ICFO – Institut de Ciències Fotòniques
&
UPC – Universitat Politècnica de Catalunya

Doctoral Thesis

Toward integrating continuous-variable quantum key distribution technology

Author:
Jennifer D. Aldama Guardia

Thesis supervisor:
Prof. Dr. Valerio Pruneri
Co-supervisor:
Dr. Sebastian Etcheverry

2023

To my family

ABSTRACT

Being able to secure confidential information is imperative in today's society, but advancements in quantum technologies pose a potential threat. In response, researchers are developing technologies based on quantum mechanics, such as quantum key distribution (QKD), in particular continuous-variable QKD (CV-QKD), which is emerging as a promising solution due to its compatibility with classical network infrastructures. However, current systems remain bulky and costly, limiting their widespread adoption. To address this challenge, the miniaturization and integration of QKD systems into monolithic photonic integrated circuits (PICs) has the potential to accelerate adoption across a broader market. This is due to the anticipated reductions in size, power consumption, production costs and overall system complexity.

This work presents four pulsed Gaussian-modulated coherent state (GMCS) CV-QKD systems based on discrete components and, in the last case, a PIC. The thesis begins with a modular system utilizing discrete components, such as phase and amplitude modulators. Notably, this prototype eliminates the need for phase locking, as the same laser serves as both a local oscillator and the source for generating quantum signals. The system mitigates Rayleigh backscattering by employing two channels, one for transmitting classical light and the other for transmitting the Gaussian modulated coherent states. Demonstrations indicate its operability over metropolitan distances.

In the second approach, the system showcases the parallelization of CV-QKD signals and the coexistence of multiple quantum signals with a classical signal, spatially multiplexed through a multicore fiber (MCF). In this scenario, two lasers are employed, with one emitting the frequency locking signal propagating along one of the MCF's core.

The third proposal introduces a simplified CV-QKD transmitter (TX) that eliminates the need for a phase modulator in the GMCS generation. This system

leverages the random properties of a distributed feedback (DFB) laser operating in the gain-switching (GS) mode. The study demonstrates the applicability of our proposed compact TX for GMCS generation in CV-QKD and its feasibility for integration into a metropolitan network.

Finally, we describe and characterize an InP-based PIC TX tailored for CV-QKD applications. System-level proof-of-principle experiments are conducted using a shared laser approach with a pulsed GMCS CV-QKD protocol over an 11 km optical fiber channel. The results indicate potential secret key rates of 52 kbps in the asymptotic regime and 27 kbps in the finite size regime, highlighting the capabilities of the proposed PIC design and, more broadly, the properties of InP technologies for monolithic integration of CV-QKD systems. All the proof-of-principle experiments outlined in this dissertation contribute significantly to the field of miniaturizing CV-QKD systems.

RESUMEN

La capacidad de asegurar información confidencial es imperativa en la sociedad actual, pero los avances en tecnologías cuánticas plantean una amenaza potencial. En respuesta, los investigadores están desarrollando tecnologías basadas en la mecánica cuántica, como la distribución cuántica de claves (QKD), en particular QKD de variable continua (CV-QKD), que está surgiendo como una solución prometedora debido a su compatibilidad con las infraestructuras de redes clásicas. Sin embargo, los sistemas actuales siguen siendo voluminosos y costosos, lo que limita su adopción generalizada. Para abordar este desafío, la miniaturización e integración de sistemas QKD en circuitos fotónicos integrados (PICs) monolíticos tienen el potencial de acelerar su adopción en un mercado más amplio. Esto se debe a las reducciones anticipadas en tamaño, consumo de energía, costos de producción y complejidad del sistema en general.

Este trabajo presenta cuatro sistemas pulsados de CV-QKD de estado coherente con modulación Gaussiana (GMCS) basados en componentes discretos y, en el último caso, en un PIC. La tesis comienza con un sistema modular que utiliza componentes discretos, como moduladores de fase y amplitud. Es importante destacar que este prototipo elimina la necesidad de bloqueo de fase, ya que el mismo láser sirve tanto como oscilador local como fuente para generar señales cuánticas. El sistema mitiga la retro dispersión de Rayleigh mediante el uso de dos canales, uno para transmitir luz y otro para transmitir estados coherentes. Las demostraciones indican su funcionamiento sobre distancias metropolitanas.

En el segundo enfoque, el sistema muestra la paralelización de las señales de CV-QKD y la coexistencia de múltiples señales cuánticas con una señal clásica, multiplexadas espacialmente a través de una fibra multi-núcleo (MCF). En este escenario, se utilizan dos láseres, con uno emitiendo la señal de

sincronización de frecuencia que se propaga a lo largo de uno de los núcleos de la MCF.

La tercera propuesta introduce un transmisor (TX) de CV-QKD simplificado que elimina la necesidad de un modulador de fase en la generación de GMCS. Este sistema aprovecha las propiedades aleatorias de un láser de retroalimentación distribuida (DFB) que opera en el modo de conmutación de ganancia (GS). El estudio demuestra la aplicabilidad de nuestro compacto TX propuesto para la generación de GMCS en CV-QKD y su viabilidad para la integración en una red metropolitana.

Finalmente, describimos y caracterizamos un TX basado en InP diseñado para aplicaciones de CV-QKD. Experimentos de prueba de concepto a nivel de sistema fueron realizados utilizando el método de láser compartido con el protocolo GMCS CV-QKD pulsada a través de un canal de fibra óptica de 11 km. Los resultados indican tasas de claves secretas potenciales de 52 kbps en el régimen asintótico y 27 kbps en el régimen de tamaño finito, destacando las capacidades del diseño de PIC propuesto y, más ampliamente, las propiedades de las tecnologías InP para la integración monolítica de sistemas de CV-QKD. Todos los experimentos de prueba de concepto delineados en esta tesis contribuyen significativamente al campo de la miniaturización de sistemas de CV-QKD.

RESUM

La capacitat d'assegurar informació confidencial és imperativa en la societat actual, però els avenços en tecnologies quàntiques plantegen una amenaça potencial. En resposta, els investigadors estan desenvolupant tecnologies basades en la mecànica quàntica, com la distribució quàntica de claus (QKD), en particular la QKD de variable contínua (CV-QKD), que està emergint com una solució prometedora a causa de la seva compatibilitat amb les infraestructures de xarxes clàssiques. No obstant això, els sistemes actuals continuen sent voluminosos i costosos i en limiten l'adopció generalitzada. Per abordar aquest desafiament, la miniaturització i la integració de sistemes QKD en circuits fotònics integrats monolítics (PICs) tenen el potencial d'accelerar l'adopció en un mercat més ampli. Això és degut a les reduccions anticipades en mida, en consum d'energia, en costos de producció i en la complexitat del sistema en general.

Aquest treball presenta quatre sistemes de CV-QKD d'estat coherent gaussià modulat per polsos (GMCS), basats en components discrets i, en l'últim cas, en un PIC. La tesi comença amb un sistema modular que utilitza components discrets, com a moduladors de fase i d'amplitud. És important destacar que aquest prototip elimina la necessitat del blocatge de fase, ja que el mateix làser serveix tant com a oscil·lador local com a font per generar senyals quàntics. El sistema redueix la retrodispersió de Rayleigh mitjançant l'ús de dos canals, l'un per transmetre llum i l'altre per transmetre estats coherents. Les demostracions indiquen la operabilitat que tenen sobre distàncies metropolitanes.

En el segon enfocament, el sistema mostra la paral·lelització dels senyals de CV-QKD i la coexistència de múltiples senyals quàntics amb la d'un senyal clàssic, multiplexades espacialment a través d'una fibra multicore (MCF). En

aquest escenari, s'empren dos làsers, un dels quals emet el senyal de sincronització de freqüència que es propaga al llarg d'un dels nuclis del MCF.

La tercera proposta introdueix un transmissor (TX) de CV-QKD simplificat que elimina la necessitat d'un modulador de fase en la generació de GMCS. Aquest sistema aprofita les propietats aleatòries d'un làser de retroalimentació distribuïda (DFB) que opera en el mode de commutació de guany (GS). L'estudi demostra l'aplicabilitat del compacte TX proposat per a la generació de GMCS en CV-QKD i la viabilitat que té per a la integració en una xarxa metropolitana.

Finalment, descrivim i caracteritzem un TX basat en InP dissenyat per a aplicacions de CV-QKD. Es realitzen experiments de prova de concepte, a nivell de sistema, utilitzant un enfocament de làser compartit amb un protocol de GMCS CV-QKD polsat sobre un canal de fibra òptica d'11 km. Els resultats indiquen potencials taxes de claus secretes de 52 kbps en el règim asimptòtic i 27 kbps en el règim de mida finita, i posen de manifest les capacitats del disseny de PIC proposat i, més àmpliament, les propietats de les tecnologies InP per a la integració monolítica de sistemes de CV-QKD. Tots els experiments de prova de concepte delineats en aquesta tesi contribueixen significativament al camp de la miniaturització de sistemes de CV-QKD.

ACKNOWLEDGMENTS

During the almost 5 years that I have been working on my PhD I have had the privilege of meeting some amazing people who have contributed, in one way or another, to the development of this thesis. The list is long, but I think is worth mentioning them here.

I would like to start by expressing my sincere gratitude to my supervisor, **Valerio,** for his guidance and time, as well as for the opportunity to work in his group on this project. I appreciate all of his support. Moreover, I would like to thank the **committee members** for examining this thesis and for their valuable comments.

I also want to thank all the post-docs from whom I have learned a lot: my co-supervisor, **Sebastian**, for his guidance, motivation and time, for introducing me to this field of QKD, and for imparting his experience in the lab; **Raju,** for sharing his lab experience with CV-QKD systems; **Ignacio**, for all the suggestions in the experimental part and for the insightful discussions; my (unofficial) co-supervisors, **Samael**, for all the motivation, orientation, time, code instruction and useful discussions - thanks for always encouraging me to do my best; **Luis**, for the motivation, time, helpful discussion and unfailing guidance with infinite patience. Thanks also to both **Samael** and **Luis** for taking the time to revise this manuscript and for always providing valuable feedback.

Thank you as well to the collaborators from outside ICFO, **Eleni**, **Amine**, **Yoann**, **Alberto** and **Tobias**, for the useful discussions regarding the PIC TXs. I have learned a lot from their experience.

Thanks to **Lisa Ruby** and **Roser** for revising the English and Catalan redaction of this manuscript.

I would also like to thank all the people with whom I had the chance to interact in the labs L101, Corning lab, and L103. I have learned from them all: **Mariela**, **Latifa**, **Sofia**, **Robin**, **Alvaro**, **Daniel T.**, **Alex**, **Stefano**, **Chiara**, **Davide**,

Abigail, **Alberto** and **Nico**. Thanks to **Saeed** and **Lorenzo** for their help with the codes for the FPGA. **Daniel M.** and **Bruno** thanks for their guidance with the probe-station and SMU instrument. Also, thank you to the **OPTO family: Kavitha**, **Rinu** and **Rafäel**, for welcoming me to the group and for such a nice time outside ICFO, and to the rest of the group for the fun, enjoyable lunchtimes, and their attentive guidance when I asked them anything.

Many thanks also to the ICFO staff: electronic (**Jose Luis** and team) and mechanical (**Xavi** and team) workshop, facilities staff (**Carlos** and team), purchasing (**Magda** and **Santiago**), PPL and chemistry lab (**Vittoria**). Their excellent work has contributed greatly to the development of this thesis. Also, HR, academic affairs, logistics, IT, KTT, travel office, outreach, front desk and the cleaning team: thank you for making my arrival and PhD journey at ICFO so delightful.

Thanks to all the lovely people that I met at ICFO for the nice talks in the corridors and cafeteria, and the plans we made outside ICFO. They have all made my time in Castelldefels, Barcelona and at ICFO so enjoyable. **Daniel U.** and **Nestor**, I never imagined that planning our first activity together on my 3rd day in Castelldefels (visiting Sitges after Claudia's house) would be the beginning of such good friendships and the first of many plans together. Thank you! **Hitesh**, **Andrew** and **Marcelo,** thank you as well for all the amazing years making after work plans at ICFO, and for your friendship. Thanks to **all five of you**, for the academic, philosophic and random talks. Special thanks to **Stephy** for your valuable friendship, the many trips, hiking, lunches, talks, etc. we spent together. Who knew that a simple chat in the washroom would be the start of a great friendship, and lead to me being a part of your wedding celebrations in India?! **Thomas**, thanks for your true friendship, and for the amazing memories here in Spain and with your family in India.

Away from the academic world, thanks to all my friends outside Spain and to those that I had the chance to meet in Castelldefels and Barcelona. I am very grateful for their friendship, suggestions, spiritual support and for making my life so enjoyable outside the lab. **Maira**, **Roser**, **Pablo O.**, **Natalia** and **Diana B.**, thanks for your always good company and interesting talks. **Acacias and Puignovell team**, **Victoria, Ivette**, **Belén**, **Gonzalo**, **Flor**, **Cris**, **Fr. Xavier**, **Catalina**, **Valentin**, **Amaka**, **Nneka**, **Kate**, **Kasia**, **Fr. Enrique**, **Fr. M. Ángel**, **Gaby**, **Daniela**, **John**, **Chris**, **Fr. Juan Antonio**, **Yasmin**, **Nerea**, **Manel, Josep**, **Judit**, **Cristina**, **Javi**, **Pablo**, **Edu**, **Diana**, **Alejandro, Andrea, Grzegorz, "DV" family**, and many more that I have not mentioned.

Mi particular agradecimiento a **Rosina** y a quien fue **Carmina**, por la buena compañía de ambas, por las buenas conversaciones y por hacer que estar en el piso sea agradable. Su alegría, espíritu servicial y juvenil, a pesar de sus años, me enseñaron tanto. Gracias a toda la **familia de Carmina y Rosina** que me ha hecho sentir muy acogida en esta tierra extranjera.

Último y no menos importante, mi gran agradecimiento a toda mi familia. En especial a mi **mamá**, mi **papá**, **Jacqui**, **Sofi** y **Janet**, que a pesar de la distancia siempre han estado apoyándome a seguir avanzando, animándome en los buenos y no tan buenos momentos. Gracias por estar siempre ahí, a través de una llamada, un mensaje, o unas agradables vacaciones familiares cuando se podía. Su apoyo ha sido pieza clave para el desarrollo de este doctorado.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY OF TERMS

AM	Amplitude Modulator
AMP	Electrical Amplifier
AS	Auxiliary Signal
ASE	Amplified Spontaneous Emission
Bd	Baud
BD, BPD	Balanced Photodetector
bps	bits per second
BS	Beam Splitter
BT	Bias Tee
BW	Bandwidth
CIPS	Current-Injection Phase Shifter
CR	Clock Rate
CW	Continuous Wave
CV-QKD	Continuous-Variable Quantum Key Distribution
DAC	Digital-to-Analog Converter
DPMCS	Dual-Phase Modulated Coherent State
DFB	Distributed Feedback Laser
DSP	Digital Signal Processing
DV-QKD	Discrete Variable Quantum Key Distribution
EAM	Electro-Absorption Modulator
ECL	External Cavity Laser
ER	Extinction Ratio
FPGA	Field Programmable Gate Array
FSE	Finite-Size Effects
GMCS	Gaussian-Modulated Coherent States
GS	Gain-switched
GSG	Ground-Signal-Ground
IL	Insertion Loss
InP	Indium Phosphide
ISO	Optical Isolator
ITS	Information Theoretic Security
Mbps	Megabits per second
MCF	Multicore Fiber
MMI	Multimode Interferometer
MPW	Multi-Project Wafer
MZI	Mach-Zehnder Interferometer
MZM	Mach-Zehnder Modulator
LO	Local Oscillator
OBPF	Optical Bandpass Filter

OH	Optical Hybrid (90º OH)
OSC	Oscilloscope
PBS	Polarization Beam Splitter
PC	Polarization Controller
PD	Photodetector
PE	Parameter Estimation
PIC	Photonic Integrated Circuit
PID	Proportional-Integral-Derivative
PM	Phase Modulator
PoM	Power Meter
PSP	Passive-State-Preparation
PW	Pulse width
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
QS	Quantum Signal
RTO	Real-Time Oscilloscope
RX	Receiver
SDM	Space Division Multiplexing
SKR	Secret Key Rate
SMF	Single Mode Fiber
SNR	Signal to Noise Ratio
SNU	Shot Noise Units
SSC	Spot Size Converter
TLO	Transmitted Local Oscillator
TOPS	Thermo-Optic Phase Shifter
TRN	True Random Number
TX	Transmitter
VOA	Variable Optical Attenuator

Chapter 1

INTRODUCTION

For thousands of years civilization has attempted to communicate securely and to find ways to hide information from non-authorized people. Examples are the Caesar cipher used by Julius Caesar around 100 BC and the Enigma machine designed by Arthur Scherbius at the beginning of the 20th century [1]. Currently, fueled by technology developments, new methods and protocols are under research to protect communications. One of these, the so-called continuous-variable quantum key distribution (CV-QKD), is the main topic of this thesis.

This chapter presents an introduction to the thesis by answering the following questions:

- **Why**, that is the motivation to develop quantum key distribution technology;
- **What**, that is the objectives of the thesis;
- **How**, that is the technology implementation to achieve the objectives.

1.1 Motivation

We are in the midst of the so-called second quantum revolution or quantum 2.0 [2], and many technologies based on quantum mechanics are under development, such as quantum computers and quantum cryptography. Quantum computers will allow us to efficiently perform computational tasks that are unattainable with classical computers. These include modeling the quantum behavior of electrons, elucidating the electronic structure in crystals,

and calculating the reaction dynamics in complex chemical and biological molecules, among others [2]. However, these advancements are a threat to some of the cryptographic systems we use to protect digital data. In 1994, it was theoretically proven by Shor [3] that a quantum computer could be used to efficiently solve factorization and discrete logarithm problems, something that would break Rivest-Shamir-Adleman (RSA) [4] and elliptic curve cryptosystems [5], widely used today in the Internet. One of the main threats against secure communications is that an eavesdropper may intercept and store the exchanged information, and then decrypt it at a later date when a sufficiently large quantum computer is available or when a way to solve the classical algorithm is discovered ("store now-decrypt later" attacks) [6]. This is a danger to the security of critical data and institutions such as finance and bank accounts, healthcare data, cloud and data centers, governments, and defense agencies. To address these challenges, quantum cryptography provides an effective solution for long-term security called quantum key distribution (QKD) [7], [8], which, combined with post-quantum cryptography (PCQ), can provide quantum-safe communication that is practical in many scenarios [9], [10].

QKD protocols enable two distant network nodes to exchange a cryptographic secret key with information-theoretic security (ITS), preventing eavesdroppers from gaining access to the key without being detected [11], [12]. This allows the distribution of secret keys with an arbitrary level of security without being vulnerable to computational attacks, thus providing a constant degree of security over time (long-term security), something that is essential for some applications (health, business, military, etc.). Being aware of this QKD advantage, for which there is currently no classical alternative, governments are investing a lot of resources into national and international projects to develop QKD technology. An example is the Quantum Flagship [13] launched in

2019, in which the Optoelectronics Group at ICFO is involved. Moreover, commercial QKD systems are being offered by several companies around the world, including LuxQuanta (Spain) [14], ID Quantique (Switzerland) [15], Toshiba (UK) [16], KEEQuant (Germany) [17], QuantumCTek (China) [18] and MagiQ QPN (USA) [19], to mention just a few.

Despite the undeniable progress over the last few decades, QKD has not yet found its way to wide adoption, commercialization, and deployment. From a technological point of view, current QKD systems are expensive, bulky, and relatively challenging to operate, and, consequently, are less accessible to the market for use on a large scale. How to overcome these roadblocks and, hence, showcase the enormous potential of QKD for securing communications and data transmission in a wide range of applications is an outstanding challenge.

To this end, the application of CV-QKD technology [20] offers a compelling alternative to the extensively studied discrete-variable (DV) QKD systems [21]–[23]. CV-QKD emerges as a particularly apt choice for this purpose due to its unique attributes. In particular, CV-QKD equipment is very similar to the hardware used in coherent optical communication networks (a prevailing standard in metro and long-haul optical networking), potentially being compatible with these systems. This facilitates the integration of the devices and the coexistence in the existing optical network infrastructure [24], also potentially reducing the cost compared with DV-QKD alternatives.

1.2 Thesis Objectives

In this thesis, we explore and experimentally implement several CV-QKD system designs for network operation with a view to miniaturizing the technology. To this end, the main objectives of this thesis are:

- Fabricate a robust CV-QKD system, employing off-the-shelf components, capable of generating secret keys for short (≤10 km) and medium (≤25 km) distances.
- Take advantage of the spatial dimensionality of multi-core optical fibers (MCF) to boost the CV-QKD secret key rate, demonstrating the coexistence of multiple CV-QKD links and a classical channel multiplexed in the same MCF.
- Reduce the CV-QKD system's complexity by using single commercially available laser component.
- Push the scalability of CV-QKD systems through the use of photonic integrated circuit (PIC).

1.3 Thesis Outline

This thesis is organized as follows (diagrams of the different CV-QKD systems implemented in this thesis are presented in Figure 1.1):

Chapter 2 introduces the concept of QKD, the advantages of CV-QKD and the GMCS CV-QKD protocol. The digital signal processing (DSP) chain used throughout this thesis is also explained, including QKD parameter estimation (PE).

Chapter 3 describes modular CV-QKD systems based on discrete/bulky components such as external cavity lasers and phase or amplitude modulators. Two different schemes are studied. The first one distributes the same laser for the generation and reception of the coherent states (shared laser with true local oscillator scheme), and the second one uses two different lasers (true local oscillator scheme). The first solution is implemented using single-mode fibers (SMFs), while the second one uses a 7-core MCF.

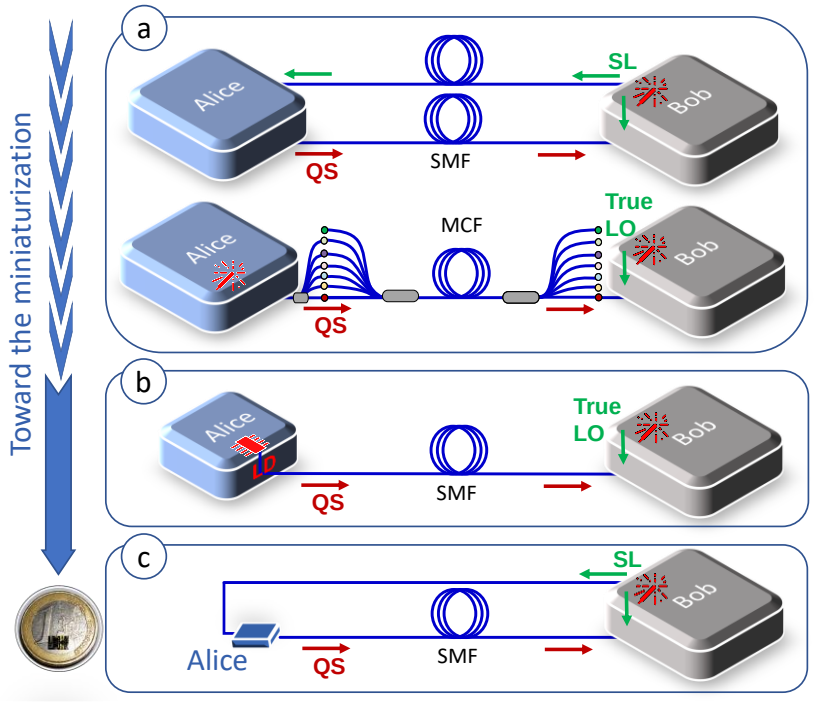

Figure 1.1: Summary of the evolution of the different implemented systems in this thesis towards the miniaturization of CV-QKD systems. (a) Chapter 3: modular CV-QKD systems using a shared laser (SL) and a true local oscillator (LO) plus single-mode fiber (SMF) and multicore fiber (MCF) in the channel. (b) Chapter 4: CV-QKD system using a gain-switched laser diode (LD) for the GMCS generation. (c) Chapter 5: CV-QKD system using a photonic integrated circuit transmitter such as the one shown on the top of the 1 euro coin on the left side of the figure. QS, quantum signal sent through the channel.

Chapter 4 provides a simple scheme for GMCS generation based on the intrinsic randomness of a laser diode working in the gain-switching mode. This avoids the use of an external quantum random number generator (QRNG).

Chapter 5 presents a PIC CV-QKD TX based on the InP integration platform. These results demonstrate the viability of miniaturizing CV-QKD TXs and bringing CV-QKD technology closer to wide adoption.

Chapter 6 summarizes the main results of this thesis and provides a brief outlook on potential future developments.

1.4 List of Publications

This thesis contains results and discussions which are in preparation or are published in peer-reviewed journals:

1.4.1. Publications Included in this Thesis

- R. Valivarthi*, S. Etcheverry*, J. Aldama, F. Zwiehoff, and V. Pruneri. **Plug-and-play continuous-variable quantum key distribution for metropolitan networks**. *Optics Express*, 28(10), 2020.

Author contribution: My contributions to this work include the characterization of the modular components and the CV-QKD experiments with the assistance of other researchers in the group. In addition, I contributed to the preparation of the manuscript.

- S. Sarmiento*, S. Etcheverry*, J. Aldama*, I. H. López, L. T. Vidarte, G. B. Xavier, D. A. Nolan, J. S. Stone, M.J. Li, D. Loeber, and V. Pruneri. **Continuous-variable quantum key distribution over a 15 km multi-core fiber**. *New Journal of Physics*, 24(6), 2022.

Author contribution: My contributions to this work include the characterization of the multi-core fiber and the characterization of the modular components. I carried out the setup implementation, the CV-QKD measurements, and the analysis of the data with other researchers involved in the project. In addition, I contributed to the preparation of the manuscript.

- J. Aldama*, S. Sarmiento*, S. Etcheverry, R. Valivarthi, I. H. López-Grande, L. Trigo-Vidarte, and V. Pruneri. **Small-form-factor Gaussian-**

modulated coherent-state transmitter for CV-QKD using a gain-switched DFB laser. *Optics Express*, 31(4), 2023.

Author contribution: My contributions to this work include the CV-QKD setup implementation, and the CV-QKD experimental measurements using codes written with the assistance of other researchers in the group. Also, I contributed to the analysis and interpretation of the data with the other researchers in the project. In addition, I contributed to the preparation and critical revision of the manuscript.

- J. Aldama*, S. Sarmiento*, S. Etcheverry, I. López-Grande, L. Trigo-Vidarte, L. Castelvero, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri. **InP-based CV-QKD PIC Transmitter**. *Optical Fiber Communication Conference*, paper M1I.3. Optica Publishing Group, 2023.

