in Figure 4.1.

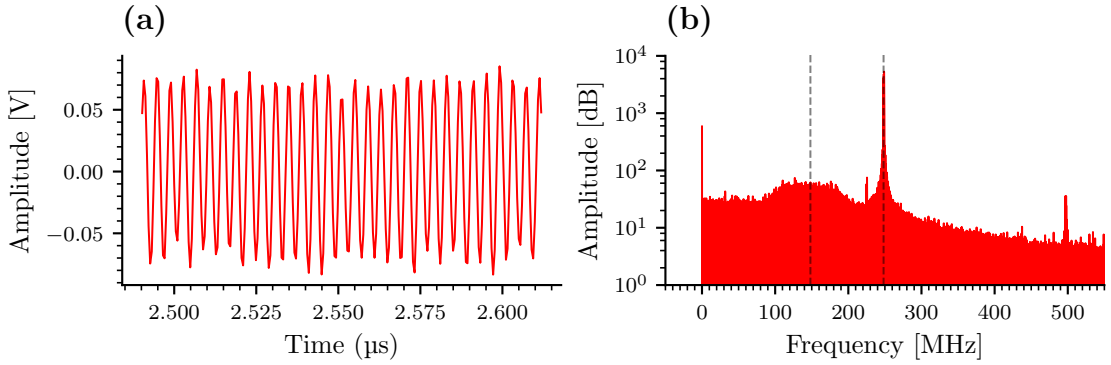

Figure 4.1: Balanced detector output characterization. (a) shows the time-domain signal, zoomed into a random 0.1 µs time window. (b) shows the frequency-domain representation of the same signal. The dashed lines in the frequency spectrum correspond to the symbol band and the pilot tone, respectively.

Once the signal is digitized, it is processed using the low-complexity heterodyne

detection method [26], which can be summarized as calculating the digital local oscillator frequency that will shift the intermediate frequency to the baseband. To do this, it is sufficient to measure the frequency at which the pilot tone is located, which we can temporarily denote as f, and subtract the frequency at which the pilot tone was generated by Alice, f_p, so that the intermediate frequency is $\omega_{\mathrm{IF}} = 2\pi(f - f_p)$. Once this intermediate frequency is known, we multiply the signal at the output of the balanced detector, $V(t)$, by a sinusoidal signal of this intermediate frequency and then filter the result with a low-pass filter to obtain only the symbol signal shifted to the baseband, without the pilot tone or any other mirrored signal.

This signal, acquired with a sampling frequency $f_s = 2$ GSa/s, is resampled at the same symbol frequency at which it was generated, $f_{\mathrm{sym}} = 100$ MBd. This consists of sampling the signal every $T_s = 1/f_{\mathrm{sym}}$, saving its value. These values can then be compared with Alice's random key values by calculating their correlation.

In Figure 4.2, a portion of the transmitted (Tx) and received (Rx) data signals is shown for both the I quadrature and the Q quadrature. The sampling points are also shown. Finally, the result of the correlation between blocks of 10 sampled symbols over the entire signal duration is shown. This way, it is possible to analyze how the correlation between transmitted and received symbols changes over the entire signal duration.

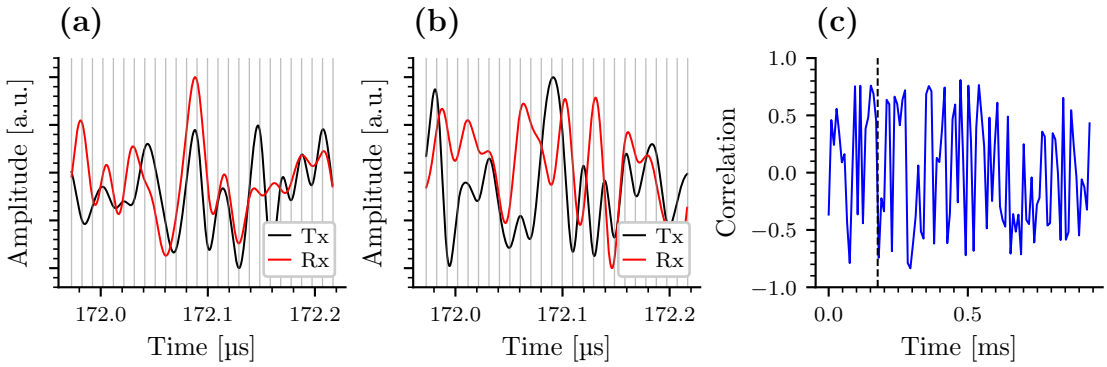

Figure 4.2: Signal demodulation using a low-complexity heterodyne detection method with direct frequency down-conversion. (a) shows the I quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (b) shows the Q quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (c) shows the evolution of the correlation between running blocks of 10 sampled symbols over the entire signal duration.

It is observed that the correlation changes randomly over time, so we cannot extract any key from this transmission. In Section 3.2.1, we analyzed the random behavior of the frequency of the two lasers and saw that during the time the

signal lasts, almost 1 ms, the frequency can change by several MHz. This means that demodulating the signal directly with a single fixed frequency, ω_{IF}, results in incorrect demodulation, as the frequency is not exactly ω_{IF} all the time.

To solve this problem, we can stabilize the lasers, using the pilot tone itself as a frequency reference and applying an electronic control loop to the laser's analog modulation inputs (if this is possible, as not all commercial laser models allow this rapid frequency modulation). This solution seemed complex since it required specific fast electronics for this purpose, and it wasn't easy to find low-cost commercial solutions that could perform this task. Given the difficulties we encountered with this solution, we opted for a software solution, designing an algorithm to recover the signal regardless of the random fluctuations in the lasers, using the pilot tone to measure the frequency and undo all the frequency and phase changes caused by the lasers.

4.1.2 Carrier Recovery Method

Here, we present the algorithm developed in [2], which, along with the experimental demonstration precisely using this algorithm, constitutes the main development of this thesis.

The main idea of the algorithm is to use only the received signal and the pilot tone to undo all frequency changes in the data signal. We start from the fact that the random frequency and phase fluctuations of the lasers will equally affect both the pilot tone and the data signal, as both are modulated on the optical carrier, which is what changes in frequency and phase. Based on this, our goal is to extract the exact intermediate frequency at each moment throughout the duration of the entire signal, $\omega_{\text{IF}}(t)$, to demodulate each symbol with the correct frequency and phase.

To extract what would be a sinusoidal signal of frequency $\omega_{\text{IF}}(t)$, we need to isolate the pilot tone and down-convert it to exactly $\omega_{\text{IF}}(t)$, as the pilot tone is placed at $\omega_{\text{IF}}(t) + \omega_p$. To do this, we multiply the signal $V(t)$ by a sinusoidal signal of frequency ω_p and then filter it with a band-pass filter within the frequency range where the pilot is measured (its location can be determined by finding the maximum of the FFT to center the band-pass filter). Subsequently, this filtered signal, which is already a sinusoidal signal of frequency $\omega_{\text{IF}}(t)$, is directly multiplied by $V(t)$ to obtain $V_{\text{IQ}}(t)$ after applying a low-pass filter to retain only the data band. The schematic of the algorithm is shown in Figure 4.3.

To illustrate how this method is useful for recovering phase and frequency fluctuations, let us assume, based on the spectrum of Figure 4.1b, that the signal $V(t)$

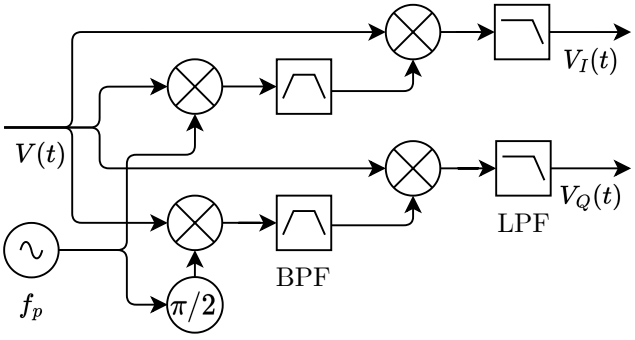

Figure 4.3: Block diagram of the pilot-assisted frequency-locking method. The input signal $V(t)$ is mixed with a signal of frequency f_p and its quadrature counterpart of $\pi/2$ phase shift. The outputs are then passed through Band-Pass Filters (BPF) and Low-Pass Filters (LPF) to produce the in-phase component $V_I(t)$ and quadrature component $V_Q(t)$, respectively.

at the output of the balanced detector can be described by a real signal similar to

$$V(t) \propto \cos(\Omega(t))\,\mathrm{Re}\{S_{\mathrm{IQ}}(t)\} - \sin(\Omega(t))\,\mathrm{Im}\{S_{\mathrm{IQ}}(t)\} + V_p\cos(\Omega(t)+\omega_p t), \quad (4.1)$$

where $S_{\mathrm{IQ}}(t)$ is the modulating signal sent by Alice and defined by Equation (3.27), ω_p is the pilot tone frequency, and $\Omega(t) = \omega_{\mathrm{IF}}(t)t + \delta(t)$, where $\delta(t)$ represents the phase difference between Alice and Bob's lasers. This result can be derived by introducing Equation (3.29) into Equation (3.32), using the approximation from Equation (3.35), and replacing the constant frequency term ω_{IF} by the drifting term $\Omega(t)$.

After $V(t)$ is digitized, it is multiplied by $e^{i\omega_p t}$. Thus, we get a resulting signal with multiple frequency components that can be expressed as

$$V(t)e^{i\omega_p t} \propto S^*_{\mathrm{IQ}}(t)e^{-i(\Omega(t)-\omega_p t)} + S_{\mathrm{IQ}}(t)e^{i(\Omega(t)+\omega_p t)} + V_p e^{i(\Omega(t)+2\omega_p t)} + V_p e^{-i\Omega(t)}. \quad (4.2)$$

After filtering it to retain only the component near the $\omega_{\mathrm{IF}}(t)$ region with a band-pass filter (BPF), the result is only the last term. So we define the displaced pilot signal $P_{\mathrm{IQ}}(t)$ as:

$$\left(h_b * \left(V(t)e^{i\omega_p t}\right)\right)(t) \propto e^{-i\Omega(t)}, \quad P_{\mathrm{IQ}}(t) = e^{-i\Omega(t)}, \quad (4.3)$$

where $h_b(t)$ is the response function for a Butterworth band-pass filter. This signal is multiplied again by $V(t)$ again and the result is

$$V(t)P_{\mathrm{IQ}}(t) \propto V_p e^{i\omega_p t} + V_p e^{-i(2\Omega(t)+\omega_p t)} + S^*_{\mathrm{IQ}}(t)e^{-2i\Omega(t)} + S_{\mathrm{IQ}}(t). \quad (4.4)$$

After that, this result is filtered using a low-pass filter (LPF) to eliminate all terms with higher frequencies than the symbol frequency, keeping only the last

term, which corresponds to the modulating signal sent by Alice. The outcome thus obtained is

$$V_{\mathrm{IQ}}(t) = \left(h_l * \left(V(t)P_{\mathrm{IQ}}(t)\right)\right)(t) \propto S_{\mathrm{IQ}}(t), \tag{4.5}$$

where $h_l(t)$ is the response function for a Butterworth low-pass filter. It follows from the above reasoning that the method eliminates all frequency and phase dependences in the demodulated signal, and the signal for the symbol band on Bob's side, $V_{\mathrm{IQ}}(t)$, is proportional to that on Alice's side $S_{\mathrm{IQ}}(t)$, regarding frequency and phase terms and ignoring all scaling or amplitude terms.

Regarding the correction of phase differences, this is an important result, as we observed in several experiments that changes in temperature and mechanical vibrations in different components caused slow phase shifts in the optical fibers, affecting both lasers differently and randomly. As long as the phase difference is consistent across all frequency components, it can be effectively removed using this method.

It is important to note that drifts are corrected upon the complete acquisition of the signal. Therefore, the detector's bandwidth must exceed the amplitude of random drifts. Once the detector fully acquires the signal, this method becomes entirely independent of experimental parameters and imperfections, as shown in the previous equations. This independence extends to factors such as the speed and amplitude of random frequency drifts, providing a highly effective and lightweight solution for addressing laser drift corrections.

After the mathematical demonstration of the principles of the frequency-locking method, we can see how it is implemented step by step in a real experimental signal acquired at the output of the balanced detector, as shown in Figure 4.4.

As long as the pilot tone is within the band-pass filter window, there will be no problem in recovering the data signal and centering it in the baseband. If we now repeat Figure 4.2 but using this new algorithm for demodulation, as shown in Figure 4.5, we see that the result improves significantly.

Although the correlation fluctuates and is not always high, it does so in a sinusoidal pattern rather than chaotically. This slow fluctuation is likely caused by a phase difference, possibly resulting from accumulated phase shifts between the symbol band and the pilot tone. Potential causes include a mismatch in the sampling frequencies of the DAC and ADC or other sampling and timing issues in the signal generation and acquisition devices. While we have not investigated the exact cause of this phase shift in detail, since we are using digital signal processing algorithms for signal recovery, we can apply a phase correction to address this issue.

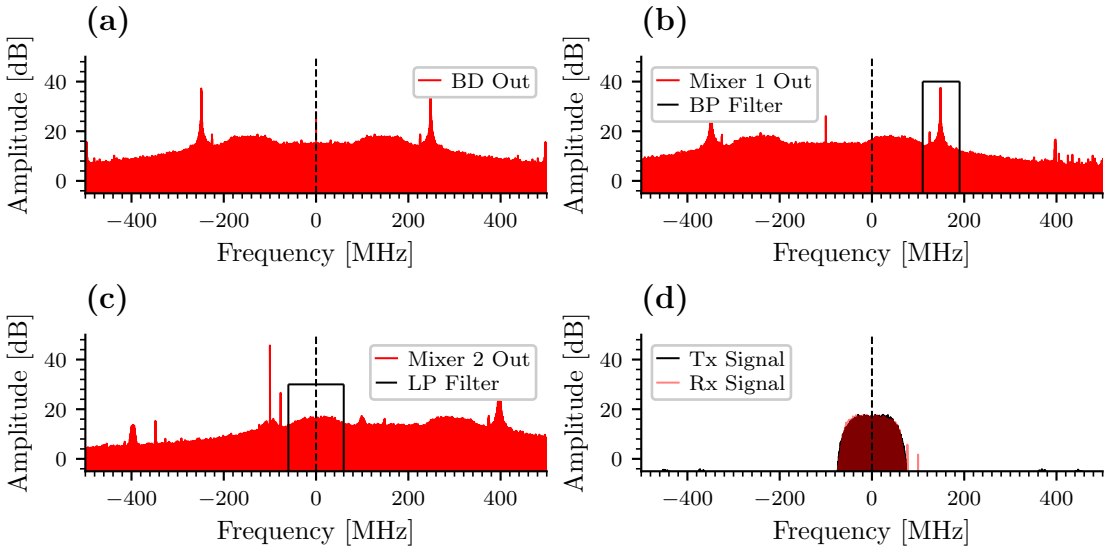

Figure 4.4: Step-by-step demonstration of the pilot-assisted frequency-locking method. (a) shows the output of the balanced detector in the frequency domain. (b) displays the output of the first mixers and the Band-Pass Filter window. (c) shows the output of the second mixer and the Low-Pass Filter window. (d) compares the transmitted and received symbol signals in the frequency domain, illustrating the effectiveness of the frequency-locking process.

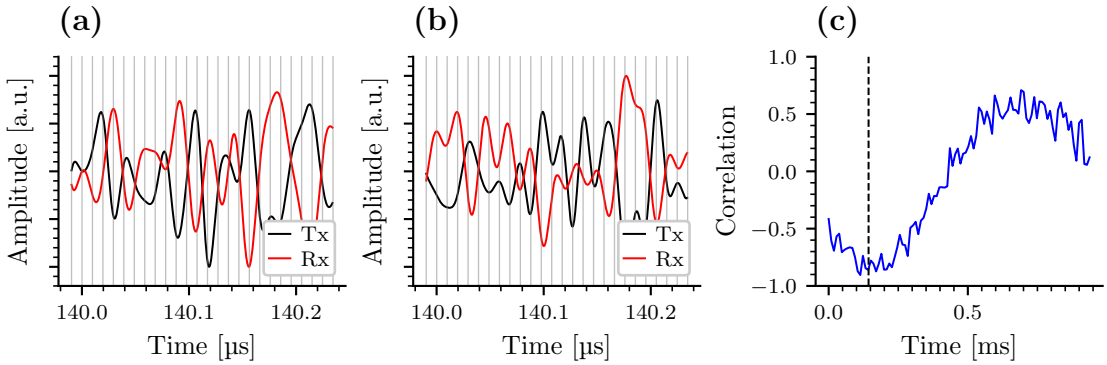

Figure 4.5: Signal demodulation using a low-complexity heterodyne detection method with the pilot-assisted frequency-locking method. (a) shows the I quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (b) shows the Q quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (c) shows the evolution of the correlation between running blocks of 10 sampled symbols over the entire signal duration.

4.1.3 Phase Recovery Method

To resolve the phase shift problem, we choose several areas randomly throughout the signal. Specifically, after sampling the signal obtained by applying the algorithm from the previous section, V_{IQ}, we obtain a complex symbol vector, y, from

which we choose m random symbols y_{PE} within the symbols sent by Alice, which are then shared over the public channel for parameter estimation. Subsequently, the same symbols from Alice, x_{PE}, are selected. Then, using any conventional optimization algorithm, we maximize the correlation between Alice's symbols and the symbols obtained by Bob after sampling but applying a phase shift.

After applying the phase shift that maximizes the correlation to the V_{IQ} signal obtained in Figure 4.5, we manage to eliminate the constant phase shift, thereby obtaining an even cleaner signal that always maintains a high correlation, as seen in Figure 4.6.

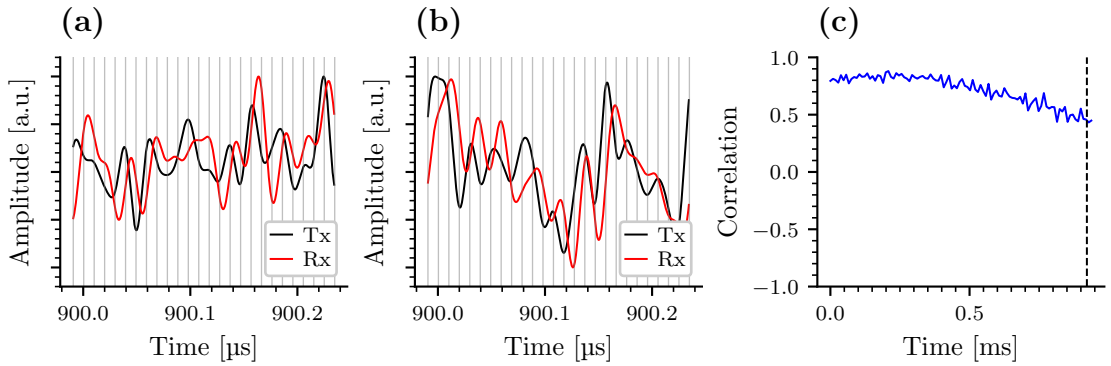

Figure 4.6: Signal demodulation using a low-complexity heterodyne detection method with the pilot-assisted frequency-locking method and the phase recovery algorithm. (a) shows the I quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (b) shows the Q quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (c) shows the evolution of the correlation between running blocks of 10 sampled symbols over the entire signal duration.

