Universidade de Aveiro
2023

Daniel Filipe
Figueiredo Pereira

Análise e Otimização de Sistemas de Chaves Quânticas com Variáveis Contínuas

Analysis and Optimization of Continuous Variables Quantum Cryptographic Systems

Universidade de Aveiro
2023

Daniel Filipe Figueiredo Pereira

Análise e Otimização de Sistemas de Chaves Quânticas com Variáveis Contínuas

Analysis and Optimization of Continuous Variables Quantum Cryptographic Systems

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Engenharia Eletrotécnica, realizada sob a orientação científica do Professor Doutor Armando Nolasco Pinto, Professor Associado com Agregação, do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, e e coorientação do Doutor Nuno Alexandre Peixoto Silva, Investigador no Instituto de Telecomunicações, Aveiro.

Este trabalho foi financiado pela Fundação para a Ciência e a Tecnologia (FCT) através de fundos nacionais e pela bolsa de doutoramento com a referência SFRH/BD/139867/2018 atribuída pela Fundação para a Ciência e a Tecnologia (FCT), pela União Europeia através do Fundo Europeu para o Desenvolvimento Regional (FEDER), através do Programa Operacional Competitividade e Internacionalização (COMPETE 2020), e projetos QuantumPrime (PTDC/EEI-TEL/8017/2020) e Quantagenomics (QuantERA/0001/2021).

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

universidade
de aveiro

instituto de
telecomunicações

o júri / the jury

presidente / president

Doutora Ana Isabel Couto Neto da Silva Miranda
Professora Catedrática, Universidade de Aveiro

vogais / examiners committee

Doutor Paulo Alexandre Carreira Mateus
Professor Catedrático, Instituto Superior Técnico de Lisboa

Doutor Armando Humberto Moreira Nolasco Pinto (Orientador)
Professor Associado com Agregação, Universidade de Aveiro

Doutora Maria do Carmo Raposo de Medeiros
Professora Associada, Universidade de Coimbra

Paulo Miguel Nepomuceno Pereira Monteiro
Professor Associado, Universidade de Aveiro

Doutora Catarina Bastos
Senior Engineer, Deimos Engenharia, Sa

agradecimentos

Quero agradecer aos meus orientadores, não só por me terem guiado ao longo deste trabalho de doutoramento, mas também pela sua ajuda incalculável ao longo dos 8 anos que passei a trabalhar no grupo de Comunicações Quânticas do Instituto de Telecomunicações de Aveiro.

Agradeço particularmente ao meu coorientador, o Doutor Nuno Silva, pela partilha de conhecimento, motivação e por ter tido uma capacidade quase sobre-humana de saber quando é que devia puxar por mim e quando é que me devia deixar matutar sobre os problemas com tempo.

Agradeço também à Universidade de Aveiro, por me acolher durante os últimos 10 anos, e ao Instituto de Telecomunicações, onde passei *apenas* 8, sem as condições de trabalho disponibilizadas por ambas as instituições, este trabalho nunca teria sido possível.

Tenho também de agradecer a imensos colegas e amigos: à Mariana Ramos, por me relembrar em tempo útil que estava na prática a trabalhar para mim próprio; ao Jorge Laranjeira, pela organização de várias e espetaculares tainadas; ao José Vítor, por me aturar nos meus momentos mais baixos; ao Marco Baptista e Filipe Pinheiro, por me ensinarem que é possível voar; e a tantos outros que tornaram os intermináveis dias e noites de trabalho um bocado menos penosos.

E um agradecimento infinito aos meus pais e à minha família pelo seu apoio incondicional ao longo de todo o meu percurso académico. Sem eles não só não teria conseguido chegar onde estou, como provavelmente não estaria a respirar neste momento.

And now, for something completely different.

palavras-chave

Distribuição de Chave Quântica com Variáveis Contínuas, Oscilador Local gerado Localmente, Diversidade na Polarização, Prova de Segurança, Modulação Discreta, Constelação Gerada Probabilisticamente, Dispositivos Imperfeitos

resumo

A teoria da informação quântica, aliada à tecnologia quântica, tem a capacidade de alterar fundamentalmente a sociedade moderna. A criptografia clássica será particularmente afetada, devido à sua segurança poder ser eficientemente quebrada por um computador quântico. A distribuição de chave quântica com variáveis contínuas (CV-QKD) apresenta uma solução a isto, permitindo estabelecer comunicações seguras entre intervenientes ao fornecer um canal que é capaz de detetar tentativas de interseção de informação, isto enquanto utiliza maioritariamente componentes actualmente usados em comunicações clássicas. Nos últimos anos, o ramo da criptografia quântica tem atraído uma quantidade crescente de investimento, com a chegada ao mercado dos primeiros sistemas comerciais. Contudo, o investigação na área ainda está muito ativo, com esforços a ser feitos para aumentar a performance, reduzir custos e fechar brechas de segurança. Nesta tese de doutoramento tentámos fazer exatamente isso. Nós começamos este trabalho por apresentar uma prova de segurança atualizada, aproximando o problema de uma forma prática e mostrando como os limites de segurança podem ser calculados numericamente. Propomos um sistema inovador utilizando um oscilador local gerado localmente para fazer deteção heteródina com diversidade na polarização com o auxílio de um sinal piloto. O nosso sistema proposto recupera de desvios de polarização exclusivamente pelo uso de processamento digital de sinal (DSP), uma escolha que torna a nossa solução experimentalmente simples e económica. Nós estabelecemos os limites de segurança do nosso sistema e testamos a sua resiliência, forçando um elevado desvio de polarização com um misturador de polarização eletrónico, com o sistema a ser capaz de funcionar nessas condições sem supervisão durante longos períodos de tempo e de gerar chaves seguras, no regime assimptótico. Também testamos o nosso sistema numa experiência de campo, a primeira de um sistema de CV-QKD em Portugal. De seguida procedemos a uma exploração de métodos para melhorar a performance do nosso sistema, começando por trocar a constelação de 1 nível de amplitude com 8 estados para uma de 128 estados com múltiplos níveis de amplitude. Assumindo os mesmos parâmetros de funcionamento, foi possível aumentar a performance do sistema por uma ordem de magnitude, quadruplicar a resistência a ruído em excesso, triplicar o número médio de fotões por símbolo e reduzir em 95% o número de amostras necessárias para funcionar o sistema em regime finito. Também explorámos métodos para melhorar a performance do sistema reduzindo o peso do DSP. Finalmente, estudámos o impacto que dispositivos imperfeitos têm na performance e segurança de sistemas de CV-QKD. Mostrámos que imperfeições nos dispositivos do transmissor podem causar com que o ritmo de chave seja reduzido em 100% e que imperfeições no recetor podem fazer com que o ritmo de chave seja sobrestimado por 44%. Os nossos resultados contribuem para o avanço do conhecimento na área dos sistemas distribuição de chave quântica ao melhorar a performance, reduzir os custos de implementação e explorar o impacto das imperfeições dos dispositivos realistas na prova de segurança teórica.