Author contribution: In this work, I contributed to the experimental part, including the characterization of the photonic integrated circuits, implementation of the system, and CV-QKD experiments using the codes written in collaboration with other members of the group. In addition, I co-wrote the manuscript with contributions from all other authors.

- J. Aldama, S. Sarmiento, L. Trigo-Vidarte, S. Etcheverry, I. López-Grande, L. Castelvero, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri. **InP-based PIC transmitter for CV-QKD systems** (in preparation).

Author contribution: My contributions to this work include the electro-optical characterization of the PICs, the development of the system, the CV-QKD measurements, and the asymptotic and finite-size analysis of the data. I performed the post-processing of the raw data using the codes discussed

and written with the assistance of other researchers in the group. I am writing the manuscript with contributions from all other authors.

1.4.2. Other Relevant Publications and Conference Presentations

- J. Aldama, S. Sarmiento, I. López-Grande, S. Signorini, L. Trigo-Vidarte, and V. Pruneri. **Integrated QKD and QRNG Photonic Technologies**. *J. Light. Technol.*, 40(23), 2022.
- I. Lopez-Grande*, S. Etcheverry*, J. Aldama, S. Ghasemi, D. Nolan, and V. Pruneri. **Adaptable transmitter for discrete and continuous variable quantum key distribution**. *Opt. Express*, 29(10), 2021.
- J. Aldama, S. Sarmiento, S. Etcheverry, I. López-Grande, L. Trigo-Vidarte, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri. **Characterization of an InP-based CV-QKD PIC Transmitter**. *ICIQP 2022*, Copenhagen, Denmark, October 2022 (Poster presentation).
- J. Aldama, S. Sarmiento, S. Etcheverry, I. López-Grande, L. Trigo-Vidarte, A. Hinojosa, T. Beckerwerth, A. Rhouni, E. Diamanti, and V. Pruneri. **Photonic Integrated CV-QKD System**. *7th ePIXfab silicon photonics summer school*, Paris, France, June 2022 (Poster Presentation-Best Poster Award).
- J. Aldama, S. Sarmiento, S. Etcheverry, I. López-Grande, L. Trigo-Vidarte, A. Hinojosa, T. Beckerwerth, A. Rhouni, E. Diamanti, and V. Pruneri. **Experimental Characterization of an InP-based PIC Transmitter for CV-QKD Applications**. *EQTC 2021*, Online Conference, December 2021 (Poster presentation).

Chapter 2

SCIENTIFIC BACKGROUND

Since the first meeting between the pioneers of quantum cryptography, Bennett and Brassard in San Juan (Puerto Rico, 1979), which resulted in the first paper ever published on quantum cryptography in 1982 [25], several publications and advances in quantum cryptography, and specifically in QKD, have materialized [26]. This chapter presents an overview of QKD and the theoretical background related to continuous-variable QKD (CV-QKD).

2.1 Introduction to QKD

QKD is an innovative technology that enables two or more spatially separated users to distribute cryptographic keys through a public communication quantum channel with ITS, preventing eavesdroppers from gaining access to the key without being detected [6], [11], [12]. The security of the key is based on the fundamental laws of quantum physics, namely the Heisenberg principle and no-cloning theorem [7], [27], [28], with the properties of quantum signals allowing for the detection of an eavesdropper in the communication channel. Generally, this process involves encoding randomly selected bits onto individual quantum states, followed by conducting independent measurements on those bits. According to the information theory and the laws of quantum mechanics, we can calculate the information exchanged by the remote trusted parties and bind the information that a potential eavesdropper could obtain

from the communication. With these premises we can derive a shared secret key that is not vulnerable to computational attacks. This makes QKD a very favorable technology for applications requiring long-term security, and many experiments have shown that it is now a mature and reliable technology [21], [29]–[32].

For its implementation, there are two main distinctive protocols: discrete-variable (DV) and continuous-variable (CV) QKD. DV-QKD protocols employ a discrete set of quantum states in conjunction with single-photon detectors (SPDs), while CV-QKD protocols use a broader set of states in conjunction with coherent detection (homodyne or heterodyne detection, depending on whether one or two quadratures are measured simultaneously for each mode) [6], [12].

The first proposed QKD protocol, named BB84 (Bennet and Brassard,1984) [33], [34], proposed encoding the information in non-orthogonal quantum states such as horizontal, vertical, diagonal, and anti-diagonal polarization directions. Later, in 2001, the first CV protocol was presented by Cerf *et al* [35] using squeezed states of light. Then in 2002, Grosshans and Grangier [36] suggested a CV-QKD system with Gaussian-modulated coherent states (GMCS) using homodyne detection, which is commonly referred to as the GG02 CV-QKD protocol. An extension to this was put forward by Weedbrook *et al* in 2004 [37] using heterodyne detection, referred to as the GMCS CV-QKD protocol. It is this last protocol that is considered in this thesis.

2.2 Introduction to CV-QKD

CV-QKD is a variant of QKD based on quadrature modulation and coherent detection [20]. The use of homodyne or heterodyne detectors (coherent

detection), instead of single-photon detectors, makes CV-QKD systems potentially less expensive compared to DV-QKD. It also makes them more suitable for implementation in photonic integrated circuits (PICs) [38], [39] since coherent receivers can be integrated more easily [40]. CV-QKD could facilitate the use of QKD in telecommunication network infrastructures, as the systems can be implemented with mature components developed for telecommunications, all operating at room temperature. In addition, the CV-QKD signals can coexist with high-power classical light in the same fiber [41], [42], and offer higher secret key rates in short-reach metropolitan networks [6], [12].

Different approaches have been suggested to simplify and miniaturize CV-QKD systems. In terms of the modulation in CV-QKD transmitters, using a laser, a pulse carver and electro-optic modulators have been demonstrated in several works [38], [43]–[45]. In all the previously mentioned systems, an external QRNG is necessary to generate the random values to be encoded. An alternative is to use a phase-seeded source, which can readily encode the phase in the pulse, avoiding the use of an external QRNG by employing the intrinsically random quantum phenomenon in gain-switched laser diodes, as proposed by [46].

Moving forward to the integration of CV-QKD systems, the aim is to reach a fully photonic integrated solution. In this respect, several approaches have been reported using different platforms to explore the integration of some of the components needed in CV-QKD TXs and RXs, such as lasers [47], modulators [48]–[52], and photodetectors [48]–[51], [53], [54].

Because of its practicality [6], [12], [36], a well-known protocol for the implementation of CV-QKD systems is the GMCS protocol, which randomly modulates the quadrature components following a zero-centered Gaussian

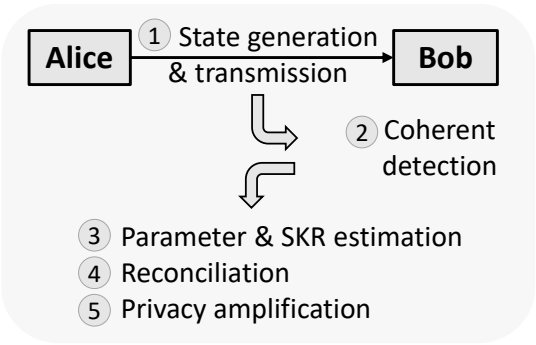

Figure 2.1: Summary of the CV-QKD process to establish a secret key. SKR: secret key rate.

distribution. GMCS systems have been proven to be secure against collective and coherent attacks [55]–[57] and under finite-size analysis [58], [59]. In experiments, this protocol has been implemented in both laboratory and field tests [41], [42], [60] – [71], showing transmission distances of up to 202.81 km [61] and high speeds of up to 66.8 Mbps [62]. The description of this protocol and the steps for establishing a secret key will be explained in the subsequent section.

2.3 GMCS CV-QKD protocol

The GMCS CV-QKD protocol involves several steps for establishing a secret key, guaranteeing the secure exchange of a cryptographic key between the users, typically referred to as Alice (transmitter) and Bob (receiver). The key can then be used to encrypt and decrypt messages, ensuring that they are kept confidential and secure. The process of CV-QKD typically involves the steps summarized in Figure 2.1 [72]. The first three steps, generation and transmission of the states, coherent detection, plus parameter and secret key rate (SKR) estimation, are covered in this thesis. Information related to the

remaining two, reconciliation (correcting the errors) and privacy amplification (key extraction), can be found in [20], [73].

2.3.1. Generation and Transmission of Quantum States

In the GMCS protocol, Alice prepares coherent states with quadratures $q_A = (X_A, P_A)$, modulated according to zero-centered Gaussian random distribution $X_A \sim P_A \sim N(0, V_A)$ with Alice's modulation variance V_A [27]. The quantum signals, consisting of coherent states, are obtained by attenuating the laser beam, and the quadratures of the electromagnetic field (X and P) can be derived from the phase and amplitude of the light field. After preparation, the coherent states are transmitted through the quantum channel to Bob, who subsequently conducts coherent detection.

2.3.2. Coherent Detection

In coherent detection, at Bob's site, the incoming optical signals interfere with a strong CW laser called a local oscillator (LO) in order to retrieve the quadrature values (the signal and the LO have the same wavelength). In contrast to direct detection, which only captures the amplitude fluctuations of the signals, coherent detection can recover the complete information of the optical signal. This includes the in-phase and quadrature (IQ) components (referred to in CV-QKD as the X and P quadratures[1]) of the optical electric field's complex amplitude, as well as the polarization state of the signal by using a second coherent detection system [74].

[1] X and P are the Cartesian coordinates corresponding to the polar coordinates, amplitude and phase.

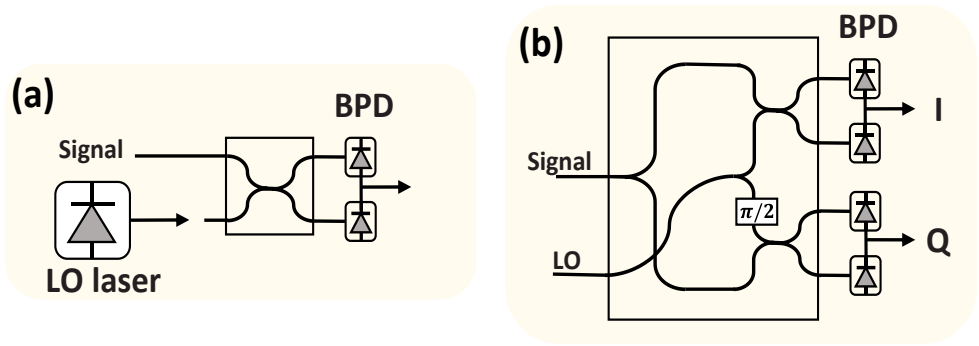

Figure 2.2: Configuration of two coherent receivers: (a) homodyne and (b) heterodyne receiver with balanced photodetectors (BPD). Adapted from [74].

The receiver can be either homodyne or heterodyne (see Figure 2.2). In homodyne detection, Bob randomly measures either the X or P quadrature by changing the phase of the LO between 0 and $\pi/2$. In heterodyne detection, both quadratures (X and P) of the signal measured by looking at the beat between the signal and the LO are measured simultaneously [74]. The simultaneous measurements are achieved by employing a 90° optical hybrid (OH) along with a pair of balanced photodetectors (BPDs), which eliminates the DC component and maximizes the beat between the signal and the LO. These definitions of "homodyne" and "heterodyne" detection are those used in CV-QKD literature [27]. Note that in the telecoms industry, the term "heterodyne receiver" refers to the data out of the baseband, while in CV-QKD it means simultaneous measurements of the quadratures (the equivalent of the term "heterodyne receiver" as defined in CV-QKD is the term "phase-diversity homodyne receiver" when used in telecoms [74]). In this thesis, we use the term "heterodyne receiver" as it is employed in CV-QKD.

At the output of the BPDs, the photocurrents are expressed as:

$$\begin{aligned} \mathrm{I(t)} &= RA_{LO}A_S\cos\big(\Delta\phi_{\mathrm{SLO}}(\mathrm{t})\big), \\ Q(\mathrm{t}) &= RA_{LO}A_S\sin\big(\Delta\phi_{\mathrm{SLO}}(\mathrm{t})\big), \end{aligned} \tag{2.1}$$

where R is the BPD responsiveness, A_{LO} is the amplitude of the local oscillator, A_S is the amplitude of the signal, and $\Delta\phi_{\mathrm{SLO}}(\mathrm{t}) = \phi_{\mathrm{S}}(\mathrm{t}) - \phi_{\mathrm{LO}}(\mathrm{t})$ is the difference in phase between the signal and the LO laser. More details related to coherent detection can be found in [75]–[77].

The heterodyne detection scheme simplifies the implementation compared with GG02 as the phase of the LO does not need to be randomly changed. In early implementations of CV-QKD, the LO was generated by Alice from the same laser as the quantum signals, and then transmitted to Bob. This scheme is called a transmitted local oscillator (TLO) and allows a stable phase relation between the quantum signals and the LO. However, transmitting the LO may open up security issues that could allow an eavesdropper to gain information about the key. Therefore, in most of the modern implementations, the LO is generated at Bob with a second laser (called a true LO, real LO, or local LO), which solves the security problems but adds complexity to the system as the two lasers need to be frequency-locked to some extent, and a phase relation between the two lasers needs to be established, by using reference pulses, for instance [43].

2.3.3. Parameter and SKR Estimation

After the coherent detection, Bob gets the states $q_B = (X_B, P_B)$ with Gaussian distribution of the form $q_B \sim N(0, V_B)$ and variance V_B, which is related to the states sent by Alice, as explained in the following subsection. From the measured experimental values, it is possible to estimate the relevant parameters involved in the QKD security proofs and obtain the information bounds between the parties (assuming that all the uncalibrated noise, or excess noise, is due to eavesdropper action). This allows us to have a preliminary

estimation of the expected average SKR in the asymptotic and finite-size scenarios (assuming a particular performance during the subsequent stages of reconciliation and privacy amplification). Implementation errors are undistinguishable from the errors introduced by an eventual eavesdropper, so it is important to reduce these as much as possible in order to obtain a good performance.

- *Parameter Estimation in the Asymptotic and Finite Size Scenarios*

QKD protocols are typically implemented using a prepare and measure scheme, but for practical purposes, it is more convenient to do the security analysis using an equivalent entanglement-based version of the protocol, as in [27]. For protocols with Gaussian modulation and heterodyne detection, the covariance matrix between Alice's mode and one of Bob's two modes $\left(\Sigma_{AB_{1,2}}\right)$ is expressed as Eq. (2.2) with the variances in shot noise units (SNUs) [27]:

$$\Sigma_{AB_{1,2}} = \begin{pmatrix} (V_A + 1)\mathbb{1}_2 & \pm\sqrt{\frac{\eta T}{2}(V_A^2 + 2V_A)}\sigma_z \\ \pm\sqrt{\frac{\eta T}{2}(V_A^2 + 2V_A)}\sigma_z & \left(\frac{1}{2}\eta T V_A + \xi_{B_q} + \nu_{elec} + 1\right)\mathbb{1}_2 \end{pmatrix}, \quad (2.2)$$

where η is the detection efficiency, T is the transmittance of the channel, ν_{elec} is the electronic noise variance, ξ_{B_q} is the excess noise measured in one of the quadratures and σ_z is the third Pauli matrix. The variance in the quadrature distribution at Alice V_A and Bob V_B, in the case of heterodyne detection, is related by:

$$V_B = \frac{1}{2}\eta T V_A + \xi_{B_q} + \nu_{elec} + 1, \quad (2.3)$$

where V_A is related to the mean photon number $\langle n \rangle$ at Alice's output by the formula $V_A = 2\langle n \rangle$. The variance in Bob's measurement conditional on Alice's data is [27]:

$$V_{B|A} = \xi_{B_q} + \nu_{elec} + 1, \quad (2.4)$$

which is equivalent to:

$$V_{B|A} = var\left(\sqrt{\frac{\eta T}{2}}\hat{q}_A - \hat{q}_B\right), \quad (2.5)$$

where $\hat{q}_A = \{X_{A_i}, P_{A_i}\}$ and $\hat{q}_B = \{X_{B_i}, P_{B_i}\}$ are Alice's and Bob's measured coherent states, respectively. Their units are $\sqrt{SNU}$ in order to be consistent with the other terms. This normalization to SNUs can be performed independently at Alice's and Bob's sites as explained in Section 2.4.4

For practical parameter estimation (PE), the excess noise at Bob's site can be estimated from Eq. (2.4) and the conditional variance $V_{B|A}$ in Eq. (2.5) [27] as:

$$\xi_{B_q} = var\left(\sqrt{\frac{\eta T}{2}}\hat{q}_A - \hat{q}_B\right) - \nu_{elec} - 1. \quad (2.6)$$

Hence, the excess noise in Alice's output will be given by Eq. (2.7):

$$\xi_A = 2\xi_{B_q}/(\eta T). \quad (2.7)$$

Here the channel loss was taken into account as a potential security threat controlled by an eavesdropper (Eve). Therefore, T has to be estimated by correlating Alice's and Bob's data as:

$$\mathrm{T} = \frac{2}{\eta}\left(\frac{\langle \mathrm{q_A q_B} \rangle}{\mathrm{V_A}}\right)^2, \tag{2.8}$$

where $\langle q_A q_B \rangle$ is the inner product of Alice's and Bob's measured states [27]. The variances and different noises are normalized to SNU. A detailed calculation of the parameters for CV-QKD system in the asymptotic regime (T, $\mathrm{V_A}$) can be found in [27], [78].

For the finite size analysis, *m* values are used for the PE from the total number of symbols *N* exchanged by Alice and Bob during the protocol. The remaining values (*n=N-m*) are not revealed and can be used for the generation of the secret key. In this scenario, for the PE, let's first consider the normal model to relate Alice and Bob's data (x and y, respectively):

$$y = tx + z, \tag{2.9}$$

with the parametrization $t = \sqrt{\eta \mathrm{T}/2}$. From this we get (when compared with Eq. (2.3)) the variance of *x* as V_A, the variance of *y* as V_B, and the variance of *z* as:

$$\sigma^2 = \xi_{B_q} + \nu_{\mathrm{elec}} + 1. \tag{2.10}$$

Consequently, from Eq. (2.2), the covariance matrix that minimizes the SKR due to the PE will be expressed as [79]:

$$\Sigma_{AB_{1,2}}^{PE} = \begin{pmatrix} (V_A + 1)\mathbb{1}_2 & \pm t_{min}\sqrt{(V_A^2 + 2V_A)}\sigma_z \\ \pm t_{min}\sqrt{(V_A^2 + 2V_A)}\sigma_z & (t_{min}^2 \mathrm{V_A} + \sigma_{max}^2)\mathbb{1}_2 \end{pmatrix}, \tag{2.11}$$

where t_{min} is the minimum value of *t* and σ_{max}^2 is the maximum value of σ^2 that minimize the SKR (these values are conditioned on being compatible with the measured data). This means that we have now bounded our confidence region.

Therefore, the PE, taking into consideration the finite size effects, can be calculated from [79]:

$$t_{min} \approx \hat{t} - \Delta\hat{t} = \hat{t} - z_{\epsilon_{PE}/2}\sqrt{\frac{\hat{\sigma}^2}{mV_A}},$$
$$\sigma^2_{max} \approx \hat{\sigma}^2 + \Delta\hat{\sigma}^2 = \hat{\sigma}^2 + z_{\epsilon_{PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \quad (2.12)$$

where $\hat{t}$ and $\hat{\sigma}^2$ are the values estimated from the experimental realization, and $z_{\epsilon_{PE}/2} = \sqrt{2}erf^{-1}(1-\epsilon_{PE}) \approx 6.5$ if we consider a security value $\epsilon_{PE} = 10^{-10}$; and *erf* is the error function.

We can rewrite Eq. (2.10) as a function of the total excess noise measured at Bob's site:

$$\sigma^2 = \xi_{B_q} + \sigma_0^2\,,$$
$$\xi_{B_q} = (\sigma^2 - \sigma_0^2)\,, \quad (2.13)$$

where $\sigma_0^2 = (\nu_{\text{elec}} + 1)$.

Taking into consideration the calibration imperfections of the electronic noise and the shot noise, the estimated excess noise in Eq. (2.13) is bound and re-defined as [80]:

$$\xi_{B_q}^{FS} = [(\hat{\sigma}^2 + \Delta\hat{\sigma}^2) - (\hat{\sigma}_0^2 - \Delta\hat{\sigma}_0^2)], \quad (2.14)$$

where $\Delta\hat{\sigma}_0^2$ is similar to $\Delta\hat{\sigma}^2$ in Eq. (2.12) and m' is the number of symbols used for the calibration estimation, then:

$$\Delta\hat{\sigma}_0^2 = z_{\epsilon_{PE}/2}\frac{\hat{\sigma}_0^2\sqrt{2}}{\sqrt{m'}}. \quad (2.15)$$

- *Secret Key Rate Estimation in the Asymptotic and Finite Size Scenarios*

Following the PE, the most pessimistic SKR in bits per second (bps), taking into consideration the finite-size effects (FSE), can be computed using the Devetak-Winter formula:

$$\mathrm{SKR_{FS}} = \left(\frac{\mathrm{N}-\mathrm{m}}{\mathrm{N}}\right)\Big[\beta \mathrm{I_{AB}}\left(\mathrm{V_A}, \boldsymbol{T_{min}}, \boldsymbol{\xi_{B_q}^{FS}}, \nu_{\mathrm{elec}}, \eta\right) - \chi_{\mathrm{BE}}\left(\mathrm{V_A}, \boldsymbol{T_{min}}, \boldsymbol{\xi_{B_q}^{FS}}, \nu_{\mathrm{elec}}, \eta\right) - \Delta(\mathrm{n})\Big]\mathrm{R_{eff}}\,, \tag{2.16}$$

where the minimum transmittance of the channel T_{min} is related to t_{min} (defined in Eq. (2.12)) as $t_{min} = \sqrt{\eta T_{min}/2}$. Eq. (2.16) is for the case of reverse reconciliation where Alice's information is corrected following Bob's measurements [20], where β stands for the reconciliation efficiency (efficiency of the error correcting code) [65], χ_{BE} is the Holevo bound, $\mathrm{R_{eff}}$ is the effective quantum pulse rate in Hz or pulses per second and $\Delta(n)$ is the parameter related to the security of the privacy amplification [79]. In this thesis, it was considered to be zero, because this work is focused on the PE finite size effect when this analysis was used. The term $\mathrm{I_{AB}}$ is the mutual information between Alice and Bob posed in Eq. (2.17) [27], and can be computed from the Shannon entropy and some experimental parameters. It gives the amount of information (in bits) that can be extracted from the system [81]:

$$\mathrm{I_{AB}} = \log_2\left(1 + \frac{\eta \mathrm{T} \mathrm{V_A}}{2 + 2\xi_{B_q} + 2\nu_{\mathrm{elec}}}\right). \tag{2.17}$$

In the asymptotic limit, it is assumed that the data used for the PE is large enough to make the correction terms ($\Delta\hat{t}, \Delta\hat{\sigma}^2, \Delta\hat{\sigma}_0^2$) all go to zero [79]. Subsequently, Eq. (2.16) in the asymptotic regime is simplified as:

$$\mathrm{SKR} = \left(\frac{\mathrm{N}-\mathrm{m}}{\mathrm{N}}\right)\Big[\beta \mathrm{I}_{\mathrm{AB}}(\mathrm{V}_{\mathrm{A}}, T, \xi_{B_q}, \nu_{\mathrm{elec}}, \eta) - \chi_{\mathrm{BE}}(\mathrm{V}_{\mathrm{A}}, T, \xi_{B_q}, \nu_{\mathrm{elec}}, \eta)\Big] \mathrm{R}_{\mathrm{eff}} \,. \tag{2.18}$$

2.4 Digital Signal Processing

In an experimental implementation of the GMCS CV-QKD protocol, the steps to obtain the secret key, explained in the previous section (Section 2.3), involve additional data manipulation. This is due to the fact that after distribution of the quantum states, the information measured by Bob is scrambled compared to the values assigned by Alice. This is mainly caused by the shot noise, in addition to the noise introduced by the channel and frequency fluctuations of the source, etc. Therefore, proper data analysis needs to be implemented.

In this thesis, the implemented digital signal processing (DSP) consists of five steps: downsampling, phase recovery, pattern synchronization, PE, and SKR estimation. These steps will be explained in the following subsections. Also, it is important to note that the first three steps are also those commonly followed in classical coherent communications.

2.4.1. Downsampling

The first step of the DSP, after signal acquisition, is the downsampling process. This involves detecting the power peaks of the received signals and obtaining one sample per symbol (state). The samples are reduced to one sample per symbol by periodically choosing those samples that maximize the energy of the

resulting signal. In the digital domain, the samples represent the signals evolving in time that contain the specific values (symbols) to be sent.

The sampling theory dictates that to accurately represent a temporal signal in the digital domain, a minimum of two samples per symbol is required. Typically, one aims to establish communication at a specific symbol rate, which is shared by both Alice and Bob. This rate is usually expressed in Bauds (1 Baud = 1 Bd = 1 symbol per second) and is directly linked to the bandwidth of the modulated signal.

2.4.2. Phase Recovery

In this thesis, the implemented phase correction procedure is that proposed by Qi *et al* [78]. It allows us to address the random phase drift of the signal pulses and the resulting scrambling of encoded information. In our systems, reference pulses are transmitted alongside the signal pulses in close proximity, allowing us to use the phase information carried by the reference pulses to extract the encoded phase information from the signal pulses.

To mitigate phase recovery noise, the intensity of the reference pulses is generally maintained at a significantly higher level than that of the signal pulses. The measured quadratures, X_{raw} and P_{raw}, are partitioned into two sets, one containing data from the reference pulses (X_R, P_R) and the other containing data from the signal pulses (X_S, P_S). The phase shift of the i^{th} quantum state ($\Delta\emptyset_{S_i}$) is calculated via a linear interpolation between the phases of the i^{th} and $(i^{th}+1)$ references ($\emptyset_{R_i}$ and $\emptyset_{R_{i+1}}$), expressed as [78]:

$$\Delta\emptyset_{S_i} = \frac{\emptyset_{R_i} + \emptyset_{R_{i+1}}}{2}, \tag{2.19}$$

where $\emptyset_{R_i} = \arctan\left(X_{R_i}/P_{R_i}\right)$, and X_{R_i} and P_{R_i} are the received quadratures of the i^{th} reference. Then the quadratures are remapped using the coordinate transformations:

$$\begin{aligned} \mathrm{X}_{corr_i} &= \mathrm{X}_{S_i}\cos\left(\Delta\emptyset_{S_i}\right) + P_{S_i}\sin\left(\Delta\emptyset_{S_i}\right), \\ P_{corr_i} &= -\mathrm{X}_{S_i}\sin\left(\Delta\emptyset_{S_i}\right) + P_{S_i}\cos\left(\Delta\emptyset_{S_i}\right). \end{aligned} \tag{2.20}$$

2.4.3. Pattern Synchronization

Regarding pattern synchronization, the time offset was removed by performing a cross-correlation between the transmitted and received quantum states.