We can see that it is almost corrected, but there is still an issue as the correlation progressively decreases over time. If we analyze Figure 4.6a and Figure 4.6b, which show the transmitted and received signals at the end of the signal, we see that the problem is that they are time-shifted, even though their frequency and phase have been fixed. This is likely caused because Alice and Bob have different clocks in their DACs and ADCs, respectively, when sampling the signals, and one clock drifts with respect to the other.

4.1.4 Clock Recovery Method

To solve the clock problem, we implement an algorithm that detects the beginning and end of the signal $V(t)$ at the output of the balanced detector, using the same procedure as in a voltage trigger, but for both the beginning and end of $V(t)$. Once the beginning and end of the signal are detected, the signal is resampled to

have the same number of samples as those sent by Alice to match exactly with her time scale. Once this is done, the frequency locking and phase recovery methods previously described are applied, and we see that the problem disappears and the correlation remains high during all the signal duration, as shown in Figure 4.7.

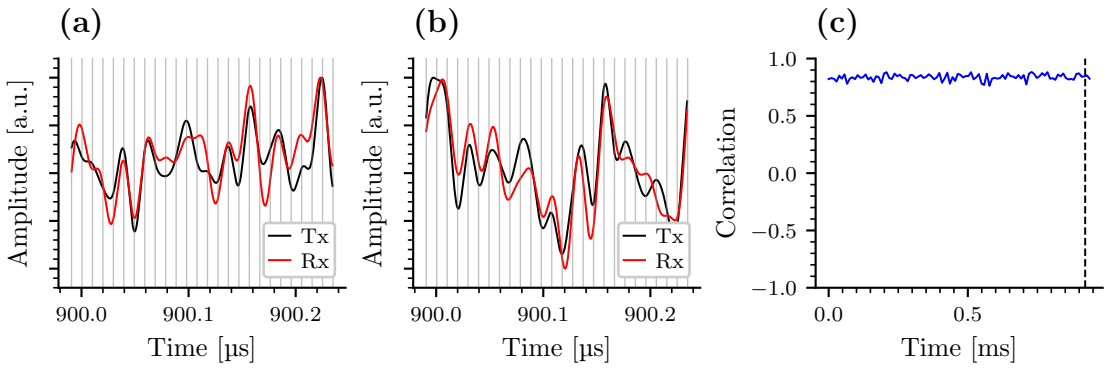

Figure 4.7: Signal demodulation using a low-complexity heterodyne detection method with the pilot-assisted frequency-locking method, the phase recovery algorithm, and the clock recovery algorithm. (a) shows the I quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (b) shows the Q quadrature of Rx and Tx data signals with the sampling time points plotted on a grid. (c) shows the evolution of the correlation between running blocks of 10 sampled symbols over the entire signal duration.

Time resampling is a very simple method but is proven to be effective in this case. It corrects the temporal drifts in Alice and Bob's clocks. Once this is done, it can be concluded that Bob has correctly recovered the time scale, frequency, and phase of the carrier and correctly demodulated the signal.

4.2 Upgrades to the Experimental Implementation

In this section, we present different enhancements made to our experimental system prior to conducting the final experiments to increase the system's robustness and stability while automating the measurements. We begin by detailing the power calibration and polarization correction algorithms, essential for automating the entire system setup process. Finally, the real-time shot noise estimation algorithm is explained.

4.2.1 Power Control Algorithm

To maintain the optical power at Alice's output at the desired level, so far, while using the experimental setup in Figure 3.15, we manually calibrated the attenuation on the VOA until achieving the desired power on the power meter, using

Equation (3.9). The problem, aside from requiring inaccurate and slow manual intervention, is that the output power varies slowly over time. Therefore, it is necessary to implement automatic power control. To do this, we replaced the manual attenuator with the voltage-controlled electronic attenuator characterized in Figure 3.14b and connected both the attenuator and the power meter to a microcontroller that implements the power control algorithm. This setup is shown in Figure 4.8.

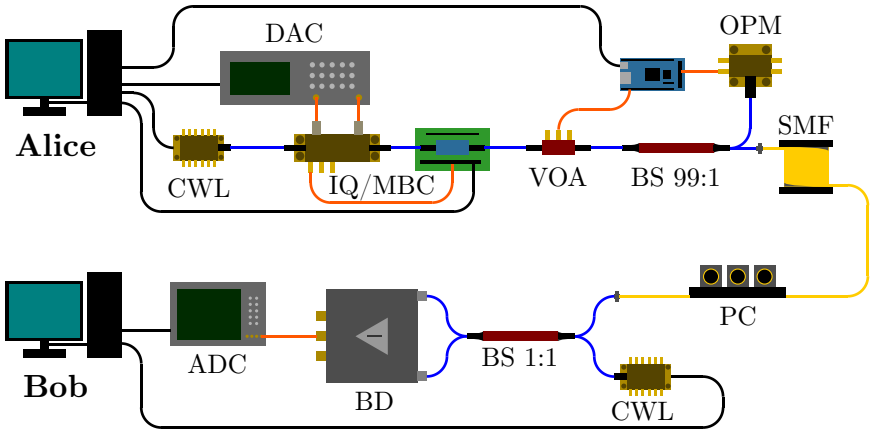

Figure 4.8: Experimental setup of the CV-QKD with LLO implementation, including an automatic power control system. A microcontroller is used to maintain constant output power at the desired modulation variance level.

The implemented algorithm consists of a PID (Proportional, Integral, and Derivative) controller, a control algorithm to maintain a variable at a desired value. This algorithm adjusts the system output based on three terms that depend on the error (the difference between the current value and the desired value of the controlled variable). The first term is proportional to the error signal; thus, the correction will also increase if the error increases. This term is expressed as

$$P = K_p e(t), \tag{4.6}$$

where K_p is the proportional term constant, $e(t) = f(t) - f_t$ with $f(t)$ being the controlled variable at time t, and f_t being the desired value for the controlled variable. On the other hand, the integral term is defined as

$$I = K_i \int_0^t e(\tau)\,\mathrm{d}\tau\,, \tag{4.7}$$

where K_i is the integral term constant. The aim of this term is to eliminate the accumulated error that may persist when using only proportional control. Lastly,

the derivative term is defined as

$$D = K_d \frac{\mathrm{d}e(t)}{\mathrm{d}t}, \tag{4.8}$$

where K_d is the derivative term constant. This term provides corrective action proportional to the rate of change of the error and helps anticipate the future behavior of the error to improve system stability.

With this algorithm implemented on the microcontroller, we managed to set the power to the desired value in about 1 s, with an average error of 1 %. Before sending a signal with the key by Alice, this algorithm must be executed and then immediately continue with the rest of the control algorithms and the key transmission.

4.2.2 Polarization Correction Algorithm

Another control that we previously performed manually was polarization control. We would arbitrarily adjust the three axes until finding the configuration (or one of them) that maximized the signal amplitude at the balanced detector output. The next natural step in the system's evolution was to automate this process. To achieve this, we replaced the manual polarization controller with the electronic one, also controlled by a microcontroller, leaving the experimental setup as shown in Figure 4.9.

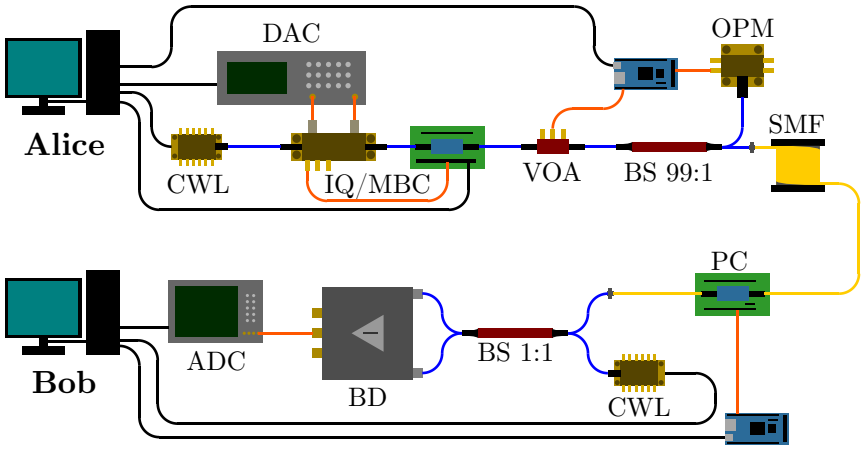

Figure 4.9: Experimental setup of the CV-QKD with LLO implementation, including an automatic polarization correction system. A microcontroller is used to align the incoming field and the local oscillator polarizations to maximize detection efficiency.

In this case, the microcontroller does not execute any control algorithms because the amplitude reading of the signal at the output of the balanced detector, which

is the function to maximize, is on the computer connected to the oscilloscope that acquires this signal. In this scenario, the microcontroller acts as a bridge to translate the values calculated by the computer into the polarization controller's axis positions and the digital signals required by the polarization controller board.

The polarization controller is programmed by sending TTL digital signals to 16 pins. The first two pins determine the axis to act on. The next pin is for read/write. The subsequent pin is for resetting to default values. Finally, the last 12 pins represent a 12-bit integer (a value between 0 and 4095) corresponding to the voltage to be applied to the piezoelectric element that deforms the fiber along the respective axis, where 0 is minimum voltage, and 4095 is maximum (in this case, 150 V).

Thus, from the computer, we directly send to the microcontroller the axis on which we want to act and the value between 0 and 4095. The microcontroller then generates the TTL digital signals and sends them to the polarization controller. The maximization algorithm we implemented can be divided into two parts. First, a coarse search brute force algorithm is implemented to find the zone that maximizes the signal amplitude at the output of the balanced detector. When this value is found, a second faster algorithm runs before each transmission, increasing or lowering each channel voltage until maximizing the amplitude to correct small polarization deviations between different transmissions.

With this, we can maintain the signal amplitude maximized when polarization slightly varies across the channel. This algorithm executes just before signal transmission because, within a few seconds, polarization can change more than the power or coarse frequency of the lasers. Therefore, as soon as the amplitude is maximized by varying polarization, the transmission of the signal containing the key information occurs. It is important to note that all these calibration algorithms are performed with a calibration signal similar to the key signal, which is discarded and does not form part of the final key.

4.2.3 SNU Estimation

Apart from these correction algorithms, we also need to accurately estimate the shot noise, as it varies over time. Just as Alice's laser power fluctuates with temperature, Bob's laser power also varies, and a variation in the local oscillator power results in an incorrect SNU estimation. Additionally, the noise level of the balanced detector varies, causing fluctuations in electronic noise estimation.

To address this issue, although there are methods to calibrate SNU in real-time parallel to signal transmission, due to complexity, we opt for a step-by-step calibration based on optical shutters [25], which is described in Appendix A. Before receiving the signal, we block the channel input signal and measure the output vari-

ance from the balanced detector, V_{LO}. Immediately after that, we turn off Bob's laser and measure the electronic noise variance V_{el}, obtaining the SNU equivalence $\phi = V_{LO} - V_{el}$. We also derive the electronic noise variance expressed in SNU, $\nu_{\text{el}} = V_{el}/\phi$. Note that this procedure is susceptible to attacks as the calibration and key states are different, and an eavesdropper could hack the SNU calibration step in a way that Alice and Bob then overestimate the security in the Parameter Estimation step [184]. We choose this implementation for simplicity, to focus on other aspects of the experimental setup. Our setup with the optical shutter is depicted in Figure 4.10.

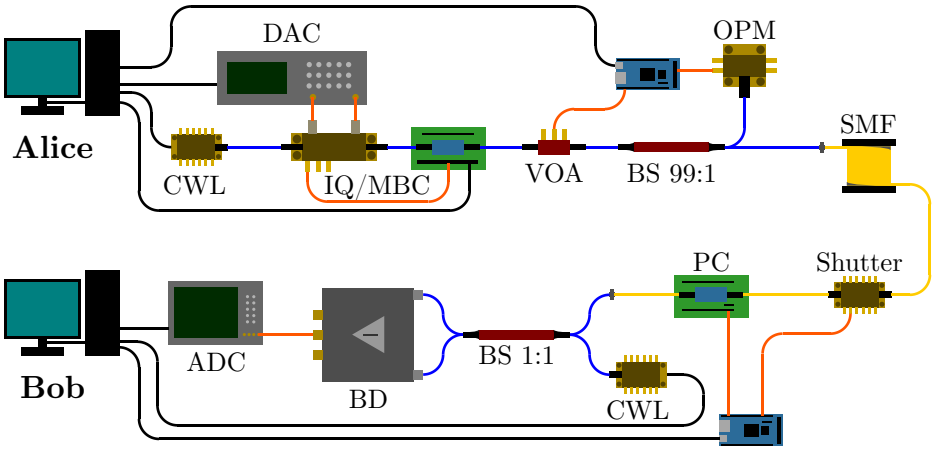

Figure 4.10: Experimental setup of the CV-QKD with LLO implementation, including an automatic SNU estimation system. A microcontroller is used to temporarily shut off the quantum signal input to measure the shot noise accurately.

This shot noise estimation must be performed before each key transmission. The conversion between values measured by the oscilloscope and SNU is determined by this measurement. A poor shot noise calibration can lead to inaccurate channel transmittance estimation and, consequently, to an inaccurate secret key rate estimation, as discussed in Section 2.3.

4.2.4 Final Experimental Setup

The last task that needs to be addressed before conducting any experimental CV-QKD transmission is isolating Alice's output and Bob's input, ensuring that light travels following a specific direction.

The first reason for this isolation is security-related, as an attacker could manipulate the transmitter's equipment directly by injecting a signal from the channel. It also prevents light from being back-reflected into Alice's or Bob's setups.

To address this problem, one option is to use optical isolators, which are devices that only allow light to pass in one direction, similar to a diode in electronics but for light. However, we opted to use circulators instead. A circulator is a device with three channels, where light entering channel 1 exits through channel 2, and light entering channel 2 exits through channel 3 instead of returning to channel 1. The setup is shown in Figure 4.11.

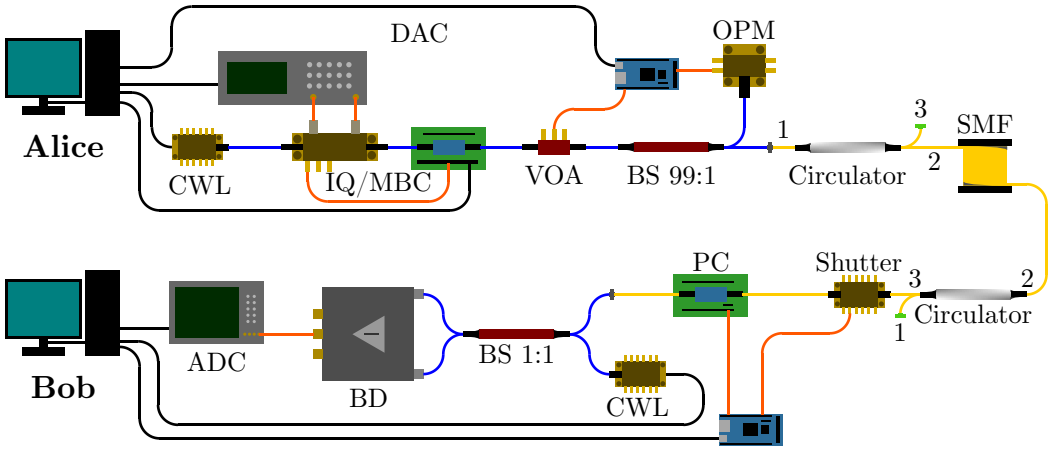

Figure 4.11: Complete experimental setup of the CV-QKD with LLO implementation, including circulators to isolate light in undesired directions. This setup was used for the experimental transmission demonstrations described in Section 4.3. It includes the power, polarization, and SNU estimation algorithms to automate the calibration process for each experimental transmission.

This setup ensures that no light exits the circulator through channel 1 and no light enters the circulator through channel 3, while channel 2 allows light in both directions. It is also ideal for implementing a transceiver in the future, consisting of combined Alice's and Bob's hardware, where light leaving the transmitter hardware is directed into the channel by the circulator, and light coming from the channel is directed to the receiver hardware by the circulator.

4.3 Results and Real-World Use Cases

This section presents the results of the experimental transmissions carried out using the frequency-locking algorithm introduced in Section 4.1. We conclude by describing several real-world use case experiments conducted with this experimental setup, including the implementation of the classical channel in standard fiber infrastructure, the development of Field Programmable Gate Arrays (FPGAs) to replace laboratory signal generation and acquisition instruments, and the demonstration of two real-world use cases for encryption using keys distilled from our

CV-QKD system.

4.3.1 Experimental Demonstration

In what follows, we verify the efficacy of the frequency-locking method and all the previous experimental implementation control algorithms by using them to perform an experimental transmission. These results were presented in [2].

Following demodulation, the security of the transmission is assessed. To achieve this, the channel noise parameters (the transmittance and the excess noise) are estimated based on the relationship between the transmitted symbols, x, and the received symbols, y, as described in Section 2.3.2. In the finite-size regime, that can be achieved by computing the maximum likelihood estimators for the channel transmittance, $\hat{T}$, and excess noise, $\hat{\xi}$ as in Equation (2.84). The estimator for the channel transmittance is thus given by

$$\hat{T} = \frac{1}{\eta}\left(\frac{\mathrm{cov}(x,y)}{\mathrm{var}(x)}\right)^2. \tag{4.9}$$

This estimator represents the covariance between x and y divided by the variance of x, scaled by the detection efficiency η. On the other hand, the excess noise is estimated as

$$\hat{\xi} = \frac{1}{\eta\hat{T}}\left[\frac{1}{2N}\sum_{i=1}^{2N}\left(y_i - \sqrt{\eta\hat{T}}x_i\right)^2 - 1 - \nu_{\mathrm{el}}\right], \tag{4.10}$$

where N stands for the total number of transmitted and received symbols, and ν_{el} represents the electronic noise assumed by Bob in the trusted noise model [158], which corresponds to the electronic noise variance measured as in Appendix A. By estimating transmittance and excess noise in this manner, and by calculating the worst-case scenario estimators T^* and ξ^* from Equation (2.90), we then calculate the worst-case scenario secret key rate K^* as described in Section 2.3. With this, we conduct both quick simulations and experimental transmissions for several increasing channel lengths. The parameters with which the setup was configured for the experimental transmission are listed in Table 4.1.

The experiment, based on the setup introduced in Figure 4.11, consists of sending blocks of 10^6 symbols following a normal distribution, all of which are subsequently filtered with an RCF and encoded in the I and Q quadratures of a 1550 nm C-Band CW tunable laser using an IQ modulator controlled by an arbitrary waveform generator and locked to the operating point by using a MBC. Afterward, the signal is attenuated to the desired modulation variance (the optimal modulation variance for each distance, as shown in Figure 3.25a), and the power is continuously monitored to keep track of such modulation variance in each transmission. The

Parameter	Value
Number of symbols (N)	10^6
Symbol frequency (f_{sym})	100 MHz
Pilot tone frequency (f_p)	100 MHz
Laser frequency (ω_A)	193.5 THz
Local oscillator power (P_B)	10 dBm
Optical fiber attenuation (α)	0.2 dB/km
Detector gain (ρ)	5 V/mW
IQ Modulator half-wave voltage (V_π)	$\approx$ 5.5 V
Electronic noise (ν_{el})	0.1084 SNU
Detector efficiency (η)	0.55
Reconciliation efficiency (β)	0.95
Confidence intervals (ε_{PE})	10^{-10}

Table 4.1: Values of the different parameters used in the experimental transmission and the secret key rate estimation. The values used for the electronic noise and detector efficiency in the security analysis were previously experimentally characterized. The chosen modulation variance V_A is the one that maximizes the SKR for each length, ranging between 2 SNU to 10 SNU, depending on the channel length.

signal is then sent to three different channels of 5 km, 25 km and 50 km, all three of which are commercial Single Mode Fiber (SMF) reels.