keywords

Continuous Variables Quantum Key Distribution, Locally generated Local Oscillator, Polarization Diverse, Security Proof, Discrete Modulated, Probabilistic Constellation Shaping, Device Imperfections

abstract

Quantum information theory, combined with quantum technologies, has the capacity to fundamentally alter modern society. Particularly affected will be public classic cryptography, whose security can be efficiently cracked by a quantum computer. Continuous Variables Quantum Key Distribution (CV-QKD) presents a solution to this, allowing for provably secure communications between differing parties to be established by providing a communication channel that is able to detect tampering attempts, all while using largely telecom-grade components. In the past couple of years, the field of quantum cryptography has attracted more and more investment, as systems have started to reach the market. However, research in the field is still very active, with efforts being made to both increase the system's performance, reduce costs and close security loopholes. In this PhD work we endeavoured to do just that. We begin this work by presenting an updated security proof, taking a practical approach on how the security limits may be computed numerically. We propose a novel pilot-aided, Locally generated Local Oscillator (LLO) system employing a polarization diverse heterodyne receiver. Our proposed system recovers from polarization drift exclusively through Digital Signal Processing (DSP), a choice which makes our solution experimentally simple and financially accessible. We establish the security of our proposed system and test its resilience in a high polarization drift scenario, forced by using an electronic State of Polarization (SOP) scrambler, with the system being capable of functioning under those conditions unattended for long periods of time and being capable of generating secure keys in the asymptotic regime. We also deploy our system in a field implementation, the first field trial of such a CV-QKD system in Portugal. We then proceed to explore methods for improving the performance of our previously proposed system, first by changing from the 8-PSK constellation used previously to a 128-Amplitude and Phase Shift Keying (APSK) one. Assuming the same functioning parameters, we are able to increase performance by an order of magnitude, almost quadruple the excess noise resistance, more than triple the number of photons per symbol that can be used and reduce the number of samples necessary for functioning in the finite-size regime by 95%. We also explore methods for improving system performance by reducing the weight of the DSP. Finally, we study the impact of device imperfections on the performance and security of CV-QKD. We show that transmitter device imperfections can cause the secure key rate to be underestimated by up to 100% and that receiver device imperfections may cause secure key rate may be overestimated by 44%. Our results contribute to the advance of knowledge in the field of CV-QKD by both improving performance, reducing costs of implementation and exploring the impact of real-word device imperfections on the theoretically derived security.

Contents

List of Figures

Acronyms

ADC Analog to Digital Converter.

AES Advanced Encryption Standard.

AM Amplitude Modulator.

AOM Acousto-Optic Modulator.

APSK Amplitude and Phase Shift Keying.

BER Bit Error Rate.

BS Beam Splitter.

CMA Constant Modulus Algorithm.

CV-QKD Continuous Variables Quantum Key Distribution.

DAC Digital to Analog Converter.

DM Discrete Modulation.

DSP Digital Signal Processing.

DV-QKD Discrete Variables Quantum Key Distribution.

E-B Entanglement-Based.

EVM Error Vector Magnitude.

FDM Frequency Division Multiplexing.

FER Finite Extinction Ratio.

FPGA Field-Programmable Gate Array.

FSE Finite Size Effects.

GM Gaussian Modulation.

GPU Graphics Processing Unit.

IQ In-phase and Quadrature.

LDPC Low Density Parity Check.

LLO Locally generated Local Oscillator.

LO Local Oscillator.

OTP One Time Pad.

P&M Prepare and Measure.

PCS Probabilistic Constellation Shaping.

PM Phase Modulator.

PRNG Pseudo Random Number Generator.

PSK Phase Shift Keying.

QAM Quadrature Amplitude Modulation.

QC Quantum Cryptography.

QKD Quantum Key Distribution.

QPSK Quadrature Phase Shift Keying.

QRNG Quantum Random Number Generator.

RIN Random Intensity Noise.

RRC Root Raised Cosine.

RSA Rivest–Shamir–Adleman.

SMF Single Mode Fibre.

SNR Signal to Noise Ratio.

SNU Shot Noise Units.

SOP State of Polarization.

SPD Single Photon Detectors.

TDM Time Division Multiplexing.

TIA Trans-Impedance Amplifier.

TLS Tuneable Laser Source.

TTL Transistor-Transistor Logic.

VOA Variable Optical Attenuator.

Chapter 1

Introduction

In this chapter we present an introduction to this PhD thesis. We contextualize the work presented, presenting a motivation for it and summarizing the state of the art of the research topic. This is followed by a delineation of the objectives of this thesis, the main contributions arising from it and its structure.

We start with the motivation for the work in Section 1.1. The current state of the art is presented in Section 1.2. Then we establish the main goals to be tackled in this project in Section 1.3. The main contributions arising from this work are then summarized in Section 1.4, followed by a list of publications that arose from it in Section 1.5 Finally, this chapter concludes with an outline of this document in Section 1.6.

1.1 Motivation

In the modern world, sensitive information is increasingly shared through channels whose security and privacy cannot be expected *a priori*. Cryptography aims to provide methods through which secure communications may be achieved through these untrusted channels [1]. This can be accomplished by encoding the message to be transmitted in such a way that it is unintelligible to anyone except for the legitimate receiver. There already exists one method of encryption that has been proven to be unconditionally secure, called One Time Pad (OTP), also know as Vernam Cypher [2]. In this technique a random key with the same length as the message is employed to encode the message and the same key is used to decode it, this is presented in visual form in Figure 1.1 (adapted from [3]). In these figures each pixel is treated as a bit, taking the value of 1 if the pixel is black and 0 if the pixel is white. The message is summed pixel by pixel with the key following a modulo-2 addition in the form:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0. \tag{1.1}$$

For the decoding process, the cyphertext is again summed pixel by pixel with the key, following the same modulo-2 addition. If the key is random then the ciphertext is also random, thus, as long as the key is kept secret and is never reused in whole or in part (multiple cyphertexts generated with the same key can be added to recover some information, as is visualized in Figure 1.2), it is impossible to break. The amount of information exchanged via digital means increases rapidly year after year. This ever increasing volume of information, coupled with the need to update the random key for every message makes this protocol impractical. As a

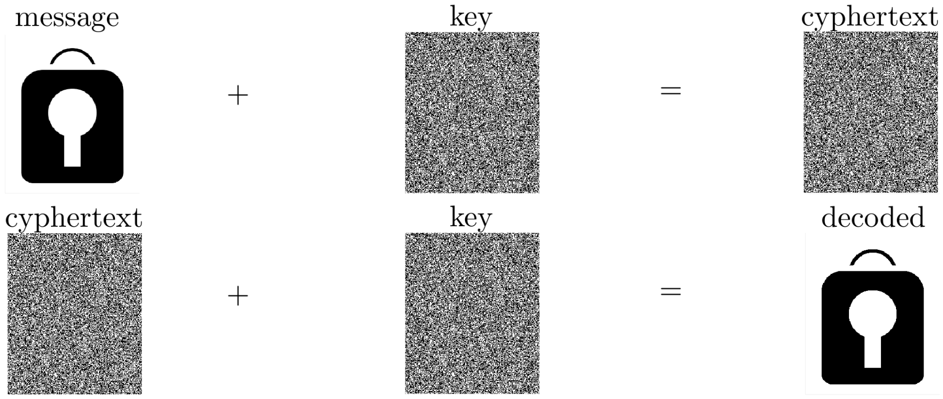


Figure 1.1: Visualization of message encoding and decoding using OTP [3].

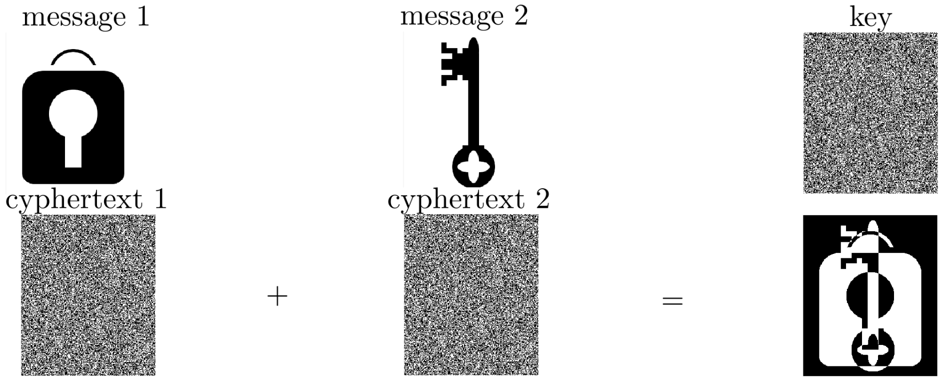


Figure 1.2: Multiple uses of the same key compromise the security of the protocol [3].

result, OTP methods have not seen widespread adoption, with public-key cryptography being currently the most widely used methods for over the internet secure communications.