2.4.4. Parameter & SKR Estimation

In CV-QKD, the measured quadrature values are converted from voltage units to SNUs [27]. For the experimental PE, a normalization of the signals to the SNUs needs to be performed before the other experimental parameters can be calculated. To do so, a calibration of the shot noise variance ($\mathrm{N_o}$) is required in the PE stage.

An estimation of $\mathrm{N_o}$ can be performed using Eq. (2.21) [82]:

$$\mathrm{N_o} = \widehat{\mathrm{N}}_{\mathrm{T}} - \widehat{\mathrm{V}}_{\mathrm{elec}}, \tag{2.21}$$

where $\widehat{N}_T$ and $\hat{V}_{elec}$ represent the variances in the total detection noise and electronic noise, respectively, measured in voltage-squared units. To measure $\widehat{N}_T$, the output-voltage variance of Bob's detectors is averaged when only the LO is activated [83], whereas the measurement of $\hat{V}_{elec}$ is conducted when both the signal and the LO are turned off. The $\mathrm{N_o}$ is used to normalize the signals to SNUs

at Bob's site. Thus, the normalized SNU value of $\hat{V}_{elec}$ is calculated as $\nu_{\mathrm{elec}} = \hat{\mathrm{V}}_{\mathrm{elec}}/\mathrm{N_o}$. And, the normalization of Alice's and Bob's experimental data ($\hat{q}_{A_0}$ and $\hat{q}_{B_0}$, respectively) to $\sqrt{SNU}$ is performed using the equations: $\hat{q}_A = \left(\hat{q}_{A_0}/std(\hat{q}_{A_0})\right)\sqrt{\mathrm{V_A}}$ and $\hat{q}_B = \hat{q}_{B_0}/\sqrt{\mathrm{N_o}}$, respectively. Using this calibration, the remaining calculations, PE and SKR, can be carried out as explained in Section 2.3.3.

The following three chapters focus on the experimental aspects. They include the specific theory related to each, and their respective analysis with experimental results.

Chapter 3

MODULAR CV-QKD SYSTEMS

The information, text, and figures in this section have been adapted, under the terms of the Creative Commons Attribution-Non Commercial license, from the original publications: "Plug-and-play continuous-variable quantum key distribution for metropolitan networks", R. Valivarthi, S. Etcheverry*, J. Aldama, F. Zwiehoff, and V. Pruneri. Optics Express, 28(10), 2020, and "Continuous-variable quantum key distribution over a 15 km multi-core fiber", S. Sarmiento*, S. Etcheverry*, J. Aldama*, I. H. López, L. T. Vidarte, G. B. Xavier, D. A. Nolan, J. S. Stone, M.J. Li, D. Loeber, and V. Pruneri. New Journal of Physics, 24(6), 2022.*

Continuous-variable quantum key distribution (CV-QKD) stands as a promising technological advancement, offering the potential to yield elevated secret key rates (SKRs) across metropolitan regions through the utilization of conventional telecoms components. In this chapter, we present a CV-QKD system employing off-the-shelf components for two different configurations. The first is based on a shared laser scheme and employs a 13 km standard single-mode fiber (SMF). In this configuration, the same laser is used as a local oscillator (LO) and as the quantum state source, so no frequency locking is required. Although the use of one laser simplifies the hardware requirements, if the LO and source of the quantum states are propagated over the same fiber, it will suffer from a strong Rayleigh back-scattering effect. To mitigate this problem, we employ two separate channels, one for laser signal distribution and the other for quantum signal transmission. The second proposed configuration considers the true LO scheme and a 15 km multi-core fiber (MCF).

Here, two lasers are frequency locked by taking advantage of a core to send a locking signal between Bob's and Alice's lasers. The remaining cores are used for the quantum signals. This proof of concept demonstrates the capacity of the MCF to boost the SKR through the parallelization of CV-QKD transmissions across multiple cores. These results highlight the viability of the proposed QKD approaches as cost-effective solutions for metropolitan optical networks. Moreover, the findings position MCFs as promising candidates for the metropolitan-scale deployment of robust QKD systems.

3.1. Introduction

In the initial demonstrations of CV-QKD, the LO, which serves as a reference signal necessary for coherent detection, was co-transmitted alongside the quantum signal [65], [66], [72], [83] – [85]. However, these early showcases have revealed susceptibilities to various side-channel attacks[2] stemming from the potential manipulation of the LO by eavesdroppers [86] – [89]. More recently, a CV-QKD system utilizing a “locally” generated LO at the receiver (also known as true LO configuration) has emerged, wherein the LO is generated at Bob's end, thereby safeguarding it from potential eavesdropping [43], [45], [47], [78], [90] – [95]. Although this advancement improves the security of practical CV-QKD systems, the implementation of CV-QKD in the true LO configuration mandates the use of two independent narrow linewidth lasers that must be frequency locked to some extent, introducing complexity to the system's experimental setup. Additionally, the maintenance of such locking over

[2] Side-channel attacks involve exploiting unintended information leakage from the physical implementation of the system in order to gain unauthorized access to the secret key exchanged between the two parties.

extended periods poses challenges, potentially compromising the long-term stability of the system [43], [93], [94].

This dilemma was overcome by Huang *et al*. [96], where a plug-and-play CV-QKD scheme featuring a true LO was conceptualized and tested. This approach utilizes a single laser, which functions both as an LO and also as the source for generating modulated quadratures, thereby obviating the need for two frequency locked lasers. The Huang *et al*. system employs two-way communication to implement a Dual-Phase Modulated Coherent State (DPMCS) protocol, employing homodyne detection. It has been demonstrated that its security is equivalent to that of the Gaussian-modulated coherent state (GMCS) protocol [20]. However, the reported plug-and-play CV-QKD method does encounter the challenge of Rayleigh back-scattering by the fiber refractive index inhomogeneities, in which the reflected light has the same wavelength as the initial laser source. Therefore, the proposed system suffers from noise generated by the high-power laser signal transmitted simultaneously with the quantum signal over the same fiber channel. The presence of this Rayleigh back-scattering noise restricts the system's performance and its maximum achievable secure communication distance when contrasted with one-way CV-QKD protocols [96]. The implications of Rayleigh back-scattering noise in the context of plug-and-play QKD, along with its effects on SKRs and maximum communication distances, have been explored both theoretically and experimentally for both DV-QKD [97], [98] and CV-QKD systems [96].

With regards to data communication, the increase in data capacity has been allowed by multiplexing different degrees of freedom in the SMF, such as wavelength, phase and time, as well as polarization multiplexing [99]. An alternative way to enhance the channel capacity and prevent future saturation in SMFs is via space division multiplexing (SDM) [100] – [103]. SDM can be

realized by employing an MCF, which has gained significant attention in recent years for augmenting data transmission rates (petabit-per-second [104]) in classical communication.

It is envisioned that MCFs, i.e., optical fibers with multiple cores within the same cladding, will play a fundamental role in future classical communications for several compelling reasons. Firstly, MCFs offer a solution to the impending shortages in network capacity [105]. Theoretically, the achievable rate of an N-core MCF corresponds to N times that of an SMF [106], [107]. In addition, they have a smaller footprint compared to a bundle of standard SMFs, making them highly advantageous, especially in telecoms data centers where space is limited.

Moreover, MCFs enable the use of a single amplifier for all the cores, reducing resource requirements and enhancing energy efficiency [108]. Furthermore, they are highly compatible with photonic integrated circuits (PICs) for multiple-input-multiple-output applications, making them promising candidates for both long-haul and metropolitan networks [108], [109]. Finally, MCFs have demonstrated low levels of crosstalk between different cores and exhibit losses similar to standard SMFs, making them suitable for co-propagating quantum and classical signals either in different cores or within the same core [107], [110] – [112]. A summary of experiments of classical and quantum signals over an MCF is shown in Table 3.1.

Table 3.1. Summary of experiments using MCF to propagate classical and quantum signals. Adapted from [8].

Ref.	Year	Number of cores	QKD system	Distance	Max. SKR	Notes
[110]	2016	7-core	DV	53 km	605 kbps	--
[113]	2018	7-core	DV	2.5 km	N/A	--
[114]	2018	7-core	DV	1 km	191 bps	--
[115]	2018	7-core	CV	9.8 km	4.8 Mbps/core	Specific details of the secret key calculation and implementation were not provided.
[112]	2019	19-core	CV	10.1 km	47 Mbps	See [44].
[116]	2019	7-core	DV	1 km	10.9 kbps	--
[107]	2019	37-core	DV	7.9 km	62.8 Mbps	See [111]
[117]	2020	7-core	DV	1 km	920 bps	--

MCFs also offer significant benefits for quantum communication. For instance, they facilitate greater phase stability among different cores due to similar environmental effects experienced by co-propagated signals, enabling the transmission of spatially encoded photonic quantum states [118]. Moreover, MCFs are well-suited for transmitting high-dimensional photonic states that utilize the transverse degree of freedom of a single photon [119]. Initial QKD experiments using MCFs employed path-encoded qudits[3] over a distance of 300 m [32], as well as silicon-based PICs [120]. In another study, a 411 m 19-core MCF was utilized to distribute polarization-entangled photon pairs through 12 channels simultaneously [121]. Notably, MCFs have extended the distance for high-dimensional quantum communication protocols from 2 km to 11 km [118], [122], and have also been utilized in constructing multiport beam splitters for quantum information applications [123].

To date, the use of CV-QKD in MCFs has not been extensively studied. In 2018, it was demonstrated that the fan-in and fan-out devices required in MCFs

[3] Quantum state in a *d*-dimensional Hilbert space

could degrade the performance of CV-QKD protocols [124], but the total secret key rate (SKR) could be increased through parallelization. In the same year, a proof of concept of a "quantum-to-the-home" network employing CV-QKD through a 9.8 km 7-core MCF was demonstrated [115]. In this case, an aggregated SKR of 33.6 Mbps was obtained using a discrete modulation with four symbols. However, specific details of the secret key calculation and implementation were not provided in [115]. Studies related to the security analysis of discrete-modulated CV-QKD can be found in [125] – [127]. In 2019, a 10.1 km 19-core MCF was used to demonstrate classical and QKD transmission [44], [112], with 6 cores utilized for QKD and 13 cores for classical coherent signals.

This chapter presents the results of two experiments employing the GMCS CV-QKD protocol. Firstly, we focus on the implementation of a modular CV-QKD prototype with a shared laser across a 13 km SMF that can be integrated into networks. The system minimizes the noise from Rayleigh back-scattering by relying on two-way communication, where two different SMF strands are used to distribute the laser signal from Bob to Alice and to send the quantum states from Alice to Bob. Contrary to previous work [96], besides minimizing the effect of Rayleigh back-scattering, the present design allows the implementation of the GMCS protocol with heterodyne detection, for which a general and composable security proof has been developed [58].

Secondly, we present the previously implemented modular CV-QKD system but with a true LO [39], [78], [90], [94] across a 15 km MCF, the longest distance over which CV-QKD has been transmitted with these fibers. This was achieved by using one core to transmit an auxiliary signal to frequency lock Alice's and Bob's lasers, a common requirement in QKD implementations, while the other cores were used to send the quantum signals. This scheme enhances

the spatial sharing capabilities of MCFs, which prove more advantageous than dedicating a single fiber solely for this purpose.

The results show that the GMCS CV-QKD protocol can be deployed in MCFs to boost the SKR by parallelizing CV-QKD across multiple cores. These outcomes offer the potential for advancing the deployment of CV-QKD systems into metropolitan networks. To elucidate these findings, this chapter starts with a detailed description of the experimental setup for both experiments, followed by the detector calibration and the phase correction procedure. Finally, parameter estimation and SKR estimation for both experiments are discussed.

3.2. Experimental Setup

In this section, we present the two implemented CV-QKD systems described above using telecoms components. Their setups and results will be shown as two experiments in independent sections.

3.2.1. Experiment 1: CV-QKD with a Shared Laser over a SMF

The implemented CV-QKD system is shown in Figure 3.1(a). The source of light, located at Bob's site, is a 10 kHz linewidth continuous-wave (CW) external cavity laser (ECL), with a tunable single-mode operation in the entire C band and 54 mW maximum power output at 1550 nm wavelength. The CW laser is followed by a 90:10 beam splitter (BS1), where, for simplicity, 90% of the light is directly used as Bob's CW local oscillator (LO) for heterodyne detection. The other 10% is sent to Alice through a 13 km fiber spool (Corning SMF28 ULL fiber) for quadrature modulation. At Alice's site, a polarization controller (PC1)

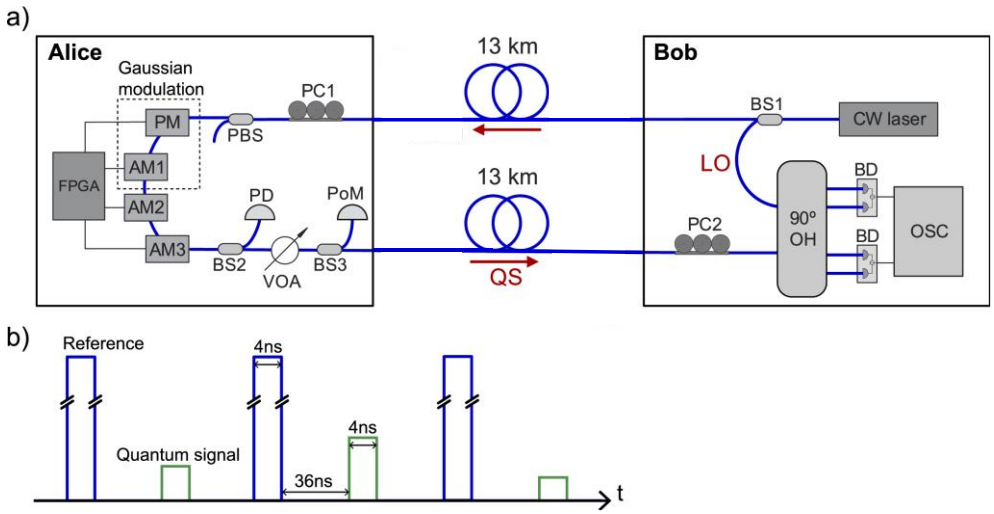

Figure 3.1: (a) Plug-and-play CV-QKD system. AM, amplitude modulator; PM, phase modulator; PD, photodiode; PoM, power meter; VOA, variable optical attenuator; PC, polarization controller; PBS, polarizing beam splitter; BS, beam splitter; 90◦ OH, 90◦ optical hybrid; OSC, oscilloscope; BD, balanced detector; LO, local oscillator; QS, quantum signal. (b) Signals sent from Alice to Bob, where the reference pulses and the quantum signals are interleaved in time.

and a polarizing beam splitter (PBS) are employed to filter out polarization modes and optimize the performance of subsequent electro-optic modulators.

Following the GMCS protocol [20], Alice generates weak optical pulses known as coherent states of light, with their X and P quadratures modulated according to zero-centered Gaussian random distributions (see Section 2.4 in Chapter 2). To achieve these Gaussian distributed quadratures, Alice employs an amplitude modulator (AM1) to pulse the light with an amplitude according to Rayleigh distribution, as well as a phase modulator (PM) to encode the phase information into the pulses following the uniform random distribution [85]. A scheme of the generated pulses is depicted in Figure 3.1(b), where the pulses of the quantum signals (with Rayleigh and uniform distribution in amplitude and phase, respectively) are interleaved in time with constant reference pulses and no encoded phase information. The reference pulses allow Bob to compensate

for phase drifts caused by the channel and the laser, and retrieve the quadrature values sent by Alice [78]. The phase correction procedure is further described in Section 3.3.2.

Following the AM1, a second AM (AM2) is incorporated to enhance the extinction ratio of the light pulses by modulating constant amplitude pulses that overlap with those generated by the AM1. For accurate recovery of the phase information, the amplitude of the reference pulses must be greater than that of the signal pulses (e.g., 500 times in Ref [91]). The ratio between the amplitudes of the reference and signal pulses (ρ) is determined by adjusting the bias set-point of a third AM (AM3) operating at half the clock frequency. The AMs are driven by a field programmable gate array (FPGA) and a 1 GSa/s digital-to-analog converter (DAC) unit. In this experiment, the RF electrical signals had a pulse width of 4 ns and a frequency of 25 MHz (Mpulses/s). The RF signals sent to the AM1 and PM consisted of two independent sets of 2048 pseudo-random values cyclically sent to the modulators. It is important to note that in a final CV-QKD system prototype, random numbers should be generated and sent continuously, using a QRNG, for instance [128].

After the AM3, a 50:50 beam splitter (BS2) and a PIN photodetector (PD) are employed to optimize the bias set-point of the modulators. A variable optical attenuator (VOA) is used to set the desired modulation variance (V_A), which maximizes the SKR for a given channel transmittance. Subsequently, a 99:1 beam splitter (BS3) directs 99% of the light to a power meter (PoM) in order to measure the mean photon number $\langle n \rangle$ and the modulation variance $V_A = 2\langle n \rangle$, which is set using the VOA (see Section 2.3.3 in Chapter 2). This modulation variance is known to the communicating parties beforehand. The remaining 1% of the light is sent to Bob through a second 13 km fiber spool (Corning SMF-28 ULL fiber). At Bob's end, a polarization controller (PC2) is

utilized to maximize the polarization overlap between the received pulses and the LO for optimal interference. The incoming optical pulses are directed to a 90° Optical Hybrid (90° OH), where they interfere with the LO. The four outputs of the 90° OH are detected by two balanced photodetectors (BDs), providing simultaneous measurements of the X and P quadratures. The output from the BDs is digitized using an Agilent MSO9404A 2.5 GSa/s oscilloscope (OSC) with a bandwidth fixed at 200 MHz, and subsequently, the data is collected and analyzed.

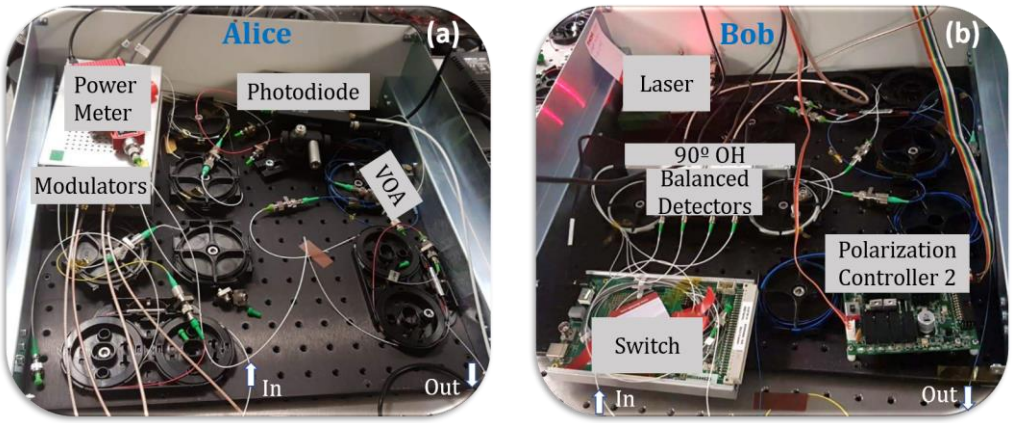

Figure 3.2: (a) Alice's rack and (b) Bob's rack containing the different components used in the plug-and-play CV-QKD experiment.

The proposed design minimizes the noise from Rayleigh backscattering, as the Rayleigh backscattered photons generated in the upper fiber spool pass through BS1 to the CW laser, which is equipped with an integrated isolator, preventing them from reaching the BDs. It should be noted that in the proposed plug-and-play system, most of the active components are located at Alice's, and Bob only needs to compensate for polarization drifts, which can be achieved by maximizing the amplitude of the detected quadratures. Another possibility is to utilize a polarization-diversity 90° OH [43] at Bob's end, eliminating the need

for active feedback mechanisms. Images of Alice's and Bob's racks implemented in this experiment are shown in Figure 3.2.

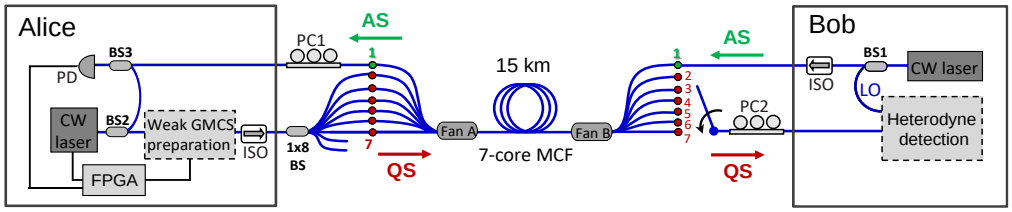

Figure 3.3: GMCS CV-QKD system using a 7-core MCF of 15 km length. FPGA, field-programmable gate array; PD, photodiode; BS, fiber beam splitter; ISO, optical isolator; PC, polarization controller; MCF, multi-core fiber; LO, local oscillator; AS, auxiliary signal used to lock the frequency of Alice's laser to the LO; QS, quantum signal.

3.2.2. Experiment 2: CV-QKD with a true LO over an MCF

This section presents a CV-QKD system with some modifications to the previous setup (Section 3.2.1). Instead of the shared laser technique, a common true LO technique was implemented in this experiment. Moreover, an MCF was utilized in the channel, taking advantage of one of the cores to propagate the light from Bob to Alice in order to lock the two 10 kHz linewidth CW ECLs. Here, one laser at Alice's site was for the generation of the signals, and the other one at Bob's site was used as the LO. At Alice, the CW laser was frequency-locked with Bob's LO at 1550 nm (see details below). The modified setup is illustrated in Figure 3.3.

The output of Alice's laser was directed into a series connection of four electro-optic modulators, BSs, PD, PoM, and a VOA to prepare and control the weak GMCS to be transmitted to Bob. The scheme used for the "weak GMCS preparation" was the same as that used at Alice's site in the previous experiment (see Section 3.2.1) shown in Figure 3.1. In this case, a ρ value of 300

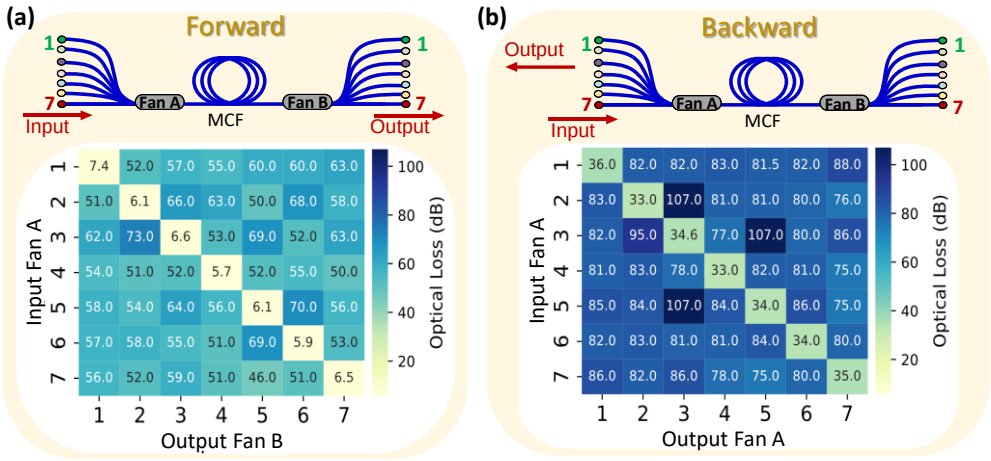

Figure 3.4: 15 km 7-core MCF characterization: optical losses including fan A and fan B devices in the (a) forward and (b) backward directions.

was determined to ensure accurate phase recovery. As with the previous experiment, the electro-optic modulators were driven by an FPGA and, again, two independent sequences of 2048 pseudo-random values were employed to generate the quantum states. As before, the pulses had a width of 4 ns (see Figure 3.1(b)), but this time the pulse rate was 31.25 Mpulses/s. The light output from the grey dashed box in Figure 3.3 was further divided by a Thorlabs 1x8 Dual-Window Fiber Optic Splitter to simulate signals originating from six different QKD transmitters. These signals were connected to an Optoscribe fan-in device (Fan A), enabling the multiplexing of the signals into a 15 km 7-core MCF spool developed by Corning Incorporated, with a cladding diameter of 132 μm and cores that support a single optical mode at telecom wavelengths[4]. Upon transmission, the signals were demultiplexed using an Optoscribe fan-out device (Fan B). The average insertion loss per core, including the fan-in and fan-out devices, was 6.3 dB (Figure 3.4(a)), while the backscattering loss remained

[4] Large cores that support a few or many spatial modes are called multimode fibers [105]. Those fibers were not employed in this thesis.

higher than 33 dB (Figure 3.4(b)). The forward crosstalk was above 46 dB, and the backward was above 75 dB, as can be seen in Figure 3.4(a) and Figure 3.4(b), respectively.

Bob, who was connected to each core of the MCF being measured, consisted of another ECL used as an LO and biased to emit 48 mW of optical power. To establish frequency locking between Alice's and Bob's lasers, the output of Bob's laser was split using a 99:1 fiber beam splitter (BS1). The 1% transmitted power was sent to Alice through core 1 (C#1), as this exhibited the highest insertion loss (7.4 dB - see Figure 3.4(a)). To minimize the frequency difference between the lasers, a voltage was applied to a piezoelectric element in Alice's laser cavity, and this real-time minimization process was facilitated by the FPGA. This involved measuring the interference between Alice's laser and the LO using a PIN photodiode (PD) and two 50:50 fiber beam splitters (BS2 and BS3), as illustrated in Figure 3.3.

The other output of the BS1 at Bob's site (99% of the laser output) was used as the LO in order to perform heterodyne detection (grey dashed box at Bob in Figure 3.3) using the same scheme as that presented in Figure 3.1(a). It includes a 90ºOH, two BDs, and a 1 GSa/s real-time OSC. Manual polarization controllers (PC1 and PC2) were utilized at Alice and Bob's inputs to optimize signal overlap, and optical isolators (ISOs) were employed at Alice and Bob's outputs to prevent Trojan horse attacks [129].

The post-processing necessary to characterize both proposed systems (CV-QKD systems using a shared laser and a true LO configuration) was conducted offline and involved several steps. It encompassed downsampling, quantum state phase recovery, pattern synchronization, parameter estimation, and SKR estimation in the asymptotic limit with reverse reconciliation. A

detailed description of the implemented digital signal processing (DSP) is presented in Section 2.4 in Chapter 2.