At the receiver, the polarization of the incoming laser beam is corrected using a polarization controller to maximize the amplitude of the beam splitter interference with Bob's laser. After the interference, the outputs are measured in a balanced detector, whose subsequent output is acquired using a digital oscilloscope.

Once the acquisition is finished, the signal is processed with the frequency-locking algorithm and afterward sampled to retrieve 10^6 symbols. Half of them will be used as the key and the remaining for parameter estimation. We repeat the experiment for each distance 100 times. The average results obtained for the channel noise parameters and the secret key rate in the worst-case scenario are listed in Table 4.2.

Note that in each of the three experiments, the shot noise is estimated just before each transmission by measuring first the variance of the local oscillator N_0 (by cutting off the channel entrance) and, secondly, the variance of the electronic noise ν_{el} (by switching off Bob's laser). The conversion factor is then given by $\phi = N_0 - \nu_{\text{el}}$.

The estimated SKR for all the experiments is shown in Figure 4.12, along with those results derived from simulations. In detail, such simulations have been car-

L (km)	$\langle T^* \rangle$	$\langle \xi^* \rangle$ (SNU)	$\langle K^* \rangle$ (b/sym)
5	0.83	0.091	0.09180
25	0.30	0.092	0.01030
50	0.09	0.091	0.00072

Table 4.2: Average results for the experimental transmissions, including the finite-size worst-case scenario estimations of channel transmittance, excess noise, and secret key rate across different channel lengths. For each distance, 100 experimental transmissions were conducted, and their average values are presented.

ried out both in the asymptotic regime, for reference, and in the worst-case scenario, considering finite-size effects.

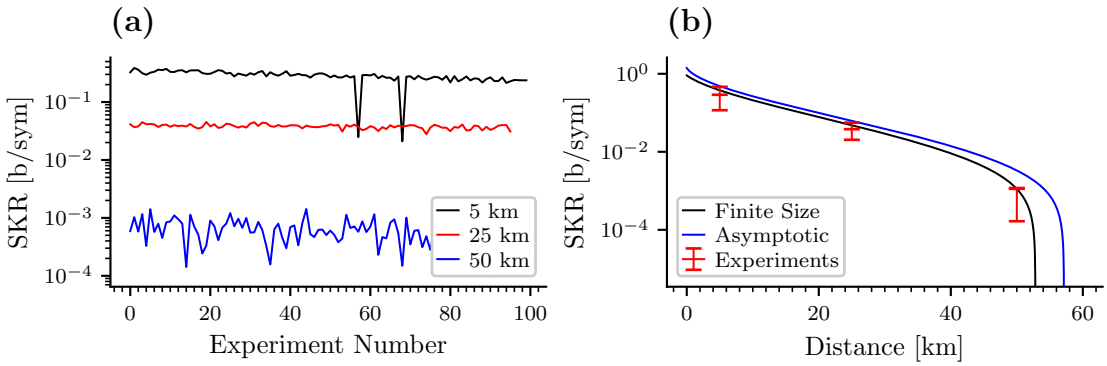

Figure 4.12: Experimental results for 5 km, 25 km, and 50 km, compared with simulations for different distances. (a) shows the SKR for each distance across 100 experiments. (b) compares the experimental results with simulations. The finite-size simulations use 10^6 symbol key blocks and apply the worst-case scenario estimator for transmittance and excess noise, leading to a more realistic estimation of the secret key rate than the asymptotic simulations.

In detail, to perform simulations in the asymptotic limit, the pre-computed transmittance values for each distance have been used, according to the analytic expression $T = 10^{-\alpha L/10}$ for distance L and channel attenuation α. Similarly, $\xi = 0.05$ SNU has been used for the simulations.

For simulations considering finite-size effects, we follow the methods described in [109] with the calculations presented in Section 2.3. We generate blocks of simulated symbols of the same size as those sent in the real transmission, N, of the form $x_i \in \mathcal{CN}(0, V_A)$ for $i = 1, \ldots, N$ following a normal distribution in the complex plane. These elements undergo attenuation due to efficiency and transmittance, as well as noise, as given by Equation (2.58):

$$y = \sqrt{\eta T} x + z, \tag{4.11}$$

where z represents Gaussian noise with zero mean and variance $1 + \xi + \nu_{\text{el}}$, with ν_{el} being the experimentally characterized electronic noise and ξ being the average estimated excess noise in the experiments given in Table 4.2. Afterward, for an error probability of ε_{PE} in the parameter estimation stage, confidence intervals for the transmittance and the excess noise from Equation (2.87) are thus given by

$$\Delta t = z_{\text{PE}}\sqrt{\frac{\sigma^2}{2NV_A}}, \quad \Delta\sigma^2 = \frac{z_{\text{PE}}\sigma^2}{\sqrt{N}}, \tag{4.12}$$

where z_{PE} is given by Equation (2.88) and where $\sigma^2 = \eta T\xi + 1 + \nu_{\text{el}}$. The worst-case estimator for the transmittance and the excess noise is given by Equation (2.90), and it can be expressed as

$$T^* = \frac{1}{\eta}\left(\sqrt{\eta T} - \Delta t\right)^2, \quad \xi^* = \frac{1}{\eta T^*}(\sigma^2 + \Delta\sigma - 1 - \nu_{\text{el}}). \tag{4.13}$$

Using these two estimators for the main channel noise parameters, we then estimate the secret key rate according to the expression given in Equation (2.91), multiplying it by the symbol frequency f_s to get the actual secret key rate expressed in b/s,

$$K^* = f_s\frac{N-m}{N}(\beta I_{\text{AB}} - \chi_{\text{BE}}), \tag{4.14}$$

where N is the length of the total sent and received symbols, including the key and PE instances per block, and m is the number of PE instances per block. The final results for the potential SKR that could be achieved using our system (assuming reconciliation is processed in real-time) are shown in Table 4.3.

L	5 km	25 km	50 km
SKR	9.18 Mb/s	1.03 Mb/s	72 kb/s

Table 4.3: Average results for the potential secret key rate in the experimental transmissions, expressed in b/s. Note that we are not considering the time required for post-processing or key reconciliation, which is later processed offline.

4.3.2 Real-World Use Cases

Finally, after successfully completing the experimental transmission, we implemented additional hardware improvements to bring the system closer to a commercially viable prototype suitable for real-world use cases. This includes implementing a classical communication channel for every communication except the transmission of the encryption key itself, as well as integrating signal generation, acquisition, and processing in FPGAs.

Then, we carried out demonstrations for real-world use cases to finalize the development of the experimental system and validate its feasibility in practical environments. After completing the experimental transmission and parameter estimation, we performed the classical post-processing for reconciliation to distill the key, as explained in Appendix B. This distilled key was then applied to the different demonstrated use cases, such as the deployment of a QKD-encrypted VPN or the simulation of the system integration into an externally managed QKD network.

With these demonstrations, all the work related to this thesis is concluded, proving the system's functionality and viability in real-world environments, and proving that it operates as intended for its designed purpose.

Classical Channel Implementation

In all previous chapters, we have discussed that Alice and Bob share certain information over a public channel, such as calibration information, control commands, or the portion of the key intended for parameter estimation. Since this channel is public, everything that happens on it can be listened to by Eve without compromising the transmission's security. However, for a practical implementation in a real system, it is better to design the system to account for this public channel, which does not need to be encrypted and can be implemented classically with standard commercial hardware.

Note that although the public channel does not need to be encrypted, it does need to be authenticated. This requirement stems from the fact that while encryption ensures the confidentiality of transmitted data, authentication guarantees that a third party has not altered the communication. In QKD, an unauthenticated classic channel could allow an attacker to impersonate one of the legitimate parties, compromising the protocol's security. Authentication mechanisms [108] are therefore critical to ensure that the information exchanged is genuine and that the integrity of the quantum communication process is maintained.

This channel could be an Internet connection at Alice's and another at Bob's, allowing them to communicate over the Internet. However, for practicality, since there must be a fiber between Alice and Bob for the quantum channel, it is most convenient to use it for implementing classical communications on the same fiber as the quantum channel. The way to do this is to multiplex the quantum and classical channels with a Wavelength Division Multiplexer (WDM) and implement the classical channel with a Small Form-factor Pluggable (SFP) optical transceiver, a standard device for classical fiber optic communications widely used in commercial networks. The setup can be seen in Figure 4.13.

This setup has been tested in the laboratory with a commercial WDM, which has

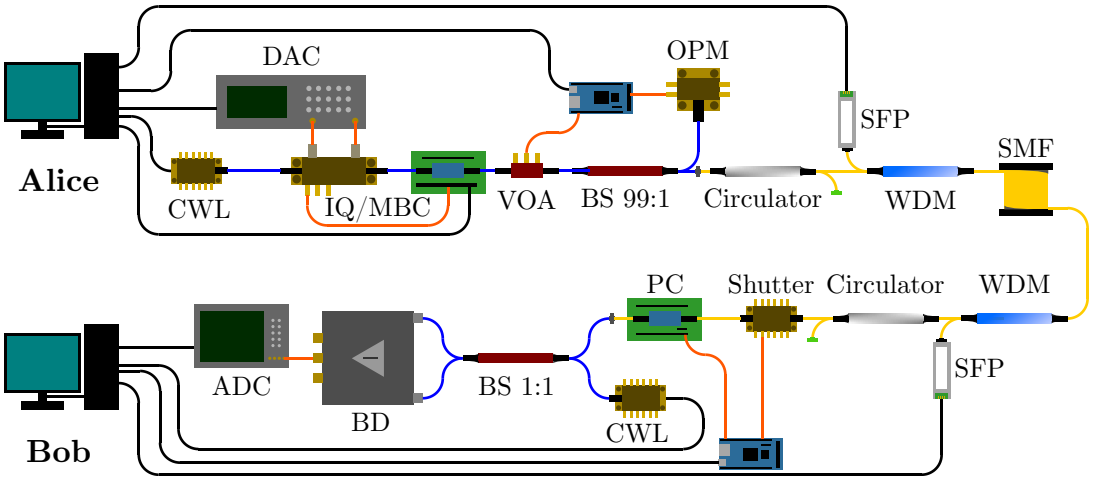

Figure 4.13: Complete experimental setup of the CV-QKD with LLO implementation, upgraded to deploy the classical channel over the same fiber as the quantum channel. This is accomplished by implementing the classical channel with Small Form-factor Pluggable optical transceivers (SFP) and using Wavelength Division Multiplexers (WDM) to separate the classical 1300 nm channel from the quantum 1550 nm channel.

a channel of (1300 ± 15) nm and another of (1550 ± 15) nm, and isolation of 15 dB, which is the ratio between the transmitted or received power in the undesired channel and the transmitted or received power in the desired channel. For the SFP, we use two bidirectional transceivers, which multiplex a 1330 nm channel and a 1270 nm channel to implement the uplink and downlink in a single fiber. Since the WDMs have a bandwidth of (1300 ± 15) nm for the classical channel, the SFP's light falls outside this bandwidth, but since the isolation is relatively low, it is sufficient to reduce the SFP's attenuation to compensate for the losses due to the WDM bandwidth.

The main advantage of using an SFP is that we can connect it directly to the computer through a standard network card, and once this is done, we can implement any communication based on the TCP/IP protocol, which is standard and robust. This way, we solve two problems at once. On the one hand, we use the existing fiber, allowing the system to function even if there is no Internet connection. At the same time, we avoid any problems in implementing the classical channel by using standard equipment.

Finally, it is verified in the laboratory that regardless of the distance used, the 1550 nm signal containing the quantum key and the 1300 nm signal used by the SFP can be multiplexed correctly, making simultaneous transmissions of classical and quantum data without affecting the secret key rate. The fact that the isolation is only 15 dB is not a problem for coherent detection, given how far the 1300 nm

band is from the 1550 nm band in the frequency spectrum (37 THz) compared to the balanced detector's bandwidth (400 MHz). That is, the noisy band of the classical channel is 37 THz away from the classical channel, so the optical down-conversion performed in Bob's beam splitter that brings the 1550 nm band down to baseband would bring the 1300 nm band at 37 THz away from the baseband, which would be completely filtered out by the detector bandwidth.

The only drawbacks observed from this classical channel implementation are the losses introduced by the connectors between the WDM and the channel, with insertion losses of 0.5 dB each, and by the WDM itself, which has an insertion loss of 0.3 dB. Adding two more connectors (one at Alice and one at Bob) and two WDMs results in an additional 1.6 dB loss, equivalent to 8 km of fiber. This is the cost of using the same fiber for both the classical and quantum channels. In practice, most of the time, it will be possible to send the quantum channel through one fiber and the classical channel through another, as fiber cables often have between 2 and 8 fibers together. Still, if there were only one fiber, it would be possible to use it for both channels with this setup.

There are studies [15] about multiplexing classical and quantum channels into multicore fibers to add up the secret key rate of a single fiber through all the cable fiber cores and also use all these cores to multiplex high-speed classical signals. Also, a CV-QKD transmission over a 25 km fiber coexisting with classical traffic using a similar wavelength division multiplexing technique has been demonstrated [67].

FPGA Implementation

Implementing a CV-QKD system using FPGAs (Field Programmable Gate Array) represents a significant advancement over the current setup, which uses a computer and an Arbitrary Waveform Generator (AWG) at Alice and a computer and a digital oscilloscope at Bob. Replacing these devices with two FPGAs, particularly with RFSoC (Radio Frequency System-on-Chip) devices, offers several advantages that can improve the performance and efficiency of the CV-QKD system.

First, one of the most notable advantages of RFSoC FPGAs is the integration of high-speed Digital-to-Analog Converters (DAC) and Analog-to-Digital Converters (ADC) directly on the chip. This feature eliminates the need for external equipment such as the AWG and oscilloscope, which not only reduces the physical space required for the system but also minimizes signal processing latency and the total cost of the equipment. With integrated converters, the synchronization and efficiency of the system improve significantly, as the signals do not need to be transmitted between separate devices. Another significant advantage of FPGAs is

their capability for parallel processing. Unlike conventional processors, which typically execute instructions sequentially, FPGAs can perform multiple operations simultaneously. This parallel processing capability greatly increases the speed of algorithms necessary for CV-QKD, such as all the digital signal processing and error correction algorithms.

Despite these advantages, implementing CV-QKD systems on RFSoC FPGAs also has several challenges and disadvantages. One of the main drawbacks is the complexity of development. Programming and configuring FPGAs require specialized knowledge in hardware description languages like VHDL or Verilog. Designing and optimizing algorithms for implementation on FPGAs can be more complex and time-consuming than software-based systems. Additionally, although FPGAs are reconfigurable, they are limited by the physical resources available on the chip. Unlike software-based systems that can be easily scaled with additional hardware, FPGAs have a limit regarding logic gates, memory, and processing capacity. This limitation can restrict the system's expandability and require highly optimized design to maximize the use of available resources.

That said, we explored the integration of FPGAs in the experimental system, acquiring two RFSoC FPGA evaluation boards. The experimental setup after replacing the AWG and the oscilloscope with these two FPGA boards is shown in Figure 4.14.

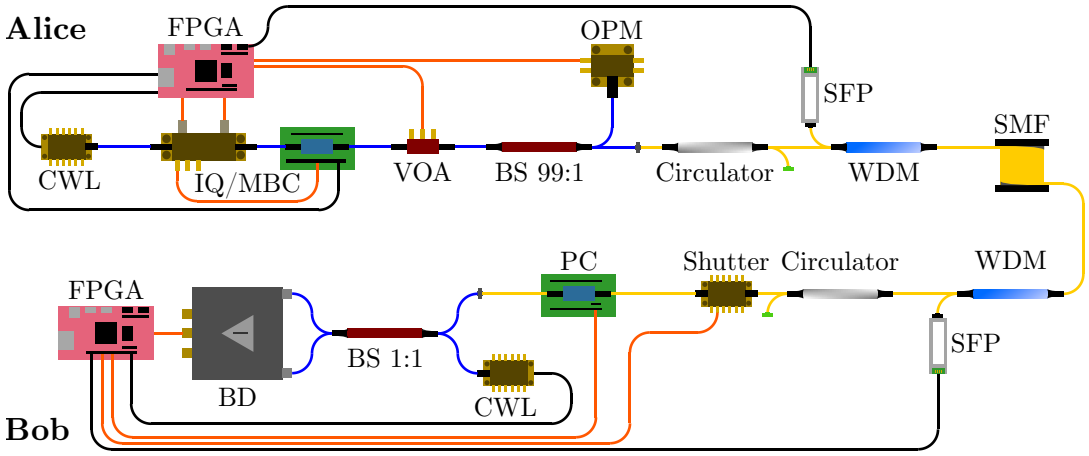

Figure 4.14: Complete experimental setup of the CV-QKD with LLO implementation, upgraded to replace the signal generation and acquisition electronics (including the arbitrary waveform generator, oscilloscope, computers, and all microcontrollers used for power, polarization, and SNU estimation algorithms) with Field Programmable Gate Arrays (FPGAs).

These FPGAs feature 8 ADCs with 12-bit resolution operating at 4 GSa/s and 8 DACs with 14-bit resolution operating at 6.5 GSa/s. It also has specialized hardware for parallelizing error correction algorithms and two ARM-type processors to

run Linux on the board and control the programmable logic from there, managing high-level programs or communications and interfaces from within the board without a computer.

After a challenging hardware design process, we concluded that we can successfully transmit and demodulate the necessary signals using the FPGA's DACs and ADCs. The correlation results between x and y were similar to those obtained with the oscilloscope and AWG, confirming the feasibility of this implementation. Despite the complexity of the development, we found this implementation to be the best option for a commercial system due to its lower cost, smaller form factor and reduced power consumption compared to other implementations.

QKD Transceivers

Another substantial advantage of FPGAs not mentioned in the previous section is that having the DACs and ADCs on the same chip allows us to implement a CV-QKD transceiver at minimal additional cost compared to an AWG and an oscilloscope. Using FPGAs and having Alice's and Bob's optical setups, a device that can be either Alice or Bob on-the-fly can be easily implemented, enabling the deployment of QKD networks in the future. For this, we need to implement the setup shown in Figure 4.15.