In public-key cryptographic protocols, which include the Rivest–Shamir–Adleman (RSA) and ELGammal protocols [4, 5], the user generates a pair of cryptographic keys, one which is divulged publicly and another which is kept private to the user. A message encrypted with the public key can only be efficiently decrypted with the corresponding private key. Moreover, even current classical implementations of symmetric encryption protocols, such as the Advanced Encryption Standard (AES), perform a step similar to the RSA protocol to share the initial key [6]. These methods base their security on the high computational complexity of factoring the product of two large primes. Although the factorization of large numbers with classical, brute-force, computation methods would require billions of years [7], the same cannot be said about quantum computation techniques. By using a quantum computer, Shor's algorithm is capable of performing prime-factorization in polynomial time, instead of exponential time using classical computation techniques [8, 9]. This means that a quantum computer is capable of breaking the security of prime number based, public key cryptographic protocols, such as the RSA [7]. Due to the AES performing an RSA-like step during inital key sharing, even it is vulnerable to the capabilities of quantum computers [10]. Shor's algorithm is also capable of solving the elliptic curve discrete logarithm problem, thus also being able to crack the security of elliptic curve cryptography [11]. Coupled with the fact that practical quantum computing is coming ever closer to reality [12], this means that classical cryptographic protocols used today are unsatisfactory in the long run. Moreover, classical cryptographic techniques are also vulnerable to *intercept now decrypt later attacks*, in which an eavesdropper can copy and store all the information and later attempt to break the keys.

Post-quantum classical cryptography schemes have been proposed, deriving their security from hard computational problems which are not yet known to have been broken by either a classical or a quantum computer. Some basis for post-quantum cryptography include, but are not limited to [13]:

- Hash-based, of which SPHINCS+ is an example, being a finalist of the 3rd round of the NIST Post-Quantum Cryptography standardization project;
- Supersingular elliptic curve isogeny based, such as the Supersingular Isogeny Diffie–Hellman (SIDH) protocol, another finalist from the 3rd round of the NIST Post-Quantum Cryptography standardization project;
- Multivariate-based, such as the Rainbow cryptographic protocol, also finalist of the 3rd round of the NIST Post-Quantum Cryptography standardization project;
- Code-based, of which the Classic McEliece is an example, being one of the current participants in the 4th round of the NIST Post-Quantum Cryptography standardization project.

However, these methods are not proven to be unconditionally secure, which means that the security of data transmitted or stored using these techniques, which includes medical and genetic data, banking information, e-commerce transactions and personal government data, is not assured, posing both a privacy and economic threat. In fact, recently there have been reported attacks on the SIDH [14], Rainbow [15] and Classic McEliece [16] post-quantum cryptographic protocols.

Quantum Cryptography (QC) derives its security not from any assumption of limited computational power available to an adversary, but from physical limits imposed on the information that can be extracted from the information carrying signal [1]. This means that QC is not susceptible to future computational developments or cracking attempts, thus providing unconditional security for the data protected by it. Quantum Key Distribution (QKD) was first proposed in 1984 by Bennet and Brassard, using the polarization of single photons as a coding basis to send a random bit string to be used as cryptographic key in a symmetric encryption system [17], such as the OTP discussed previously. The security of this protocol is assured by the non-commutation of the two employed polarization basis and the no-cloning theorem, with the combination of these two factors meaning that an eavesdropper, assuming the availability of an authenticated channel and provided that the eavesdropper doesn't break the laws of physics, cannot intercept the key being shared without revealing their presence. Multiple QKD protocols have been proposed since, using anything from the polarization of single-photons to phase and amplitude encoding of coherent states, similar to the encoding that is used in current classical optical communication networks, the latter consisting of Continuous Variables Quantum Key Distribution (CV-QKD) protocols. The advantage of CV-QKD is the ability to take advantage of highly mature technology from optical communications to drive down the costs of implementation.

1.2 State of the Art

The expected near-future emergence of a practical quantum computer [12] is a threat to classical cryptography, with prime number based classical cryptography being particularly affected [7, 10, 11]. IBM has recently announced to have built a 433-qubit quantum computer, dubbed Osprey, the largest to date [18], and are on track to introduce the first 1000+-qubit processor in 2023 [19].

In that scenario, QC appears as a solution, enabling the secure generation and transmission of symmetric cryptographic keys without assuming any limitations on the computational power of possible adversaries [20].

1.2.1 Quantum Cryptography

In the 1970s Stephen Wiesner suggested a method to make money unforgeable by using properties of Quantum Mechanics [21]. This pioneer work gave rise to the field of Quantum Information which is continuously expanding, much aided by the now very prolific field of QC, in which QKD inserts itself. First proposed in 1984 by Charles Bennet and Gilles Brassard in their seminal paper [17], QKD allows for the random key necessary to implement any symmetric key cryptographic protocol to be generated and transmitted between two parties through an unsecure channel while allowing for possible tampering to be detected, relying on the inability to measure a quantum system without fundamentally altering it for this detection [17]. Bennet and Brassard's proposed protocol, usually referred to as BB84, had the sender, usually dubbed Alice, prepare polarized single photon states, encoding the classical bits 0 and 1 into orthogonal quantum states in two different non-orthogonal bases. After encoding, Alice then sends these states to Bob through a quantum channel, which we assume to be controlled by an untrusted eavesdropper, usually dubbed Eve. Due to the no-cloning theorem, in order for Eve to gain information on the transmitted bits, she will have to measured the single photon states prepared by Alice, and, because of the use of non-orthogonal polarization bases, she will not be able to obtain all the information encoded. At the output of the quantum channel, the receiver, usually called Bob, measures the single photon states using a randomly chosen basis, obtaining a random classical variable. After measurement, Bob reveals publicly which basis he used in his measurements, with him and Alice discarding the states in which they used different basis for encoding and measurement. After this step, Alice and Bob should be in possession of the same shared secret key, with any errors in the key being attributed to the action of Eve. Due to the nature of the preparation of the single photon states in the BB84 protocol, it consists of a Prepare and Measure (P&M) scheme. An Entanglement-Based (E-B) version of this protocol was proposed later in [22], with the single photon states, with this approach being explored due to it providing source-independent security [23]. A multitude of other single-photon based protocols, being dubbed a Discrete Variables Quantum Key Distribution (DV-QKD) system [17], have also been proposed, using different encoding methods for the transmitted key [24].

However, in using single-photon based approaches, these DV-QKD protocols pose some difficulties in their practical implementation, namely the specialized equipment needed for single photon generation and detection [25]. One vulnerability of DV-QKD protocols is the photon-splitting attack, which consists in exploiting situations in which more than one photon is outputted by Alice, with Eve being able to perform a quantum non-demolition measurement to determine the number of photons present and then stealing one of the excess photons while allowing the others to proceed to Bob [26]. This attack arises precisely due to the general non-availability of ideal single photon sources, which results in probabilistic sources, usually highly attenuated lasers, being used [27]. This problem was circumvented by the introduction of *decoy state* methods, in which Alice randomly chooses the intensity levels to be sent, corresponding to her actively injecting multiple photon states into the channel (the so called decoy states) alongside her single photon, signal states. After the transmission Alice announces which intensity level she used for each transmitted state, she and Bob then proceed to compute the Bit Error Rate (BER) associated with each intensity level separately. In this manner, Alice and Bob are capable of detecting Eve's tampering on the multiple photon states, thus disabling her photon-splitting attack. Furthermore, the usage of Single Photon Detectors (SPD) limits the achievable performance of DV-QKD, because, in order to reduce the occurrence of dark counts, SPD require either functioning at very low temperatures or at slow gating rates [27]. To ameliorate this, efforts have been made recently to perform DV-QKD using balanced coherent detectors, similar to the ones used in classical communications [28].

As an alternative, Continuous Variables Quantum Key Distribution (CV-QKD) protocols were proposed, which encoded the key not on single photon polarization but on the quadratures of quantum states [25] and derive their security through a fundamentally different method [29].