3.3. Analysis and Results

3.3.1. Detector Calibration

In order to achieve high sensitivity and shot noise limited detection, it is important to maximize the power of the LO within the linear operation range of the BDs. Figure 3.5(a) presents the shot noise variance as a function of the LO power, with the electronic noise variance subtracted from the measurements. In our setup, a linear relationship between the LO power and the shot noise variance was determined during the calibration of both BDs for power levels up to 54 mW, which is the maximum power of the laser. These measurements were performed by deactivating the signal from Alice and only activating the LO. For the experimental results described in this chapter, an LO power of around 49 mW was utilized, taking into consideration that 10% of the laser power was transmitted to Alice for quadrature modulation in Experiment 1 (see Figure

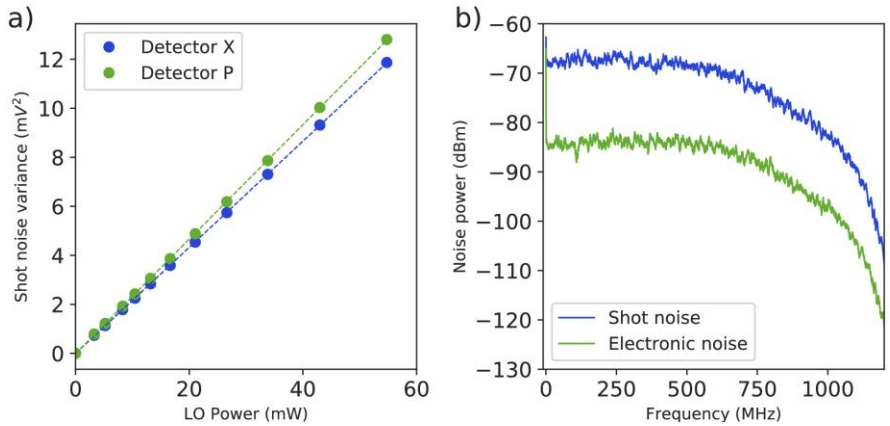

Figure 3.5: Balanced photodetector calibration. (a) Shot noise variance as a function of the local oscillator (LO) power, measured for both detectors. Electronic noise was subtracted from the measurements. (b) Comparison of the frequency spectrum of the shot noise and the electronic noise for an LO power of 49 mW.

3.1(a)), while 1% of the optical power output (48 mW) was sent to Alice to perform the locking of both lasers in Experiment 2 (see Figure 3.3).

Figure 3.5(b) displays the Fourier transform of the electronic noise and the shot noise for a power of 49 mW. An average clearance (defined as the ratio between shot noise variance and electronic noise variance) of 15.8 dB was achieved over the entire bandwidth of the detector (20 kHz-1 GHz). To enhance the signal-to-noise ratio, a low-pass bandwidth filter with a cutoff frequency of 200 MHz was employed at the input of the oscilloscope, resulting in an average clearance of 16.8 dB.

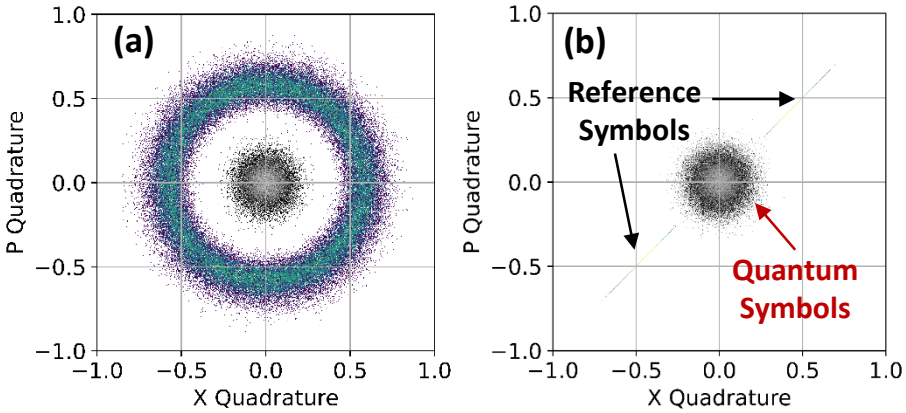

Figure 3.6: Constellation in arbitrary units (a) before and (b) after phase recovery using reference symbols (external ring). This testing was carried out using core 2 (C#2) of the 15 km 7-core MCF (similar results are obtained when using an SMF).

3.3.2. Phase Correction

As part of the DSP, phase correction of the signals has to be done. Figure 3.6 shows an example of the phase-space density of the received signal, before (a) and after (b) the phase recovery process, where the external symbols correspond to the reference and the inner symbols are the quantum symbols obtained from the received quantum states. As anticipated, the phase

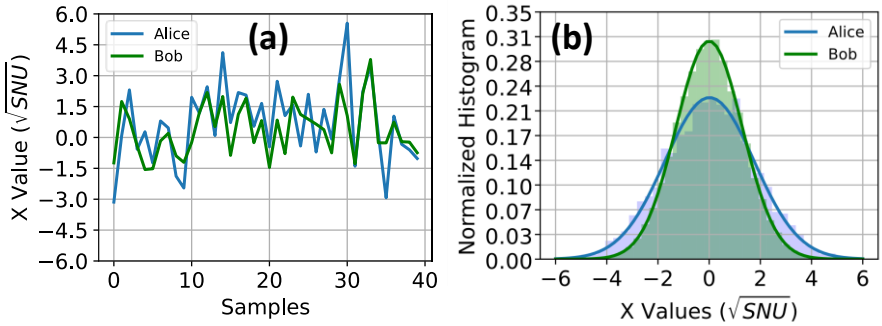

Figure 3.7: (a) Comparison of the first 40 symbols of Alice's (blue) and Bob's (green) data for the X quadrature obtained using C#2 of the 15 km 7-core MCF. (b) Histogram of the X quadrature data for Alice (blue) and Bob (green).

distribution of the raw signal and reference pulse exhibits are randomly distributed from 0 to 2π (Figure 3.6(a)). However, through the application of phase correction using Eq. (2.2), the quadratures are aligned to a specific phase value predetermined by Alice (Figure 3.6(b)). As previously mentioned, to minimize phase recovery noise, the intensity of the reference pulses is typically significantly higher than that of the quantum pulses. The resulting corrected quadratures are subsequently analyzed to determine the CV-QKD parameters and compute the SKR, as outlined in the following sections.

Figure 3.7(a) depicts the X quadrature of 40 symbols for Alice and Bob. Bob's data represents the signals detected following the phase recovery process, indicating a high level of correlation. Furthermore, Figure 3.7(b) illustrates that the quadratures from both Alice and Bob exhibit zero-centered Gaussian distributions.

3.3.3. Parameter and SKR Estimation

- *Experiment 1: CV-QKD with a Shared Laser Over a SMF*

A summary of the transmission parameters is listed in Table 3.2. Figure 3.8(a) illustrates the variation of the excess noise over 11 measurements conducted over a time span of 90 minutes, with V_A set to 2.18 SNU. The selected V_A was chosen because preliminary tests showed that a value of approximately V_A=2 SNU optimizes the SKR for a distance of 13 km. At this variance, the mean value of the total excess noise at Bob ξ_B was 16 mSNU (dashed blue line), ranging from 13 to 20 mSNU. The solid black line at $\xi_B = 37.5$ mSNU represents the threshold beyond which the SKR becomes zero. The measured excess noise comes from several sources [27], such as the error in the phase correction due to phase drift of the signal pulse compared to the reference pulse as they are generated at a time delay, errors due to the channel noise and shot noise added to the reference pulses, and the error coming from leak photons due to the finite dynamic range of the amplitude modulator [92] (details in Appendix A).

Table 3.2. Summary of the transmission parameters using an SMF in the channel and a shared laser configuration.

Parameter	Value
Alice's mean modulation variance, V_A	2.08 SNU
Electronic noise variance, ν_{elec}	22 mSNU
Reconciliation efficiency, β	0.95[65]
Detection efficiency, η	0.38
Ratio of intensity of reference pulses to that of quantum pulses, ρ	274
Effective quantum pulse rate, R_{eff}	12.5 Mpulses/s

In addition, the parameters V_A and $T\eta$ were monitored as depicted in Figure 3.8(b). The fluctuations primarily stem from variations in the bias set-point of the electro-optic modulators and polarization changes in the fiber, producing variations in the estimated SKR of between 0.49 Mbps and 0.88 Mbps, with an average value of 0.74 Mbps, as shown in Figure 3.9(a). Implementing

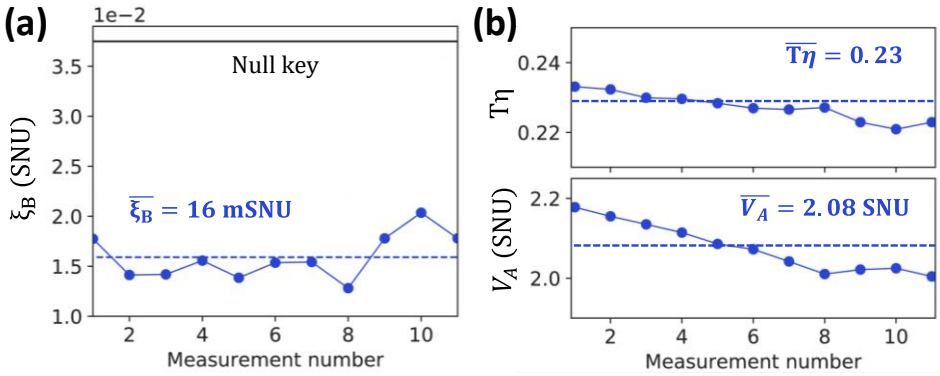

Figure 3.8: Results of 11 measurements taken over 90 minutes using an SMF in the channel. (a) Excess noise measured at Bob, where the dashed line is the average value and the black solid line represents the null SKR threshold. (b) Fluctuations of Tη (top) and modulation variance V_A (bottom) with their respective mean values as dashed lines. The experimental parameters are shown in Table 3.2.

active feedback mechanisms for polarization and modulator bias can enhance the system's stability and enable field demonstrations.

Lastly, Figure 3.9(b) presents an estimation of the SKR versus distance for the asymptotic analysis and trusted detectors. The graph highlights the potential for the present system to operate over a longer distance (28 km approx.) than that tested in the lab. Experimentally, we obtained an average SKR of 0.74 Mbps using a 13 km SMF, as marked with a blue dot on the graph. It is important to note that longer distances may reduce the accuracy of the phase correction algorithm and increase the excess noise, as the intensity of reference pulses decreases due to channel losses. This could be compensated, in principle, by increasing the intensity of the reference pulses at Alice [93].

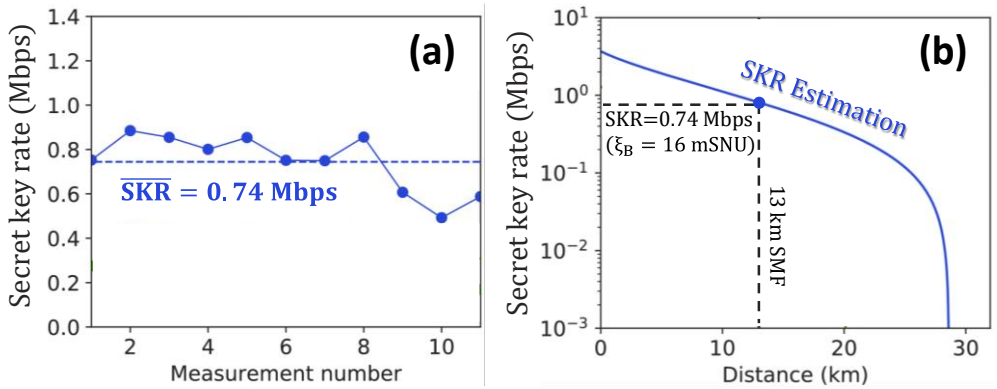

Figure 3.9: Estimated SKR (a) for 11 consecutive measurements (90 minutes) and (b) as a function of the distance. The employed experimental parameters are shown in Table 3.2.

- *Experiment 2: CV-QKD with a true LO Over an MCF*

Table 3.3. Summary of the transmission parameters using an MCF as the channel and a true LO configuration.

Parameter	Value
Alice's modulation variance, V_A	1.764 SNU
Electronic noise variance, v_{elec}	21 mSNU
Reconciliation efficiency, β	0.95 [65]
Detection efficiency, η	0.18
Ratio of intensity of reference pulses to that of quantum pulses, ρ	300
Effective quantum pulse rate, R_{eff}	15.625 Mpulses/s

The parameters used in this experiment are listed in Table 3.3. Figure 3.10 presents the results of 30 consecutive measurements taken over a period of 90 minutes using the MCF with C#2 (see Figure 3.3) to analyze the reproducibility and stability of the system. The monitored values are the excess noise ξ_B (Figure 3.10 (a)), and the transmittance T with the SKR (Figure 3.10 (b)). Each measurement considered a block size of 10^6 symbols (coherent states), and each independent block of symbols was used to calculate the ξ_B, T and SKR. Also, before each measurement, the shot noise and electronic noise variances were

calibrated. Experimentally, we obtained a mean excess noise value of 12 mSNU, with individual values consistently remaining well below the threshold where the SKR becomes null, which, in this system, was 45 mSNU (dashed red line in Figure 3.10 (a)). The excess noise encompassed different source noises, such as the phase estimation error due to the time delay between the reference and quantum symbols, and the noise due to the reference symbols [27] [92]. With regard to the other monitored parameters, the transmittance and SKR showed mean values of 0.673 and 0.3722 Mbps, respectively, for C#2. In addition, Figure 3.10(b) demonstrates that the value of T remained stable throughout the measurement period, with a relative standard deviation of 0.5%, while the SKR showed minimum and maximum values of 0.254 Mbps and 0.533 Mbps, respectively. The SKR was determined by utilizing the values obtained for the ξ_B and T, following Eq. (2.18) and using the whole symbols for the parameter and SKR estimation.

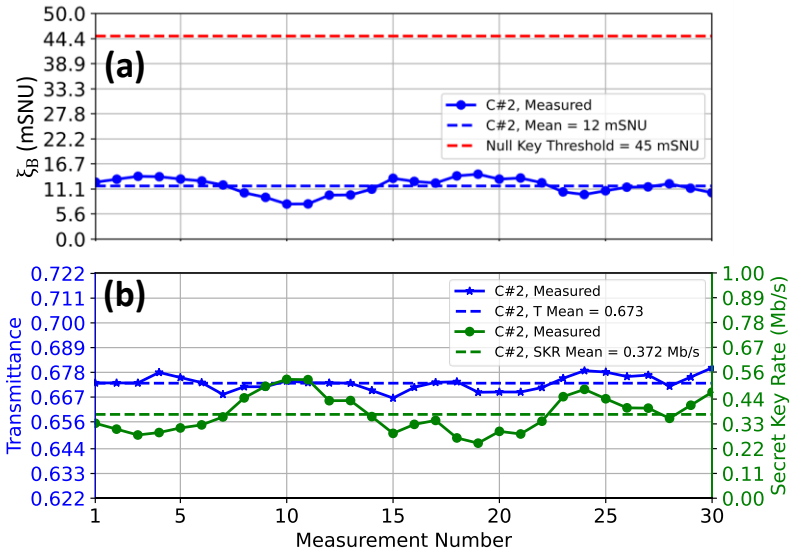

Figure 3.10: Results for 30 measurements taken over 90 minutes when C#2 of the 15 km 7-core MCF was being tested: (a) excess noise ($\boldsymbol{\xi_B}$), (b) channel transmittance ($\boldsymbol{T}$), and secret key rate ($\boldsymbol{SKR}$). Each measurement corresponded to a block size of 10^6 symbols or coherent states.

Finally, Table 3.4 shows the average values for the ξ_B, T and SKR obtained from 30 measurements (10^6 symbols per measurement) performed for each connected core of the 15 km 7-core MCF. It can be seen that the results were consistent across all six cores, leading to a potential aggregated SKR value of 2.3 Mbps. This aggregated SKR represents the sum of all the individual SKRs, as indicated in Table 3.4. Considering that the light from the QKD transmitter was divided into six cores (each measured individually at Bob), our experiment simulates a scenario involving six transmitters and six receivers. It is worth noting that the same V_A (Table 3.3) was employed in all CV-QKD cores, being nearly optimal for each of them to maximize the SKR. In practical scenarios, V_A values could differ within the margins of positive SKRs, which are relatively narrow for transmissions at medium and long-range distances. Therefore, exploring the diverse V_A values and assessing crosstalk between cores are pertinent aspects to consider. Preliminary measurements indicate that in order to observe a noticeable degradation in the SKR of a specific core, the average power of adjacent CV-QKD signals would need to exceed the V_A used in our reported experiment (see Table 3.2) by at least two orders of magnitude. Such a condition would allow for an adjacent power span higher than the practical V_A value range.

Table 3.4. Summary of the characterization of the proposed CV-QKD system, using a 15 km 7-core MCF, in terms of excess noise ($\boldsymbol{\xi_B}$), channel transmittance ($\boldsymbol{T}$), and secret key rate ($\boldsymbol{SKR}$) for each core. Each value is an average of 30 measurements, with a block size of 10^6 symbols per measurement.

C#	$\boldsymbol{\xi_B}$ (mSNU)	$\boldsymbol{T}$	$\boldsymbol{SKR}$ (Mb/s)
2	11.8	0.673	0.372
3	10.2	0.650	0.378
4	11.6	0.678	0.378
5	12.4	0.692	0.389
6	14.7	0.667	0.371
7	12.3	0.645	0.375

3.4. Conclusions

In a first experiment, we have presented a simple modular CV-QKD system over a 13 km ULL SMF with a shared laser, avoiding the need for two frequency stable lasers or frequency locking the lasers. The implemented system used the same laser as an LO and as a source for preparing the GMCS. In a second experiment, we demonstrated the implementation of a CV-QKD system over a 15 km MCF using a true LO configuration, where one core was used to transmit an auxiliary signal to facilitate the locking of the two lasers. Moreover, the MCF's ability to enhance the SKR through parallelization of CV-QKD across multiple cores was showcased, resulting in a potential aggregated SKR value of 2.3 Mbps. These findings hold significant promise for advancing the deployment of CV-QKD systems in metropolitan regions, harnessing the capabilities of next-generation telecom optical fibers.

Chapter 4

SINGLE-COMPONENT GMCS GENERATOR FOR CV-QKD

The information, text, and figures in this section have been adapted, under the terms of the Creative Commons Attribution-NonCommercial license, from the original publication: "Small-form-factor Gaussian-modulated coherent-state transmitter for CV-QKD using a gain-switched DFB laser", J. Aldama, S. Sarmiento*, S. Etcheverry, R. Valivarthi, I. H. López-Grande, L. Trigo-Vidarte, and V. Pruneri. Optics Express, 31(4), 2023.*

In the last years, different approaches have been proposed to simplify and miniaturize CV-QKD systems. In this chapter, we propose and implement a CV-QKD transmitter (TX) in which the Gaussian-modulated coherent states (GMCS) are generated and directly modulated following the random properties of quantum mechanics. In particular, we take advantage of the random nature of the phase when using a gain-switched (GS) laser diode. Our CV-QKD TX principally consists of a GS distributed feedback (DFB) laser and avoids the use of external modulators for the GMCS generation, reducing the system's complexity. The proposed CV-QDK TX has been proved over an 11 km fiber link, showing a potential asymptotic secret key rate value of 2.63 Mbps. The results make the proposed GMCS TX particularly suitable for metropolitan optical networks where compactness, robustness, and low cost are key desirable features.

4.1. Introduction

Random numbers are required in several applications. Some examples are the one-use PINs (bank tokens) for carrying out financial transactions, Monte Carlo simulations, and QKD systems. More specifically, in QKD systems there is a need for true random numbers (TRNs) to ensure that the key cannot be predicted and, thereby, maintain security. TRNs can be generated in different ways based on the unpredictable nature of classical phenomena that are complex now but could become predictable in the future by the development of mature theory. Another way to obtain TRNs is to use quantum random phenomena, which are inherently non-deterministic. These TRNs sources are random-certified and are known as quantum random number generators (QRNGs) [81], [130], [131].

QRNGs have been exploited by measuring different physical properties [81], [132], including single photon events [133] – [138], amplified spontaneous emission (ASE) [139], vacuum fluctuations [140], and phase noise in both continuous-wave (CW) [141] – [144] and pulsed semiconductor laser diodes [46], [128], [145], [146]. Among all these solutions, QRNGs based on laser phase noise have proven to be the fastest, with records showing a random generation speed of up to 68 Gbps using a CW laser diode driven by a constant current slightly above threshold and a coherent detector [143]. By pulsing the laser, the highest speed achieved thus far was 43 Gbps [46]. Specifically, in [46], a GS DFB laser was continuously modulated from below to above threshold in order to generate pulses with nearly identical amplitudes and completely randomized phases. The coherent detector was used to convert the phase fluctuations into amplitude fluctuations, which, after appropriate digitization, were transformed into random numbers. This scheme offers simplicity,

robustness, low cost, and flexibility in terms of multi-clock frequency, all suitable features for QKD systems which will require high-speed QRNG sources in the future. Finally, this technology has also been demonstrated using photonic integrated circuits (PICs) [147], [148].

The implementation of GMCS CV-QKD systems (see Section 2.3 in Chapter 2) needs random coherent states following a two-dimensional Gaussian distribution to make them unpredictable and irreproducible, in order to enhance the protocol's security. In the majority of GMCS CV-QKD implementations, the generation of random numbers and the preparation of coherent states are typically carried out using separate devices. This leads to a higher degree of complexity and cost, meaning that standardization is more difficult [36], [41], [42], [55], [56], [58] – [62], [64] – [71], [79], [149] – [151]. To address this issue, a passive-state-preparation (PSP) GMCS CV-QKD protocol has been proposed and experimentally validated in [152] – [155]. In this approach, the amplitude and phase modulators required for the state preparation, as well as the QRNG, have been replaced by an ASE source. While the PSP approach offers potential advantages in terms of lower complexity and cost, it presents technical challenges in frame synchronization due to the absence of modulators, necessitating additional bulk optical delay lines [155]. An alternative cost-effective solution that enables the preparation of GMCS and robust synchronization mechanisms without modulators, while also providing moderate complexity and high compactness, is the use of a directly modulated DFB laser. By exploiting the inherent frequency chirp of the DFB laser at large biasing currents, specific phase values can be generated for synchronization purposes [156] – [158]. Additionally, random coherent states can be generated

and prepared by operating the DFB laser in the gain-switching mode to ensure the true randomness of the coherent states.

Here, we present and demonstrate a simple and compact module for generating and modulating the coherent states required in the GMCS CV-QKD protocol. The module consists of a single pulsed GS DFB laser, which has the advantage that can be more easily integrated into PICs compared to narrow-linewidth lasers, leading to ultra-compact and ultra-low-cost GMCS CV-QKD components and subsystems.

The rest of the chapter is structured as follows. We begin by explaining the generation of the coherent states with random phase using a DFB laser, as well as presenting the detection and validation of the generated coherent states. Next, the implementation of the GMCS CV-QKD protocol over an 11-km link using the GS DFB laser for preparing the coherent states is explained in detail, including the digital signal processing with the proposed quantum state phase recovery process. Finally, we present the experimental results achieved with our proposed solution.

4.2. Generation of Random Coherent States

The generation of random states can be obtained by relying on quantum phenomena that take place in a laser cavity. In a laser, light emission consists of two mechanisms, spontaneous emission followed by stimulated emission. In spontaneous emission, the phase of the generated photons is randomly distributed, while in stimulated emission, all the generated photons have the same phase. This means the total phase of the generated photons will contain a random phase [143]. When a pulse current is applied to an empty laser cavity biased below the threshold, a sudden change in the carrier density occurs,

producing changes in the index of refraction of the cavity. Consequently, after some time an initial overshoot is observed in the optical pulse (see Figure 4.1(a)). If the current pulse continues, a steady-state is then reached due to the equilibrium between the electrical and photon density, meaning that the refraction index of the laser cavity is now stable, as shown in Figure 4.1(a) [145], [159].

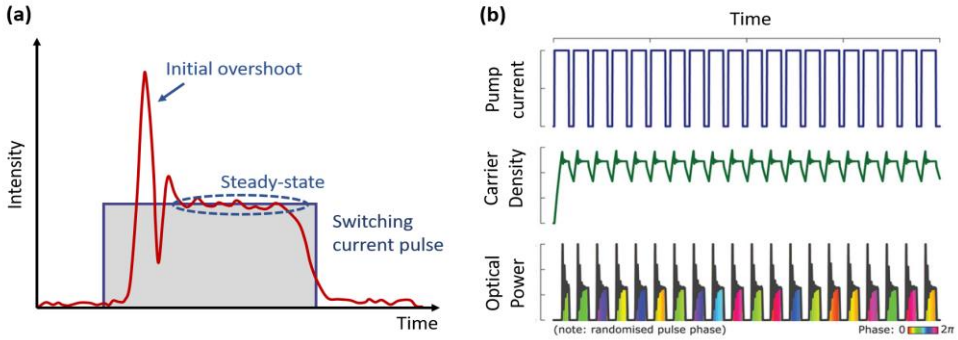

Figure 4.1: (a) Typical photon density evolution (red curve) when a switching current cycle (blue curve) is applied. After the initial overshoot, the steady-state is reached. Figure adapted from Ref. [145]. (b) Generation of a phase-randomized pulse train when a switching current signal is applied to a GS DFB laser. Figure adapted from Ref. [160].

The generation of optical pulses with the previously mentioned random phase can be carried out using a DFB laser diode. In DFB lasers working in GS mode, the laser is driven below and above the laser threshold by using an external electronic signal generator. In this way, the laser's gain is periodically switched between below and above the threshold level [46], [128], [143], [145], [146], producing short and phase-independent optical pulses, with each new pulse being seeded with a random phase (see Figure 4.1(b)). By going below threshold, the DFB laser's cavity field is significantly attenuated, while the ASE becomes dominant. This effectively reduces any prior coherence to a negligible level, with the ASE providing a masking field with true random phase [46], [128], [143], [145], [146]. This technique is attractive because it allows flexible

repetition rates from a relatively simple, stable, and compact pulse, which can be implemented without the need for a high-quality external high-speed modulator [159], [160].

4.3. Detection and Validation of GMCS

Measurement of the coherent pulses, containing the random quantum states generated as explained in the previous section, is carried out by coherent optical detection (see Section 2.3.2 in Chapter 2). In our case, the coherent receiver (see Figure 4.2(a)) consists of heterodyne detection, which simultaneously measures both quadratures (X and P) of the beating between the optical signal (S) and the CW local oscillator (LO) [74]. The simultaneous measurements are performed using a 90° optical hybrid (OH) and a pair of balanced photodetectors (BPDs).