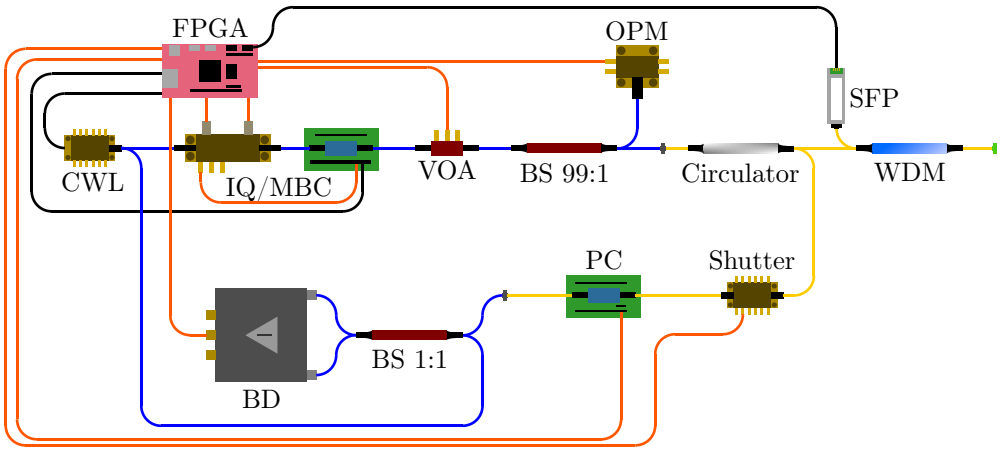

Figure 4.15: Conceptual design of a CV-QKD transceiver, integrating all the components from previous experimental setups into a combined transmitter and receiver device. The system features an FPGA for signal processing and control algorithms and implements the classical channels via WDM and SFP transceivers. Note that the circulator, previously used in our setup, is particularly useful here as it separates the incoming and outgoing signals.

We can see that by using the circulator, which in previous setups had an unused output, and taking advantage of using the same FPGA and the same laser for

both the receiver and the transmitter, we can implement a device that can act as Alice or Bob depending on the situation. The additional cost of having two transceivers instead of a transmitter and a receiver includes a balanced detector, a polarization controller, an IQ modulator, an MBC, a power meter, and a variable attenuator. When implementing a single point-to-point link, it makes more sense to use a transmitter and a receiver module. However, for implementing a network of only three nodes with two point-to-point links, three transceivers result in a lower cost than two transmitters and two receivers.

QKD Networks

After the first experimental demonstrations of CV-QKD, a symmetric point-to-point encryption channel using CV-QKD keys was also demonstrated [75], showcasing the relevance of demonstrating real use cases for this technology. More recently, the extension of standard VPN interfaces to work with QKD-derived keys was proposed [28].

To achieve something similar, we deployed a QKD-encrypted VPN between Alice and Bob to encrypt the information shared over the VPN using a key previously distributed by our system. After transmitting the raw key and the parameter estimation, the key is distilled using the classical post-processing methods from Appendix B. After the error correction and privacy amplification, Alice and Bob share exactly the same binary secret key. We used this key as a pre-shared key for deploying an OpenVPN connection. The diagram for this is shown in Figure 4.16.

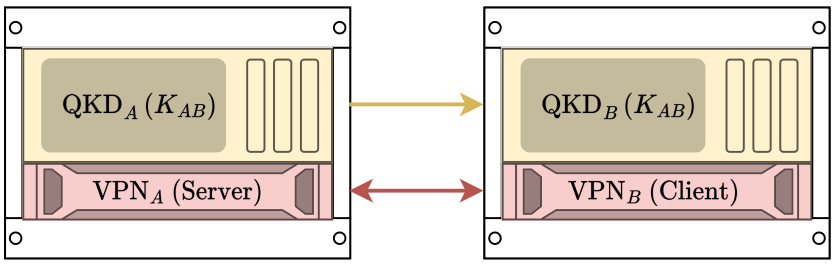

Figure 4.16: Schematic of a VPN connection using a QKD key to encrypt all traffic. The figure illustrates the interaction between the QKD devices A (server) and B (client), which generate a shared QKD key K_{AB} used to encrypt all traffic in the VPN connection between them.

OpenVPN is an open-source software solution that provides a secure virtual private network (VPN) connection. It uses tunneling protocols to create encrypted point-to-point connections and remote access. Using OpenVPN with a pre-shared key

(PSK) involves a relatively simple and effective symmetric encryption method. In this method, a secret key is generated and manually distributed to all parties participating in the VPN connection. This key is used to authenticate and encrypt communications between the OpenVPN client and server. The pre-shared key file must be securely transferred to both ends of the connection before establishing the VPN. Therefore, instead of manually sharing a key, we use the QKD key as the pre-shared key in the OpenVPN configurations, achieving a secure point-to-point connection based on a QKD key.

A natural extension of this concept is a network of multiple nodes with QKD links. After a first demonstration of the implementation of CV-QKD over a 50 km commercial fiber [180], different experimental QKD networks were deployed in different places over the world like Japan [137], Switzerland [151], China [179] or United Kingdom [42], and specifically using CV-QKD we can highlight a fully operative CV-QKD upstream quantum access network deployed in China with average distilled key rates of 55 kb/s for the end-user [69]. The basic diagram of a QKD network is shown in Figure 4.17.

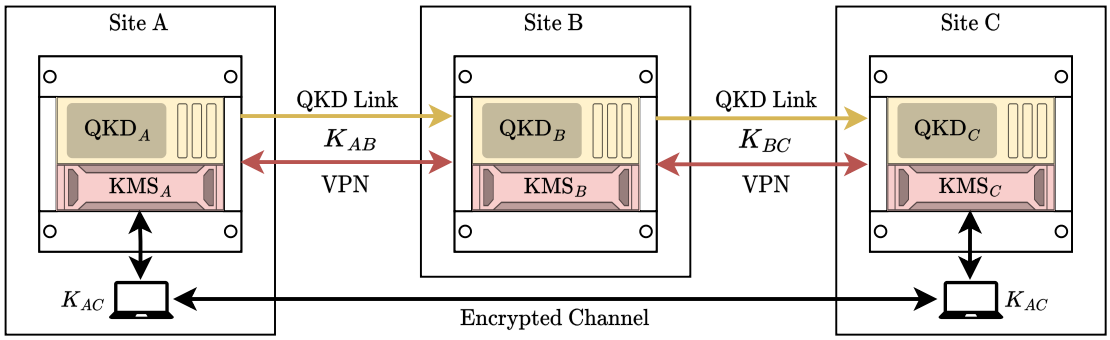

Figure 4.17: Schematic of a QKD network consisting of three nodes, A, B, and C, each equipped with a QKD device and a Key Management System (KMS). The figure shows QKD links between A and B, generating the shared key K_{AB}, and between B and C, generating the shared key K_{BC}. These keys secure the VPN connections between the sites. An encrypted channel between A and C is established by securely exchanging a key K_{AC} through the QKD-secured VPN links between the KMS devices. The KMS coordinates the secure key management and distribution across the network.

To this end, we have participated alongside Universidad Politécnica de Madrid (UPM) in demonstrations of real-world use cases related to the Madrid Quantum Network [105], where they implement the network and key management. To provide our distilled QKD keys to the network KMS server, we have implemented the ETSI GS QKD 004 standard [47] in our system, which specifies the technical requirements for designing an API for communication between a QKD network

manager and the QKD devices, regardless of the protocol they implement, to provide identical keys to two endpoints in the network.

The most straightforward configuration of a QKD network assumes that there are QKD links between pairs of nodes and public channels between all nodes, with a KMS connected to each QKD device on each local network. The KMS uses the QKD key from each link to establish a secure, VPN-like connection with the KMS on the other side of the link. This process is repeated across all links, resulting in a network of VPN-like links protected by QKD keys. Through these QKD-protected VPN-like links, any key can be requested within each Local Area Network (LAN) between that node and any other node in the network. The KMS calculates a final key, which results from different mathematical operations on all the keys from the intermediate links, and provides it to both nodes. With this key, secure communication between one device in a LAN and another in a different LAN is established, even where there is no direct fiber connection, using the provided key from each KMS to encrypt the connection between them.

Note that this network configuration requires trust in the intermediate nodes, all acting as trusted repeaters. However, there are many alternatives and solutions for implementing this architecture in an untrusted manner. An extensive survey on QKD networks can be found in [106].

4.4 Conclusions

In this chapter, we have presented a pilot-assisted frequency-locking method, which constitutes the main contribution of this work to the field of frequency and phase stabilization in CV-QKD systems using a locally generated local oscillator (LLO). By employing simple digital signal processing techniques, the algorithm corrects frequency and phase fluctuations between the signal and the local oscillator without relying on complex hardware-based solutions. This is achieved by using the pilot tone as a frequency reference for dynamically measuring and correcting phase and frequency variations caused by the random behavior of the lasers after signal acquisition.

The experimental validation of this method was performed through different transmissions over various channel lengths. Experimental transmissions were conducted using commercial optical fibers of 5 km, 25 km, and 50 km, with results closely matching the expected outcomes from simulations. The algorithm successfully enabled correct frequency locking in each experiment, regardless of the random frequency fluctuations of the lasers.

The Secret Key Rates obtained in our experiments, as presented in Table 4.3, are

comparable to the values reported in other works discussed in the CV-QKD state of the art from Section 2.2.2. Although our results are slightly lower in terms of secret key rate when compared to the record-breaking publications [121, 60], this is to be expected since we are using low-cost commercial optical fibers, lasers, and detectors, instead of the ultralow noise fibers, low-noise detectors, and ultrastable lasers. Nevertheless, our results are very similar to other demonstrations that focus on low-complexity deployments using commercial fibers and devices [129, 180].

In addition to developing the frequency-locking method, several improvements were made to enhance the experimental system's automation, robustness, and stability. These upgrades included automatic power control, polarization correction, and SNU estimation algorithms, all integrated to fully automate the system calibration before each transmission. Using a PID algorithm, the power control kept the optical power at Alice's output constant, compensating automatically for fluctuations caused by temperature changes or environmental conditions. Polarization correction was automated with an electronic polarization controller, which maximized the signal amplitude at the balanced detector output by aligning the polarization axes of the signals, a key factor for optimal detection efficiency. Finally, the automated SNU calibration method allowed for quick shot noise estimation between transmissions, significantly improving parameter estimation accuracy.

Once this experimental system was validated, further upgrades were carried out to implement these systems in real environments, such as the development of a coexistent classical and quantum channel over the same fiber and successful signal transmission and reception tests using FPGA boards. These demonstrated the feasibility of implementing all the system's electronics in FPGAs, enabling the development of CV-QKD transceivers.

Finally, the practical implications of these developments were explored, including integrating the CV-QKD system in secure networks and deploying QKD-encrypted Virtual Private Networks (VPNs) for easily establishing secure communication channels. In both cases, the tests were conducted using keys distilled from the classical post-processing methods described in Appendix B, applied to raw keys obtained from our experimental system.

Overall, the results obtained in this chapter validate the effectiveness of the pilot-assisted frequency-locking algorithm and demonstrate the feasibility of integrating this technology into more advanced CV-QKD systems and real-world quantum networks. These developments represent a significant step toward the industrialization of this technology, making it a viable solution for information security in future networks.

Chapter 5

Discussion and Future Work

In this thesis, the development and experimental validation of a Continuous-Variable Quantum Key Distribution (CV-QKD) system with a locally generated local oscillator (LLO) were studied. The work primarily focused on developing a method for correcting the received signal, eliminating the problems introduced by using two free-running independent lasers with random frequency and phase drifts. It also focused on the characterization of the experimental devices and the simulation and modeling of different impairments that affect the transmission of the quantum key.

Discussion

Chapter 3 focused on the simulation and modeling of the effects of various impairments that affect transmission in CV-QKD systems. These studies were crucial for understanding how different factors present in experimental systems affect the secret key rate (SKR) and, ultimately, the system's security. The simulations conducted allowed us to model the system's behavior under different conditions and determine performance limits in terms of distance and secret key rate. These models provided a foundation that guided the development of the frequency-locking algorithm and allowed us to accurately predict how the system would behave in real experiments. The combination of detailed simulations and controlled experiments offered essential cross-validation, ensuring that the results obtained in the laboratory were consistent with theoretical expectations. Different results from these simulations led to a peer-reviewed journal article [1], two conference talks [5, 6], and one poster [8].

The development of the pilot-assisted frequency-locking algorithm, presented in

Chapter 4, constitutes the most significant contribution of this thesis. This algorithm effectively solves the fundamental challenge of frequency stabilization in CV-QKD systems with independent lasers. This problem has historically been difficult to resolve without using complex and costly specialized hardware. Through the use of digital signal processing, the algorithm can correct the frequency and phase fluctuations of Alice and Bob's lasers after signal acquisition, thus ensuring the necessary coherence for secure quantum transmission while reducing costs and the complexity of the experimental system. The method is based on software techniques that can be implemented in real-time without requiring high-precision and high-speed optical or electronic devices. The experimental validation of this algorithm, through transmissions carried out over optical fibers of different distances (5 km, 25 km, and 50 km), has demonstrated its effectiveness, showing secret key rates similar to those expected from simulations, which supports the robustness of the algorithm and its ability to operate under significant frequency fluctuations. The results of these experiments were published in a peer-reviewed journal [2] and presented in a poster [9]. The pilot-assisted frequency-locking method was submitted and accepted for a patent application [3].

Apart from these two main contributions, another minor contribution was made, resulting in a poster presentation about the component characterization [5] and in a review paper on the state of the art of CV-QKD security analysis, published in a conference proceeding [4].

Although not the primary focus of the thesis, the work related to the system's enhancements for testing real use cases represents significant advances in integrating CV-QKD technology into practical environments. The validation of FPGAs as a viable alternative to traditional oscilloscopes and arbitrary waveform generators demonstrates that it is possible to miniaturize and optimize CV-QKD systems for industrial and commercial applications. Moreover, deploying a VPN based on keys distilled from our experimental system suggests immediate real-world applications. These developments, although complementary to the main results of this thesis, highlight the potential of CV-QKD technology to be integrated into existing infrastructures and underscore the importance of continued research in the development of Quantum Key Distribution systems. These networking demonstrations are part of the EuroQCI Spain [10] and QUBIP [11] projects from the European Commission, where the integration of our QKD systems into standard telecommunications environments must be demonstrated.

In summary, the research presented in this thesis has contributed to the advancement of CV-QKD technology, particularly in frequency stabilization methods through the pilot-assisted frequency-locking algorithm. The experimental results obtained validate the viability of this solution in real-world environments and open

the door to new research and developments in the field of quantum cryptography, which will lead to the future deployment of secure and efficient quantum communication systems.

Future Work

The work conducted in this thesis opens several avenues for future research, both in academia and industry. A possible research direction to continue the work of this thesis would be the study of the miniaturization of CV-QKD systems through integrated photonics, which could lead to more compact and robust devices suitable for use in industrial and commercial environments. This includes the development of integrated photonic chips covering all the necessary optical functions, from key generation to quantum detection.

Although most research has focused on fiber-optic transmission, implementing CV-QKD systems in free space is another field to explore. Using CV-QKD protocols would enable the distribution of quantum keys between buildings in urban environments or scenarios where fiber deployment is not feasible, such as in satellite communications.

From a more industrial perspective, the manufacture of specific CV-QKD devices ready for integration into existing telecommunications networks represents a significant opportunity. This includes the development of commercial QKD transceivers that are easily deployable in existing telecommunications infrastructures, as well as the creation of metropolitan quantum networks employing these technologies. For this, the development of FPGAs will be essential to properly integrate all the electronics into fast and low-cost chips, as well as the machining of all system components to ensure a robust assembly of the different components.

From an academic perspective, although this thesis primarily focused on the experimental development of the CV-QKD system, future research could focus on the study of security proofs to increase the secret key rate by employing discrete modulation schemes or to enhance the efficiency of error correction and privacy amplification protocols, which would require the development and implementation of new reconciliation algorithms or new modulation schemes.

Even more interesting from an academic point of view, future research could focus on studying new, more secure QKD protocols, such as MDI, TF, or DI, both from a theoretical perspective or, more specifically, from the perspective of carrying out experimental implementations.

In any case, there are a wide variety of options available to continue the devel-

opment of this technology. It is clear that this is a field with significant future potential, both academic and industrial, so there will always be open opportunities to continue researching and advancing the maturity of the field of quantum cryptography.

Appendix A

Shot Noise Units

This appendix analyzes how to measure the shot noise and how to convert all voltage and power measurements into Shot-Noise Units (SNU), following the analysis in [82]. The appendix begins by introducing the Shot-Noise Units framework and concludes by explaining how to experimentally convert from SI units to SNU in a practical way.

A.1 SI Units vs Natural Units vs Shot Noise Units

Shot noise units are similar to natural units. Both are specialized systems of units that simplify equations and enhance clarity in specific contexts. Natural units simplify equations by setting fundamental constants equal to 1, which removes the constants from equations, making the underlying physics easier to work with.

Shot Noise Units (SNU) are typically used in CV-QKD because they provide a natural and standardized way to measure and compare quantum fluctuations in the context of optical signals, as the information is encoded in the quadratures of the electromagnetic field, and these quadratures are subject to quantum noise, primarily due to the inherent uncertainty in quantum measurements, known as shot noise.

By expressing signal amplitudes, noise levels, and all measured quantities in terms of the shot noise, we can directly relate these measurements to the system's fundamental quantum noise floor. This makes SNU particularly useful for CV-QKD protocols, as it allows for consistent and comparable measurement of quantum noise and signal-to-noise ratios across different experimental setups and conditions.

Coherent states can be described using annihilation and creation operators. However, we can freely scale the definition of the quadrature operators $\hat{q}$ and $\hat{p}$ with respect to $\hat{a}$ and $\hat{a}^\dagger$. Depending on this, different expressions will arise. These definitions are summarized in Table A.1.

Definition	Shot Noise Units	Natural Units	SI Units
$\hat{a} =$	$\frac{1}{2}(\hat{q} + i\hat{p})$	$\frac{1}{\sqrt{2}}(\hat{q} + i\hat{p})$	$\frac{1}{\sqrt{2\hbar\omega}}(\omega\hat{q} + i\hat{p})$
$\hat{a}^\dagger =$	$\frac{1}{2}(\hat{q} - i\hat{p})$	$\frac{1}{\sqrt{2}}(\hat{q} - i\hat{p})$	$\frac{1}{\sqrt{2\hbar\omega}}(\omega\hat{q} - i\hat{p})$
$\hat{q} =$	$\hat{a} + \hat{a}^\dagger$	$\frac{1}{\sqrt{2}}(\hat{a} + \hat{a}^\dagger)$	$\sqrt{\frac{\hbar}{2\omega}}(\hat{a} + \hat{a}^\dagger)$
$\hat{p} =$	$-i(\hat{a} - \hat{a}^\dagger)$	$\frac{-i}{\sqrt{2}}(\hat{a} - \hat{a}^\dagger)$	$-i\sqrt{\frac{\hbar\omega}{2}}(\hat{a} - \hat{a}^\dagger)$
$\hat{n} =$	$\frac{1}{4}(\hat{q}^2 + \hat{p}^2) - \frac{1}{2}$	$\frac{1}{2}(\hat{q}^2 + \hat{p}^2) - \frac{1}{2}$	$\frac{1}{2\hbar\omega}(\omega^2\hat{q}^2 + \hat{p}^2) - \frac{1}{2}$
$[\hat{q}, \hat{p}] =$	$2i$	i	$i\hbar$
$\Delta q \Delta p \geq$	1	$\frac{1}{2}$	$\frac{\hbar}{2}$

Table A.1: Comparison of the representation of quantum operators, commutators, and uncertainties in shot noise units, natural units, and SI units. The table details the mathematical expressions for creation and annihilation operators ($\hat{a}$ and $\hat{a}^\dagger$), position ($\hat{q}$), momentum ($\hat{p}$), and number ($\hat{n}$) operators across these unit systems. Additionally, the commutation relation $[\hat{q}, \hat{p}]$ and the uncertainty principle $\Delta q \Delta p$ are shown in each unit system.