1.2.2 Continuous Variables Quantum Key Distribution

The first proposed CV-QKD methods employed so-called squeezed states, which encoded the key on the uncertainty of each quadrature [25, 30, 31]. These techniques can be seen as continuous variables extension of the BB84 protocol, deriving their security in much the same way [32], while allowing the use of a detection scheme similar to that used in classical communications. However, the use of squeezed states still demands complex, non standard encoding methods [30], for example through parametric down-conversion [33]. Thus, a further development of CV-QKD was the switch to a coherent-state based approach, encoding the information in the phase and amplitude of weak coherent-states, this allows for implementation with current modulation methods and telecom-grade equipment [34]. These modulation methods can be, for example, an Amplitude Modulator (AM) and Phase Modulator (PM) pair [35] or a single In-phase and Quadrature (IQ) modulator [36]. The first protocols of this type to be proposed used Gaussian Modulation (GM), where the values encoded on the shared coherent states being chosen from a continuous bi-variate Gaussian distribution [34]. These GM CV-QKD protocols maximize the transmitted information [37], however they put a high burden on the transmitter's random source [38] and tend to be more susceptible to imperfect state preparation [39]. As a result, Discrete Modulation (DM) approaches have been proposed [29]. Although these do not maximize the transmitted information, they are much easier to implement [40].

At the receiver, detection can theoretically be performed using any classical detection scheme [41]. Coherent detection is the most common employed detection method, which, depending on the relation between the frequencies of the signal and Local Oscillator (LO) used as reference. When the frequencies of the signal and LO are equal or only slightly different (frequency difference is smaller than the signal's bandwidth), the coherent detection is dubbed homodyne or intradyne, respectively [42]. A variation of these two methods exists in which, prior to detection, the signal is split in two and coherent detection applied to each half individually, with the LO used for the coherent detection of one of the halves being phase-shifted by $\frac{\pi}{2}$, thus recovering both quadratures of the incoming signal [42]. Another alternative is heterodyne detection, in which the signal and LO have greatly different optical frequencies (i.e. the frequency difference is larger than the signal's bandwidth) [42]. Heterodyne detection allows for the recovery of both quadratures of the incoming signal without having to split it beforehand, by essentially having the LO alternate which quadrature it is measuring multiple times for each received symbol. Note that, in the CV-QKD community, any system that allows for simultaneous measurement of both quadratures is usually dubbed heterodyne, while for the telecommunications community at large heterodyne detection refers to detection systems where the frequencies of the signal and LO are different [42]. In order to distinguish between these two, we refer in this work to telecommunication community's definition of heterodyne detection as true heterodyne.

The first CV protocols required a high intensity pulse to be sent, polarization multiplexed, alongside the quantum pulses, to be used as the LO in the detection scheme [34]. Due to the signal and LO being extracted from the same source, the two will have the same optical frequency, meaning that theses methods used either homodyne or double-homodyne detection. This transmitted LO scheme both limited the effective distance achievable by the protocol, because the LO would be subject to the same attenuation as the signal, and posed a security risk, because an eavesdropper could manipulate the LO, thus hiding their tampering on the quantum signal itself [43], proposed attacks included manipulating the wavelength [44–46] and the shape of the LO pulses [47]. In [35, 43, 48] Locally generated Local Oscillator (LLO) methods were proposed, where the LO is extracted from a source local to the receiver, with reference pulses sent time multiplexed to allow for phase and frequency recovery. In [49] an alternative LLO technique was presented in which the reference pulses are sent frequency and polarization multiplexed. Furthermore, the use of machine learning to aid in the recovery from phase and frequency noise has been explored [50]. Low-frequency noise is a major impairment on the performance of CV-QKD systems, to avoid low-frequency noise methods which insert the quantum signal at an intermediate frequency were proposed [36]. Random polarization drift occurs naturally in fibres subjected to vibrations, temperature fluctuations, among others [51]. Misalignments between the polarizations of the two laser fields interfering in the coherent detection scheme will severely reduce the efficiency of the detection scheme employed [36, 52]. In CV-QKD communication systems, polarization drift is typically avoided, during a limited time window, by manually aligning the polarization of the signal with that of the LO [36, 49]. This may be appropriate in a laboratory environment, where stability times are typically in the range of hours [52]. However, in field deployed fibres, especially aerially deployed ones, this stability will be on the order of minutes [51]. A CV-QKD system using an electronic polarization controller coupled with a dynamic feedback system was proposed in [52], using a transmitted LO design. However, this solution increases cost and introduces experimental complexity. Conversely, in classical communications, random polarization drift is compensated for by detecting both polarizations of the incoming light field and then compensating for the time-evolving drift in Digital Signal Processing (DSP) [53]. A system employing DSP aided polarization mismatch recovery was presented in [54], using two optical hybrids coupled with four balanced coherent receivers. After Bob performs his measurements and applies his DSP stage, he and Alice can be seen as sharing a correlated, but not equal, raw key [29]. In order for them to share a symmetric key, they have to perform some classical post-processing, which can entail sifting (reconciling the measurement bases, as is done in DV-QKD, this is not required for every CV-QKD protocol), error correction and privacy amplification [55]. This classical post-processing is performed through a publicly accessible albeit authenticated channel.

The security of these Coherent State based CV-QKD protocols is evaluated with recourse to the mutual informations observed in the system [34]. For some time it was thought that CV-QKD would not be able to ensure secure communications through channels with transmission below 50% [34], because in that scenario Eve will always have access to more of the signal than Bob can recover. Experimentally, this could be achieved through a beam splitting attack, where Eve would substitute the lossy channel with a lossless one and a beam-splitter with a transmission coefficient equal to that of the lossy channel. This limitation was beaten by the implementation of reverse-reconciliation [41], i.e., in the key reconciliation stage, it is not Bob that corrects his key to match Alice's, but rather Alice who changes her key to include Bob's errors. In [29] an unconditional proof of security for both Gaussian and 2- and 4-state DM CV-QKD was presented, with the security being dependent on the channel transmission and noise. This proof of security was expanded to an 8-state protocol in [56] and further into arbitrary constellations in [57].

The security proofs mentioned above assume that Eve performs a collective attack [29]. In a collective attack, Eve generates a set of separable probe states, usually dubbed ancilla states, and interacts them individually with the quantum states being shared between Alice and Bob, afterwards storing them in a quantum memory. Eve will then perform an optimal collective measurement on all her ancilla states after Alice and Bob have performed their public post-processing steps [55]. An alternative to collective attacks are individual ones, in which Eve proceeds in the same way as in the collective attack scenario but does not, or cannot, postpone the measurement of her ancilla states until after Alice and Bob perform their post-processing [55]. Further, the most general class of attacks is the coherent one, in which Eve is not assumed to interact with each quantum state being shared between Alice and Bob individually, but rather generates a single, global ancilla state that she interacts with all signal pulses and then stores in her quantum memory, for measurement after Alice and Bob perform their classical post-processing [55]. Collective attacks give more advantage to Eve than individual ones and, in the asymptotic regime, i.e. the situation in which an infinitely large number of states are used by Alice and Bob to estimate the channel parameters, are equivalent to coherent ones, which in turn are the strongest possible attack [55]. In actuality, no real world implementation can use an infinite amount of states, so the the fact that the channel parameters are not known perfectly but are rather estimated needs to be taken into account, a finite size analysis that does this is presented in [58]. This includes both the uncertainties of the estimated parameters as well as the fact that the states used in this estimation, since they are revealed publicly, cannot be included in the final key [58]. In these security proofs, the optical system itself is assumed to be balanced [29, 55–57]. A study on the security impact of imperfect state preparation on GM CV-QKD has been performed [39], which shows that an incorrect calibration of the modulators causes the channels parameters to be significantly misestimated.