At the output of the BPD, in the absence of noise, the normalized photocurrent can be expressed as:

$$\begin{aligned} X(t) &\propto \sqrt{I_S(t)}\cos\left(\Delta\phi_{SLO}(t)\right), \\ P(t) &\propto \sqrt{I_S(t)}\sin\left(\Delta\phi_{SLO}(t)\right), \end{aligned} \tag{4.1}$$

where $I_S(t)$ is the RF signal sent to the DFB laser [74] and $\Delta\phi_{SLO}(t) = \phi_S(t) - \phi_{LO}(t)$ is the difference in phase between the signal S and the LO laser. This difference in phase $\Delta\phi_{SLO}(t)$ is random and uniform distributed in the range [-π, π). The phases are wrapped around this range due to the modular nature of the cosine/sine functions [46], [128], [143] – [146]. The uncorrelation of the phase ensures that the values cannot be predicted, and its uniform distribution U[-π, π) means that all the phase values have the same probability of appearing

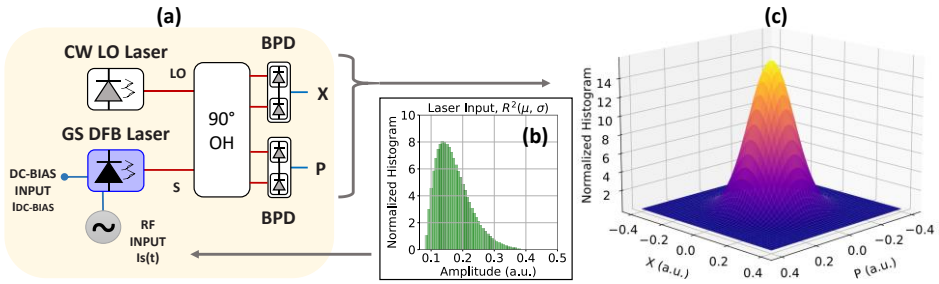

Figure 4.2: (a) Configuration for the measurements of the Gaussian-modulated coherent states (GMCS), generated with a gain-switched (GS) distributed-feedback (DFB) laser. BPD, balanced photodetector; CW, continuous-wave; LO, local oscillator; OH, optical hybrid; S, signal. (b) Histogram of the amplitude of the RF electrical pulses sent to the GS DFB laser following a squared Rayleigh distribution. (c) 3D normalized histogram with Gaussian fit of the expected X and P projections at the output of the BPDs in arbitrary units (a.u.).

[46]. With regard to the amplitude of the optical signals in the X and P projections, this is controlled by the amplitude of the pulsed current signal $I_S(t)$ injected into the GS DFB laser. In our case, by sending electrical pulses with an amplitude that follows a squared Rayleigh distribution (Figure 4.2(b)), we can get optical signals with an amplitude that obeys a Gaussian probability distribution in both the X and P projections, as shown in Figure 4.2(c).

In order to generate the GMCS with a GS DFB laser (using the structure presented in Figure 4.2), a preliminary characterization of the laser and a validation of the results should be performed. The obtained experimental results of the characterization and validation of our model are presented in Figure 4.3 and Figure 4.4, respectively. Here, the laser used for preparing the GMCS is a 2.5-GHz-bandwidth GS DFB laser, emitting at 1550 nm. Figure 4.3(a) shows the optical power output as a function of the DC bias current injected into the laser, where the inflection point around 9 mA corresponds to the current threshold of our DFB laser. Below this threshold level (specifically at $I_{DC\text{-}BIAS}$=6.5 mA), the spectrum of the optical power output looks like the gray curve presented in Figure 4.3(b). When the RF signal $I_S(t)$ is injected at this point ($I_{DC\text{-}}$

$_{BIAS}$ = 6.5 mA) into the DFB laser, we obtain an optical spectrum like the one presented in blue in Figure 4.3(b). It can be seen that the cavity field of the DFB laser experiences an attenuation of 40 dB when modulating from above to below the threshold level. Examples of the temporal shapes of electrical pulses $I_S(t)$ at three different amplitudes are presented in Figure 4.3(c), with corresponding optical pulse outputs shown in Figure 4.3(d). The amplitudes of the sent $I_S(t)$ signals were Rayleigh-distributed with a mean of μ = 0.5 mA and a standard deviation of σ = 5.6 mA. The pulse width (PW) and pulse rate (R) of $I_S(t)$ were 1 ns and 100 Mpulses/s, respectively. Figure 4.3(d) shows the initial overshoot followed by the steady-state condition where the equilibrium in the carrier density within the laser cavity is balanced between depletion via stimulated emission and excitation from the driving signal, and the chirp is minimized. The red vertical line in Figure 4.3(d) corresponds to the temporal position of the sampling point after the beating between the signal and the LO laser.

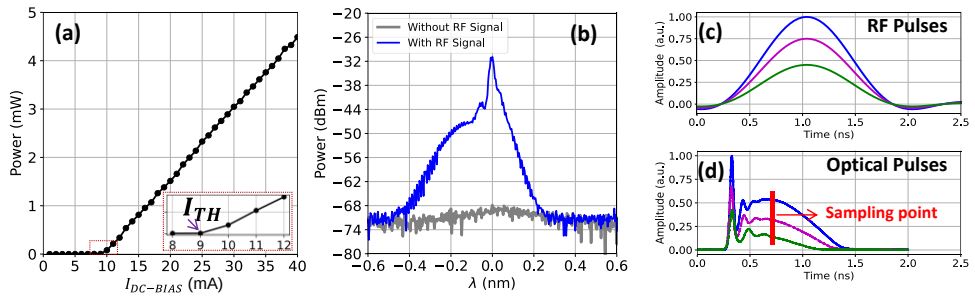

Figure 4.3: Experimental generation and characterization of the Gaussian-modulated coherent states (GMCS), using a gain-switched distributed feedback (GS DFB) laser. (a) Optical power output as a function of the DC bias current ($I_{DC\text{-}BIAS}$) applied to the DFB laser, where the inflection point is related to the current threshold (I_{TH}). (b) Optical power spectrum of the laser emission with (blue curve) and without (gray curve) the electrical RF signal at $I_{DC-BIAS}$ = 6.5 mA (below the threshold level, 9 mA). (c) Electrical pulse shape with three different amplitudes used to drive the DFB laser. (d) Temporal profile of the optical pulses generated with the electrical signals presented in (c).

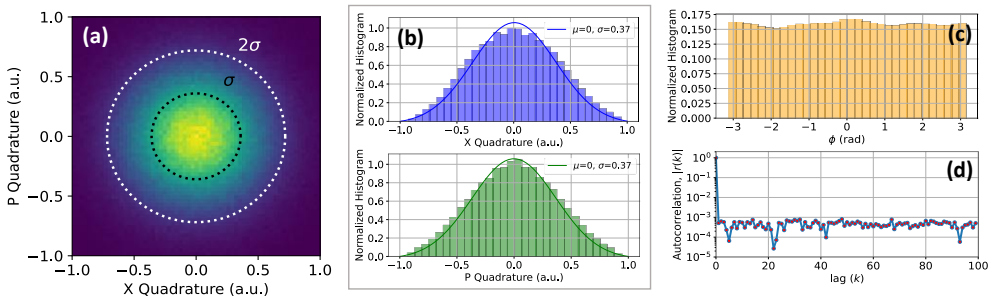

Figure 4.4: Experimental validation of the Gaussian-modulated coherent states (GMCS), using a gain-switched distributed feedback (GS DFB) laser. (a) Phase-space density measured at the coherent receiver output. Normalized histograms of the (b) amplitude projection in the X and P quadratures, and (c) phases of the measured coherent states. (d) Normalized autocorrelation of 10^5 consecutive coherent states until a delay of lag(k) = 100.

Following generation of the GMCS, detection is performed using the coherent detection method shown in Figure 4.2(a). A typical measured phase-space density is presented in Figure 4.4(a), and normalized histograms of the amplitudes (in X and P quadratures) and phases of the measured coherent states are depicted in Figure 4.4(b) and Figure 4.4(c), respectively. Figure 4.4(b) shows that both measured quadratures follow a Gaussian distribution, while the phases of the measured coherent states follow a uniform distribution (see Figure 4.4(c)). Therefore, it can be observed that the measured coherent states are suitably fitted to a Gaussian distribution in which the coherent state phases are uniformly distributed. Figure 4.4(d) shows the autocorrelation as a function of the applied lag k to a sequence of values Z with $N = 10^5$ coherent states, defined as Eq. (4.2) [135], [148]:

$$|r(k)| = \left| \frac{\sum_{i=1}^{N-k} (Z_i - \bar{Z})\,(Z_{i+k} - \bar{Z})}{\sum_{i=1}^{N} (Z_i - \bar{Z})^2} \right|, \tag{4.2}$$

where each coherent state of Z ($Z_i = X_i + jP_i$) corresponds to one sample per pulse, as marked in red in Figure 4.3(d). Also, in Figure 4.4(d) it can be seen that at the non-lagged position (k = 0), the autocorrelation value |r(k)| is higher

than that of the 30-dB level, showing a delta-function-like behavior. This proves the random nature of the coherent states prepared with the GS DFB laser.

4.4. Experiments using the GS DFB laser

4.4.1. CV-QKD Setup

Figure 4.5(a) shows the implemented scheme for the generation and measurement of the GMCS for CV-QKD using a DFB laser. At Alice's site, a QPhotonics DFB laser (QDFBLD-1550-5-5) was used in the GS mode by biasing it below its threshold level in order to produce the true random phase-independent coherent states containing the quantum symbols to be transmitted to Bob's site [46], [128], [143], [145], [146]. Details of the functionality and the characterization of the GS DFB laser can be found in Sections 4.2 and 4.3, respectively. For our DFB laser, the threshold level was 9 mA at 1550 nm, and

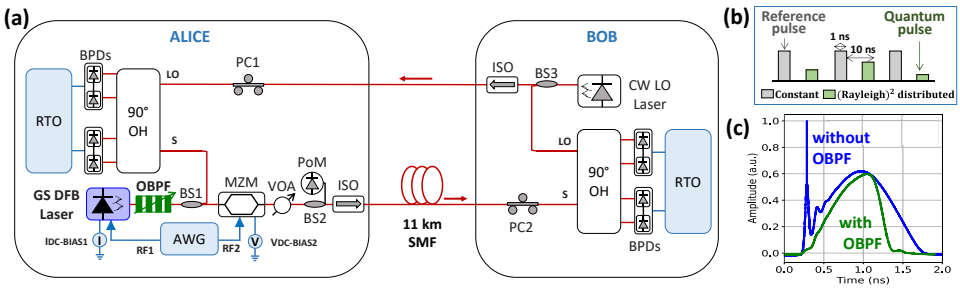

Figure 4.5: (a) Scheme of the CV-QKD system. AWG, arbitrary waveform generator; BPDs, balanced photodetectors; BS, beam splitter; CW, continuous-wave; DFB, distributed-feedback; GS, gain-switched; I, DC current source for DFB laser biasing; ISO, optical isolator; LO, local oscillator; MZM, Mach–Zehnder modulator; OBPF, optical bandpass filter; PC, polarization controller; PoM, power meter; RTO, real-time oscilloscope; SMF, single-mode fiber; V, DC voltage source for biasing the MZM; VOA, variable optical attenuator; OH, optical hybrid. (b) Electrical signal sent to the laser for the direct modulation of GMCS, where reference and quantum pulses are interleaved in time. (c) Optical pulse profile measured at the output of the GS DFB laser with (green) and without (blue) OBPF.

it was temperature-stabilized using a proportional-integral-derivative (PID) controller (Thorlabs ITC 510 laser diode combi controller).

The electrical pulsed signal RF1 employed for the direct modulation of the GS DFB laser consisted of reference and quantum pulses interleaved in time (Figure 4.5(b)). The purpose of the interleaved reference pulses is to ensure accurate phase recovery and estimation of the phase difference between the LO and the GS DFB laser, as well as the phase fluctuations caused by channel variations (see Chapter 2, Section 2.4.2). These reference signals are pulses with constant amplitude, while the quantum signals follow a squared Rayleigh random distribution (see Figure 4.2(a)). The Rayleigh distribution of the quantum symbols enables the implementation of the desired GMCS CV-QKD protocol[5] [36] explained in detail in Section 2.3 (see Chapter 2). In this case, the Rayleigh distribution consisted of 10^4 pseudo-random values with $\mu = 0.5$ mA and $\sigma = 5.6$ mA. For the generation of the random coherent states, the DFB laser was set to work at $I_{DC-BIAS1} = 6.5$ mA and the modulation pulses had a PW of 1 ns and pulse rate (R) of 100 Mpulses/s. It is important to note that in common CV-QKD systems, a separate QRNG is used to generate the random values, while in our proposed TX, an external QRNG is not required.

After the DFB laser, a tunable fiber-Bragg grating optical bandpass filter (OBPF) with a 3 dB bandwidth of 2.5 GHz was included to mitigate the spectrum spreading of the DFB laser's gain-switching mode configuration [161]. Moreover, the OBPF alleviates the driving current-dependent effects on pulse width, chirped tail, and pulse shape (Figure 4.5(c)), and reduces the risk of side-channel attacks [162]. However, future work should be carried out to evaluate this effect on the security of the system and also the laser seed attack [163]. At

[5] In GMCS protocol, both quadratures (X and P) are independent and modulated following a zero-centered Gaussian random distribution.

this point, the phase-space distribution of the quantum pulses resembles Figure 4.2(c).

Next, the light was split into two beams using a 50:50 fiber beam splitter (BS1). The light travelling through the first path was sent to a 90ºOH to perform heterodyne coherent detection and locally measure Alice's values (see Section 4.3). The second path was sent to an IMP-1550-10-PM-HER Mach Zehnder modulator (MZM) which was biased controlled with a voltage source ($V_{DC\text{-}BIAS2}$). The electrical signals RF2 sent to the MZM were two-amplitude pulsed signals with R = 100 Mpulses/s and PW = 2 ns. The PW of the electrical signals sent to the MZM was broader than the pulses generated by the DFB laser in order not to modify their pulse shape but, rather, to just control the intensity ratio (ρ) between the reference and quantum pulses. The MZM was biased at its null transmission point and ρ was set to 115 to ensure accurate phase recovery [91]. It should be noted that the use of the MZM can be avoided by either increasing the number of reference pulses or by employing a phase recovery process based on the maximization of the correlation between the symbols disclosed by Alice and Bob [155]. The former approach reduces the effective transmission rate, while the latter increases the complexity of digital signal processing. Both the GS DFB laser and the MZM were driven by an AT-AWG-GS 2500 arbitrary waveform generator (AWG) with a 3-dB 1-GHz electrical bandwidth and set to 2.5 GSa/s. The electrical signals from each AWG output (RF1 and RF2) were amplified using a 20-dB gain driver amplifier.

After the MZM, a variable optical attenuator (VOA) was installed to control Alice's modulation variance (V_A). Then, in order to enable the real-time V_A calculation, a 90:10 fiber beam splitter (BS2) was employed, directing 90% of the light to an optical power meter (PoM), with the remaining 10% sent to

Bob by the quantum channel. The optical channel consisted of an 11 km ULL single-mode fiber (SMF) with a loss coefficient of 0.22 dB/km.

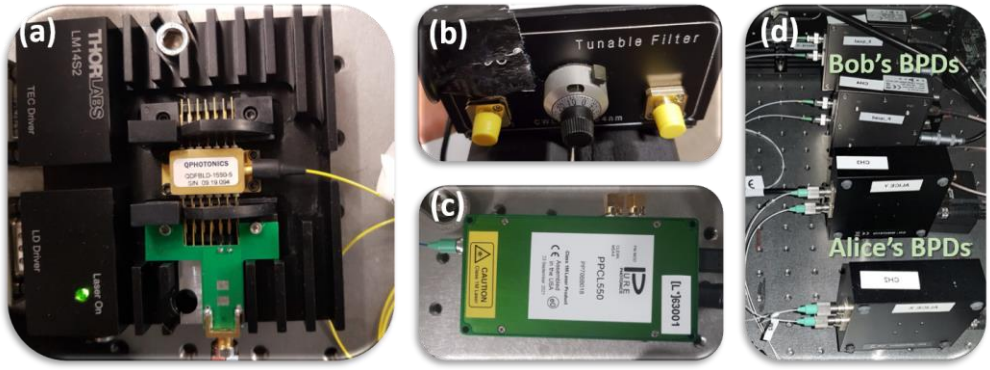

Figure 4.6: (a) QPhotonics gain-switched DFB laser used for the generation of the random quantum symbols. (b) Optical bandpass filter (OBPF) located after the DFB laser. (c) Pure Photonics CW laser, used as a local oscillator for the coherent detection. (d) Set of Thorlabs and FEMTO balanced photodetectors (BPDs), used for the coherent detection at Alice's and Bob's site, respectively.

At Bob's site, the quantum values were measured by performing heterodyne coherent detection as described in Section 4.3. For the coherent detection, the LO was generated using a tunable CW external cavity laser with a linewidth of 10 kHz, biased to emit 48 mW at 1550 nm. From there, 90% of the light was kept at Bob's site using a 90:10 BS3 and connected to the 90º OH. The other output of the BS3 was directed to Alice to be used as LO. In this proof of concept experiment, sharing the LO simplifies the system implementation, but in practical applications, it is more suitable to generate Alice's LO locally instead of transmitting it from Bob [154].

In this experiment, the balanced photodetectors (BPDs) used by Alice were two Thorlabs with 350MHz of electrical bandwidth, and those used by Bob were two FEMTO (HBPR-500M-10K-IN-FC) with 500 MHz of bandwidth. The output of the BPDs was digitized using a 10-GSa/s real-time oscilloscope with an electrical bandwidth for each oscilloscope channel fixed at 250 MHz. At Bob's site, an average clearance (ratio between shot noise variance and electronic

noise variance) of 14.9 dB was obtained. However, at Alice's site, the effects associated with shot and electronic noise were negligible since the measurement of the coherent states was performed at a classical level. At both sites, a polarization controller (PC) was included at the input location to adjust the polarization of the light to the maximum interference between the signal and the LO. Finally, a 35-dB optical isolator (ISO) was incorporated at both Alice's and Bob's output locations to safeguard against Trojan horse attacks [129], as included in practical systems. An image of the lasers, OBPF, and BPDs used in this experiment are shown in Figure 4.6.

4.4.2. Digital Signal Processing

Digital signal processing (DSP) was performed offline, comprising five main processes (see Section 2.4 in Chapter 2). First was the downsampling of Alice's and Bob's signals ($Z^Y = X^Y + jP^Y$, with Y = {Alice, Bob}). The second process was the phase recovery of the quantum states which is slightly different to the one explained in Section 2.4.2 in Chapter 2. Since the phases of the optical pulses leaving the GS DFB laser are random, reference pulses with a specific phase cannot be established. Therefore, a phase recovery process based on a differential approach is a better solution. Accordingly, by redefining Z^Y as the set of reference and quantum states obtained for Alice or Bob after the downsampling process, we obtained $Z^Y = \{R_i^Y, Q_i^Y, R_{i+1}^Y, Q_{i+1}^Y, \dots\}$, where R_i^Y and Q_i^Y (complex numbers) are the i-th reference and quantum states, respectively. The corrected i-th quantum state ($\widehat{Q}_i^Y$) can be calculated using the phase information of the preceding reference state, as indicated in Eq. (4.3), after which the references can be discarded,

$$\widehat{Q}_i^Y = Q_i^Y \exp\left(-j \arctan\left(\frac{\Im\{R_i^Y\}}{\Re\{R_i^Y\}}\right)\right). \quad (4.3)$$

The third process was frame synchronization. The time offset was removed by performing a cross-correlation between the sequence of coherent states measured by Alice and Bob. The fourth step in the DSP involved a parameter estimation of excess noise and channel transmittance, followed by the final step, which was the secret key rate estimation. These two last steps are explained in detail in Chapter 2, Section 2.3.3.

4.5. Analysis and Results

As part of the DSP, a critical step is the correction of the phase errors between Alice's and Bob's data. These errors are introduced by the phase fluctuations in the optical link during the transmission and by the frequency mismatches between the optical frequency of the signal and the LO laser, hindering the extraction of the secret key. Variations in the fiber link during the communication lead to variations in the optical wavefront reaching the

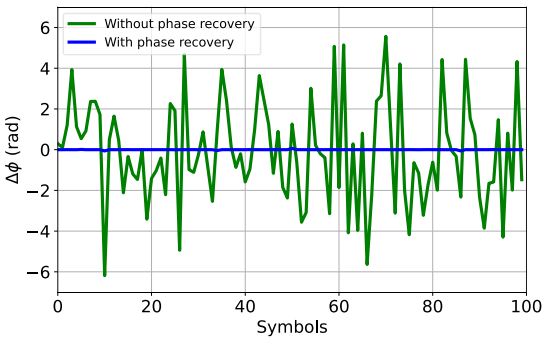

Figure 4.7: Phase difference ($\Delta\boldsymbol{\phi}$) of 100 Alice and Bob symbols without (green line) and with (blue line) phase recovery. These symbols (measured states) were measured using 11 km SMF in the channel and at $\mathbf{V_A}$ = 30 SNU.

detectors of both parties over time. Given the slow changes in the optical path during transmission (< 1 kHz) and the relatively high transmission rate (> 1 MHz), it is reasonable to assume that the relative phase drift between consecutive symbols remains constant. Hence, by subtracting the phase of a reference from its preceding quantum state, as demonstrated in Eq. (4.3), it becomes possible to compensate for any phase differences between Alice and Bob resulting from the optical path. Furthermore, the differential approach employed in the phase recovery process described in the previous Section 4.4.2 also enables compensation for phase errors caused by frequency mismatches between the signal and the LO laser. A comparison of the difference between Alice's and Bob's phase ($\Delta\phi$) before (green line) and after (blue line) the phase recovery can be seen in Figure 4.7, having been carried out over 100 states, utilizing 11-km SMF and at V_A = 30 SNU. It can be seen how the phase difference is zero only after the phase recovery (blue line), meaning that this process was performed correctly.

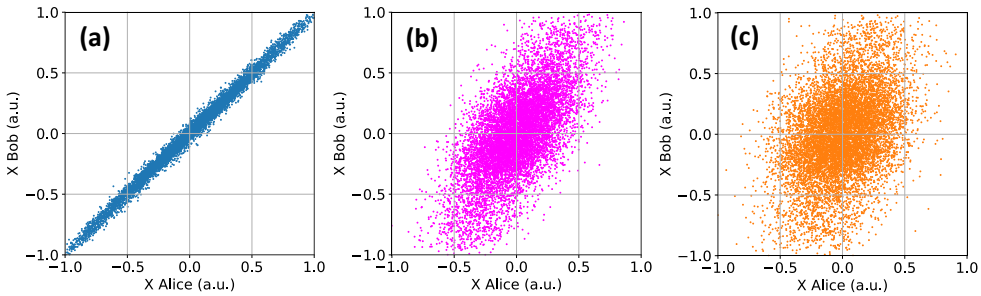

Figure 4.8: Plot correlation between 10^5 Alice and Bob **X**-quadrature states after the proposed phase recovery and at different $\mathbf{V_A}$: (a) 30 SNU, (b) 3.35 SNU, and (c) 1.50 SNU.

A comparison of 10^5 states measured by Alice and Bob in the X-quadrature is demonstrated in Figure 4.8. These are the states obtained after their propagation through the quantum channel, phase recovery, and frame synchronization at three different V_A values (30, 3.35, and 1.5 SNU for Figure 4.8(a), Figure 4.8(b) and Figure 4.8(c), respectively), showing how the

correlation decreases as the V_A value is reduced. Notably, Figure 4.8(c) demonstrates a minimal correlation between Alice's and Bob's data.

The parameters utilized in our CV-QKD system, with coherent states generated by a GS DFB laser (see Figure 4.5) are summarized in Table 4.1. These are the parameters used for the last part of the DSP: parameter and SKR estimation.

Table 4.1. Summary of Parameters

Parameter	Symbol	Value
Alice's modulation variance	V_A	3.35 SNU
Electronic noise variance	ν_{el}	36 mSNU
Reconciliation efficiency	β	0.95 [65]
Detection efficiency	η	0.29
Ratio of the intensity of reference pulses to quantum pulses	ρ	115
Effective quantum pulse rate	R_{eff}	50 Mpulses/s

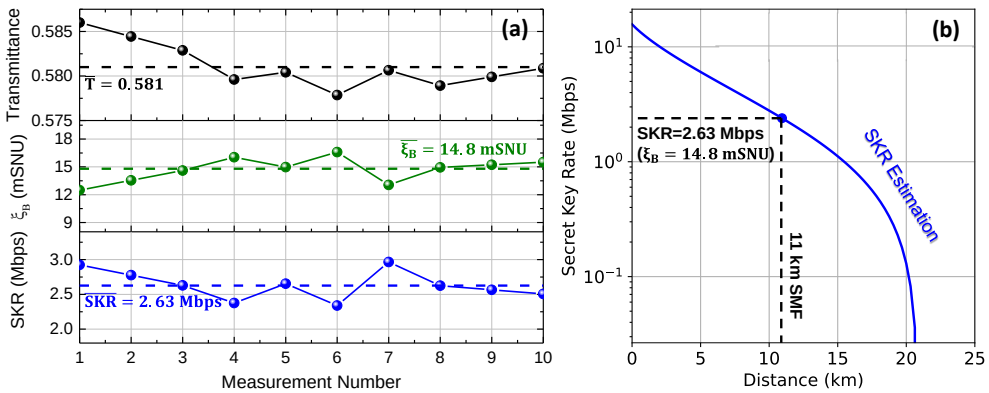

Figure 4.9: (a) Experimental results for channel transmittance (**T**), excess noise at Bob's site ($\boldsymbol{\xi_B}$), and secret key rate (**SKR**) for 10 measurements acquired over 20 mins through an 11-km SMF. Each measurement corresponds to a block size of 10^5 coherent states. (c) Simulation of the **SKR** as a function of link distance in the asymptotic regime.