As can be seen, all expressions from Section 2.1, reviewing the fundamentals of quantum mechanics, were expressed in the natural units framework, as this is typically used in that context to eliminate all constants from the mathematical expressions. On the other hand, all expressions from Section 2.2.2, reviewing the CV-QKD protocol, were expressed in the shot noise unit framework.

In addition to the different expressions for quantum operators and uncertainties, we are also interested in expressing all power and voltage measurements in terms of shot noise. The following section studies this.

A.2 Shot noise and electronic noise measurement

To show how to express different magnitudes in shot noise units, we start with the equation for the variance of the coherent states received by Bob, which, in the shot noise unit framework where the noise variance is 1, is expressed as

$$V_{\mathrm{SNU}} = \frac{T}{\mu}V + 1 + \frac{T\xi}{\mu^2}, \tag{A.1}$$

where $V = V_A + 1$ with V_A being the modulation variance expressed in SNU and related to the photon number as $V_A = 2\langle\hat{n}\rangle$, and where $\mu = 1$ for homodyne detection and $\mu = 2$ for heterodyne detection. Assuming that the excess noise ξ originates partly from the channel, ξ_{ch}, and partly from the receiver, ξ_{rec}, the previous equation can be expressed as

$$V_{\mathrm{SNU}} = \frac{T}{\mu}V + 1 + \frac{T\xi_{\mathrm{ch}}}{\mu^2} + \frac{T\xi_{\mathrm{rec}}}{\mu^2}. \tag{A.2}$$

In the experimental setup, Bob measures voltages on an oscilloscope or an ADC (analog-to-digital converter). If Bob has a set of N measurements of amplitude in the phase space, expressed as voltages V_i, for $i = 1, \ldots, \mu N$, the variance of these measurements is

$$V_{\mathrm{SI}} = \frac{1}{\mu N}\sum_{i=1}^{\mu N} V_i^2 - \left(\frac{1}{\mu N}\sum_{i=1}^{\mu N} V_i\right)^2. \tag{A.3}$$

Using this equation, Bob can calculate the variance of a series of measurements and then estimate the SNU. The relationship between the variance measured by Bob in SI units and the state variance in SNU can be expressed as

$$V_{\mathrm{SI}} = \phi V_{\mathrm{SNU}}, \tag{A.4}$$

Where ϕ is the conversion factor between the two systems of units. The first step to determine ϕ is to cut off the input signal from Alice so that $TV = \xi_{\mathrm{ch}} = 0$, reducing Equation (A.2) to

$$V_{\mathrm{SNU}} = 1 + \frac{T\xi_{\mathrm{rec}}}{\mu}. \tag{A.5}$$

Therefore, what Bob measures with his detector will be

$$V_{\mathrm{SI}} = \phi + \phi\frac{T\xi_{\mathrm{rec}}}{\mu} := \phi + \phi\nu_{\mathrm{el}} := \phi + V'_{\mathrm{SI}}, \tag{A.6}$$

where ν_{el} is the electronic noise variance expressed in SNU and V'_{SI} the electronic noise variance measured in SI units. Then, Bob performs another series of measurements with the local oscillator turned off, measuring only the receiver noise

variance or electronic noise, V'_{SI} in SI units. The conversion factor ϕ is then given by

$$\phi = V_{\mathrm{SI}} - V'_{\mathrm{SI}}. \tag{A.7}$$

This conversion factor relates the equivalence between SNU and V^2. Finally, we can express the electronic noise variance in the SNU framework as

$$\nu_{\mathrm{el}} = \frac{V'_{\mathrm{SI}}}{\phi}. \tag{A.8}$$

Bob only needs to divide any voltage by $\sqrt{\phi}$ and any voltage variance by ϕ to convert SI units to SNU. In other words, Bob calculates the difference between the variances of two sets of measured voltages: one with the signal off and another with both the signal and the local oscillator off. This difference in variances results in the conversion factor between SI and SNU units. This method is commonly known as *two-time estimation*.

Alternatively, a *one-time estimation* approach was proposed in [183], which can be a better approach as it requires only one measurement, reducing statistical errors. However, this method involves revisiting the security analysis and modifying all the secret key rate estimation calculations. For this reason, we employ the conventional two-time estimation in our implementation.

From an experimental perspective, to reduce potential variations in the shot noise calibration, the SNU estimation should be repeated for each transmission block. This is essential since parameter estimation depends on transmittance and excess noise, both of which are expressed in SNU. Even slight deviations in SNU estimation can significantly impact the secret key rate, particularly for longer distances [183]. Therefore, a precise SNU calibration is critical for the system's security. Ideally, the conversion factor between SI units and SNU should be recalculated at each transmission as fast as possible to minimize errors or, better yet, computed in real-time using the *one-time estimation* method.

Appendix B

Classical Post-processing

This appendix replicates the classical post-processing part of the GG02 protocol as presented in [109]. This combines elements from various sources related to CV-QKD reconciliation techniques [116], information theory [104], Low-Density Parity-Check (LDPC) codes [107, 36], and hashing functions for privacy amplification [157]. Although key distillation techniques are not the primary focus of this thesis, they are an essential part of the GG02 protocol and are used at the end of Chapter 4 to distill the keys used in the QKD network and VPN demonstrations. The following briefly overviews the error correction and privacy amplification used to distill the CV-QKD keys.

B.1 Error Correction using LDPC Codes

For each block of symbols sent from Alice to Bob, after the parameter estimation stage, the parties process their remaining $n = N - m$ pairs of key generation symbols in an error correction procedure. This process can be divided into normalization, discretization, splitting, encoding, decoding, and verification.

B.1.1 Normalization

For each block of transmitted symbols of size N, Alice and Bob have n pairs of their variables x and y that can be used for key generation, while the rest m pairs were discarded for parameter estimation. As a first step, Alice and Bob normalize their variables by dividing them by their respective standard deviations, defining two new normalized variables:

$$X := \frac{x}{\sigma_x}, \quad Y := \frac{y}{\sigma_y}, \tag{B.1}$$

so X and Y have the following covariance matrix:

$$\Sigma_{XY} = \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}, \tag{B.2}$$

where X and Y follow a standard normal bivariate distribution, with correlation ρ given by

$$\rho = \sqrt{\frac{\mathrm{SNR}}{1+\mathrm{SNR}}}, \tag{B.3}$$

where the signal-to-noise ratio, SNR, can be approximately given by its maximum-likelihood estimator:

$$\widehat{\mathrm{SNR}} = \frac{(V_A - 1)\eta\hat{T}}{1 + \nu_{\mathrm{el}} + \hat{\xi}}. \tag{B.4}$$

B.1.2 Discretization

Bob discretizes his normalized variable Y into a p-ary variable K with a generic value $\kappa \in \{0, \ldots, 2^p - 1\}$, being an element of a Galois field $\mathcal{GF}(2^p)$. To achieve this discretization, he sets a cut-off α such that $|Y| \leq \alpha$ occurs with negligible probability, typically $\alpha \geq 3$. Then, Bob chooses the size $\delta = 2\alpha 2^{-p}$ of the discretization intervals $[a_\kappa, b_\kappa)$ of his lattice, whose border points are given by

$$a_\kappa = \begin{cases} -\infty, & \text{for } \kappa = 0, \\ -\alpha + \kappa\delta, & \text{for } \kappa > 0, \end{cases} \tag{B.5}$$

and

$$b_\kappa = \begin{cases} -\alpha + (\kappa+1)\delta, & \text{for } \kappa < 2^p - 1, \\ \infty, & \text{for } \kappa = 2^p - 1. \end{cases} \tag{B.6}$$

Finally, for any value of $Y \in [a_\kappa, b_\kappa)$, Bob sets that value equal to κ. Thus, the normalized string Y is transformed into a string of discrete values K.

B.1.3 Splitting

Bob sets an integer value for $q < p$ and computes $d = p - q$. Then, he splits his discretized variable into two parts $K = (\overline{K}, \underline{K})$, where the top variable $\overline{K}$ is q-ary and the bottom variable $\underline{K}$ is d-ary. Their values are defined by splitting the generic value κ into two parts:

$$\overline{\kappa} = \frac{\kappa - \kappa \bmod 2^d}{2^d}, \quad \underline{\kappa} = \kappa \bmod 2^d. \tag{B.7}$$

In other words, we can express κ in terms of these two parts as

$$\kappa = \overline{\kappa} 2^d + \underline{\kappa}. \tag{B.8}$$

With the top variable $\overline{K}$, Bob creates 2^q super bins, each containing 2^d bins associated with the bottom variable $\underline{K}$. The most significant string $\overline{K}$ is locally processed by an LDPC code, while the least significant string $\underline{K}$ is side information revealed through the public channel.

B.1.4 LDPC encoding and decoding

Following [104], Bob constructs an $l \times n$ parity check matrix G with q-ary entries from $\mathcal{GF}(2^q)$, where l is the length of the code, which is previously determined from the desired code rate in Equation (B.9). This matrix is applied to the top string $\overline{K}$ to derive the l-long syndrome $K^l = G\overline{K}$, where the matrix-vector product is defined in $\mathcal{GF}(2^q)$. The syndrome is sent to Alice together with the direct communication of the bottom string $\underline{K}$. The parity check matrix is associated with an LDPC code, which may encode $k = n - l$ source symbols into n output symbols, so it has a code rate given by

$$R_{\text{code}} = \frac{k}{n} = 1 - \frac{l}{n}. \tag{B.9}$$

From the knowledge of the syndrome K^l, Bob's bottom string $\underline{K}$, and her local string X, Alice decodes Bob's top string $\overline{K}$. This is done via an iterative belief propagation algorithm [36], where in every iteration, she updates a codeword likelihood function.

At every iteration, Alice finds the $\overline{K}$ that maximizes the function. If its syndrome equals K^l, Alice forms her guess $\hat{K}$ of Bob's $\overline{K}$. However, if this Syndrome Matching Test (SMT) is not satisfied within a maximum number of allowed iterations, then the block is discarded.

Before this iterative algorithm, they calculate the LDPC code rate R_{code} to generate the parity check matrix. This arises from Alice and Bob's mutual information decreasing as a consequence of the discretization process [35], which is represented as

$$I_{AB} \geq H(K) - H(K|X) \geq H(K) - \text{leak}_{\text{EC}}, \tag{B.10}$$

where $\text{leak}_{\text{EC}} \geq H(K|X)$ comes from the Wolf-Slepian limit [149, 177] and $H(K)$ is the Shannon entropy of K. The parties empirically estimate the entropy by building the MLE given by

$$\hat{H}(K) = -\sum_{\kappa=0}^{2^p-1} f_\kappa \log_2 f_\kappa, \tag{B.11}$$

where $f_\kappa = n_\kappa/n$ stands for the frequencies of the symbols κ, defined as the ratio between the number of times n_κ that a symbol appears in the string over the string's length n. For this estimator, it can be shown [14] that the entropy satisfies

$$H(K) \geq \hat{H}(K) - \delta_{\text{ent}}, \tag{B.12}$$

with a penalty parameter δ_{ent} defined by

$$\delta_{\text{ent}} = \log_2(n)\sqrt{\frac{2\log(2/\varepsilon_{\text{ent}})}{n}}. \tag{B.13}$$

This bound is valid up to an error probability ε_{ent}. In Equation (B.10), the leakage associated with error correction, leak_{EC}, is upper-bounded by the equivalent number of bits per use that are broadcasted after the LDPC encoding in each block,

$$\text{leak}_{\text{EC}} \leq d + \frac{ql}{n}. \tag{B.14}$$

Therefore, combining the two previous bounds, we may write

$$I_{AB} \geq \beta I_{AB} = \hat{H}(K) - \delta_{\text{ent}} + qR_{\text{code}} - p. \tag{B.15}$$

Note that in a practical implementation, the expression for the mutual information depends on the MLE for the signal-to-noise ratio,

$$I_{AB} = \frac{1}{2}\log_2(1 + \widehat{\text{SNR}}). \tag{B.16}$$

From Equations (B.15) and (B.16), we see that the LDPC code must be chosen to have an optimal code rate

$$R_{\text{code}} = \frac{1}{q}\left[\frac{\beta}{2}\log_2\left(1 + \widehat{\text{SNR}}\right) + p - \hat{H}(K) + \delta_{\text{ent}}\right], \tag{B.17}$$

for some estimated SNR and key entropy. The expression for the secret key rate, taking into account the error correction procedure, becomes

$$R = \beta I_{AB} - \chi_{EB} = \hat{H}(K) - \delta_{\text{ent}} + qR_{\text{code}} - p - \chi_{EB}, \tag{B.18}$$

where R is used instead of K to distinguish the secret key rate and the discretized key array, and where χ_{EB} represents the Holevo bound as calculated in Section 2.3. A value of the reconciliation efficiency β is acceptable only if we can choose parameters $\alpha \geq 3$ and q, such that $R_{\text{code}} \leq 1$. Once R_{code} is known, the sparse parity check matrix G of the LDPC code can be constructed following [104].

B.1.5 Verification

A crucial final step in the EC procedure is verifying the error-corrected blocks that have successfully passed the SMT. For each block, the parties have two n-long q-ary strings with identical syndromes, i.e., Bob's top string $\overline{K}$ and Alice's guess $\hat{K}$. The parties convert their strings into a binary representation, $\overline{K}_2$ and $\hat{K}_2$, so that each of them is qn bits long. Next, Alice and Bob compute t-bit long hashes of their converted binary strings following [157]. They set $t = \lceil -\log_2 \varepsilon_{\text{cor}} \rceil$, where ε_{cor} is known as *correctness*.

Then, Bob discloses his hash to Alice, who compares it with hers. If the hashes are identical, the verification stage is successful. The two strings $\overline{K}_2$ and $\hat{K}_2$ are identical up to a small error probability $2^{-t} \leq \varepsilon_{\text{cor}}$. In this case, the associated bottom string $\underline{K}$ held by both parties is converted by both parties into binary and appended to the respective strings. These binary concatenations move on to the next step of privacy amplification.

B.2 Privacy Amplification and Key Distillation

The final step of the protocol is Privacy Amplification (PA), which generates the secret key. In this final step, all the surviving error-corrected strings are compressed into shorter strings that are decoupled from Eve (up to a small error probability discussed below). By concatenating their local error-corrected binary strings from the previous part, Alice and Bob create two long binary sequences $S \simeq \hat{S}$, each with $\tilde{n} = np$ bits. These sequences will be compressed to a final secret key of $\tilde{r} = n\tilde{R}$ bits, where $\tilde{R}$ is determined by Equation (B.20). The compression is achieved using universal hashing with a Toeplitz matrix $T_{\tilde{r},\tilde{n}}$, calculated efficiently using an algorithm based on the FFT [109]. Thus, from their sequences, Alice and Bob finally retrieve the secret key

$$\tilde{K} = T_{\tilde{r},\tilde{n}} S \simeq T_{\tilde{r},\tilde{n}} \hat{S}. \tag{B.19}$$

Finally, the secret key rate of the protocol, secure against collective attacks up to a ε error probability, and taking into account error correction and privacy amplification, is given [124] by the following expression:

$$R = \frac{n}{N}\tilde{R}, \quad \tilde{R} := \left(R - \frac{\Delta}{\sqrt{n}} + \frac{\Theta}{n} \right), \tag{B.20}$$

where R is given in Equation (B.18) and the extra terms are given by

$$\begin{aligned} \Delta &:= 4 \log_2 \left(2^{p/2} + 2\right) \sqrt{\log_2 \left(18/\varepsilon^4\right)}, \\ \Theta &:= \log_2 \left(1 - \varepsilon^2/3\right) + 2 \log_2 (\sqrt{2}\varepsilon). \end{aligned} \tag{B.21}$$

List of Publications

Peer-Reviewed Journal Articles

[1] Ruiz-Chamorro, A., Cano, D., Garcia-Callejo, A., and Fernandez, V. "Effects of Experimental Impairments on the Security of Continuous-Variable Quantum Key Distribution". In: *Heliyon* 9.6 (June 2023), e16670. ISSN: 2405-8440. DOI: 10.1016/j.heliyon.2023.e16670. (Visited on 11/16/2023).

[2] Ruiz-Chamorro, A., Garcia-Callejo, A., and Fernandez, V. "Low-Complexity Continuous-Variable Quantum Key Distribution with True Local Oscillator Using Pilot-Assisted Frequency Locking". In: *Scientific Reports* 14.1 (May 2024), p. 10770. ISSN: 2045-2322. DOI: 10.1038/s41598-024-61461-0.

Patents

[3] Ruiz Chamorro, A., Cano, D., and Fernandez, V. "Dispositivo y procedimiento de demodulación asistida por tono piloto en sistemas de comunicación óptica coherente". June 2023. (Visited on 09/14/2024).

Conference Proceedings

[4] Garcia-Callejo, A., Ruiz-Chamorro, A., Cano, D., and Fernandez, V. "A Review on Continuous-Variable Quantum Key Distribution Security". In: *Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2022)*. Ed. by J. Bravo, S. Ochoa, and J. Favela. Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 2023, pp. 1073–1085. ISBN: 978-3-031-21333-5. DOI: 10.1007/978-3-031-21333-5_107.

Conference Talks

[5] RUIZ-CHAMORRO, A. *Enhancing Continuous-Variable Quantum Key Distribution through Impairment Optimization*. Oral. Photon 2022, Nottingham, UK, Aug. 2022. (Visited on 11/16/2023).

[6] RUIZ-CHAMORRO, A. *Effect of Experimental Imperfections in Continuous-Variable Quantum Key Distribution*. Oral. QTYR23, Madrid, Spain, July 2023. (Visited on 11/16/2023).

Poster Presentations

[7] RUIZ CHAMORRO, A. *Optimizing Experimental Calibration in Continuous Variable Quantum Key Distribution to Minimize Excess Noise*. Poster. ICE-6, Barcelona, Spain, May 2021. (Visited on 01/26/2024).

[8] RUIZ-CHAMORRO, A. *Impairments Optimization for Continuous-Variable Quantum Key Distribution*. Poster. Qcrypt 22, Taipei, Taiwan, Aug. 2022. (Visited on 11/16/2023).

[9] RUIZ-CHAMORRO, A. *Pilot Tone-Assisted Frequency Locking in Low-Complexity Continuous Variable Quantum Key Distribution Systems*. Poster. Qcrypt 24, Vigo, Spain, Sept. 2024. (Visited on 11/16/2023).

Participation in Projects

[10] *EuroQCI Spain, EuroQCI deployment in Spain*. 1011091638, EU Secure Quantum Communication Infrastructure (DIGITAL-2021-QCI-01). 2021.

[11] *QUBIP, Quantum-oriented Update to Browsers and Infrastructures for the PQ Transition*. 101119746, Horizon Europe (HORIZON). 2021.

Bibliography

[12] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., and Scarani, V. "Device-Independent Security of Quantum Cryptography against Collective Attacks". In: *Physical Review Letters* 98.23 (June 2007), p. 230501. doi: 10.1103/PhysRevLett.98.230501. (Visited on 07/28/2024).