Experimental implementations of DM CV-QKD started by using Phase Shift Keying (PSK) constellations, 2-PSK and 4-PSK at first [49], this was followed quickly by the adoption of 8-PSK [36], since increasing the constellation size brings the performance of DM implementations closer to that of GM ones. However, further increasing the PSK constellation does not produce an appreciable improvement [57]. As a consequence, the use of M-symbol Quadrature Amplitude Modulation (QAM) constellations coupled with Probabilistic Constellation Shaping (PCS) has been explored, with the performance of these constellations approaching that of GM systems [59].

1.3 Thesis Objectives and Outline

The main goal of this work is to develop, study and implement a novel CV-QKD system to be used in secure communications. We prioritize the use of telecom-grade equipment at every step of this process, in order to assemble an accessible and robust quantum system that can easily be deployed. To accomplish this the following specific goals were defined:

1. Propose and analyze a novel CV-QKD system capable of generating symmetric keys through an optical fibre connection, including an updated security proof;

2. Implement the CV-QKD system in a laboratory environment, dealing with both the physical layer and post-processing steps required, developing both in such a way that the system may be used for field experiments;

3. Improve the performance of the developed system and study the impact of realistic, imperfect devices on the security of the CV-QKD systems.

1.4 Main Contributions

In the opinion of the author, the main achievements of this PhD are:

- The development and implementation of a fully-functioning polarization diverse DM-CV-QKD system capable of functioning unaided for extended periods of time and is agnostic in relation to the employed modulation format. The system encodes information in the phase and amplitude of weak coherent states extracted from a Tuneable Laser Source (TLS) using an IQ Modulator followed by a Variable Optical Attenuator (VOA), all components being telecom-grade. The polarization diverse receiver works by splitting the two incoming polarizations and performing heterodyne dectetion independently on both.

- The expansion of the security proof of CV-QKD to our proposed polarization-diverse system. We show that, when using our polarization diverse receiver, it is possible to achieve the performance of a channel with zero polarization drift.

- The successful deployment of the first field implementation of a CV-QKD system in Portugal.

- Assessment of the impact of device imperfections on the security and performance of CV-QKD systems. We show that, due to the erroneously estimated channel parameters, non-monitored imbalances can greatly reduce the system's performance and even pose a security risk.

1.5 List of Publications

The following publications have been released/submitted in the context of this PhD work:

Journals

- **Pereira, Daniel**, Margarida Almeida, Armando N. Pinto, and Nuno A. Silva. "Impact of Transmitter Imbalances on the Security of Continuous Variables Quantum Key Distribution." EPJ Quantum Technology 10, no. 1 (2023): 1-13;

- **Pereira, Daniel**, Armando N. Pinto, and Nuno A. Silva. "Polarization diverse true heterodyne receiver architecture for continuous variable quantum key distribution." Journal of Lightwave Technology 41, no. 2 (2022): 432-439;

- **Pereira, Daniel**, Margarida Almeida, Margarida Facão, Armando N. Pinto, and Nuno A. Silva. "Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres." Optics Letters 47, no. 15 (2022): 3948-3951;

- Almeida, Margarida, **Daniel Pereira**, Nelson J. Muga, Margarida Facão, Armando N. Pinto, and Nuno A. Silva. "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution." Optics Express 29, no. 23 (2021): 38669-38682;

- **Pereira, Daniel**, Margarida Almeida, Margarida Facão, Armando N. Pinto, and Nuno A. Silva. "Impact of receiver imbalances on the security of continuous variables quantum key distribution." EPJ Quantum Technology 8, no. 1 (2021): 1-12;

- Almeida, Margarida, **Daniel Pereira**, Margarida Facão, Armando N. Pinto, and Nuno A. Silva. "Impact of imperfect homodyne detection on measurements of vacuum states shot noise." Optical and Quantum Electronics 52, no. 11 (2020): 1-13.

Conferences

- **Pereira, Daniel**, Nuno A. Silva, Margarida Almeida, and Armando N. Pinto. "Optimization of continuous variables quantum key distribution using discrete modulation.", in SPIE Security+Defense, September 2022;

- Almeida, Margarida, **Daniel Pereira**, Nelson J. Muga, Margarida Facão, Armando N. Pinto, and Nuno A. Silva. "CV-QKD Security Limits Using Higher-Order Probabilistic Shaped Regular M-APSK Constellations.", in SBRC Workshop de Comunicação e Computação Quântica (WQuantum), May 2022;

- **Pereira, Daniel**, Armando N. Pinto, and Nuno A. Silva. "Impact of Shot Noise Estimation on the Secret Key Rate of a CV-QKD System.", in SBRC Workshop de Comunicação e Computação Quântica (WQuantum), May 2022;

- **Pereira, Daniel**, Nuno Silva and Armando Pinto, "A polarization diversity CV-QKD detection scheme for channels with strong polarization drift.", in IEEE International Conference on Quantum Computing and Engineering (QCE), October 2021;

- Ferreira, Maurício, **Daniel Pereira**, Nelson Muga, Nuno Silva and Armando Pinto, "Time-interleaved quantum random number generation within a coherent classical communication channel", in SBRC Workshop de Comunicação e Computação Quântica (WQuantum), August 2021;

- Silva, Nuno A., **Daniel Pereira**, Nelson Muga and Armando Pinto, ”Practical Imperfections Affecting the Performance of CV-QKD Based on Coherent Detection”, in International Conf. on Transparent Optical Networks (ICTON), July 2020;

- Silva, Nuno A., Margarida Almeida, **Daniel Pereira**, Margarida Facão, Nelson Muga and Armando Pinto, ”Role of Device Imperfections on the Practical Performance of Continuous-Variable Quantum Key Distribution Systems”, presented at International Conf. on Transparent Optical Networks (ICTON), July 2019.

1.6 Outline

This thesis is organized into 6 chapters, with the first being the current introduction and the content of the following being:

- Chapter 2 contains a detailed introduction to the topic of CV-QKD. A theoretical study of a generic system is presented, followed by a corresponding security proof for DM-CV-QKD, based on the one published in [57]. The impact of imperfect estimation of experimental parameters is studied, in an in depth Finite Size Effects (FSE) study.

- Chapter 3 presents results pertaining to the implementation of the polarization diverse CV-QKD system described previously in Chapter 2. A numerical study of the system described in Chapter 2 is presented, with results from the numerical simulation of the system presented alongside for use in an in-depth description of the Digital Signal Processing (DSP) routine employed. The proposed experimental system is then described in detail, with all hardware and software methods being specified. The presented system utilizes a frequency multiplexed pilot tone to aid in frequency and phase recovery and measures each incoming polarization individually, which are then combined in a Constant Modulus Algorithm (CMA) step to recover the original input signal. We expand the security proof presented previously in Chapter 2 to include our novel proposed polarization diverse CV-QKD system. We also demonstrate that our system, that prioritizes the use of telecom-grade components whenever possible, can withstand very high polarization noise scenarios, where a single polarization receiver system could not function. We finish by presenting results from our field trial in Lisbon.

- In Chapter 4 we explore methods for improving the resilience and performance of CV-QKD systems through the usage of complex constellations formats. Two different M-APSK constellations are implemented experimentally and their performance is compared to that of the 8-PSK constellation used previously in Chapter 3. Methods for improving the performance of the CV-QKD system by reducing the weight of the DSP stage, using an auxiliary 4-PSK channel, are also explored.

- Chapter 5 considers the impact of device imperfections and imbalances on the security and performance of the CV-QKD system presented in Chapter 2. The imperfect components considered are imbalanced beam-splitters (deviating from the ideal 50/50 splitting scenario), unequal quantum efficiencies of the photodiodes, incorrectly set bias voltages on the modulators and incorrectly driven modulators. The ideal constellation format under imperfect modulation scenario is also explored.

- Chapter 6 summarizes the main results obtained in this thesis and presents suggestions for future work.

Bibliography

[1] Alexander V Sergienko. *Quantum communications and cryptography.* CRC press, 2005.