Figure 4.9(a) presents the experimental results of 10 consecutive measurements (obtained over a 20 minute period) of transmittance T (Eq. (2.8)), total excess noise ξ_B ($\xi_B = 2\xi_{B_q}$, Eq. (2.6)), and their related SKR (Eq.(2.18)) (see Chapter 2). The mean values are shown with dashed lines. Specifically, the obtained mean values for T, ξ_B, and SKR were 0.581, 14.8

mSNU, and 2.63 Mbps, respectively, using an 11 km SMF as a channel and asymptotic analysis. Each measurement involved a block size of 10^5 coherent states, with T, ξ_B, and SKR independently estimated for each block. Before all of these measurements, the shot noise variance (N_o) was manually calibrated (see Eq. (2.21) in Chapter 2). From Figure 4.9(a) we can observe the stability of the measurements over 20 minutes. Finally, Figure 4.9(b) demonstrates the experimental SKR value obtained at 11 km (blue dot), together with an estimation of the SKR as a function of the transmission distance (blue line), taking into consideration the experimental mean values of T and ξ_B previously mentioned (see Figure 4.9(a)). Figure 4.9(b) also shows that positive SKR could be obtained up to a distance of 20.5 km, assuming a constant $\xi_B$value for longer distances.

4.6. Conclusions

In this chapter, we have successfully demonstrated the utilization of a directly modulated DFB laser in the gain-switching mode for the generation of random coherent states. This source of coherent states was used for the implementation of the GMCS CV-QKD protocol, achieving an experimental asymptotic secret key rate of 2.63 Mbps at a distance of 11 km. Our proposed CV-QKD system using a GS DFB laser eliminates the need for additional phase modulators and QRNGs, while enabling the generation of optical pulses with random phases. Furthermore, a phase recovery scheme based on a differential approach has also been proposed and implemented. The simplicity, compactness, and cost-effectiveness of the proposed system make it suitable for implementation in CV-QKD networks due to its excellent performance at short distances.

Chapter 5

ON-CHIP TRANSMITTER FOR CV-QKD SYSTEM

The content of this chapter is currently being prepared in a paper format to submit to a journal: "InP-based PIC transmitter for CV-QKD systems", J. Aldama, S. Sarmiento, L. Trigo-Vidarte, S. Etcheverry, I. López-Grande, L. Castelvero, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri.

The integration of quantum key distribution (QKD) systems into monolithic photonic integrated circuits (PICs) has the potential to accelerate their adoption across various markets, thanks to reduction of size, power consumption, production costs, and overall system complexity. This chapter presents a detailed description and characterization of a cost-effective indium phosphide (InP)-based PIC transmitter (TX), specifically designed for CV-QKD applications. Proof-of-principle experiments at the system level are conducted using a shared laser scheme, employing a pulsed Gaussian-modulated coherent-state (GMCS) CV-QKD protocol over an 11 km optical fiber channel. The obtained results demonstrate compatibility with secret key rates of 52 kbps and 27 kbps in the asymptotic and finite-size regimes, respectively. These findings highlight the potential of the proposed PIC design towards the integration of CV-QKD technology.

5.1. Introduction

Commercial QKD systems are now available, although they remain expensive, bulky, and relatively challenging to operate and to standardize. Consequently, QKD is less accessible to the market and difficult to use on a large scale. To overcome these issues, the photonic integration of QKD systems can significantly reduce their cost, size, weight, and power consumption, and can also facilitate mass production, making QKD accessible to a wider range of users [164]–[166]. For integrated QKD implementation, CV-QKD is better suited for this purpose than the commonly used discrete variable QKD (DV-QKD). A well-known protocol for the implementation of CV-QKD systems is Gaussian-modulated coherent-state (GMCS), which is explained in detail in Section 2.3.

Recently, various research groups have worked to downsize QKD systems using different photonic integrated circuit (PIC) platforms, such as silicon, III-V compound semiconductors, and lithium niobate (LiNbO3)[132], [165], [167], [168]. Among these, on-chip CV-QKD systems have been investigated by combining external lasers and integrated components on a silicon photonics (Si) platform [40], [49], [50], [53], [54], [169]. Although Si offers several advantages, it cannot support monolithic laser integration, making it impossible for use in the development of full monolithic CV-QKD systems. In a recent work [47], an integrated laser was used for a CV-QKD system, where the laser was made up of an InP reflective semiconductor optical amplifier (RSOA) chip butt-coupled with a low-loss silicon nitride cavity extension chip. In this case, the CV-QKD transmitter included an integrated laser combined with discrete components. InP has the inherent advantage of allowing the monolithic integration of a range of components necessary for CV-QKD systems, including lasers, as their direct bandgap permits laser emission

[170], [171]. Thus, the InP-based platform is a highly promising option for fully integrated CV-QKD technology, as demonstrated in the preliminary results presented in [51]. Table 5.1 lists the research efforts for miniaturizing CV-QKD systems using different platform materials, as well as different clock rates (CRs) and secret key rates (SKRs) obtained at different link distances.

This chapter starts by describing the proposed PIC TX design and an experimental proof-of-principle CV-QKD setup to evaluate its potential performance in realistic conditions. Then we present the electro-optical characterization of the most relevant building blocks of the PIC TX, as well as the CV-QKD experimental system-level results, including the SKR estimation in the asymptotic and finite size regimes.

Table 5.1. Chip-based CV-QKD experiments, where CR: clock rate and App: approach

Ref	Year	Platform		App	Protocol	CR	SKR (Distance)	Notes
		TX	RX					
[48]	2017	Si	Si	P&M	GMCS	0.5 MHz	0.1 kbps (15 km)	TX: 2D GC, TOPMs, CDPMs, MZIs, and a VOA. RX: BS + Ge BPD.
[49]	2018	Si	Si	P&M	GMCS	3.5 MHz	37 kbps (45 km)	Transmitted LO with Pol. MUX. TX: EAM, PM and AM. RX: BS + MZI + CDPMs + Ge BPD.
[40]	2019	Si	Si	P&M	GMCS	10 MHz	0.14 kbps (100 km)	See [49].
[53]	2019	–	Si	P&M	GMCS	1 MHz	1 kbps (15 km)	Homodyne RX: BS + Ge BPD.
[169]	2020	Si	Si	P&M	GMCS	10 MHz	2.3 kbps (100 km)	See [49].
[50]	2021	–	Si	P&M	GMCS	1.5 GHz	–	RX + TIA: 2 2D GC, 1 TOPM, 1 2×2 MMI, 2 MZIs, and 2 PDs.
[54]	2023	–	Si	P&M	GMCS	100 MBaud	280 kbps (6.9 km)	Homodyne RX: BS+ BPD
[51]*	2023	InP	–	P&M	GMCS	8 MBaud	0.4 Mbps (11 km)	External laser and transmitted LO. TX: EAM+IQ modulator+VOA
[47]	2023	III-V/Si_3N_4	III-V/Si_3N_4	P&M	GMCS	0.25 GBaud	0.75 Mbps (50 km)	TX & RX: On-chip tunable lasers. External modulation.
[52]	2023	–	Si	P&M	16 QAM	10 GBaud	0.3 Gbps (10 km)	Phase diversity RX + TIA: MMI+MZI+BPD Finite size analysis.

*Our preliminary results

5.2. Description of the CV-QKD PIC TX

5.2.1. PIC TX design

The InP platform boasts good capabilities for laser integration and provides the basic building blocks for IQ modulation, suitable for CV-QKD. Our focus is on monolithically integrating the building blocks required for the state preparation in a CV-QKD implementation and testing the modulation performance using an external laser. However, we anticipate that future steps will involve the inclusion within the InP-based PIC TX of a fully integrated laser with a narrow linewidth in order to achieve long coherence times in phase and low phase noise [96].

During the design phase of the first version of the PIC, we considered the development of a flexible system with redundant paths, which provides access to most of the individual building blocks, enabling the use of pulses (via electro-absorption modulator, EAM) or pulse shaping directly (without EAM). Furthermore, the design was conceived to be independent of the system-level implementation, such as transmitted local oscillator (TLO) or real LO, homodyne or heterodyne detection, type of modulation (BPSK, M-QAM), etc. For this reason, our PIC TX includes three main building blocks - an EAM, an IQ modulator and a variable optical attenuator (VOA) – see Figure 5.1(a). This scheme is similar to those used in classical coherent optical communication. However, we note that in classical communication the higher the TX power the better for compensating the fiber losses, while a CV-QKD TX requires low power output.

Due to its robustness and practicality, in this work our PIC TX was characterized using the GMCS CV-QKD protocol [20]. As discussed previously, this protocol is performed by continuously modulating the phase and amplitude

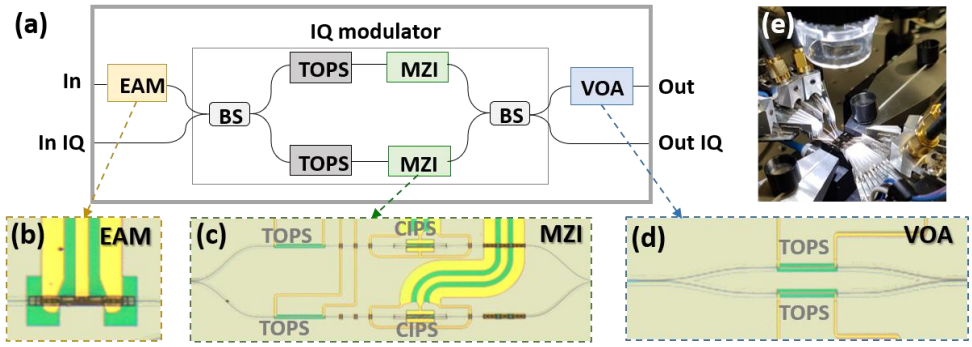

Figure 5.1: (a) Block diagram of the CV-QKD PIC Tx. EAM, electro-absorption modulator; BS, beam splitter 2x2 MMI 50:50 ratio; TOPS, thermo-optic phase shifter; MZI, Mach-Zehnder interferometer; VOA, variable optical attenuator. Microscope image of the (b) EAM; (c) MZI (CIPS, current-injection phase shifter); (d) VOA. (e) Setup including the fabricated 12 × 6 mm^2 InP-based CV-QKD PIC Tx, Fraunhofer HHI Foundry, in the center.

of coherent light pulses at the site of the TX and sending weak coherent pulses to the channel. To achieve this, one approach is to use the amplitude modulator to pulse the light, the IQ modulator to encode the key in amplitude and phase, and the VOA to adjust the power output to the quantum level.

5.2.2. Components of the PIC TX

Our proposed PIC TX includes active components such as an EAM, thermo-optic phase shifters (TOPSs), and current-injection phase shifters (CIPSs). It also contains passive components like waveguides, spot size converters, and a power splitter 2x2 based on 3dB multimode interferometers (MMIs) - see Figure 5.1(a). It is designed to operate at the C-band (~1550 nm) and is fabricated using the available building blocks in the HHI's transceiver (TX-RX) platform for multi-project wafers (MPWs).

The fabricated EAM is 200 μm long and its purpose is to pulse the light with an adequate extinction ratio, ER (Figure 5.1(b)). Preparation of the coherent quantum states is carried out in the IQ modulator, which is made up

of two nested Mach-Zehnder interferometers, MZIs (Figure 5.1(c)). Each MZI combines two CIPSs and two TOPSs. The phase shift of π/2 between these two MZIs is set with the two TOPSs. The VOA is also based on an MZI design, where the interferometry process is managed by the two TOPS (Figure 5.1(d)). The purpose of the VOA is to attenuate the light power to the quantum level. Extra ports were added on the side of the main input edge (e.g., In IQ) and output port edge (e.g., Out IQ) for monitoring the IQ modulator output as well as the performances of the VOA and MZIs separately.

For fiber coupling, our PIC TX includes spot size converters (SSCs) at the facet to increase the coupling efficiency to standard single-mode fiber (SMF). In order to avoid stray light issues, the optical ports were positioned facet to facet and shifted in our chip design. The electrical DC and RF components were placed along the longest edges of the cell while the waveguides were positioned along the shortest sides. The standard distance between the SSCs was set at 125 μm, while the electrical DC and ground-signal-ground (GSG) RF pads had a pitch of 150 and 130 μm, respectively. An image of the PIC TX mounted in our probe station can be seen in Figure 5.1(e).

5.3. CV-QKD Experimental Setup

The developed pulsed GMCS CV-QKD system with the InP-based PIC TX is presented in Figure 5.2(a). It was conceived to be a simple proof-of-principle setup to verify the performance of our PIC and simplify the digital signal processing (DSP). The complexity of the DSP is intentionally maintained low, so that the reported performance is not highly dependent on its implementation and optimization and the results reflect the behavior of the chip. Therefore, we

can shift our focus towards the PIC itself. Future work could be extended to other more practical setups, where the performance of the chip should remain as reported in this thesis.

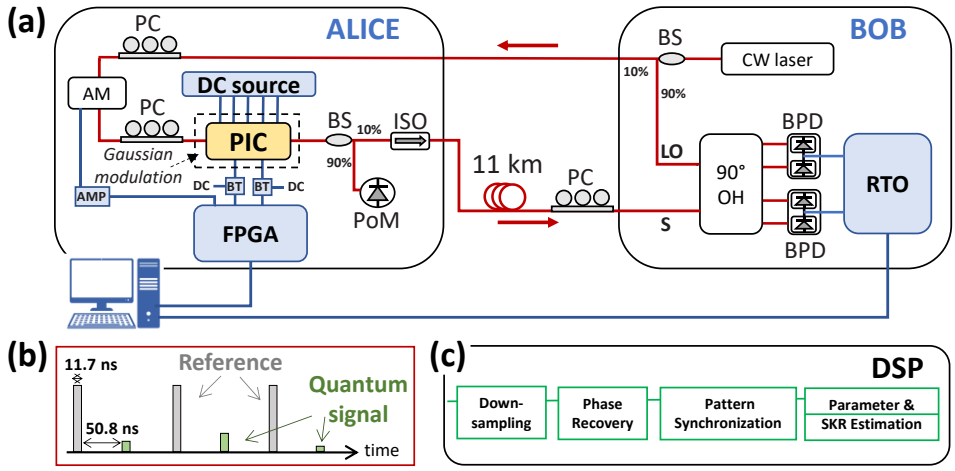

Figure 5.2: (a) CV-QKD system. S, signal; LO, local oscillator; BS, beam splitter; PC, polarization controller; AM, amplitude modulator; AMP, electrical amplifier; PIC, photonic integrated circuit; BT, bias tee; FPGA, field-programmable gate array; PoM, power meter; ISO, isolator; OH, optical hybrid; BPD, balanced photodetector; RTO, real-time oscilloscope. (b) Pulses obtained at the output of the PIC and sent by Alice to Bob (right). Reference pulses were interleaved with pulses containing the quantum signal. (c) Digital signal processing (DSP) chain performed to the analysis of the data.

In our system, the light source is the same type of laser source as that used in previous experiments presented in this thesis. It is a continuous-wave (CW) external cavity laser by Pure Photonics with a 10 kHz nominal linewidth and biased to emit 50 mW at a frequency of 193.4 THz (1550 nm wavelength). The CW laser, located at Bob's side, is followed by a 90:10 beam splitter (BS), where, for simplicity, the 90% BS output is directly used as Bob's CW local oscillator (LO), and the other 10% is sent to Alice [86] – [88]. This scheme reduces complexity in the DSP by avoiding carrier frequency recovery. In pulsed CV-QKD systems, a high ER is a priority in order to reduce noise, and in our PIC TX, the integrated EAM demonstrated a high ER. However, the EAM was

replaced with an external 30 dB ER Optilab IMP-1550-10-PM-HER lithium niobate amplitude modulator (AM), because it has a lower insertion loss (IL) than the EAM. In our integrated system, the total losses in our TX were too high to allow us to measure the power at the output of the PIC. Therefore, replacing the EAM with an AM with lower IL was considered a solution. Thus, at Alice, the light was pulsed using the AM to define the pulses with high ER and then coupled to the PIC using an SMF at the input of the PIC. At the output of the PIC, another SMF was also employed. This is where we encode the secret key that Alice wants to share with Bob.

In the PIC, the DC signals applied to the TOPSs are regulated with a NICSLAB DC multichannel source. Meanwhile, the RF signals applied to the IQ modulator are controlled with a field-programmable gate array (FPGA) electronic board with a 1 GSa/s 16-bit nominal resolution digital-to-analog converter unit. The RF signal sent to the AM is also controlled via an FPGA and requires an electrical amplifier (AMP) to reach the voltage necessary to change from minimum transmission to maximum transmission or V_π of the AM. For the IQ modulation, the CIPSs are connected to a bias-tee. This is so that the bias point where the RF signals are applied can be adjusted. The Gaussian-modulated symbols consist of 2040 pseudo-random values, of which two independent sets are cyclically sent to the PIC's IQ modulator. The quantum symbols modulated according to zero-centered Gaussian random distributions are interleaved in time with reference pulses of constant amplitude and alternating sign to facilitate the phase recovery accuracy at Bob's site (Figure 5.2(b)). The repetition rate of the generated pulses is 16 MHz with a pulse width of 11.7 ns. Afterwards, the coherent states of light (weak optical pulses) generated by Alice are sent to a 90:10 beam splitter (BS). 90% of the light is measured using a power meter (PoM) to estimate the modulation variance (V_A),

defined as two times the mean photon number $\langle n \rangle$ at Alice's output ($V_A = 2\langle n \rangle$), as discussed in Chapter 2, Section 2.3.3. The remaining 10% of the light is sent to Bob through an 11 km fiber spool (Corning SMF-28 ULL fiber).

At Bob's optical signal channel input, a manual polarization controller (PC) is used to maximize the interference by adjusting the polarization of the signal with that of the LO. The signal sent by Alice interferes with the LO in a COH24 Kylia 90º optical hybrid (90° OH), detected using two 500 MHz bandwidth FEMTO balanced photodetectors (BPDs), and digitized by means of a 2 GSa/s real-time oscilloscope Agilent MSO9404A with a digital filter at a bandwidth of 50 MHz.

After that, the DSP (see Section 2.4 in Chapter 2) is performed offline with the same computer as that used to control the FPGA. The DSP (see Figure 5.2(c)) includes the downsampling, quantum state phase recovery using the reference symbols, pattern synchronization, and calculation of QKD parameters to estimate the expected secret key rate (SKR). The SKR estimates are calculated taking into consideration trusted receiver electronic noise and reverse reconciliation [36], [172]. Moreover, the SKR is evaluated for both the

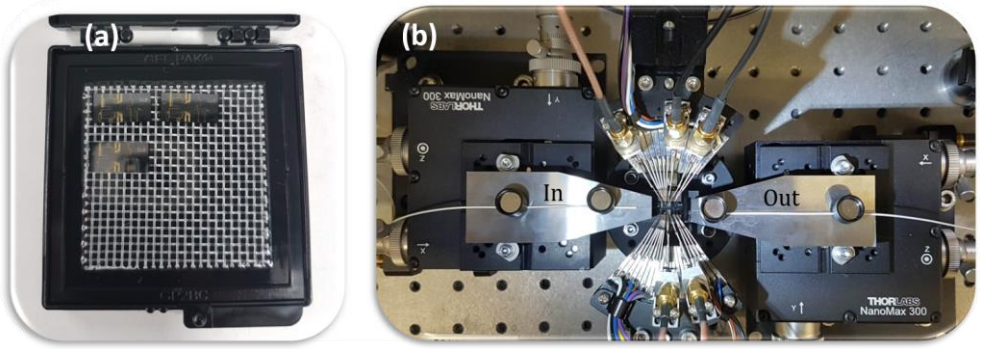

Figure 5.3: (a) Box containing three of the several PIC TXs tested during this thesis. (b) Top view of the probe station, including the PIC in the center with the electrical connections and the fiber coupling.

asymptotic limit and finite size regimes. An image of some of PICs tested during this work and a top view of our probe station are shown in Figure 5.3.

5.4. Analysis and Results

5.4.1. Block-by-Block Electro-Optical Characterization

Results of the steady-state electro-optical characterization of the main blocks (EAM, MZI, and VOA) are presented in Figure 5.4 and Figure 5.5, where the measured transmittance of each component is normalized to the maximum value of each plot. The measurements were performed using auxiliary paths connected to each block and a setup similar to that presented in [173].

The electro-optical results of the EAM for both TM and TE polarizations of the incident light are presented in Figure 5.4(a) and Figure 5.4(b), respectively. In both figures, changes in the EAM transmittance can be seen at different frequencies when a sweep in voltage is applied to the EAM. The highest ER value was ER_{EAM}=28.5 dB and was obtained at 191.55 THz and TE polarization (Figure 5.4(b)). Meanwhile, the results using TM polarization

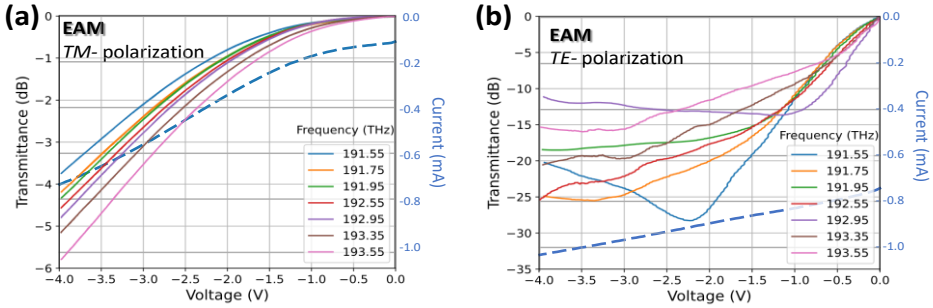

Figure 5.4: Transmittance and current as a function of the voltage applied to the EAM for different frequencies and two polarizations of the incident light: (a) TM- and (b) TE-polarization. Dashed light blue lines are the electrical response of the EAM.

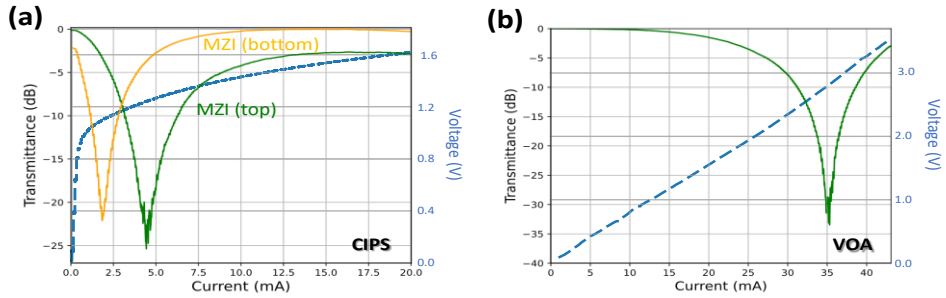

Figure 5.5: Electro-optical response of the MZIs when a sweep in current is applied to the (a) CIPS and (b) VOA. Dashed light blue lines are the electrical responses of the components.

showed changes of only a few dB (Figure 5.4(a)). Therefore, since a high ER is required by CV-QKD systems using pulses, TE polarization was selected. The electrical responses are also shown in Figure 5.4(a) and Figure 5.4(b), where the dashed light blue lines are the electrical responses when a sweep in voltage is applied to the EAM. As demonstrated, the current consumption in the EAM for TE polarization (from -0.75 mA to -1.03 mA) is higher than when TM polarized light is used (from -0.10 mA to -0.72 mA).

Figure 5.5(a) shows the transmission of the top and bottom MZIs (green and yellow lines, respectively) of the IQ modulator (see Figure 5.1(a)) when a sweep in current (dashed light blue line) is applied to one of the CIPSs. The top and bottom MZIs show an ER of 25 and 22 dB, respectively. Moreover, the difference in the optical response of both MZIs and the no-symmetry of each produces a distortion to the optical signals when IQ modulation is performed. Hence, the digital compensation of the signals has to be considered to correct this. Finally, Figure 5.5(b) presents the electro-optical VOA performance when just a TOPS is used (see Figure 5.1(e)). A current sweep from 0 to 40 mA was applied and 33 dB attenuation was obtained at 35 mA.

A summary of the parameters obtained during the electro-optical characterization of each block of the InP-based CV-QKD PIC TX is presented in Table 5.2. The component performance of our TX is presented in terms of the

ER of the EAM and IQ modulator (IQM), the maximum attenuation of the VOA, and the electro-optic 3 dB bandwidth of the system (BW). In terms of bandwidth, a higher 3dB BW can be seen for the EAM (10 GHz) than for the other components (1 GHz). Despite working in the order of only a few MHz of modulation, our PIC TX allows us to increase this modulation value. In this case, the frequency of modulation is limited by the detector's bandwidth in the receiver site. The obtained results show that our PIC TX meets the requirements of good ER and bandwidth for the implementation of a pulsed GMCS CV-QKD protocol.

Regarding the IL, in principle the losses in the TX are not critical because the light will be attenuated at the output in order to reach the quantum level. It is more important to have enough power to allow measurement by a power meter at the output of the PIC as, later, this value will be used to estimate the number of photons sent by Alice to Bob. In our case, the total IL from In IQ to Out IQ (see Figure 5.1(a)) was IL_{IQM}= 37.9 dB. This value includes losses due to fiber coupling, components, and the additional port outputs that our PIC TX contains to monitor the different components. In the case of the EAM, the IL at TE polarization was IL_{EAM}=12.4 dB. The IL produced by a combination of the EAM and the IQM was too high to allow us to measure the optical power at the output of the PIC due to the need for part of the laser power to be used as LO. This is because although the EAM showed a relatively high ER at TE polarization (Table 5.2), its measured IL was also high, preventing its use in a shared LO scheme with the available laser power. Thus, the light from the source was pulsed externally with an AM with lower IL (see Figure 5.2(a)), and injected into the In IQ port (see Figure 5.1(a)). Even though the signal pulsing, which should have been performed by the integrated EAM, was substituted with an external

AM, the need for time pulsing of the optical signal could be avoid by operating in continuous wave mode and using pulse shaping signal modulation [174].

Table 5.2. Summary of main parameters characterizing the InP-based CV-QKD PIC TX.

Component	ER @ DC (dB)	3 dB BW (GHz)*
EAM	28.5	10.0
IQM	25.0	1.0
VOA	33.0	1.0

*According to HHI PDK

5.4.2. Digital Signal Processing

The GMCS protocol was implemented on the CV-QKD system using the characterized PIC TX and 11 km of optical fiber in the channel, proving that InP is a mature platform to integrate a CV-QKD transmitter at the system level. To demonstrate this concept, the DSP was implemented as presented in Section 2.4 (Chapter 2) and is divided into 5 parts: downsampling, phase recovery, pattern synchronization, parameter estimation (PE), and the secret key rate calculation.