[13] Agrawal, G. P. *Nonlinear Fiber Optics*. Academic Press, Aug. 2019. isbn: 978-0-12-817043-4.

[14] Antos, A. and Kontoyiannis, I. "Convergence Properties of Functional Estimates for Discrete Distributions". In: *Random Structures & Algorithms* 19.3-4 (2001), pp. 163–193. issn: 1098-2418. doi: 10.1002/rsa.10019. (Visited on 07/19/2024).

[15] Bacco, D., Da Lio, B., Cozzolino, D., Da Ros, F., Guo, X., Ding, Y., Sasaki, Y., Aikawa, K., Miki, S., Terai, H., Yamashita, T., Neergaard-Nielsen, J. S., Galili, M., Rottwitt, K., Andersen, U. L., Morioka, T., and Oxenløwe, L. K. "Boosting the Secret Key Rate in a Shared Quantum and Classical Fibre Communication System". In: *Communications Physics* 2.1 (Nov. 2019), pp. 1–8. issn: 2399-3650. doi: 10.1038/s42005-019-0238-1. (Visited on 03/23/2023).

[16] Bell, S. C., Heywood, D. M., White, J. D., Close, J. D., and Scholten, R. E. "Laser Frequency Offset Locking Using Electromagnetically Induced Transparency". In: *Applied Physics Letters* 90.17 (Apr. 2007), p. 171120. issn: 0003-6951. doi: 10.1063/1.2734471. (Visited on 09/25/2023).

[17] Bennett, C. H. "Quantum Cryptography Using Any Two Nonorthogonal States". In: *Physical Review Letters* 68.21 (May 1992), pp. 3121–3124. doi: 10.1103/PhysRevLett.68.3121. (Visited on 07/29/2024).

[18] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. "Experimental Quantum Cryptography". In: *Journal of Cryptology* 5.1 (Jan. 1992), pp. 3–28. ISSN: 1432-1378. DOI: 10.1007/BF00191318. (Visited on 09/25/2023).

[19] Bennett, C. H. and Brassard, G. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Theoretical Computer Science*. Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84 560 (Dec. 2014), pp. 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025. (Visited on 02/01/2023).

[20] Bennett, C. H., Brassard, G., and Mermin, N. D. "Quantum Cryptography without Bell's Theorem". In: *Physical Review Letters* 68.5 (Feb. 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557. (Visited on 07/29/2024).

[21] Bennett, C. H., Brassard, G., and Robert, J.-M. "Privacy Amplification by Public Discussion". In: *SIAM Journal on Computing* 17.2 (Apr. 1988), pp. 210–229. ISSN: 0097-5397. DOI: 10.1137/0217014. (Visited on 07/29/2024).

[22] Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M.-J., Nolan, D., Martin, A., and Zbinden, H. "Secure Quantum Key Distribution over 421 Km of Optical Fiber". In: *Physical Review Letters* 121.19 (Nov. 2018), p. 190502. DOI: 10.1103/PhysRevLett.121.190502. (Visited on 07/28/2024).

[23] Brassard, G. and Salvail, L. "Secret-Key Reconciliation by Public Discussion". In: *Advances in Cryptology — EUROCRYPT '93*. Ed. by T. Helleseth. Berlin, Heidelberg: Springer, 1994, pp. 410–423. ISBN: 978-3-540-48285-7. DOI: 10.1007/3-540-48285-7_35.

[24] Braunstein, S. L. and van Loock, P. "Quantum Information with Continuous Variables". In: *Reviews of Modern Physics* 77.2 (June 2005), pp. 513–577. DOI: 10.1103/RevModPhys.77.513. (Visited on 08/25/2024).

[25] Brunner, H. H., Bettelli, S., Fung, C.-H. F., and Peev, M. "Precise Noise Calibration for CV-QKD". In: *2020 22nd International Conference on Transparent Optical Networks (ICTON)*. July 2020, pp. 1–4. DOI: 10.1109/ICTON51198.2020.9203405. (Visited on 05/31/2024).

[26] Brunner, H. H., Comandar, L. C., Karinou, F., Bettelli, S., Hillerkuss, D., Fung, F., Wang, D., Mikroulis, S., Yi, Q., Kuschnerov, M., Poppe, A., Xie, C., and Peev, M. "A Low-Complexity Heterodyne CV-QKD Architecture". In: *2017 19th International Conference on Transparent Optical Networks (ICTON)*. July 2017, pp. 1–4. doi: 10.1109/ICTON.2017.8025030.

[27] Bruss, D. "Optimal Eavesdropping in Quantum Cryptography with Six States". In: *Physical Review Letters* 81.14 (Oct. 1998), pp. 3018–3021. doi: 10.1103/PhysRevLett.81.3018. (Visited on 07/29/2024).

[28] Buruaga, J. S., Brunner, H. H., Fung, F., Peev, M., Pastor, A., López, D. R., Ortiz, L., Martín, V., and Brito, J. P. "VPN Protection with QKD-Derived Keys Using Standard Interfaces". In: *2023 23rd International Conference on Transparent Optical Networks (ICTON)*. July 2023, pp. 1–4. doi: 10.1109/ICTON59386.2023.10207212. (Visited on 05/31/2024).

[29] Carter, J. L. and Wegman, M. N. "Universal Classes of Hash Functions". In: *Journal of Computer and System Sciences* 18.2 (Apr. 1979), pp. 143–154. issn: 0022-0000. doi: 10.1016/0022-0000(79)90044-8. (Visited on 07/23/2024).

[30] Cerf, N. J., Lévy, M., and Assche, G. V. "Quantum Distribution of Gaussian Keys Using Squeezed States". In: *Physical Review A* 63.5 (Apr. 2001), p. 052311. doi: 10.1103/PhysRevA.63.052311. (Visited on 07/30/2024).

[31] Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., Han, S.-L., Yu, Q., Liang, K., Zhou, F., Yuan, X., Zhao, M.-S., Wang, T.-Y., Jiang, X., Zhang, L., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Lu, C.-Y., Shu, R., Wang, J.-Y., Li, L., Liu, N.-L., Xu, F., Wang, X.-B., Peng, C.-Z., and Pan, J.-W. "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres". In: *Nature* 589.7841 (Jan. 2021), pp. 214–219. issn: 1476-4687. doi: 10.1038/s41586-020-03093-8. (Visited on 07/28/2024).

[32] Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhang, W.-J., Han, Z.-Y., Ma, S.-Z., Hu, X.-L., Li, Y.-H., Liu, H., Zhou, F., Jiang, H.-F., Chen, T.-Y., Li, H., You, L.-X., Wang, Z., Wang, X.-B., Zhang, Q., and Pan, J.-W. "Twin-Field Quantum Key Distribution over a 511 Km Optical Fibre Linking Two Distant Metropolitan Areas". In: *Nature Photonics* 15.8 (Aug.

2021), pp. 570–575. ISSN: 1749-4893. DOI: 10.1038/s41566-021-00828-5. (Visited on 07/28/2024).

[33] CHIN, H.-M., JAIN, N., ZIBAR, D., ANDERSEN, U. L., and GEHRING, T. "Machine Learning Aided Carrier Recovery in Continuous-Variable Quantum Key Distribution". In: *npj Quantum Information* 7.1 (Feb. 2021), pp. 1–6. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00361-x. (Visited on 09/25/2023).

[34] COMANDAR, L. C., BRUNNER, H. H., BETTELLI, S., FUNG, F., KARINOU, F., HILLERKUSS, D., MIKROULIS, S., WANG, D., KUSCHNEROV, M., XIE, C., POPPE, A., and PEEV, M. "A Flexible Continuous-Variable QKD System Using off-the-Shelf Components". In: *Quantum Information Science and Technology III*. Vol. 10442. SPIE, Oct. 2017, pp. 37–43. DOI: 10.1117/12.2279913. (Visited on 09/29/2023).

[35] COVER, T. M. and THOMAS, J. A. *Elements of Information Theory*. John Wiley & Sons, Nov. 2012. ISBN: 978-1-118-58577-1.

[36] DAVEY, M. and MACKAY, D. "Low-Density Parity Check Codes over GF(q)". In: *IEEE Communications Letters* 2.6 (June 1998), pp. 165–167. ISSN: 1558-2558. DOI: 10.1109/4234.681360. (Visited on 07/19/2024).

[37] DEMARIE, T. F. *Pedagogical Introduction to the Entropy of Entanglement for Gaussian States*. Sept. 2012. DOI: 10.48550/arXiv.1209.2748. arXiv: 1209.2748 [quant-ph]. (Visited on 08/25/2024).

[38] DENYS, A., BROWN, P., and LEVERRIER, A. "Explicit Asymptotic Secret Key Rate of Continuous-Variable Quantum Key Distribution with an Arbitrary Modulation". In: *Quantum* 5 (Sept. 2021), p. 540. DOI: 10.22331/q-2021-09-13-540. (Visited on 07/20/2022).

[39] DEVETAK, I. and WINTER, A. "Distillation of Secret Key and Entanglement from Quantum States". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461.2053 (Jan. 2005), pp. 207–235. DOI: 10.1098/rspa.2004.1372. (Visited on 03/25/2022).

[40] DIAMANTI, E., LO, H.-K., QI, B., and YUAN, Z. "Practical Challenges in Quantum Key Distribution". In: *npj Quantum Information* 2.1 (Nov. 2016), pp. 1–12. ISSN: 2056-6387. DOI: 10.1038/npjqi.2016.25. (Visited on 02/01/2023).

[41] Diffie, W. and Hellman, M. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (Nov. 1976), pp. 644–654. ISSN: 1557-9654. DOI: 10.1109/TIT.1976.1055638. (Visited on 08/25/2024).

[42] Dynes, J. F., Wonfor, A., Tam, W. W.-S., Sharpe, A. W., Takahashi, R., Lucamarini, M., Plews, A., Yuan, Z. L., Dixon, A. R., Cho, J., Tanizawa, Y., Elbers, J.-P., Greisser, H., White, I. H., Penty, R. V., and Shields, A. J. "Cambridge Quantum Network". In: *npj Quantum Information* 5.1 (Nov. 2019), pp. 1–8. ISSN: 2056-6387. DOI: 10.1038/s41534-019-0221-4. (Visited on 07/28/2024).

[43] Einstein, A., Podolsky, B., and Rosen, N. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Physical Review* 47.10 (May 1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777. (Visited on 08/08/2024).

[44] Ekert, A. K. "Quantum Cryptography Based on Bell's Theorem". In: *Physical Review Letters* 67.6 (Aug. 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661. (Visited on 07/29/2024).

[45] Elkouss, D., Leverrier, A., Alleaume, R., and Boutros, J. J. "Efficient Reconciliation Protocol for Discrete-Variable Quantum Key Distribution". In: *2009 IEEE International Symposium on Information Theory*. June 2009, pp. 1879–1883. DOI: 10.1109/ISIT.2009.5205475. (Visited on 07/29/2024).

[46] Elliott, C. "The DARPA Quantum Network". In: *Quantum Communications and Cryptography*. CRC Press, 2005. ISBN: 978-1-315-22112-0.

[47] European Telecommunications Standards Institute. *ETSI GS QKD 004*. Aug. 2020. (Visited on 08/26/2024).

[48] Evans, J. M., O'Neill, J. T., Little, J. L., Albus, J. S., Barbera, A. J., Fife, D. W., Fong, E. N., Gilsinn, D. E., Holberton, F. E., Lucas, B. G., Lyon, G. E., Marron, B. A. S., Neumann, A. J., and Mabel, V. V. *Standards for Computer Aided Manufacturing:* Jan. 1977. (Visited on 08/26/2024).

[49] "Continuous Variable Systems". In: *Quantum Processes and Measurement: Theory and Experiment*. Ed. by C. Fabre. Cambridge: Cambridge University Press, 2023, pp. 142–177. ISBN: 978-1-108-47777-2. DOI: 10.1017/9781108774918.010. (Visited on 08/25/2024).

[50] Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Brouri, R., and Grangier, P. "Improvement of Continuous-Variable Quantum Key Distribution Systems by Using Optical Preamplifiers". In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 42.11 (June 2009), p. 114014. ISSN: 0953-4075, 1361-6455. DOI: 10.1088/0953-4075/42/11/114014. arXiv: 0812.4314 [quant-ph]. (Visited on 06/03/2024).

[51] Fox, M. and Fox, M. *Quantum Optics: An Introduction*. Oxford Master Series in Physics. Oxford, New York: Oxford University Press, Apr. 2006. ISBN: 978-0-19-856673-1.

[52] Ghorai, S., Grangier, P., Diamanti, E., and Leverrier, A. "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation". In: *Physical Review X* 9.2 (June 2019), p. 021059. ISSN: 2160-3308. DOI: 10.1103/PhysRevX.9.021059. arXiv: 1902.01317. (Visited on 12/01/2021).

[53] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. "Quantum Cryptography". In: *Reviews of Modern Physics* 74.1 (Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145. (Visited on 02/01/2023).

[54] Gottesman, D. and Preskill, J. "Secure Quantum Key Distribution Using Squeezed States". In: *Physical Review A* 63.2 (Jan. 2001), p. 022309. DOI: 10.1103/PhysRevA.63.022309. (Visited on 12/02/2021).

[55] Griffiths, D. J. *Introduction to Quantum Mechanics*. Cambridge University Press, 2017. ISBN: 978-1-107-17986-8.

[56] Grosshans, F., Cerf, N., Wenger, J., Tualle-Brouri, R., and Grangier, P. "Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables". In: *Quantum Information and Computation* 3.special (Oct. 2003), pp. 535–552. ISSN: 15337146, 15337146. DOI: 10.26421/QIC3.s-6. (Visited on 08/09/2024).

[57] Grosshans, F. "Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution". In: *Physical Review Letters* 94.2 (Jan. 2005), p. 020504. DOI: 10.1103/PhysRevLett.94.020504. (Visited on 07/26/2024).

[58] Grosshans, F. and Grangier, P. "Continuous Variable Quantum Cryptography Using Coherent States". In: *Physical Review Letters* 88.5 (Jan.

2002), p. 057902. DOI: 10.1103/PhysRevLett.88.057902. (Visited on 12/01/2021).

[59] GROSSHANS, F. and GRANGIER, P. "Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables". In: *arXiv:quant-ph/0204127* (Apr. 2002). arXiv: quant-ph/0204127. (Visited on 12/01/2021).

[60] HAJOMER, A. A. E., DERKACH, I., JAIN, N., CHIN, H.-M., ANDERSEN, U. L., and GEHRING, T. "Long-Distance Continuous-Variable Quantum Key Distribution over 100-Km Fiber with Local Local Oscillator". In: *Science Advances* 10.1 (Jan. 2024), eadi9474. DOI: 10.1126/sciadv.adi9474. (Visited on 04/17/2024).

[61] HAJOMER, A. A. E., JAIN, N., MANI, H., CHIN, H.-M., ANDERSEN, U. L., and GEHRIN, T. *Modulation Leakage-Free Continuous-Variable Quantum Key Distribution*. May 2022. DOI: 10.48550/arXiv.2205.07245. arXiv: 2205.07245 [quant-ph]. (Visited on 07/22/2022).

[62] HEIM, B., PEUNTINGER, C., KILLORAN, N., KHAN, I., WITTMANN, C., MARQUARDT, C., and LEUCHS, G. "Atmospheric Continuous-Variable Quantum Communication". In: *New Journal of Physics* 16.11 (Nov. 2014), p. 113018. ISSN: 1367-2630. DOI: 10.1088/1367-2630/16/11/113018. (Visited on 07/28/2024).

[63] HOLEVO, A. S. "Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel". In: *Probl. Peredachi Inf.* Problems Inform. Transmission 9.3 (1973), pp. 3–11. (Visited on 09/25/2023).

[64] HSIEH, G.-C. and HUNG, J. "Phase-Locked Loop Techniques. A Survey". In: *IEEE Transactions on Industrial Electronics* 43.6 (Dec. 1996), pp. 609–615. ISSN: 1557-9948. DOI: 10.1109/41.544547. (Visited on 09/25/2023).

[65] HUANG, D., HUANG, P., LIN, D., WANG, C., and ZENG, G. "High-Speed Continuous-Variable Quantum Key Distribution without Sending a Local Oscillator". In: *Optics Letters* 40.16 (Aug. 2015), pp. 3695–3698. ISSN: 1539-4794. DOI: 10.1364/OL.40.003695. (Visited on 12/02/2021).

[66] HUANG, D., HUANG, P., LIN, D., and ZENG, G. "Long-Distance Continuous-Variable Quantum Key Distribution by Controlling Excess Noise". In: *Scientific Reports* 6.1 (Jan. 2016), p. 19201. ISSN: 2045-2322. DOI: 10.1038/srep19201. (Visited on 12/02/2021).

[67] Huang, D., Lin, D., Wang, C., Liu, W., Fang, S., Peng, J., Huang, P., and Zeng, G. "Continuous-Variable Quantum Key Distribution with 1 Mbps Secure Key Rate". In: *Optics Express* 23.13 (June 2015), pp. 17511–17519. ISSN: 1094-4087. DOI: 10.1364/OE.23.017511. (Visited on 12/02/2021).

[68] Huang, J.-Z., Weedbrook, C., Yin, Z.-Q., Wang, S., Li, H.-W., Chen, W., Guo, G.-C., and Han, Z.-F. "Quantum Hacking of a Continuous-Variable Quantum-Key-Distribution System Using a Wavelength Attack". In: *Physical Review A* 87.6 (June 2013), p. 062329. DOI: 10.1103/PhysRevA.87.062329. (Visited on 09/25/2023).

[69] Huang, Y., Zhang, Y., Shen, T., Huang, G., and Yu, S. "Experimental Demonstration of Upstream Continuous-variable QKD Access Network". In: *Conference on Lasers and Electro-Optics (2020), Paper JTu2A.24*. Optica Publishing Group, May 2020, JTu2A.24. DOI: 10.1364/CLEO_AT.2020.JTu2A.24. (Visited on 07/20/2022).

[70] Hughes, R. J., Buttler, W. T., Kwiat, P. G., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G. "Free-Space Quantum Key Distribution in Daylight". In: *Journal of Modern Optics* 47.2-3 (Feb. 2000), pp. 549–562. ISSN: 0950-0340. DOI: 10.1080/09500340008244059. (Visited on 07/29/2024).

[71] Hughes, R. J., Morgan, G. L., and Peterson, C. G. "Quantum Key Distribution over a 48 Km Optical Fibre Network". In: *Journal of Modern Optics* 47.2-3 (Feb. 2000), pp. 533–547. ISSN: 0950-0340. DOI: 10.1080/09500340008244058. (Visited on 07/29/2024).

[72] Hwang, W.-Y. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Physical Review Letters* 91.5 (Aug. 2003), p. 057901. DOI: 10.1103/PhysRevLett.91.057901. (Visited on 07/29/2024).

[73] Inoue, K., Waks, E., and Yamamoto, Y. "Differential Phase Shift Quantum Key Distribution". In: *Physical Review Letters* 89.3 (June 2002), p. 037902. DOI: 10.1103/PhysRevLett.89.037902. (Visited on 07/29/2024).