[2] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Tech. J.*, 1949.

[3] Encrypting with xor: a graphic example. `https://cryptosmith.com/2007/06/09/xor/`. [Last access: 10/11/2022].

[4] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[5] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[6] Jim Schaad and Russell Housley. Advanced encryption standard (aes) key wrap algorithm. 2002.

[7] Martin Roetteler and Krysta M. Svore. Quantum computing: Codebreaking and beyond. *IEEE Security & Privacy*, 16(5):22–36, 2018.

[8] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *CoRR*, abs/1804.00200, 2018.

[9] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[10] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. Implementing grover oracles for quantum key search on aes and lowmc. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 280–310, Cham, 2020. Springer International Publishing.

[11] Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken. Improved quantum circuits for elliptic curve discrete logarithms. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 425–444, Cham, 2020. Springer International Publishing.

[12] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[13] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[14] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. `https://eprint.iacr.org/2022/975`.

[15] Ward Beullens. Breaking rainbow takes a weekend on a laptop. Cryptology ePrint Archive, Paper 2022/214, 2022. https://eprint.iacr.org/2022/214.

[16] Qian Guo, Andreas Johansson, and Thomas Johansson. A key-recovery side-channel attack on classic mceliece. *Cryptology ePrint Archive*, 2022.

[17] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems and Signal Processing*, 1984.

[18] Ibm unveils world's largest quantum computer at 433 qubits. https://www.newscientist.com/article/2346074-ibm-unveils-worlds-largest-quantum-computer-at-433-qubits/. [Last access: 10/11/2022].

[19] Our new 2022 development roadmap. https://www.ibm.com/quantum/roadmap. [Last access: 10/11/2022].

[20] Alexander V Sergienko. *Quantum communications and cryptography.* CRC press, 2018.

[21] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[22] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell's theorem. *Physical review letters*, 68(5):557, 1992.

[23] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Physical review letters*, 90(5):057902, 2003.

[24] Ali Ibnun Nurhadi and Nana Rachmana Syambas. Quantum key distribution (qkd) protocols: A survey. In *2018 4th International Conference on Wireless and Telematics (ICWT)*, pages 1–5. IEEE, 2018.

[25] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999.

[26] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.

[27] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236, 2020.

[28] Mariana F Ramos, Armando N Pinto, and Nuno A Silva. Polarization based discrete variables quantum key distribution via conjugated homodyne detection. *Scientific Reports*, 12(1):1–13, 2022.

[29] Anthony Leverrier. *Theoretical study of continuous-variable quantum key distribution.* PhD thesis, Télécom ParisTech, 2009.

[30] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2):022309, 2000.

[31] Margaret D Reid. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Physical Review A*, 62(6):062308, 2000.

[32] Nicolas J Cerf, Marc Levy, and Gilles Van Assche. Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63(5):052311, 2001.

[33] Ling-An Wu, HJ Kimble, JL Hall, and Huifa Wu. Generation of squeezed states by parametric down conversion. *Physical review letters*, 57(20):2520, 1986.

[34] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, 2002.

[35] Daniel BS Soh, Constantin Brif, Patrick J Coles, Norbert Lütkenhaus, Ryan M Camacho, Junji Urayama, and Mohan Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, 5(4):041010, 2015.

[36] Sebastian Kleis, Max Rueckmann, and Christian G Schaeffer. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics letters*, 42(8):1588–1591, 2017.

[37] Claude E Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[38] Eneet Kaur, Saikat Guha, and Mark M Wilde. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A*, 103(1):012412, 2021.

[39] Wenyuan Liu, Xuyang Wang, Ning Wang, Shanna Du, and Yongmin Li. Imperfect state preparation in continuous-variable quantum key distribution. *Physical Review A*, 96(4):042312, 2017.

[40] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[41] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv preprint quant-ph/0204127*, 2002.

[42] Hans Brunner, Lucian Comandar, Fotini Karinou, Stefano Bettelli, David Hillerkuss, Fred Fung, Dawei Wang, Spiros Mikroulis, Yi Qian, Maxim Kuschnerov, Andreas Poppe, Changsong Xie, and Momtchil Peev. A low-complexity heterodyne cv-qkd architecture. pages 1–4, 07 2017.

[43] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, 5(4):041009, 2015.

[44] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Physical Review A*, 87(5):052309, 2013.

[45] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Physical Review A*, 87(6):062329, 2013.

[46] Jing-Zheng Huang, Sébastien Kunz-Jacques, Paul Jouguet, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking on quantum key distribution using homodyne detection. *Physical Review A*, 89(3):032304, 2014.

[47] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Physical Review A*, 87(6):062313, 2013.

[48] Adrien Marie and Romain Alléaume. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, 95(1):012316, 2017.

[49] Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher, Michael Hentschel, Chi-Hang Fred Fung, Fotini Karinou, Andreas Poppe, Momtchil Peev, and Hannes Hübel. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*, 3:193, 2019.

[50] Sebastian Kleis, Max Rueckmann, and Christian G Schaeffer. Continuous-variable quantum key distribution with a real local oscillator and without auxiliary signals. *arXiv preprint arXiv:1908.03625*, 2019.

[51] Rende Liu, Hao Yu, Jiye Zan, Song Gao, Liwei Wang, Mulan Xu, Jun Tao, Jianhong Liu, Qing Chen, and Yong Zhao. Analysis of polarization fluctuation in long-distance aerial fiber for qkd system design. *Optical Fiber Technology*, 48:28–33, 2019.

[52] Wenyuan Liu, Yanxia Cao, Xuyang Wang, and Yongmin Li. Continuous-variable quantum key distribution under strong channel polarization disturbance. *Physical Review A*, 102(3):032625, 2020.

[53] Md Saifuddin Faruk and Seb J Savory. Digital signal processing for coherent transceivers employing multilevel formats. *Journal of Lightwave Technology*, 35(5):1125–1141, 2017.

[54] Tao Wang, Peng Huang, Shiyu Wang, and Guihua Zeng. Polarization-state tracking based on kalman filter in continuous-variable quantum key distribution. *Opt. Express*, 27(19):26689–26700, Sep 2019.

[55] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[56] A Becir, FAA El-Orany, and MRB Wahiddin. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10(01):1250004, 2012.

[57] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 2021.

[58] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

[59] François Roumestan, Amirhossein Ghazisaeidi, Jérémie Renaudier, Luis Trigo Vidarte, Eleni Diamanti, and Philippe Grangier. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In *2021 European Conference on Optical Communication (ECOC)*, pages 1–4. IEEE, 2021.

Chapter 2

Continuous Variables Quantum Key Distribution Systems

In this Chapter a detailed study on Continuous Variables Quantum Key Distribution (CV-QKD) is presented. The content of this Chapter will serve as the theoretical backing underlining the topics tackled in this thesis.

In Section 2.1 the basic principles of Quantum Key Distribution (QKD) are presented, followed by a further description of CV-QKD proper in Section 2.2. The proposed system is described in Section 2.2.1. The security proof for the described system is presented in Section 2.3, followed by an study on how the channel parameters can be estimated and how estimation uncertainties impact the performance of the proposed system in Section 2.3.1.

2.1 Quantum Key Distribution

The objective of QKD is to distribute a secret random key between the two honest parties while detecting the presence of possible eavesdroppers by their effect on the system. Physical systems described by quantum models are capable of doing this due to the following two properties:

- Heisenberg's uncertainty principle, which expresses the impossibility of measuring two complementary physical properties with arbitrary precision [1];
- The no-cloning theorem, that states that it is impossible to create a perfect copy of an arbitrary unknown quantum state [2].

Both of these properties provide the theoretical backing for the security of QKD.