The different steps of the DSP process are illustrated in Figure 5.6. The output of each detector is sampled using the oscilloscope, producing two real sequences of samples that can be interpreted as a sequence of complex numbers, and the density takes the shape of a constellation (Figure 5.6(a)). The sequences are downsampled to the symbol rate by periodically choosing the samples that maximize the energy of the resulting signal, allowing for the conversion from samples to symbols (Figure 5.6(b)). At this stage, the innermost symbols correspond to the quantum information while the outermost ones correspond to the reference symbols. The ring shape is due to the phase noise introduced by the 11 km of fiber and the laser, which need to be calculated and corrected in the following DSP element. The reference symbols are used to estimate the

instantaneous phase of the channel and the laser [71]. The constellation after applying the correction of the estimated phase is shown in Figure 5.6(c). After removing the references, we get the constellation shown in Figure 5.6(d), where the outer histograms are the distributions of the X and P quadratures with a zero-centered Gaussian distribution. After the phase recovery of the Gaussian symbols received by Bob, we perform pattern synchronization using cross-correlation, and then we are ready to perform PE and secret key estimation.

One of the last processes of the DSP is the PE of the excess noise and transmittance of the channel in order to obtain an estimate of the potential SKR. The estimation of these parameters can be realized considering the asymptotic scenario (parameters are known with infinite precision) [27], [78], and finite size, FS, scenario (parameters are calculated with a long limited data set and, hence, have an associated uncertainty) [80]. Detailed descriptions of the PE and SKR estimations in both scenarios are included in Chapter 2, Section 2.3.3.

In the asymptotic regime, the excess noise in Alice's site is given by Eq. (2.7) (see Chapter 2). As usual, the channel loss was considered a potential security threat that could be controlled by an eavesdropper. In the FS scenario, the estimates of T and ξ_{B_q} will be different to the asymptotic case (see Eqs. (2.12) and (2.14) in Chapter 2). Here, our PE analysis will focus on the

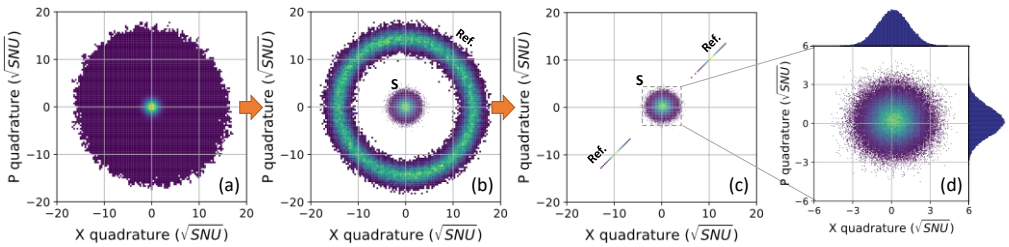

Figure 5.6: Received optical constellation after: (a) acquisition using the oscilloscope; (b) downsampling; and (c) phase recovery of the references (Refs) and symbols (S). (d) Phase-space density of the quantum symbols measured at the coherent receiver output after downsampling and phase recovery for Gaussian signals. (outside) Histogram for the amplitude of X and P quadratures of received optical Gaussian signal.

estimation of ξ_{B_q} and T, assuming that the other relevant parameters can be estimated with arbitrary precision (as shown in Table 5.3). After the PE, the SKR in bits per second (bps) can be computed as Eqs. (2.16) and (2.18) (see Chapter 2) for the FS and asymptotic regime, respectively. This is for the case of reverse reconciliation, where Bob sends correction information and Alice corrects her key elements to have the same values as Bob's [20].

Table 5.3. Transmission parameters used for asymptotic and finite size (FS) approach

Parameter	Symbol	Value
Electronic noise variance	ν_{el}	13 mSNU
Reconciliation efficiency	β	0.95 [65]
Detection efficiency	η	0.296
The ratio of the intensity of reference pulses to quantum pulses	ρ	342.6
Effective quantum pulse rate	R_{eff}	8 Msymbols/s

5.4.3. CV-QKD Experimental Results

Due to experimental limitations derived from the memory of our acquisition devices, our system is capable of working with blocks of N=3.08 x 10^6 symbols. The analysis in the asymptotic regime allows us to identify the boundaries under the current conditions, while the FS analysis gives us more realistic bounds but it is subject to a trade-off between the accuracy of the PE and the remaining symbols available for secret key generation. We perform the estimation of $\xi_B = 2\xi_{B_q}$ and T using different random choices of size m from the total experimental symbols N, obtaining the curves displayed in Figure 5.7(a) and Figure 5.7(b) using the Eqs. (2.12) and (2.14) in Chapter 2. If we compare the parameters calculated from the FS analysis with those from the asymptotic analysis, we can observe that as m increases the FS estimations get closer to the asymptotic ones. But we are interested in maximizing the SKR; therefore, we need to evaluate this parameter as a function of m, using the results from the

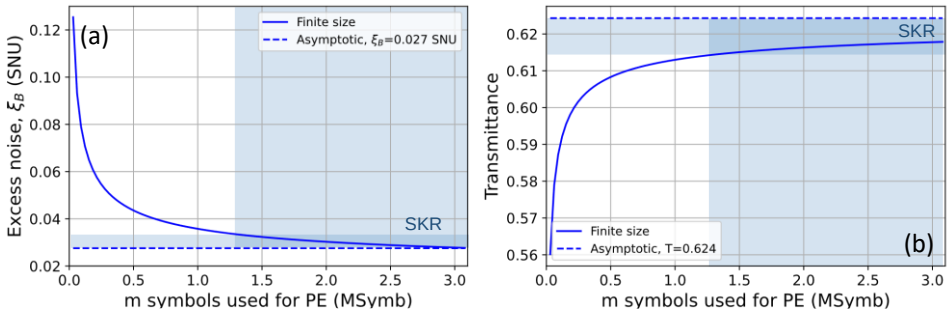

Figure 5.7: (a) Total excess noise $\boldsymbol{\xi_B = 2\xi_{B_q}}$; (b) Transmittance T as a function of the number of samples used for the parameter estimation using finite size analysis (blue line) and asymptotic analysis (dashed blue line). The asymptotic limit was calculated using all the symbols (N=3.08 x 10^6 symbols). The intersection of both rectangular areas corresponds to the range of values where it is possible to obtain a positive SKR.

previous calculation of $\xi_B(m)$ and $T(m)$. These evaluations of the SKR are displayed in Figure 5.8(a) and compared with the asymptotic parameters (see Eqs. (2.16) and (2.18) in Chapter 2). As expected, we find an optimal m value, which in this case corresponds to 2.03x10^6 symbols. For this number and for the values in Table 5.3 we can estimate the expected SKR as a function of the fiber distance (channel attenuation), as illustrated in Figure 5.8(b). In particular, for the 11 km fiber used in the experiment, the expected SKR with the considered FS regime is 27 kbps, which remains in the same order of magnitude indicated by the asymptotic regime (52 kbps), assuming the same ratio of symbols used for PE in both cases. Under the same conditions, the system could operate at distances of up to 12 km. In terms of security, we have taken into consideration the realistic mode or trusted detectors, where the electronic noise is attributed to Bob's detection and is calibrated [172]. Table 5.4 provides a numeric summary of the expected performance of the setup.

The effects of the FS analysis on Alice's modulation variance calculation are not addressed in this work, as it is calculated from the measured power, which in our case is not affected by the number of symbols measured by Bob and used for the PE. The FS effects become less relevant as N increases, so

systems with higher memory capacity can perform better. The presented results could be refined, for example to take into consideration the finite-size effects in the reconciliation phase. However, this is out of the scope of the study of this chapter, which primarily focuses on demonstrating the feasibility of employing an InP-based PIC TX in a CV-QKD system.

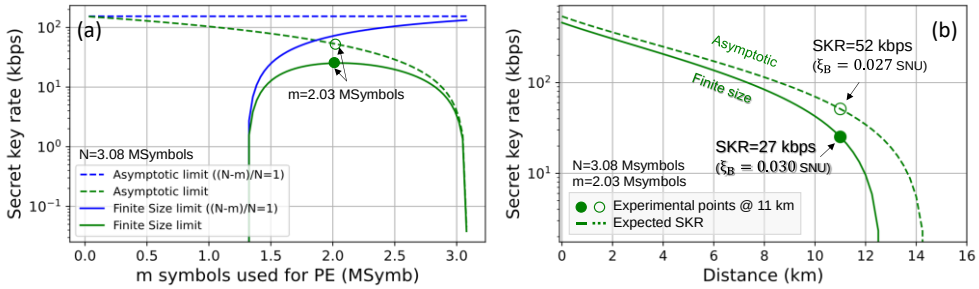

Figure 5.8: (a) Experimental secret key rate (SKR) as a function of the number of symbols *m* used for parameter estimation in asymptotic (dashed lines) and finite size (continuous lines) limits with 11 km of fiber in the channel. (b) Comparison of the expected SKR versus distance using asymptotic (dashed green line) and finite size (green line) analysis with N-m symbols used for the SKR generation. The experimental results are marked with a green dot and ring.

Table 5.4. Summary of the estimated parameters for asymptotic and finite size (FS) analysis

Parameter	Symbol	Asymptotic analysis	FS analysis ($2x10^6$ symbols)
Alice's modulation variance	V_A	2.778 SNU	2.778 SNU
Total excess noise measured at Bob	ξ_B	0.027 SNU	0.030 SNU
Transmittance of the channel	T	0.624	0.616
Secret key rate @ 11km ((N-m)/N=1)	SKR_{max}	154 kbps	79 kbps
Secret key rate @ 11km	SKR	52 kbps	27 kbps

5.5. Conclusions

We have reported a cost-effective InP-based PIC phase and amplitude encoder with an off-chip laser, used for the implementation of a pulsed GMCS CV-QKD protocol. In the first part of our study, we showed the design and electro-optical characterization of the PIC TX. The device exhibited high performance in terms

of extinction ratio, bandwidth, and linearity, making it well-suited for the pulsed GMCS CV-QKD protocol. In the second part, we conducted experimental demonstrations showcasing the viability of our PIC TX in CV-QKD systems. At a distance of 11 km, we achieved a potential SKR of 52 kbps in the asymptotic regime and 27 kbps in the finite size regime, using $2x10^6$ symbols. These SKR values seem promising and they serve as a proof of concept for the application of an InP PIC TX in CV-QKD systems. These results could be improved by increasing the symbol repetition rate and expanding the memory size, for instance, opening up the possibility of using the InP platform for the monolithic integration of CV-QKD systems.

To this end, future advancements in this field could focus on the monolithic integration of our proposed PIC TX with other components, such as an integrated laser and an integrated power meter (photodiode for feedback). Furthermore, there are areas in the PIC that require improvement, such as reducing losses introduced by certain components (e.g., the EAM and IQ modulator), and addressing distortions in IQ modulation. Pulse shaping modulation should also be explored in order to reduce the need of an amplitude modulator. Optical and electronic packaging is another relevant factor that would facilitate the testing of these devices. In terms of system-level performance, conducting experiments with more realistic setups (utilizing a real LO) and performing joint demonstrations with an integrated receiver would be beneficial. These improvements would dynamize the full integration of CV-QKD products in the consumer market.

Chapter 6

SUMMARY AND OUTLOOK

6.1. Summary

In this thesis, we have presented four different continuous-variable quantum key distribution (CV-QKD) systems. All of these were designed to move towards miniaturization and to increase the distance with positive secret-key-rate (SKR) for use in a metropolitan area. To this end, the implemented systems and related transmission channels were conceived in several specific configurations and with adapted features: (i) shared laser and true local oscillator scheme, (ii) use of single-mode and multi-core optical fibers (MCFs) in the quantum channel, (iii) transmitters (TXs) with and without phase modulators for the generation of the Gaussian-modulated coherent states (GMCSs), (iv) modular and photonic integrated circuit (PIC) TXs, and (v) systems tested using asymptotic and finite size analysis. The main specific achievements of this thesis can be summarized as follows:

- In Chapter 3, our first experiment presented a modular CV-QKD protocol using a shared laser. We showed that this system can work at metropolitan distances and avoid the back-scattering Rayleigh noise by using an additional fiber strand. Moreover, the system could be modified to a true local oscillator configuration using an MCF in the channel. In this second system, we took advantage of one of the cores to propagate the light for the locking of the lasers, demonstrating the ability to

parallelize CV-QKD signals through multi-cores and enhance in this way the SKR.

- In Chapter 4, we proposed a simplified CV-QKD TX that avoids the use of a phase modulator for the generation of the random GMCSs. This system takes advantage of the ability to directly modulate a distributed feedback (DFB) laser working in the gain-switching mode to obtain optical pulses with random phases. This involved the implementation of a phase recovery different from that implemented in the experiments presented in Chapter 3. The results show the possibility of using modulated DFB lasers in CV-QKD systems, thereby simplifying the scheme by avoiding the use of phase modulators and external random generators. In addition, the single-component TX was used in a CV-QKD system, demonstrating that we can reach experimental distances of 11 km with 2.63 Mbps of potential SKR.
- In Chapter 5, we characterized, implemented and demonstrated the use of an InP-based PIC TX for CV-QKD applications. We showed that the InP platform can give good performance and is a promising platform for the monolithic implementation of CV-QKD TX in PIC format. Moreover, we demonstrated that the implemented system can reach distances of up to 11 km and get a positive SKR even under finite size condition analysis, with the possibility of improvements thanks to the broad bandwidth of the integrated components that were not fully exploited in this thesis.

6.2. Outlook

The proposed schemes were designed as proof-of-concept and rigorously tested in the lab. However, for their practical implementation in a metropolitan

network, several key features are still missing or need to be improved. To this end, future work should focus on:

- Increasing distance and SKR. There remain several ways to enhance these, including (i) the use of sources with narrower linewidth, (ii) integration of superior detectors with higher efficiency, (iii) fiber components with lower insertion loss, (iv) parallelization via a combination of spatial multiplexing (multi-core fibers) and wavelength division multiplexing.
- Extending the use of integrated photonics, a technology that has just started being used for miniaturizing and reducing the cost of QKD systems. The objective is to increase the performance of PIC-based CV-QKD subsystems to levels comparable to those of larger modular counterparts. Key actions to consider include (i) integration of a laser source into the PIC platform, (ii) optimized design based on hybrid material and integration, (iii) integration of the control, reading and processing electronics with the PIC. It is worth noting that in the case of heterogeneous and hybrid integration, precise control in the manufacturing is required to mitigate coupling losses and reflections, which can introduce noise or compromise the security of the CV-QKD system.

The long-term goal is the development of a small form factor CV-QKD transceiver that includes both a TX and RX based on PIC also integrated with the electronics. This would create new applications for the technology and make it competitive and easily integrated with other approaches, including post-quantum cryptography. In this way, the use of secure communication

would go beyond the governmental infrastructures and reach the much larger private telecom market.

APPENDIX

A. Noise Model

There are several source of noise that affect the excess noise [27]. Some of them are the contributions from the effect introduces by the phase noise and the leakage due to the finite dynamic of the amplitude modulator (AM). Considering these effects, the noise at Alice's output can be model as [92]:

$$\xi_{noise} \approx \xi_{phase} + \xi_{AM}. \quad \text{(A. 1)}$$

And if it is defined at the channel output (Bob's input), the effect of the channel has to be considered. Then, the Eq (A. 1) takes the form:

$$\xi_{noise,B} = \xi_{phase} T\eta + \xi_{AM} T\eta \, . \quad \text{(A. 2)}$$

A.1. Phase Noise

$$\xi_{phase} = 2V_A\left(1 - e^{-V_{est}/2}\right) \quad \text{(A. 3)}$$

For low V_{est}, Eq. (A. 3) can be expressed as:

$$\xi_{phase} = V_A V_{est} \, , \quad \text{(A. 4)}$$

where V_{est} is:

$$V_{est} = V_{drift} + V_{error} + V_{channel} \, . \quad \text{(A. 5)}$$

Defining the terms in Eq. (A. 5), the first term is related to the error in the phase correction:

$$V_{drift} = 2\pi(\Delta\nu_A + \Delta\nu_B)\tau \quad \text{(A. 6)}$$

where $\Delta\nu_A$and $\Delta\nu_B$are the linewidth of the lasers (lasers used as a LO and for signal modulation) and $\tau = |t_R - t_S|$ is the time separation between the reference and signal pulses.

The second term is associated to the error in the reference pulses due to the channel noise and shot noise:

$$V_{error} = \frac{\chi + 1}{E_R^2}, \tag{A. 7}$$

where the variance χ is defined as $\chi = \frac{\delta_{det} - T}{T} + \xi_A$ and E_R is the amplitude of the reference pulse. In this thesis it is equivalent to the extinction ratio $R = E_R^2$, and $\delta_{det}$is 2 or 1 if it is heterodyne or homodyne detection, respectively.

Lastly, in the case that the reference and the signal pulses follow the same optical path $\theta_S^{ch} = \theta_R^{ch}$, as it is the case in all the experiments presented in this thesis, $V_{channel} \approx 0$.

A.2. Amplitude Modulator Finite Dynamics

Considering the contributions to the excess noise due to the leak photons due to the dynamic range of the amplitude modulator:

$$\xi_{AM} = E_{max}^2 10^{-d_{dB}/10}, \tag{A. 8}$$

where $d_{dB}$is the dynamic range of the AM and can be calculated as:

$$d_{dB} = 10log_{10}\left(E_{max}^2 / E_{min}^2\right). \tag{A. 9}$$

Finally, we can express a lower bound on the total excess noise in the transmitted LO (same laser used as a LO and for signal generation) design and at the channel output as:

$$\xi_{noise,B} = \xi_{phase} T\eta + \xi_{AM} T\eta \geq \left[V_A\left(V_{drift} + V_{error}\right)\right] T\eta + \left[R10^{-d_{dB}/10}\right] T\eta$$
$$\geq V_A \left[(4\pi\Delta\nu\tau) + \frac{\chi + 1}{R}\right] T\eta + \left[R10^{-d_{dB}/10}\right] T\eta. \quad \text{(A. 10)}$$

REFERENCES

[1] D. Davies, “A brief history of cryptography,” *Inf. Secur. Tech. Rep.*, vol. 2, no. 2, pp. 14–17, Jan. 1997, doi: 10.1016/S1363-4127(97)81323-4.

[2] L. Jaeger, *The Second Quantum Revolution*. Cham: Springer International Publishing, 2018.

[3] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[5] J. Proos and C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves,” *arXiv:0301141[quant-ph]*, Jan. 2004, doi: 10.26421/qic3.4-3.

[6] S. Pirandola *et al.*, “Advances in quantum cryptography,” *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, Dec. 2020, doi: 10.1364/AOP.361502.

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2010.

[8] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, “The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet,” *IEEE Commun. Surv. Tutorials*, vol. 24, no. 2, pp. 839–894, 2022, doi: 10.1109/COMST.2022.3144219.

[9] L.-J. Wang *et al.*, “Experimental authentication of quantum key distribution with post-quantum cryptography,” *npj Quantum Inf.*, vol. 7, no. 67, May 2021, doi: 10.1038/s41534-021-00400-7.

[10] Y.-H. Yang *et al.*, “All optical metropolitan quantum key distribution network with post-quantum cryptography authentication,” *Opt. Express*, vol. 29, no. 16, pp. 25859–25867, Aug. 2021, doi: 10.1364/OE.432944.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009, doi: 10.1103/RevModPhys.81.1301.

[12] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key

distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, p. 025002, 2020, doi: 10.1103/revmodphys.92.025002.

[13] "Quantum Flagship." https://qt.eu/ (accessed Aug. 25, 2023).

[14] "LuxQuanta." https://www.luxquanta.com/ (accessed Aug. 25, 2023).

[15] "ID Quantique." https://www.idquantique.com/ (accessed Aug. 25, 2023).

[16] "TOSHIBA Europe." https://www.toshiba.co.uk/ (accessed Aug. 25, 2023).

[17] "KEEQuant." https://www.keequant.com/ (accessed Aug. 25, 2023).

[18] "QuantumCTek." http://www.quantum-info.com/English/#hero (accessed Aug. 25, 2023).

[19] "MagiQ." https://www.magiqtech.com/ (accessed Aug. 25, 2023).

[20] F. Grosshans, G. Van Asschet, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003, doi: 10.1038/nature01289.

[21] A. Boaron *et al.*, "Secure Quantum Key Distribution over 421 km of Optical Fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, p. 190502, 2018, doi: 10.1103/PhysRevLett.121.190502.

[22] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, May 2011, doi: 10.1364/oe.19.010387.

[23] A. Stein, I. H. L. Grande, L. Castelvero, and V. Pruneri, "Robust polarization state generation for long-range quantum key distribution," *Opt. Express*, vol. 31, no. 9, pp. 13700–13707, Apr. 2023, doi: 10.1364/OE.481797.

[24] K. A. Patel *et al.*, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, no. 4, p. 041010, 2012, doi: 10.1103/PhysRevX.2.041010.

[25] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum Cryptography, or Unforgeable Subway Tokens," in *Advances in cryptology: Proceedings of Crypto 82*, 1982, pp. 267–275, doi: 10.1007/978-1-4757-0602-4_26.

[26] G. Brassard, "Brief history of quantum cryptography: a personal perspective," in *IEEE Information Theory Workshop on Theory and*

Practice in Information-Theoretic Security, 2005., 2005, pp. 19–23, doi: 10.1109/ITWTPI.2005.1543949.

[27] F. Laudenbach *et al.*, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations," *Adv. Quantum Technol.*, vol. 1, p. 1800011, Jun. 2018, doi: 10.1002/qute.201800011.

[28] S. Kreinberg *et al.*, "Modelling weak-coherent CV-QKD systems using a classical simulation framework," *Int. Conf. Transparent Opt. Networks*, vol. 2019-July, pp. 4–7, 2019, doi: 10.1109/ICTON.2019.8840253.

[29] S. Etcheverry *et al.*, "Quantum key distribution session with 16-dimensional photonic states," *Sci. Reports 2013 31*, vol. 3, no. 1, pp. 1–5, Jul. 2013, doi: 10.1038/srep02316.

[30] K. A. Patel *et al.*, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, p. 051123, 2014, doi: 10.1063/1.4864398.

[31] A. Sit *et al.*, "High-dimensional intracity quantum cryptography with structured photons," *Optica*, vol. 4, no. 9, pp. 1006–1010, Sep. 2017, doi: 10.1364/OPTICA.4.001006.

[32] G. Cañas *et al.*, "High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers," *Phys. Rev. A*, vol. 96, no. 2, p. 022317, Aug. 2017, doi: 10.1103/PhysRevA.96.022317.

[33] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems & Signal Processing*, 1984, pp. 175–179.

[34] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. P1, pp. 7–11, 2014, doi: 10.1016/j.tcs.2014.05.025.

[35] N. J. Cerf, M. Lévy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A. At. Mol. Opt. Phys.*, vol. 63, no. 5, pp. 523111–523115, 2001, doi: 10.1103/PhysRevA.63.052311.

[36] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, Jan. 2002, doi: 10.1103/PhysRevLett.88.057902.

[37] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, no. 17, p. 170504, Oct. 2004, doi: 10.1103/PhysRevLett.93.170504.

[38] L. C. Comandar *et al.*, "A flexible continuous-variable QKD system using off-the-shelf components," in *Quantum Information Science and Technology III*, 2017, no. 10442, p. 9, doi: 10.1117/12.2279913.

[39] H. Wang *et al.*, "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," *Opt. Express*, vol. 28, no. 22, pp. 32882–32893, Oct. 2020, doi: 10.1364/OE.404611.

[40] G. Zhang *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics*, vol. 13, no. 12, pp. 839–842, Dec. 2019, doi: 10.1038/s41566-019-0504-5.

[41] D. Pan, S. Xing Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, "Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states," *Phys. Rev. A*, vol. 101, no. 1, p. 012343, 2020, doi: 10.1103/PhysRevA.101.012343.

[42] A. Aguado *et al.*, "The Engineering of Software-Defined Quantum Key Distribution Networks," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 20–26, Jul. 2019, doi: 10.1109/MCOM.2019.1800763.

[43] F. Laudenbach *et al.*, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum*, vol. 3, p. 193, Oct. 2019, doi: 10.22331/q-2019-10-07-193.

[44] T. A. Eriksson *et al.*, "Inter-Core Crosstalk Impact of Classical Channels on CV-QKD in Multicore Fiber Transmission," in *Optical Fiber Communication Conference (OFC)*, 2019, p. Th1J.1, doi: 10.1364/OFC.2019.Th1J.1.

[45] Y. Pi *et al.*, "Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber," *Opt. Lett.*, vol. 48, no. 7, pp. 1766–1769, Apr. 2023, doi: 10.1364/OL.485913.

[46] C. Abellán *et al.*, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Opt. Express*, vol. 22, no. 2, p. 1645, 2014, doi: 10.1364/oe.22.001645.

[47] L. Li *et al.*, "Continuous-variable quantum key distribution with on-chip light sources," *Photonics Res.*, vol. 11, no. 4, pp. 504–516, 2023, doi: 10.1364/prj.473328.

[48] M. Persechino, "Experimental study of the integration of continuous-variable quantum key distribution into a silicon photonics device,"

Université Paris-Saclay, 2017.

[49] G. Zhang *et al.*, “Integrated Chip for Continuous-variable Quantum Key Distribution using Silicon Photonic Fabrication,” in *Conference on Lasers and Electro-Optics (CLEO)*, 2018, p. paper FTu3G.2, Accessed: May 04, 2023. [Online]. Available: https://opg.optica.org/abstract.cfm?URI=CLEO_QELS-2018-FTu3G.2.

[50] C. Bruynsteen, M. Vanhoecke, J. Bauwelinck, and X. Yin, “Integrated balanced homodyne photonic–electronic detector for beyond 20 GHz shot-noise-limited measurements,” *Optica*, vol. 8, no. 9, pp. 1146–1152, Sep. 2021, doi: 10.1364/OPTICA.420973.

[51] J. Aldama *et al.*, “InP-based CV-QKD PIC Transmitter,” in *Optical Fiber Communication Conference (OFC)*, 2023, p. paper M1I.3, [Online]. Available: https://opg.optica.org/abstract.cfm?uri=OFC-2023-M1I.3.

[52] A. A. E. Hajomer *et al.*, “Continuous-Variable Quantum Key Distribution at 10 GBaud using an Integrated Photonic-Electronic Receiver,” *arXiv:2305.19642 [quant-ph]*, May 2023, Accessed: Jun. 01, 2023. [Online]. Available: http://arxiv.org/abs/2305.19642.

[53] L. Trigo Vidarte, “Design and implementation of high-performance devices for continuous-variable quantum key distribution,” Université Paris-Saclay, 2020.

[54] Y. Piétri, L. Trigo-Vidarte, M. Schiavon, P. Grangier, A. Rhouni, and E. Diamanti, “CV-QKD Receiver Platform Based On A Silicon Photonic Integrated Circuit,” in *Optical Fiber Communication Conference (OFC)*, 2023, p. paper M1I.2, [Online]. Available: https://opg.optica.org/abstract.cfm?uri=OFC-2023-M1I.2.