[74] Jain, N., Chin, H.-M., Mani, H., Lupo, C., Nikolic, D. S., Kordts, A., Pirandola, S., Pedersen, T. B., Kolb, M., Ömer, B., Pacher, C., Gehring, T., and Andersen, U. L. "Practical Continuous-Variable Quan-

tum Key Distribution with Composable Security". In: *Nature Communications* 13.1 (Aug. 2022), p. 4740. ISSN: 2041-1723. DOI: 10.1038/s41467-022-32161-y. (Visited on 09/29/2023).

[75] JOUGUET, P., KUNZ-JACQUES, S., DEBUISSCHERT, T., FOSSIER, S., DIAMANTI, E., ALLÉAUME, R., TUALLE-BROURI, R., GRANGIER, P., LEVERRIER, A., PACHE, P., and PAINCHAULT, P. "Field Test of Classical Symmetric Encryption with Continuous Variables Quantum Key Distribution". In: *Optics Express* 20.13 (June 2012), pp. 14030–14041. ISSN: 1094-4087. DOI: 10.1364/OE.20.014030. (Visited on 12/02/2021).

[76] JOUGUET, P., KUNZ-JACQUES, S., DIAMANTI, E., and LEVERRIER, A. "Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution". In: *Physical Review A* 86.3 (Sept. 2012), p. 032309. DOI: 10.1103/PhysRevA.86.032309. (Visited on 02/01/2023).

[77] JOUGUET, P., KUNZ-JACQUES, S., and LEVERRIER, A. "Long-Distance Continuous-Variable Quantum Key Distribution with a Gaussian Modulation". In: *Physical Review A* 84.6 (Dec. 2011), p. 062317. DOI: 10.1103/PhysRevA.84.062317. (Visited on 07/23/2024).

[78] JOUGUET, P., KUNZ-JACQUES, S., LEVERRIER, A., GRANGIER, P., and DIAMANTI, E. "Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution". In: *Nature Photonics* 7.5 (May 2013), pp. 378–381. ISSN: 1749-4893. DOI: 10.1038/nphoton.2013.63. (Visited on 12/02/2021).

[79] KISH, S. P., GLEESON, P. J., WALSH, A., LAM, P. K., and ASSAD, S. M. "Comparison of Discrete Variable and Continuous Variable Quantum Key Distribution Protocols with Phase Noise in the Thermal-Loss Channel". In: *Quantum* 8 (June 2024), p. 1382. DOI: 10.22331/q-2024-06-20-1382. (Visited on 07/30/2024).

[80] KLEIS, S., RUECKMANN, M., and SCHAEFFER, C. G. "Continuous Variable Quantum Key Distribution with a Real Local Oscillator Using Simultaneous Pilot Signals". In: *Optics Letters* 42.8 (Apr. 2017), pp. 1588–1591. ISSN: 1539-4794. DOI: 10.1364/OL.42.001588. (Visited on 12/02/2021).

[81] LAUDENBACH, F., PACHER, C., FUNG, C.-H., PEEV, M., POPPE, A., and HÜBEL, H. *Practical Noise Models for CV-QKD Implementations*. Sept. 2017. DOI: 10.13140/RG.2.2.24607.25767.

[82] Laudenbach, F., Pacher, C., Fung, C.-H. F., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P., and Hübel, H. "Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations". In: *Advanced Quantum Technologies* 1.1 (2018), p. 1800011. ISSN: 2511-9044. DOI: 10.1002/qute.201800011. (Visited on 12/02/2021).

[83] Laudenbach, F., Schrenk, B., Pacher, C., Hentschel, M., Fung, C.-H. F., Karinou, F., Poppe, A., Peev, M., and Hübel, H. "Pilot-Assisted Intradyne Reception for High-Speed Continuous-Variable Quantum Key Distribution with True Local Oscillator". In: *Quantum* 3 (Oct. 2019), p. 193. DOI: 10.22331/q-2019-10-07-193. (Visited on 02/01/2023).

[84] Leverrier, A. "Theoretical Study of Continuous-Variable Quantum Key Distribution". PhD thesis. Télécom ParisTech, Nov. 2009. (Visited on 07/20/2022).

[85] Leverrier, A. "Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States". In: *Physical Review Letters* 114.7 (Feb. 2015), p. 070501. DOI: 10.1103/PhysRevLett.114.070501. (Visited on 07/24/2024).

[86] Leverrier, A., Alléaume, R., Boutros, J., Zémor, G., and Grangier, P. "Multidimensional Reconciliation for a Continuous-Variable Quantum Key Distribution". In: *Physical Review A* 77.4 (Apr. 2008), p. 042325. DOI: 10.1103/PhysRevA.77.042325. (Visited on 07/23/2024).

[87] Leverrier, A., García-Patrón, R., Renner, R., and Cerf, N. J. "Security of Continuous-Variable Quantum Key Distribution Against General Attacks". In: *Physical Review Letters* 110.3 (Jan. 2013), p. 030502. DOI: 10.1103/PhysRevLett.110.030502. (Visited on 07/20/2022).

[88] Leverrier, A. and Grangier, P. "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation". In: *Physical Review Letters* 102.18 (May 2009), p. 180504. DOI: 10.1103/PhysRevLett.102.180504. (Visited on 07/21/2022).

[89] Leverrier, A., Grosshans, F., and Grangier, P. "Finite-Size Analysis of a Continuous-Variable Quantum Key Distribution". In: *Physical Review A* 81.6 (June 2010), p. 062343. DOI: 10.1103/PhysRevA.81.062343. (Visited on 02/01/2023).

[90] Li, C., Qian, L., and Lo, H.-K. "Simple Security Proofs for Continuous Variable Quantum Key Distribution with Intensity Fluctuating Sources". In: *npj Quantum Information* 7.1 (Oct. 2021), pp. 1–8. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00482-3. (Visited on 03/23/2023).

[91] Li, L., Wang, T., Li, X., Huang, P., Guo, Y., Lu, L., Zhou, L., and Zeng, G. "Continuous-Variable Quantum Key Distribution with on-Chip Light Sources". In: *Photonics Research* 11.4 (Apr. 2023), pp. 504–516. ISSN: 2327-9125. DOI: 10.1364/PRJ.473328. (Visited on 04/17/2024).

[92] Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., Zhou, Y.-L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.-A., Liu, N.-L., Wang, X.-B., Zhu, Z.-C., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W. "Satellite-to-Ground Quantum Key Distribution". In: *Nature* 549.7670 (Sept. 2017), pp. 43–47. ISSN: 1476-4687. DOI: 10.1038/nature23655. (Visited on 07/28/2024).

[93] Liu, W., Peng, J., Qi, J., Cao, Z., and He, C. "Imperfect Basis Choice in Continuous-Variable Quantum Key Distribution". In: *Laser Physics Letters* 17.5 (Apr. 2020), p. 055203. ISSN: 1612-202X. DOI: 10.1088/1612-202X/ab7eb7. (Visited on 04/19/2023).

[94] Liu, W., Wang, X., Wang, N., Du, S., and Li, Y. "Imperfect State Preparation in Continuous-Variable Quantum Key Distribution". In: *Physical Review A* 96.4 (Oct. 2017), p. 042312. DOI: 10.1103/PhysRevA.96.042312. (Visited on 04/19/2023).

[95] Liu, Y., Zhang, W.-J., Jiang, C., Chen, J.-P., Zhang, C., Pan, W.-X., Ma, D., Dong, H., Xiong, J.-M., Zhang, C.-J., Li, H., Wang, R.-C., Wu, J., Chen, T.-Y., You, L., Wang, X.-B., Zhang, Q., and Pan, J.-W. "Experimental Twin-Field Quantum Key Distribution over 1000 Km Fiber Distance". In: *Physical Review Letters* 130.21 (May 2023), p. 210801. DOI: 10.1103/PhysRevLett.130.210801. (Visited on 04/17/2024).

[96] Liu, Z. and Slavík, R. "Optical Injection Locking: From Principle to Applications". In: *Journal of Lightwave Technology* 38.1 (Jan. 2020), pp. 43–59. (Visited on 09/25/2023).

[97] Lo, H.-K., Curty, M., and Qi, B. "Measurement-Device-Independent Quantum Key Distribution". In: *Physical Review Letters* 108.13 (Mar.

2012), p. 130503. DOI: 10.1103/PhysRevLett.108.130503. (Visited on 12/01/2021).

[98] LODEWYCK, J., BLOCH, M., GARCÍA-PATRÓN, R., FOSSIER, S., KARPOV, E., DIAMANTI, E., DEBUISSCHERT, T., CERF, N. J., TUALLE-BROURI, R., MCLAUGHLIN, S. W., and GRANGIER, P. "Quantum Key Distribution over 25 Km with an All-Fiber Continuous-Variable System". In: *Physical Review A* 76.4 (Oct. 2007), p. 042305. DOI: 10.1103/PhysRevA.76.042305. (Visited on 12/02/2021).

[99] LOUDON, R. *The Quantum Theory of Light*. OUP Oxford, Sept. 2000. ISBN: 978-0-19-158978-2.

[100] LU, W., HUANG, C., HOU, K., SHI, L., ZHAO, H., LI, Z., and QIU, J. "Recurrent Neural Network Approach to Quantum Signal: Coherent State Restoration for Continuous-Variable Quantum Key Distribution". In: *Quantum Information Processing* 17.5 (Mar. 2018), p. 109. ISSN: 1573-1332. DOI: 10.1007/s11128-018-1877-y. (Visited on 07/22/2022).

[101] LUCAMARINI, M., YUAN, Z. L., DYNES, J. F., and SHIELDS, A. J. "Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters". In: *Nature* 557.7705 (May 2018), pp. 400–403. ISSN: 1476-4687. DOI: 10.1038/s41586-018-0066-6. (Visited on 07/29/2024).

[102] MA, X.-C., SUN, S.-H., JIANG, M.-S., and LIANG, L.-M. "Local Oscillator Fluctuation Opens a Loophole for Eve in Practical Continuous-Variable Quantum-Key-Distribution Systems". In: *Physical Review A* 88.2 (Aug. 2013), p. 022339. DOI: 10.1103/PhysRevA.88.022339. (Visited on 12/02/2021).

[103] MA, X.-C., SUN, S.-H., JIANG, M.-S., and LIANG, L.-M. "Wavelength Attack on Practical Continuous-Variable Quantum-Key-Distribution System with a Heterodyne Protocol". In: *Physical Review A* 87.5 (May 2013), p. 052309. DOI: 10.1103/PhysRevA.87.052309. (Visited on 09/25/2023).

[104] MACKAY, D. J. C. and NEAL, R. M. "Near Shannon Limit Performance of Low Density Parity Check Codes". In: *Electronics Letters* 33.6 (Mar. 1997), pp. 457–458. ISSN: 1350-911X. DOI: 10.1049/el:19970362. (Visited on 07/19/2024).

[105] MARTIN, V., AGUADO, A., SALAS, P., SANZ, A. L., BRITO, J. P., LOPEZ, D. R., LOPEZ, V., PASTOR, A., FOLGUEIRA, J., BRUNNER, H. H., BET-

TELLI, S., FUNG, F., COMANDAR, L. C., WANG, D., POPPE, A., and PEEV, M. "The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure". In: *OSA Advanced Photonics Congress (AP) 2019 (IPR, Networks, NOMA, SPPCom, PVLED) (2019), Paper QtW3E.5*. Optica Publishing Group, July 2019, QtW3E.5. DOI: 10.1364/NETWORKS.2019.QtW3E.5. (Visited on 07/22/2024).

[106] MEHIC, M., NIEMIEC, M., RASS, S., MA, J., PEEV, M., AGUADO, A., MARTIN, V., SCHAUER, S., POPPE, A., PACHER, C., and VOZNAK, M. "Quantum Key Distribution: A Networking Perspective". In: *ACM Comput. Surv.* 53.5 (Sept. 2020), 96:1–96:41. ISSN: 0360-0300. DOI: 10.1145/3402192. (Visited on 09/10/2024).

[107] MILICEVIC, M. "Low-Density Parity-Check Decoder Architectures for Integrated Circuits and Quantum Cryptography". Thesis. Nov. 2017. (Visited on 07/19/2024).

[108] MOSCA, M., STEBILA, D., and USTAOĞLU, B. "Quantum Key Distribution in the Classical Authenticated Key Exchange Framework". In: *Post-Quantum Cryptography*. Ed. by P. GABORIT. Berlin, Heidelberg: Springer, 2013, pp. 136–154. ISBN: 978-3-642-38616-9. DOI: 10.1007/978-3-642-38616-9_9.

[109] MOUNTOGIANNAKIS, A. G., PAPANASTASIOU, P., BRAVERMAN, B., and PIRANDOLA, S. "Composably Secure Data Processing for Gaussian-modulated Continuous-Variable Quantum Key Distribution". In: *Physical Review Research* 4.1 (Feb. 2022), p. 013099. ISSN: 2643-1564. DOI: 10.1103/PhysRevResearch.4.013099. (Visited on 01/10/2024).

[110] NAKAZAWA, M. "Rayleigh Backscattering Theory for Single-Mode Optical Fibers". In: *JOSA* 73.9 (Sept. 1983), pp. 1175–1180. DOI: 10.1364/JOSA.73.001175. (Visited on 07/03/2024).

[111] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Advanced Encryption Standard (AES)*. May 2023. DOI: 10.6028/NIST.FIPS.197-upd1. (Visited on 08/25/2024).

[112] NAVASCUÉS, M. and ACÍN, A. "Security Bounds for Continuous Variables Quantum Key Distribution". In: *Physical Review Letters* 94.2 (Jan. 2005), p. 020505. DOI: 10.1103/PhysRevLett.94.020505. (Visited on 07/26/2024).

[113] Navascués, M., Grosshans, F., and Acín, A. "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography". In: *Physical Review Letters* 97.19 (Nov. 2006), p. 190502. DOI: 10.1103/PhysRevLett.97.190502. (Visited on 08/25/2024).

[114] Nielsen, M. A. and Chuang, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Dec. 2010. ISBN: 978-1-139-49548-6.

[115] Noe, R. "Phase Noise-Tolerant Synchronous QPSK/BPSK Baseband-Type Intradyne Receiver Concept with Feedforward Carrier Recovery". In: *Journal of Lightwave Technology* 23.2 (Feb. 2005), pp. 802–808. ISSN: 1558-2213. DOI: 10.1109/JLT.2004.838818. (Visited on 09/25/2023).

[116] Pacher, C., Martinez-Mateo, J., Duhme, J., Gehring, T., and Furrer, F. *Information Reconciliation for Continuous-Variable Quantum Key Distribution Using Non-Binary Low-Density Parity-Check Codes*. Feb. 2016. DOI: 10.48550/arXiv.1602.09140. arXiv: 1602.09140 [quant-ph]. (Visited on 07/19/2024).

[117] Pan, Y., Wang, H., Shao, Y., Pi, Y., Li, Y., Liu, B., Huang, W., Huang, W., Xu, B., and Xu, B. "Experimental Demonstration of High-Rate Discrete-Modulated Continuous-Variable Quantum Key Distribution System". In: *Optics Letters* 47.13 (July 2022), pp. 3307–3310. ISSN: 1539-4794. DOI: 10.1364/OL.456978. (Visited on 07/20/2022).

[118] Park, H.-c., Lu, M., Bloch, E., Reed, T., Griffith, Z., Johansson, L., Coldren, L., and Rodwell, M. "40Gbit/s Coherent Optical Receiver Using a Costas Loop". In: *Optics Express* 20.26 (Dec. 2012), B197–B203. ISSN: 1094-4087. DOI: 10.1364/OE.20.00B197. (Visited on 03/30/2022).

[119] Pereira, D., Almeida, M., Facão, M., Pinto, A. N., and Silva, N. A. "Impact of Receiver Imbalances on the Security of Continuous Variables Quantum Key Distribution". In: *EPJ Quantum Technology* 8.1 (Dec. 2021), pp. 1–12. ISSN: 2196-0763. DOI: 10.1140/epjqt/s40507-021-00112-z. (Visited on 04/19/2023).

[120] Peuntinger, C., Heim, B., Müller, C. R., Gabriel, C., Marquardt, C., and Leuchs, G. "Distribution of Squeezed States through an Atmospheric Channel". In: *Physical Review Letters* 113.6 (Aug. 2014), p. 060502. DOI: 10.1103/PhysRevLett.113.060502. (Visited on 07/28/2024).

[121] Pi, Y., Wang, H., Pan, Y., Shao, Y., Li, Y., Yang, J., Zhang, Y., Huang, W., and Xu, B. "Sub-Mbps Key-Rate Continuous-Variable Quantum Key Distribution with Local Local Oscillator over 100-Km Fiber". In: *Optics Letters* 48.7 (Apr. 2023), pp. 1766–1769. ISSN: 1539-4794. DOI: 10.1364/OL.485913. (Visited on 04/17/2024).

[122] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., and Wallden, P. "Advances in Quantum Cryptography". In: *Advances in Optics and Photonics* 12.4 (Dec. 2020), p. 1012. ISSN: 1943-8206. DOI: 10.1364/AOP.361502. arXiv: 1906.01645. (Visited on 12/07/2021).

[123] Pirandola, S. "Symmetric Collective Attacks for the Eavesdropping of Symmetric Quantum Key Distribution". In: *International Journal of Quantum Information* 06.supp01 (July 2008), pp. 765–771. ISSN: 0219-7499. DOI: 10.1142/S0219749908004080. (Visited on 07/31/2024).

[124] Pirandola, S. "Limits and Security of Free-Space Quantum Communications". In: *Physical Review Research* 3.1 (Mar. 2021), p. 013279. DOI: 10.1103/PhysRevResearch.3.013279. (Visited on 07/19/2024).

[125] Pirandola, S., Mancini, S., Lloyd, S., and Braunstein, S. L. "Continuous-Variable Quantum Cryptography Using Two-Way Quantum Communication". In: *Nature Physics* 4.9 (Sept. 2008), pp. 726–730. ISSN: 1745-2481. DOI: 10.1038/nphys1018. (Visited on 07/30/2024).

[126] Poppe, A., Fung, F., Peev, M., Hillerkuss, D., Karinou, F., Comandar, L., Mikroulis, S., Brunner, H., Bettelli, S., Kuschnerov, M., Yi, Q., Wang, D., Schrenk, B., Laudenbach, F., Pacher, C., and Hübel, H. "Prospects of CV-QKD Systems Limited by Commercial Telecom Equipment". In: *2017 European Conference on Lasers and Electro-Optics and European Quantum Electronics Conference (2017), Paper EB_P_17*. Optica Publishing Group, June 2017, EB_P_17. (Visited on 10/01/2024).

[127] Qi, B., Lougovski, P., Pooser, R., Grice, W., and Bobrek, M. "Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection". In: *Physical Review X* 5.4 (Oct. 2015), p. 041009. DOI: 10.1103/PhysRevX.5.041009. (Visited on 03/23/2022).

[128] Ralph, T. C. "Continuous Variable Quantum Cryptography". In: *Physical Review A* 61.1 (Dec. 1999), p. 010303. DOI: 10.1103/PhysRevA.61.010303. (Visited on 07/30/2024).

[129] Ren, S., Yang, S., Wonfor, A., White, I., and Penty, R. "Demonstration of High-Speed and Low-Complexity Continuous Variable Quantum Key Distribution System with Local Local Oscillator". In: *Scientific Reports* 11.1 (May 2021), p. 9454. ISSN: 2045-2322. DOI: 10.1038/s41598-021-88468-1. (Visited on 07/20/2022).