Two communication channels are employed, one dubbed the quantum channel, through which the random key will be communicated, and the other consisting of am authenticated classical channel, allowing for key reconciliation. After the symmetric key is recovered and its security is established, secure communications are established over the classical channel with recourse to a symmetric encryption protocol, such as the One Time Pad (OTP) or the Advanced Encryption Standard (AES) protocols. Eve is assumed to have access to both channels, being limited by the quantum properties of the objects shared through the quantum channel and by the authentication scheme in the classical channel, which allows Alice and Bob to be assured their communications through this latter channel are not being altered.

A typical QKD protocol is composed of the following steps:

1. Alice sends N quantum states to Bob through the quantum channel, who measures every state as it arrives to his system;

2. Alice and Bob then choose a random subset of m states and share their results through the authenticated public channel. These results are used to evaluate the correlation between their quantum subsystems and decide whether or not to proceed with the protocol, if the transmission is found to have been insecure, the protocol restarts from step 1;

3. If the transmission is deemed secure, Alice and Bob then use the $n = N - m$ states to obtain a pair of *raw keys*, A^n and B^n, usually these are only partially correlated and necessitate further distillation;

4. By communicating through the authenticated public channel, Alice and Bob reconcile A^n and B^n through the application of some error correction algorithm until they reach a common bit string U^n;

5. Alice and Bob now turn U^n into a shorter, secure key S^l, where $l < n$, this step is called *privacy amplification*. This is done to erase any information a possible eavesdropper might have accrued during the previous steps;

6. Finally, Alice and Bob use the resulting key to feed into the symmetric encryption protocol (for example a One Time Pad (OTP) method) and communications can proceed.

At step 2 of the protocol, Alice and Bob share information about a random bit string and at that step attempt to discover if Eve has intercepted information. The decision is made by evaluating the mutual information between Alice and Bob, I_{AB}, and estimating that between Eve and Bob, I_{BE}. Note that the information Eve has on Bob's setup can be either classical or quantum in nature. It is necessary that Alice and Bob share more information on the random bit string between them than the information Eve has on it. This can be represented in terms of key rate (number of secure bits per second):

$$K = (\beta I_{BA} - I_{BE}) f_{\text{rep}}, \tag{2.1}$$

where β is the reconciliation efficiency, describing the ratio of information that is consumed in step 3 of the protocol, and f_{rep} is the utilized repetition frequency. To simplify comparisons, the key rate in QKD is commonly normalized by the repetition frequency, being thus presented in number of secure bits per symbol. The results presented further in this work will follow this convention. The security of QKD will be further explored in Section 2.3.

2.2 Continuous Variables Quantum Key Distribution

The aim of CV-QKD in particular is to implement QKD while encoding information in observables whose measurements give continuous values, for example the quadratures of quantum states. This choice allows for measurements to be made using standard telecom techniques instead of photon-counting ones. There are two main families of CV-QKD protocols depending on the kind of quantum state used for encoding:

- Squeezed state based protocols, where the information is encoded on the uncertainty of each quadrature [3, 4];

- Coherent state based protocols, where the information is encoded in the phase and amplitude of week coherent states [5].

Squeezed states require the use of non standard encoding methods [4], while coherent states can be generated through modulation schemes already deployed in classical coherent communications [5], thus being considerably easier to generate practically. As a result, in this work we will explore the use of coherent states, more specifically, discrete modulation of the coherent states will be employed.

2.2.1 CV Quantum Communication System description

A high-level diagram of the system assumed in this work is presented in Figure 2.1. The system can be split into a lower physical layer, where both the quantum and classical communications take place, and an upper software layer, where the keys are generated and reconciliation and privacy amplification are done. The system can also be split vertically into an emitter, usually named Alice, and a receiver, usually named Bob, that are connected by a quantum channel and a classical channel. For the purposes of this work, we adopted the realistic mode [6], where we assume that Eve has full access to the quantum communication channel and has full technological power, i.e. her measurement capabilities are only limited by physical laws [7]. We assume that Eve can tap but not tamper with the authenticated messages that are transmitted through the classical channel and cannot tamper with Alice's and Bob's apparatuses, this last assumption means that we are working in a trusted device scenario. In this scenario it is assumed that Eve does not know, nor can she influence, what states Alice generates to send to Bob, and neither can she control the parameters of Bob's receiver (for example the detector noise) [8].

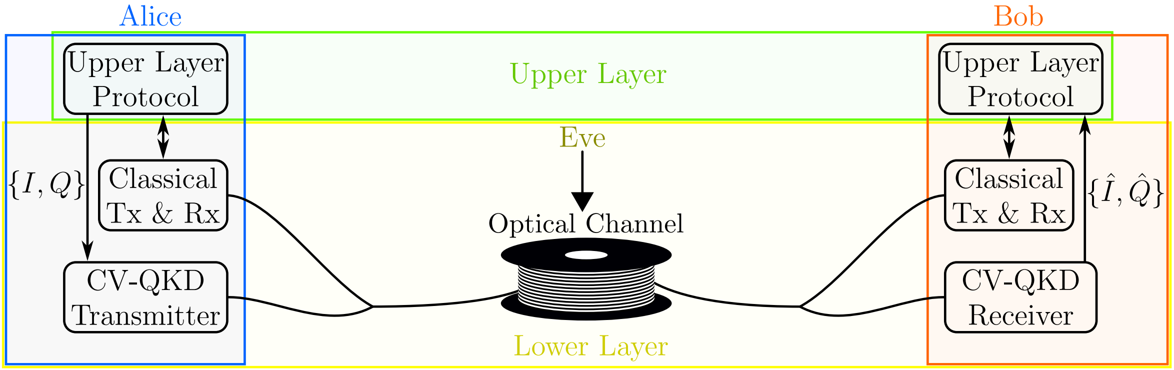


Figure 2.1: Diagram of a generic CV-QKD communication system.

Alice starts by generating a bit sequence in her upper layer protocol which she then passes to her CV-QKD transmitter, where she proceeds to encode her bit sequence in the phase and amplitude of quantum coherent states. These quantum coherent states are then injected into the quantum channel, which consists of a standard optical fibre. Eve is assumed to have free access to the quantum channel. Bob will then decode the coherent states based on the measurements made in his CV-QKD receiver of the in-phase and quadrature components of the optical field, then passing his decoded results to his upper layer protocol. Afterwards, Bob and Alice use a shared subset of the transmitted states, either through previous knowledge, sharing the information at run time through the classical communication channel or another method, in order to obtain the channel parameters [6]. Subsequently, the obtained channel parameters and the knowledge of the transmitted symbols will be used by Alice to estimate the mutual information between Bob and herself and the information lost to the channel, i.e. the information Eve may have obtained. If it is determined that Bob and Alice share more information than Eve could have obtained, a secret key can, in principle, be extracted through some distillation process [6].

A block diagram of Alice's transmission stage in a generic CV-QKD system is presented in Figure 2.2. The sequence of states generated in the upper layer is submitted to some pre-processing procedure (pulse-shaping, for example) before it is fed into a Digital to Analog Converter (DAC). In turn, this DAC drives the system's modulation stage, which can be an IQ Modulator, an Amplitude Modulator (AM)&Phase Modulator (PM) pair, or another. The modulated signal is then attenuated to a quantum level using a Variable Optical Attenuator (VOA) and sent to Bob through a non-amplified optical communication channel. The exact power level depends on, among other things, the modulation format employed.

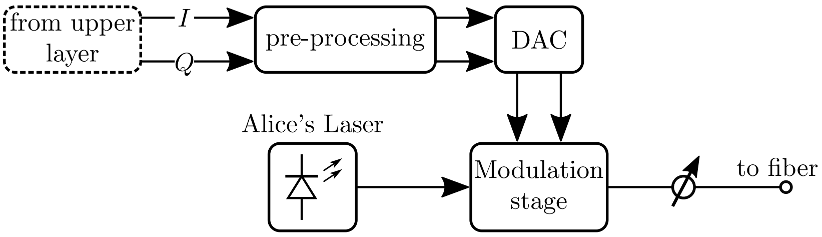


Figure 2.2: High level diagram of a generic CV-QKD transmitter stage.