[55] M. Navascués, F. Grosshans, and A. Acín, “Optimality of Gaussian attacks in continuous-variable quantum cryptography,” *Phys. Rev. Lett.*, vol. 97, no. 19, p. 190502, Nov. 2006, doi: 10.1103/PhysRevLett.97.190502.

[56] R. Renner and J. I. Cirac, “de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography,” *Phys. Rev. Lett.*, vol. 102, no. 11, p. 110504, Mar. 2009, doi: 10.1103/PhysRevLett.102.110504.

[57] R. García-Patrón and N. J. Cerf, “Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution,” *Phys. Rev. Lett.*, vol. 97, no. 19, p. 190503, 2006, doi: 10.1103/PhysRevLett.97.190503.

[58] A. Leverrier, “Composable security proof for continuous-variable quantum key distribution with coherent states,” *Phys. Rev. Lett.*, vol. 114, no. 7, p. 070501, 2015, doi: 10.1103/PhysRevLett.114.070501.

[59] A. Leverrier, “Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction,” *Phys. Rev. Lett.*, vol. 118, no. 20, 2017, doi: 10.1103/PhysRevLett.118.200501.

[60] I. H. Lopez Grande, S. Etcheverry, J. Aldama, S. Ghasemi, D. Nolan, and V. Pruneri, “Adaptable transmitter for discrete and continuous variable quantum key distribution,” *Opt. Express*, vol. 29, no. 10, p. 14815, May 2021, doi: 10.1364/OE.425382.

[61] Y. Zhang *et al.*, “Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber,” *Phys. Rev. Lett.*, vol. 125, no. 1, p. 010502, Jul. 2020, doi: 10.1103/PhysRevLett.125.010502.

[62] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, “High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM,” in *European Conference on Optical Communication (ECOC)*, Sep. 2021, pp. 1–4, doi: 10.1109/ECOC52684.2021.9606013.

[63] S. Sarmiento *et al.*, “Continuous-variable quantum key distribution over a 15 km multi-core fiber,” *New J. Phys.*, vol. 24, no. 6, p. 063011, Jun. 2022, doi: 10.1088/1367-2630/ac753b.

[64] J. Lodewyck *et al.*, “Quantum key distribution over 25 km with an all-fiber continuous-variable system,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 76, no. 4, pp. 1–10, 2007, doi: 10.1103/PhysRevA.76.042305.

[65] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *Nat. Photonics*, vol. 7, no. 5, pp. 378–381, 2013, doi: 10.1038/nphoton.2013.63.

[66] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Sci. Rep.*, vol. 6, p. 19201, Jan. 2016, doi: 10.1038/srep19201.

[67] P. Jouguet *et al.*, “Field test of classical symmetric encryption with continuous variables quantum key distribution,” *Opt. Express*, vol. 20, no. 13, pp. 14030–14041, Jun. 2012, doi: 10.1364/OE.20.014030.

[68] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, “Field demonstration of a continuous-variable quantum key distribution

network," *Opt. Lett.*, vol. 41, no. 15, p. 3511, 2016, doi: 10.1364/ol.41.003511.

[69] F. Karinou *et al.*, "Toward the integration of CV quantum key distribution in deployed optical networks," *IEEE Photonics Technol. Lett.*, vol. 30, no. 7, pp. 650–653, 2018, doi: 10.1109/LPT.2018.2810334.

[70] Y.-C. Zhang *et al.*, "Continuous-variable QKD over 50km commercial fiber," *Quantum Sci. Technol.*, vol. 4, no. 3, p. 035006, 2019, doi: 10.1088/2058-9565/ab19d1.

[71] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," *Opt. Express*, vol. 28, no. 10, p. 14547, May 2020, doi: 10.1364/OE.391491.

[72] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," *New J. Phys.*, vol. 11, no. 4, p. 045023, Apr. 2009, doi: 10.1088/1367-2630/11/4/045023.

[73] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Key Reconciliation with Low-Density Parity-Check Codes for Long-Distance Quantum Cryptography," *arXiv:1702.07740v2 [quant-ph]*, 2017, doi: 10.1038/s41534-018-0070-6.

[74] K. Kikuchi, "Fundamentals of coherent optical fiber communications," *J. Light. Technol.*, vol. 34, no. 1, pp. 157–179, Jan. 2016, doi: 10.1109/JLT.2015.2463719.

[75] A. Davis, M. Pettitt, J. King, and S. Wright, "Phase diversity techniques for coherent optical receivers," *J. Light. Technol.*, vol. 5, no. 4, pp. 561–572, 1987, doi: 10.1109/JLT.1987.1075539.

[76] J. A. Altabas, S. Sarmiento, and J. A. Lazaro, "Passive Optical Networks: Introduction," *Wiley Encyclopedia of Electrical and Electronics Engineering, J.G. Webster (Ed.)*. 2018.

[77] I. Roudas, "Coherent optical communication systems," in *WDM Systems and Networks*, N. Antoniades, G. Ellinas, and I. Roudas, Eds. New York: Elsevier, 2012, pp. 373–417.

[78] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X*, vol. 5, no. 4, p. 041009, 2015, doi: 10.1103/PhysRevX.5.041009.

[79] A. Leverrier, F. Grosshans, and P. Grangier, “Finite-size analysis of a continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 81, no. 6, p. 062343, 2010, doi: 10.1103/PhysRevA.81.062343.

[80] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, “Analysis of imperfections in practical continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 86, no. 3, p. 032309, 2012, doi: 10.1103/PhysRevA.86.032309.

[81] V. Mannalath, S. Mishra, and A. Pathak, “A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness,” *arXiv:2203.00261 [quant-ph]*, 2022, doi: 10.48550/arXiv.2203.00261.

[82] M. Zou, Y. Mao, and T.-Y. Chen, “Rigorous calibration of homodyne detection efficiency for continuous-variable quantum key distribution,” *Opt. Express*, vol. 30, no. 13, pp. 22788–22797, Jun. 2022, doi: 10.1364/OE.461680.

[83] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, “Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 87, no. 6, p. 062313, Jun. 2013, doi: 10.1103/PhysRevA.87.062313.

[84] B. Heim *et al.*, “Atmospheric continuous-variable quantum communication,” *New J. Phys.*, vol. 16, no. 11, p. 113018, Nov. 2014, doi: 10.1088/1367-2630/16/11/113018.

[85] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, “25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel,” *Sci. Rep.*, vol. 5, no. 9, p. 14607, Sep. 2015, doi: 10.1038/srep14607.

[86] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, “Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol,” *Phys. Rev. A*, vol. 87, no. 5, p. 052309, May 2013, doi: 10.1103/PhysRevA.87.052309.

[87] J. Z. Huang *et al.*, “Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack,” *Phys. Rev. A*, vol. 87, no. 6, p. 062329, Jun. 2013, doi: 10.1103/PhysRevA.87.062329.

[88] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, “Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems,” *Phys. Rev. A*, vol. 88, no. 2, p. 022339, Aug. 2013, doi: 10.1103/PhysRevA.88.022339.

[89] H. Häseler, T. Moroder, and N. Lütkenhaus, “Testing quantum devices: Practical entanglement verification in bipartite optical systems,” *Phys. Rev. A*, vol. 77, no. 3, p. 032303, Mar. 2008, doi: 10.1103/PhysRevA.77.032303.

[90] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, “High-speed continuous-variable quantum key distribution without sending a local oscillator,” *Opt. Lett.*, vol. 40, no. 16, p. 3695, 2015, doi: 10.1364/ol.40.003695.

[91] D. B. S. Soh *et al.*, “Self-referenced continuous-variable quantum key distribution protocol,” *Phys. Rev. X*, vol. 5, no. 4, p. 041010, 2015, doi: 10.1103/PhysRevX.5.041010.

[92] A. Marie and R. Alléaume, “Self-coherent phase reference sharing for continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 95, no. 1, p. 012316, 2017, doi: 10.1103/PhysRevA.95.012316.

[93] T. Wang *et al.*, “High key rate continuous-variable quantum key distribution with a real local oscillator,” *Opt. Express*, vol. 26, no. 3, pp. 2794–2806, 2018, doi: 10.1364/OE.26.002794.

[94] S. Kleis, M. Rueckmann, and C. G. Schaeffer, “Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals,” *Opt. Lett.*, vol. 42, no. 8, pp. 1588–1591, Apr. 2017, doi: 10.1364/ol.42.001588.

[95] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, “Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator,” *arXiv:2305.08156 [quant-ph]*, May 2023, doi: doi.org/10.48550/arXiv.2305.08156.

[96] D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, and G. Zeng, “Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol,” *Phys. Rev. A*, vol. 94, no. 3, p. 032305, Sep. 2016, doi: 10.1103/PhysRevA.94.032305.

[97] D. Subacius, A. Zavriyev, and A. Trifonov, “Backscattering limitation for fiber-optic quantum key distribution systems,” *Appl. Phys. Lett.*, vol. 86, p. 011103, 2005, doi: 10.1063/1.1842862.

[98] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum key distribution over 67 km with a plug & play system,” *New J. Phys.*, vol. 4, p. 41, 2002.

[99] T. Mizuno and Y. Miyamoto, “High-capacity dense space division

multiplexing transmission," *Opt. Fiber Technol.*, vol. 35, pp. 108–117, 2017, doi: 10.1016/j.yofte.2016.09.015.

[100] K. Saitoh and S. Matsuo, "Multicore fibers for large capacity transmission," *Nanophotonics*, vol. 2, no. 5–6, pp. 441–454, Dec. 2013, doi: 10.1515/nanoph-2013-0037.

[101] D. J. Richardson, J. M. Fini, and L. E. Nelson, "Space-division multiplexing in optical fibres," *Nat. Photonics*, vol. 7, no. 5, pp. 354–362, 2013, doi: 10.1038/NPHOTON.2013.94.

[102] P. J. Winzer, "Making spatial multiplexing a reality," *Nat. Photonics*, vol. 8, no. 5, pp. 345–348, 2014, doi: 10.1038/nphoton.2014.58.

[103] B. Zhu *et al.*, "Seven-core multicore fiber transmissions for passive optical network," *Opt. Express*, vol. 18, no. 11, pp. 11117–11122, May 2010, doi: 10.1364/OE.18.011117.

[104] R. S. Luis *et al.*, "Demonstration of a 1 Pb/s spatial channel network node," 2019, doi: 10.1049/cp.2019.1032.

[105] R.-J. Essiambre and R. W. Tkach, "Capacity Trends and Limits of Optical Communication Networks," *Proc. IEEE*, vol. 100, no. 5, pp. 1035–1055, 2012.

[106] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, no. 1, pp. 1–15, Apr. 2017, doi: 10.1038/ncomms15043.

[107] D. Bacco *et al.*, "Boosting the secret key rate in a shared quantum and classical fibre communication system," *Commun. Phys.*, vol. 2, no. 140, pp. 1–8, Nov. 2019, doi: 10.1038/s42005-019-0238-1.

[108] M. Nooruzzaman and T. Morioka, "Multicore fibers for high-capacity submarine transmission systems," *J. Opt. Commun. Netw.*, vol. 10, no. 2, pp. A175–A184, 2018, doi: 10.1364/JOCN.10.00A175.

[109] D. Zavitsanos, A. Ntanos, G. Giannoulis, and H. Avramopoulos, "On the QKD Integration in Converged Fiber/Wireless Topologies for Secured, Low-Latency 5G/B5G Fronthaul," *Appl. Sci.*, vol. 10, no. 15, p. 5193, 2020.

[110] J. F. Dynes *et al.*, "Quantum key distribution over multicore fiber," *Opt. Express*, vol. 24, no. 8, p. 8081, 2016, doi: 10.1364/oe.24.008081.

[111] B. Da Lio *et al.*, "Record-High Secret Key Rate for Joint Classical and Quantum Transmission over a 37-Core Fiber," 2018, doi: 10.1109/IPCon.2018.8527341.

[112] T. A. Eriksson *et al.*, "Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission," *IEEE Photonics Technol. Lett.*, vol. 31, no. 6, pp. 467–470, Mar. 2019, doi: 10.1109/LPT.2019.2898458.

[113] R. Lin *et al.*, "Telecom Compatibility Validation of Quantum Key Distribution Co-Existing with 112 Gbps/λ/core Data Transmission in Non-Trench and Trench-Assistant Multicore Fibers," 2018, doi: 10.1109/ECOC.2018.8535406.

[114] E. Hugues-Salas, R. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Co-existence of 9.6 Tb/s Classical Channels and a Quantum Key Distribution (QKD) Channel over a 7-core Multicore Optical Fibre," in *2018 IEEE British and Irish Conference on Optics and Photonics (BICOP)*, 2018, no. December, pp. 1–4, doi: 10.1109/BICOP.2018.8658328.

[115] R. Asif, M. Haithem, and W. J. Buchanan, "Experimental High Speed Data Encryption via SDM-CV-QKD Signaling for High-Capacity Access Network," in *Advanced Photonics 2018 (BGPP, IPR, NP, NOMA, Sensors, Networks, SPPCom, SOF)*, 2018, p. NeTh2F.3, doi: 10.1364/NETWORKS.2018.NeTh2F.3.

[116] C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, and Y. Ji, "Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber.," *Opt. Express*, vol. 27, no. 4, pp. 5125–5135, Feb. 2019, doi: 10.1364/OE.27.005125.

[117] E. Hugues-Salas *et al.*, "11.2 Tb/s Classical Channel Coexistence With DV-QKD Over a 7-Core Multicore Fiber," *J. Light. Technol.*, vol. 38, no. 18, pp. 5064–5070, Sep. 2020, Accessed: Aug. 03, 2023. [Online]. Available: https://opg.optica.org/abstract.cfm?uri=jlt-38-18-5064.

[118] B. Da Lio *et al.*, "Stable Transmission of High-Dimensional Quantum States over a 2-km Multicore Fiber," *IEEE J. Sel. Top. Quantum Electron.*, vol. 26, no. 4, p. 6400108, Jul. 2020, doi: 10.1109/JSTQE.2019.2960937.

[119] G. B. Xavier and G. Lima, "Quantum information processing with space-division multiplexing optical fibres," *Commun. Phys.*, vol. 3, no. 9, Dec. 2020, doi: 10.1038/s42005-019-0269-7.

[120] Y. Ding *et al.*, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Inf.*, vol. 3, no. 1, p. 25, Jun. 2017, doi: 10.1038/s41534-017-0026-2.

[121] E. A. Ortega *et al.*, "Experimental Space-Division Multiplexed Polarization-Entanglement Distribution through 12 Paths of a Multicore

Fiber," *PRX Quantum*, vol. 2, no. 4, p. 040356, Dec. 2021, doi: 10.1103/PRXQuantum.2.040356.

[122] X.-M. Hu *et al.*, "Efficient distribution of high-dimensional entanglement through 11 km fiber," *Optica*, vol. 7, no. 7, pp. 738–743, Jul. 2020, doi: 10.1364/OPTICA.388773.

[123] J. Cariñe *et al.*, "Multi-core fiber integrated multi-port beam splitters for quantum information processing," *Optica*, vol. 7, no. 5, pp. 542–550, 2020, doi: 10.1364/optica.388912.

[124] F. Li, H. Zhong, Y. Wang, Y. Kang, D. Huang, and Y. Guo, "Performance analysis of continuous-variable quantum key distribution with multi-core fiber," *Appl. Sci.*, vol. 8, no. 10, p. 1951, 2018, doi: 10.3390/app8101951.

[125] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation," *Phys. Rev. X*, vol. 9, no. 2, p. 21059, 2019, doi: 10.1103/PhysRevX.9.021059.

[126] J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution," *Phys. Rev. X*, vol. 9, no. 4, p. 041064, Dec. 2019, doi: 10.1103/PhysRevX.9.041064.

[127] S. Bäuml, C. Pascual García, V. Wright, O. Fawzi, and A. Acín, "Security of discrete-modulated continuous-variable quantum key distribution," *arXiv:2303.09255 [quant-ph]*, 2023, doi: 10.48550/arXiv.2303.09255.

[128] M. Jofre *et al.*, "True random numbers from amplified quantum vacuum," *Opt. Express*, vol. 19, no. 21, p. 20665, Oct. 2011, doi: 10.1364/OE.19.020665.

[129] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A*, vol. 73, no. 2, p. 022320, 2006, doi: 10.1103/physreva.73.022320.

[130] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, no. 1, p. 015004, Feb. 2017, doi: 10.1103/RevModPhys.89.015004.

[131] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Inf.*, vol. 2, no. 1, pp. 1–9, 2016, doi: 10.1038/npjqi.2016.21.

[132] J. Aldama, S. Sarmiento, I. H. Lopez Grande, S. Signorini, L. T. Vidarte, and

V. Pruneri, “Integrated QKD and QRNG Photonic Technologies,” *J. Light. Technol.*, vol. 40, no. 23, pp. 7498–7517, Dec. 2022, doi: 10.1109/JLT.2022.3218075.

[133] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator,” *Rev. Sci. Instrum.*, vol. 71, no. 4, pp. 1675–1680, Apr. 2000, doi: 10.1063/1.1150518.

[134] Q. Yan, B. Zhao, Q. Liao, and N. Zhou, “Multi-bit quantum random number generation by measuring positions of arrival photons,” *Rev. Sci. Instrum.*, vol. 85, no. 10, p. 103116, 2014, doi: 10.1063/1.4897485.

[135] M. Stipčević and B. M. Rogina, “Quantum random number generator based on photonic emission in semiconductors,” *Rev. Sci. Instrum.*, vol. 78, no. 4, p. 045104, Apr. 2007, doi: 10.1063/1.2720728/349822.

[136] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, “High speed optical quantum random number generation,” *Opt. Express*, vol. 18, no. 12, pp. 13029–13037, Jun. 2010, doi: 10.1364/OE.18.013029.

[137] W. Wei and H. Guo, “Bias-free true random-number generator,” *Opt. Lett.*, vol. 34, no. 12, pp. 1876–1878, Jun. 2009, doi: 10.1364/OL.34.001876.

[138] T. Durt, C. Belmonte, L. P. Lamoureux, K. Panajotov, F. Van Den Berghe, and H. Thienpont, “Fast quantum-optical random-number generators,” *Phys. Rev. A*, vol. 87, no. 2, p. 022339, Feb. 2013, doi: 10.1103/PHYSREVA.87.022339/FIGURES/10/MEDIUM.

[139] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, “Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals,” *J. Light. Technol.*, vol. 30, no. 9, pp. 1329–1334, 2012, doi: 10.1109/JLT.2012.2188377.

[140] Y. Shen, L. Tian, and H. Zou, “Practical quantum random number generator based on measuring the shot noise of vacuum states,” *Phys. Rev. A*, vol. 81, no. 6, p. 063814, Jun. 2010, doi: 10.1103/PhysRevA.81.063814.

[141] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” *Opt. Lett.*, vol. 35, no. 3, pp. 312–314, Feb. 2010, doi: 10.1364/OL.35.000312.

[142] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Express*, vol. 20, no. 11, p. 12366, 2012, doi: 10.1364/oe.20.012366.

[143] Y. Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J. W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Rev. Sci. Instrum.*, vol. 86, no. 6, p. 063105, Jun. 2015, doi: 10.1063/1.4922417.

[144] J. R. Alvarez Velasquez, S. Sarmiento-Hernández, J. Lazaro, J. Gené, and J. Torres, "Random number generation by coherent detection of quantum phase noise," *Opt. Express*, vol. 28, no. 4, pp. 5538–5547, 2020, doi: 10.1364/oe.383196.

[145] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Appl. Phys. Lett.*, vol. 104, no. 26, p. 261112, Jul. 2014, doi: 10.1063/1.4886761.

[146] R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, "Influence of Chirp, Jitter, and Relaxation Oscillations on Probabilistic Properties of Laser Pulse Interference," *IEEE J. Quantum Electron.*, vol. 57, no. 2, pp. 1–7, Apr. 2021, doi: 10.1109/JQE.2021.3055149.

[147] C. Abellan *et al.*, "Quantum entropy source on an InP photonic integrated circuit for random number generation," *Optica*, vol. 3, no. 9, pp. 989–994, 2016, doi: 10.1364/OPTICA.3.000989.

[148] T. Roger, T. Paraiso, I. De Marco, D. G. Marangon, Z. Yuan, and A. J. Shields, "Real-time interferometric quantum random number generation on chip," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B137–B142, Mar. 2019, doi: 10.1364/JOSAB.36.00B137.

[149] F. Furrer *et al.*, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, no. 10, p. 100502, Sep. 2012, doi: 10.1103/PHYSREVLETT.109.100502/FIGURES/3/MEDIUM.

[150] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of Continuous-Variable Quantum Key Distribution Against General Attacks," *Phys. Rev. Lett.*, vol. 110, no. 3, p. 030502, Jan. 2013, doi: 10.1103/PhysRevLett.110.030502.

[151] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution:

Composable security against coherent attacks," *Phys. Rev. A*, vol. 97, no. 5, p. 052327, May 2018, doi: 10.1103/PhysRevA.97.052327.

[152] B. Qi, P. G. Evans, and W. P. Grice, "Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution," *Phys. Rev. A*, vol. 97, no. 1, p. 012317, Jan. 2018, doi: 10.1103/PhysRevA.97.012317.

[153] B. Qi, H. Gunther, P. G. Evans, B. P. Williams, R. M. Camacho, and N. A. Peters, "Experimental Passive-State Preparation for Continuous-Variable Quantum Communications," *Phys. Rev. Appl.*, vol. 13, p. 54065, 2020, doi: 10.1103/PhysRevApplied.13.054065.

[154] X. Wu, Y. Wang, Y. Guo, H. Zhong, and D. Huang, "Passive continuous-variable quantum key distribution using a locally generated local oscillator," *Phys. Rev. A*, vol. 103, no. 3, p. 32604, 2021, doi: 10.1103/PhysRevA.103.032604.

[155] P. Huang, T. Wang, R. Chen, P. Wang, Y. Zhou, and G. Zeng, "Experimental continuous-variable quantum key distribution using a thermal source," *New J. Phys.*, vol. 23, no. 11, p. 113028, Nov. 2021, doi: 10.1088/1367-2630/AC3684.

[156] I. N. Cano, J. C. Velasquez, and J. Prat, "7.5 Gb/s Direct DFB Phase Modulation with 8-DPSK for 6.25 GHz Spaced Coherent UDWDM-PONs," in *Optical Fiber Communication Conference (OFC)*, Mar. 2016, p. M3C.4, doi: 10.1364/OFC.2016.M3C.4.

[157] J. Camilo Velásquez, I. N. Cano, V. Polo, and J. Prat, "Direct Beat Phase Modulated DFB for flexible 1.25-5 Gb/s Coherent UDWDM-PONs," in *Optical Fiber Communication Conference (OFC)*, 2017, p. Th2A.32.

[158] I. N. Cano, A. Lerín, and J. Prat, "DQPSK directly phase modulated DFB for flexible coherent UDWDM-PONs," *IEEE Photonics Technol. Lett.*, vol. 28, no. 1, pp. 35–38, Sep. 2016, doi: 10.1109/LPT.2015.2478972.

[159] D. M. Pataca *et al.*, "Gain-switched DFB lasers," *J. Microwaves Optoelectron.*, vol. 1, no. 1, pp. 46–63, 1997.

[160] T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. L. Yuan, and A. J. Shields, "Advanced Laser Technology for Quantum Communications (Tutorial Review)," *Adv. Quantum Technol.*, vol. 4, no. 10, p. 2100062, Aug. 2021, doi: 10.1002/qute.202100062.

[161] H. T. G. Bookey and A. K. Kar, "Characterisation and optimisation of a dual-channel picosecond gain-switched DFB laser system for use as a

pump–probe source," *Opt. Commun.*, vol. 248, no. 1–3, pp. 229–239, Apr. 2005, doi: 10.1016/J.OPTCOM.2004.12.009.

[162] S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130502, 2012, doi: 10.1103/PhysRevLett.108.130502.

[163] A. Huang, Á. Navarrete, S. H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding Attack in Quantum Key Distribution," *Phys. Rev. Appl.*, vol. 12, no. 6, p. 064043, 2019, doi: 10.1103/PhysRevApplied.12.064043.

[164] M. Ziebell *et al.*, "Towards On-Chip Continuous-Variable Quantum Key Distribution," in *European Conference on Lasers and Electro-Optics (CLEO)*, 2015, p. JSV-4.2.

[165] A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," *J. Opt.*, vol. 18, no. 8, p. 083002, Jul. 2016, doi: 10.1088/2040-8978/18/8/083002.

[166] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," *Nat. Photonics*, vol. 14, no. 5, pp. 273–284, May 2020, doi: 10.1038/s41566-019-0532-1.

[167] S. Tanzilli, A. Martin, F. Kaiser, M. P. de Micheli, O. Alibart, and D. B. Ostrowsky, "On the genesis and evolution of integrated quantum optics," *Laser Photonics Rev.*, vol. 6, no. 1, pp. 115–143, 2012, doi: 10.1002/lpor.201100010.

[168] G. Moody *et al.*, "2022 Roadmap on integrated quantum photonics," *J. Phys. Photonics*, vol. 4, no. 1, p. 012501, Jan. 2022, doi: 10.1088/2515-7647/AC1EF4.

[169] Y. Shen *et al.*, "On-Chip Continuous-Variable Quantum Key Distribution(CV-QKD) and Homodyne Detection," in *Optical Fiber Communication Conference (OFC)*, Mar. 2020, p. paper W2A.53, doi: 10.1364/OFC.2020.W2A.53.

[170] M. Smit *et al.*, "An introduction to InP-based generic integration technology," *Semicond. Sci. Technol.*, vol. 29, no. 8, p. 083001, Jun. 2014, doi: 10.1088/0268-1242/29/8/083001.

[171] F. M. Soares *et al.*, "InP-based foundry PICs for optical interconnects," *Appl. Sci.*, vol. 9, no. 8, 2019, doi: 10.3390/app9081588.

[172] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Improvement of continuous-variable quantum key

distribution systems by using optical preamplifiers," *J. Phys. B At. Mol. Opt. Phys.*, vol. 42, no. 11, 2009, doi: 10.1088/0953-4075/42/11/114014.

[173] H. Agarwal *et al.*, "Supporting information for '2D-3D integration of hBN and a high- κ dielectric for ultrafast graphene-based electro-absorption modulators' Optical conductivity model for graphene," *Nat. Commun.*, vol. 12, no. 1, 2021.

[174] F. Roumestan *et al.*, "Experimental Demonstration of Discrete Modulation Formats for Continuous Variable Quantum Key Distribution," *arXiv:2207.11702 [quant-ph]*, Jul. 2022, doi: 10.48550/arxiv.2207.11702.