[130] Renner, R. and Cirac, J. I. "De Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography". In: *Physical Review Letters* 102.11 (Mar. 2009), p. 110504. DOI: 10.1103/PhysRevLett.102.110504. (Visited on 07/29/2024).

[131] Renner, R. "Security of Quantum Key Distribution". PhD thesis. ETH Zurich, Jan. 2006. arXiv: quant-ph/0512258. (Visited on 07/20/2022).

[132] Richardson, T. and Urbanke, R. *Modern Coding Theory*. Cambridge University Press, Mar. 2008. ISBN: 978-0-521-85229-6.

[133] Rivest, R. L., Shamir, A., and Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. (Visited on 08/25/2024).

[134] Roudas, I. "Coherent Optical Communication Systems". In: *WDM Systems and Networks: Modeling, Simulation, Design and Engineering*. Ed. by N. (Antoniades, G. Ellinas, and I. Roudas. New York, NY: Springer, 2012, pp. 373–417. ISBN: 978-1-4614-1093-5. DOI: 10.1007/978-1-4614-1093-5_10. (Visited on 10/04/2024).

[135] Roumestan, F., Ghazisaeidi, A., Renaudier, J., Vidarte, L. T., Leverrier, A., Diamanti, E., and Grangier, P. *Experimental Demonstration of Discrete Modulation Formats for Continuous Variable Quantum Key Distribution*. July 2022. DOI: 10.48550/arXiv.2207.11702. arXiv: 2207.11702 [quant-ph]. (Visited on 04/17/2024).

[136] Salehi, M. and Proakis, J. *Digital Communications*. McGraw-Hill Education, Nov. 2007. ISBN: 978-0-07-295716-7.

[137] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J. F., Dixon, A. R., Sharpe, A. W., Yuan, Z. L., Shields, A. J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.-B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A. "Field Test of Quantum Key Distribution in the Tokyo QKD Network". In: *Optics Express* 19.11 (May 2011), pp. 10387–10409. ISSN: 1094-4087. DOI: 10.1364/OE.19.010387. (Visited on 07/28/2024).

[138] Sax, R., Boaron, A., Boso, G., Atzeni, S., Crespi, A., Grünenfelder, F., Rusca, D., Al-Saadi, A., Bronzi, D., Kupijai, S., Rhee, H., Osellame, R., and Zbinden, H. "High-Speed Integrated QKD System". In: *Photonics Research* 11.6 (June 2023), pp. 1007–1014. ISSN: 2327-9125. DOI: 10.1364/PRJ.481475. (Visited on 04/17/2024).

[139] Scarani, V., Acín, A., Ribordy, G., and Gisin, N. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". In: *Physical Review Letters* 92.5 (Feb. 2004), p. 057901. DOI: 10.1103/PhysRevLett.92.057901. (Visited on 07/29/2024).

[140] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. "The Security of Practical Quantum Key Distribution". In: *Reviews of Modern Physics* 81.3 (Sept. 2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. (Visited on 02/01/2023).

[141] Schrödinger, E. "An Undulatory Theory of the Mechanics of Atoms and Molecules". In: *Physical Review* 28.6 (Dec. 1926), pp. 1049–1070. DOI: 10.1103/PhysRev.28.1049. (Visited on 08/08/2024).

[142] Shannon, C. E. "A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (July 1948), pp. 379–423. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1948.tb01338.x. (Visited on 09/25/2023).

[143] Shor, P. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700. (Visited on 08/25/2024).

[144] Shor, P. W. and Preskill, J. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: *Physical Review Letters* 85.2 (July 2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441. (Visited on 07/29/2024).

[145] Silberhorn, C., Ralph, T. C., Lütkenhaus, N., and Leuchs, G. "Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit". In: *Physical Review Letters* 89.16 (Sept. 2002), p. 167901. DOI: 10.1103/PhysRevLett.89.167901. (Visited on 12/01/2021).

[146] Silva, N. A., Almeida, M., Pereira, D., Facão, M., Muga, N. J., and Pinto, A. N. "Role of Device Imperfections on the Practical Performance of Continuous-Variable Quantum Key Distribution Systems". In: *2019 21st International Conference on Transparent Optical Networks (ICTON)*. July 2019, pp. 1–4. DOI: 10.1109/ICTON.2019.8840330.

[147] Silva, N. A., Pereira, D., Muga, N. J., and Pinto, A. N. "Practical Imperfections Affecting the Performance of CV-QKD Based on Coherent Detection". In: *2020 22nd International Conference on Transparent Optical Networks (ICTON)*. July 2020, pp. 1–4. DOI: 10.1109/ICTON51198.2020.9203349.

[148] Simon, R., Chaturvedi, S., and Srinivasan, V. "Congruences and Canonical Forms for a Positive Matrix: Application to the Schweinler–Wigner Extremum Principle". In: *Journal of Mathematical Physics* 40.7 (July 1999), pp. 3632–3642. ISSN: 0022-2488. DOI: 10.1063/1.532913. (Visited on 08/25/2024).

[149] Slepian, D. and Wolf, J. "Noiseless Coding of Correlated Information Sources". In: *IEEE Transactions on Information Theory* 19.4 (July 1973), pp. 471–480. ISSN: 1557-9654. DOI: 10.1109/TIT.1973.1055037. (Visited on 07/19/2024).

[150] Soh, D. B. S., Brif, C., Coles, P. J., Lütkenhaus, N., Camacho, R. M., Urayama, J., and Sarovar, M. "Self-Referenced Continuous-Variable Quantum Key Distribution Protocol". In: *Physical Review X* 5.4 (Oct. 2015), p. 041010. DOI: 10.1103/PhysRevX.5.041010. (Visited on 02/01/2023).

[151] Stucki, D., Legré, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., Henzen, L., Junod, P., Litzistorf, G., Monbaron, P., Monat, L., Page, J.-B., Perroud, D., Ribordy, G., Rochas, A., Robyr, S.,

Tavares, J., Thew, R., Trinkler, P., Ventura, S., Voirol, R., Walenta, N., and Zbinden, H. "Long-Term Performance of the SwissQuantum Quantum Key Distribution Network in a Field Environment". In: *New Journal of Physics* 13.12 (Dec. 2011), p. 123001. ISSN: 1367-2630. DOI: 10.1088/1367-2630/13/12/123001. (Visited on 07/28/2024).

[152] Stucki, D., Brunner, N., Gisin, N., Scarani, V., and Zbinden, H. "Fast and Simple One-Way Quantum Key Distribution". In: *Applied Physics Letters* 87.19 (Nov. 2005), p. 194108. ISSN: 0003-6951. DOI: 10.1063/1.2126792. (Visited on 07/29/2024).

[153] Suleiman, I., Nielsen, J. A. H., Guo, X., Jain, N., Neergaard-Nielsen, J., Gehring, T., and Andersen, U. L. "40 Km Fiber Transmission of Squeezed Light Measured with a Real Local Oscillator". In: *Quantum Science and Technology* 7.4 (July 2022), p. 045003. ISSN: 2058-9565. DOI: 10.1088/2058-9565/ac7ba1. (Visited on 07/20/2022).

[154] Tamaki, K., Koashi, M., and Imoto, N. "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States". In: *Physical Review Letters* 90.16 (Apr. 2003), p. 167904. DOI: 10.1103/PhysRevLett.90.167904. (Visited on 07/29/2024).

[155] Tamaki, K. and Lütkenhaus, N. "Unconditional Security of the Bennett 1992 Quantum Key-Distribution Protocol over a Lossy and Noisy Channel". In: *Physical Review A* 69.3 (Mar. 2004), p. 032316. DOI: 10.1103/PhysRevA.69.032316. (Visited on 10/01/2024).

[156] Thorpe, J. I., Numata, K., and Livas, J. "Laser Frequency Stabilization and Control through Offset Sideband Locking to Optical Cavities". In: *Optics Express* 16.20 (Sept. 2008), pp. 15980–15990. ISSN: 1094-4087. DOI: 10.1364/OE.16.015980. (Visited on 09/25/2023).

[157] Thorup, M. *High Speed Hashing for Integers and Strings*. May 2020. DOI: 10.48550/arXiv.1504.06804. arXiv: 1504.06804 [cs]. (Visited on 07/19/2024).

[158] Usenko, V. C. and Filip, R. "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense". In: *Entropy* 18.1 (Jan. 2016), p. 20. ISSN: 1099-4300. DOI: 10.3390/e18010020. (Visited on 09/25/2023).

[159] Van Assche, G., Cardinal, J., and Cerf, N. "Reconciliation of a Quantum-Distributed Gaussian Key". In: *IEEE Transactions on Information Theory* 50.2 (Feb. 2004), pp. 394–400. ISSN: 1557-9654. DOI: 10.1109/TIT.2003.822618. (Visited on 07/23/2024).

[160] Vasylyev, D., Semenov, A. A., Vogel, W., Günthner, K., Thurn, A., Bayraktar, Ö., and Marquardt, C. "Free-Space Quantum Links under Diverse Weather Conditions". In: *Physical Review A* 96.4 (Oct. 2017), p. 043856. DOI: 10.1103/PhysRevA.96.043856. (Visited on 07/28/2024).

[161] Wang, H., Li, Y., Pi, Y., Pan, Y., Shao, Y., Ma, L., Zhang, Y., Yang, J., Zhang, T., Huang, W., and Xu, B. "Sub-Gbps Key Rate Four-State Continuous-Variable Quantum Key Distribution within Metropolitan Area". In: *Communications Physics* 5.1 (June 2022), pp. 1–10. ISSN: 2399-3650. DOI: 10.1038/s42005-022-00941-z. (Visited on 04/17/2024).

[162] Wang, H., Pi, Y., Huang, W., Li, Y., Shao, Y., Yang, J., Liu, J., Zhang, C., Zhang, Y., and Xu, B. "High-Speed Gaussian-modulated Continuous-Variable Quantum Key Distribution with a Local Local Oscillator Based on Pilot-Tone-Assisted Phase Compensation". In: *Optics Express* 28.22 (Oct. 2020), pp. 32882–32893. ISSN: 1094-4087. DOI: 10.1364/OE.404611. (Visited on 02/01/2023).

[163] Wang, P., Zhang, Y., Lu, Z., Wang, X., and Li, Y. "Discrete-Modulation Continuous-Variable Quantum Key Distribution with a High Key Rate". In: *New Journal of Physics* 25.2 (Feb. 2023), p. 023019. ISSN: 1367-2630. DOI: 10.1088/1367-2630/acb964. (Visited on 07/01/2024).

[164] Wang, S., Huang, P., Wang, T., and Zeng, G. "Feasibility of All-Day Quantum Communication with Coherent Detection". In: *Physical Review Applied* 12.2 (Aug. 2019), p. 024041. DOI: 10.1103/PhysRevApplied.12.024041. (Visited on 07/28/2024).

[165] Wang, S., Yin, Z.-Q., He, D.-Y., Chen, W., Wang, R.-Q., Ye, P., Zhou, Y., Fan-Yuan, G.-J., Wang, F.-X., Chen, W., Zhu, Y.-G., Morozov, P. V., Divochiy, A. V., Zhou, Z., Guo, G.-C., and Han, Z.-F. "Twin-Field Quantum Key Distribution over 830-Km Fibre". In: *Nature Photonics* 16.2 (Feb. 2022), pp. 154–161. ISSN: 1749-4893. DOI: 10.1038/s41566-021-00928-2. (Visited on 07/28/2024).

[166] Wang, T., Huang, P., Zhou, Y., Liu, W., Ma, H., Wang, S., and Zeng, G. "High Key Rate Continuous-Variable Quantum Key Distribution with a

Real Local Oscillator". In: *Optics Express* 26.3 (Feb. 2018), pp. 2794–2806. ISSN: 1094-4087. DOI: 10.1364/OE.26.002794. (Visited on 12/02/2021).

[167] WANG, T., HUANG, P., ZHOU, Y., LIU, W., and ZENG, G. "Pilot-Multiplexed Continuous-Variable Quantum Key Distribution with a Real Local Oscillator". In: *Physical Review A* 97.1 (Jan. 2018), p. 012310. DOI: 10.1103/PhysRevA.97.012310. (Visited on 09/29/2023).

[168] WANG, T., ZUO, Z., LI, L., HUANG, P., GUO, Y., and ZENG, G. "Continuous-Variable Quantum Key Distribution Without Synchronized Clocks". In: *Physical Review Applied* 18.1 (July 2022), p. 014064. DOI: 10.1103/PhysRevApplied.18.014064. (Visited on 02/01/2023).

[169] WANG, X., ZHANG, Y., YU, S., and GUO, H. "High Speed Error Correction for Continuous-Variable Quantum Key Distribution with Multi-Edge Type LDPC Code". In: *Scientific Reports* 8.1 (July 2018), p. 10543. ISSN: 2045-2322. DOI: 10.1038/s41598-018-28703-4. (Visited on 07/20/2022).

[170] WANG, X., ZHANG, Y., YU, S., and GUO, H. "High Efficiency Postprocessing for Continuous-Variable Quantum Key Distribution: Using All Raw Keys for Parameter Estimation and Key Extraction". In: *Quantum Information Processing* 18.9 (July 2019), p. 264. ISSN: 1573-1332. DOI: 10.1007/s11128-019-2381-8. (Visited on 07/26/2024).

[171] WEEDBROOK, C., LANCE, A. M., BOWEN, W. P., SYMUL, T., RALPH, T. C., and LAM, P. K. "Quantum Cryptography Without Switching". In: *Physical Review Letters* 93.17 (Oct. 2004), p. 170504. DOI: 10.1103/PhysRevLett.93.170504. (Visited on 12/02/2021).

[172] WEEDBROOK, C., PIRANDOLA, S., GARCIA-PATRON, R., CERF, N. J., RALPH, T. C., SHAPIRO, J. H., and LLOYD, S. "Gaussian Quantum Information". In: *Reviews of Modern Physics* 84.2 (May 2012), pp. 621–669. ISSN: 0034-6861, 1539-0756. DOI: 10.1103/RevModPhys.84.621. arXiv: 1110.3234. (Visited on 12/08/2021).

[173] WEEDBROOK, C., PIRANDOLA, S., LLOYD, S., and RALPH, T. C. "Quantum Cryptography Approaching the Classical Limit". In: *Physical Review Letters* 105.11 (Sept. 2010), p. 110501. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.105.110501. arXiv: 1004.3345 [quant-ph]. (Visited on 09/29/2023).

[174] Wei, K., Hu, X., Du, Y., Hua, X., Zhao, Z., Chen, Y., Huang, C., and Xiao, X. "Resource-Efficient Quantum Key Distribution with Integrated Silicon Photonics". In: *Photonics Research* 11.8 (Aug. 2023), pp. 1364–1372. ISSN: 2327-9125. DOI: 10.1364/PRJ.482942. (Visited on 04/17/2024).

[175] Wei, K., Li, W., Tan, H., Li, Y., Min, H., Zhang, W.-J., Li, H., You, L., Wang, Z., Jiang, X., Chen, T.-Y., Liao, S.-K., Peng, C.-Z., Xu, F., and Pan, J.-W. "High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics". In: *Physical Review X* 10.3 (Aug. 2020), p. 031030. DOI: 10.1103/PhysRevX.10.031030. (Visited on 04/17/2024).

[176] Weyl, H. *The Classical Groups: Their Invariants and Representations*. Princeton University Press, 1946. ISBN: 978-0-691-05756-9.

[177] Wyner, A. "Recent Results in the Shannon Theory". In: *IEEE Transactions on Information Theory* 20.1 (Jan. 1974), pp. 2–10. ISSN: 1557-9654. DOI: 10.1109/TIT.1974.1055171. (Visited on 07/19/2024).

[178] Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W. "Secure Quantum Key Distribution with Realistic Devices". In: *Reviews of Modern Physics* 92.2 (May 2020), p. 025002. DOI: 10.1103/RevModPhys.92.025002. (Visited on 02/01/2023).

[179] Yang, Y.-H., Li, P.-Y., Ma, S.-Z., Qian, X.-C., Zhang, K.-Y., Wang, L.-J., Zhang, W.-L., Zhou, F., Tang, S.-B., Wang, J.-Y., Yu, Y., Zhang, Q., and Pan, J.-W. "All Optical Metropolitan Quantum Key Distribution Network with Post-Quantum Cryptography Authentication". In: *Optics Express* 29.16 (Aug. 2021), pp. 25859–25867. ISSN: 1094-4087. DOI: 10.1364/OE.432944. (Visited on 07/28/2024).

[180] Zhang, Y.-C., Li, Z., Chen, Z., Weedbrook, C., Zhao, Y., Wang, X., Huang, Y., Xu, C., Zhang, X., Wang, Z., Li, M., Zhang, X., Zheng, Z., Chu, B., Gao, X., Meng, N., Cai, W., Wang, Z., Wang, G., Yu, S., and Guo, H. "Continuous-Variable QKD over 50km Commercial Fiber". In: *Quantum Science and Technology* 4.3 (May 2019), p. 035006. ISSN: 2058-9565. DOI: 10.1088/2058-9565/ab19d1. arXiv: 1709.04618. (Visited on 12/02/2021).

[181] Zhang, G., Haw, J. Y., Cai, H., Xu, F., Assad, S. M., Fitzsimons, J. F., Zhou, X., Zhang, Y., Yu, S., Wu, J., Ser, W., Kwek, L. C., and Liu, A. Q. "An Integrated Silicon Photonic Chip Platform for Continuous-

Variable Quantum Key Distribution". In: *Nature Photonics* 13.12 (Dec. 2019), pp. 839–842. ISSN: 1749-4893. DOI: 10.1038/s41566-019-0504-5. (Visited on 02/01/2023).

[182] ZHANG, Y., CHEN, Z., PIRANDOLA, S., WANG, X., ZHOU, C., CHU, B., ZHAO, Y., XU, B., YU, S., and GUO, H. "Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 Km of Fiber". In: *Physical Review Letters* 125.1 (June 2020), p. 010502. DOI: 10.1103/PhysRevLett.125.010502. (Visited on 04/17/2024).

[183] ZHANG, Y., HUANG, Y., CHEN, Z., LI, Z., YU, S., and GUO, H. "One-Time Shot-Noise Unit Calibration Method for Continuous-Variable Quantum Key Distribution". In: *Physical Review Applied* 13.2 (Feb. 2020), p. 024058. DOI: 10.1103/PhysRevApplied.13.024058. (Visited on 07/23/2024).

[184] ZHAO, Y., ZHANG, Y., HUANG, Y., XU, B., YU, S., and GUO, H. "Polarization Attack on Continuous-Variable Quantum Key Distribution". In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 52.1 (Nov. 2018), p. 015501. ISSN: 0953-4075. DOI: 10.1088/1361-6455/aaf0b7. (Visited on 09/25/2023).

[185] ZOU, M., MAO, Y., and CHEN, T.-Y. "Rigorous Calibration of Homodyne Detection Efficiency for Continuous-Variable Quantum Key Distribution". In: *Optics Express* 30.13 (June 2022), pp. 22788–22797. ISSN: 1094-4087. DOI: 10.1364/OE.461680. (Visited on 07/24/2024).