A diagram of Bob's receiver stage of the considered system is presented in Figure 2.3. The signal arriving from the quantum channel is mixed in a balanced Beam Splitter (BS) with a reference coherent tone extracted from a Local Oscillator (LO). The outputs of the 50/50 BS are fed into a pair of photodetectors connected in tandem, with the subtraction of the current passing through a Trans-Impedance Amplifier (TIA). This amplifier is then followed by a band-pass filter, which sets the maximum and minimum frequencies readable by the receiver, with its output being converted to the digital domain in an Analog to Digital Converter (ADC). The digitized samples are then subjected to some form of post-processing (phase and frequency mismatch recovery, for example) in order to extract the states encoded by Alice. The output of the post-processing step is then sent to the upper layer, where channel parameter estimation, key reconciliation and privacy amplification are performed.

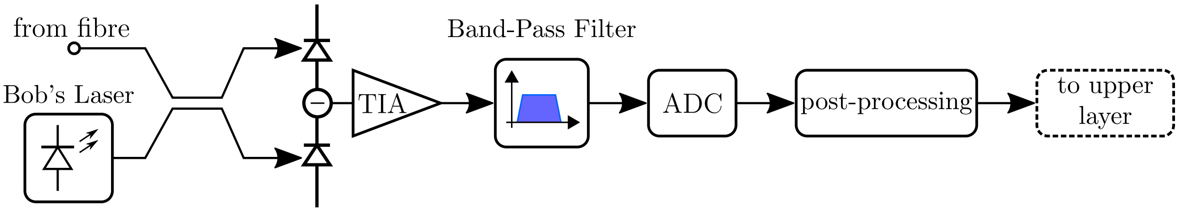


Figure 2.3: High level diagram of a generic CV-QKD receiver stage.

2.3 Security of CV-QKD

After Bob performs his post-processing, him and Alice can be seen as sharing information about a random bit string. They then turn this correlated random sequence of bits into a shared secret key by applying some form of error correction and key distillation process. To this purpose, Bob and Alice need to estimate their mutual information, I_{BA}, and how much information could have been leaked to Eve, χ_{BE}. If Bob and Alice share more information than that which could've been leaked to Eve, i.e.

$$\beta I_{BA} > \chi_{BE}, \tag{2.2}$$

where β is the reconciliation efficiency, given by [9, 10]

$$\beta = 2\frac{R}{I_{\text{BA}}}, \tag{2.3}$$

so that βI_{BA} describes the amount of information Bob and Alice share after the reconciliation stage [6]. The value of β is usually assumed to be some constant value, however recent results have shown that it is highly dependent on the Signal to Noise Ratio (SNR) of the system, and not taking this into account will greatly impact its performance [9, 10]. If the inequality in (2.2) is verified, a theoretically secure key can, in principle, be generated, with the key rate being given by

$$K = \beta I_{BA} - \chi_{BE}. \tag{2.4}$$

Since we assume that Eve is only limited by physical laws, we have to assume that the information she is able to extract is quantum bounded, because of this we label the mutual information between Bob and Eve as χ_{BE}, representing Holevo mutual information [11], instead of I_{BE}, representing Shannon mutual information [12]. Likewise, the mutual information between Bob and Alice is extracted using a classical receiver, therefore we use I_{BA} to represent the mutual information between the two.

To estimate the mutual informations, we are going to start by modelling the quantum physical communication channel. The coherent states, i.e. the symbols sent by Alice to Bob, can be written in bra-ket notation as [1]

$$|\alpha\rangle = ||\alpha|e^{i\theta}\rangle = |x + iy\rangle\,, \tag{2.5}$$

where α is related to the average number of photons in the state,$\bar{n}$, through $\bar{n} = |\alpha|^2 = x^2+y^2$, θ is the phase of the coherent state and x and y are the quadrature components of the coherent state. The annihilation, $\hat{a}$, and creation, $\hat{a}^\dagger$, operators act on these states according to [1]

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,,\ \langle\alpha|\,\hat{a}^\dagger = \langle\alpha|\,\alpha^*. \tag{2.6}$$

It is also of interest to define the quadrature operators

$$\hat{X} = \hat{a}^\dagger + \hat{a}, \qquad \hat{Y} = i(\hat{a}^\dagger - \hat{a}), \tag{2.7}$$

these operators act on the coherent states according to [1]

$$\hat{X}\,|\alpha\rangle = x\,|\alpha\rangle\,,\ \hat{Y}\,|\alpha\rangle = y\,|\alpha\rangle\,, \tag{2.8}$$

and are defined here in Shot Noise Units (SNU). Shot noise refers to the uncertainty on the number of photons, n, of a given coherent state with a mean number of photons $\bar{n}$, which is known to follow a Poisson distribution of the form

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{e^{-\bar{n}}\bar{n}^n}{n!}, \tag{2.9}$$

where $\langle n|$ indicates a Fock state containing n photons [1]. With the definition in (2.7), the variance of the shot-noise will have unit value [7]. Working with SNU both simplifies mathematical developments and comparisons between different implementations. The signal sampled by the ADC can be expressed in volts or ADC counts, the signal at the end of the post-processing stage will be in the same units. For ease of work, it is useful to convert the signal at Bob's output to Shot Noise Units (SNU), this can be achieved theoretically by dividing it by [7]

$$\Sigma = Rg\sqrt{P_B h f B_{\text{eff}} \Gamma_{\text{coef}}}, \tag{2.10}$$

where R is the responsivity of Bob's photodiodes, g is the gain factor of Bob's TIA, P_B is the power of Bob's local oscillator laser, h is Planck's constant, f is the frequency of the optical signal, B_{eff} is the effective bandwidth of the receiver and Γ_{coef} is a loss coefficient due to the filtering process [13]. The value of Σ in (2.10) is the theoretically expected value of the shot noise observed in a receiver system with the same parameters. Nevertheless, in experimental setups many of these parameters can fluctuate with time, as a consequence the SNU conversion is accomplished by measuring the receiver's shot-noise empirically and then dividing the Digital Signal Processing (DSP) output by that value. This process is not trivial and the precision of this measurement is of high importance, this topic is further explored in Section 2.3.1.

The information transmitted between Alice and Bob can be described by Shannon's formalism, due to Bob's classical detection scheme [14]. The maximum mutual information per symbol of a band limited additive white Gaussian noise channel is obtained using Shannon's equation [12]

$$I_{BA} = I_{AB} = \log_2(1 + \text{SNR}) = \log_2\left(1 + \frac{\text{S}}{\text{N}}\right) \tag{2.11}$$

where SNR here signifies the Signal to Noise Ratio, S is the power of the signal and N is the power of the noise. This maximum mutual information assumes the signal to be Gaussian Modulation (GM) [12]. While our system uses Discrete Modulation (DM), for low SNR values, which is the case in CV-QKD, the mutual information of a DM modulated signal is nearly equal to that of the GM signal [6]. Assuming both signal and noise to have null-mean values, their powers will coincide with their respective variances [15].

We can model the individual state quadratures x and y as realizations of the normal random variables $\mathbb{X}$ and $\mathbb{Y}$, which have a zero-mean and variance V_{mod} [7]

$$\mathbb{X} \sim \mathbb{Y} \sim \mathbb{N}(0, V_{\text{mod}}). \tag{2.12}$$

Recalling the relation between α and the average number of photons in the coherent state, we can relate the modulation variance of each individual quadrature to the mean photon number of the ensemble of states generated by Alice through

$$\langle n\rangle = \langle \mathbb{X}^2\rangle + \langle \mathbb{Y}^2\rangle = 2V_{\text{mod}} \iff V_{\text{mod}} = \frac{\langle n\rangle}{2}, \tag{2.13}$$

subsequently, the variance of the quadrature operators in the same state ensemble, V, is given by [7]

$$V = \mathrm{Var}[\hat{X}] = \langle \hat{X}^2 \rangle - \cancelto{0}{\langle \hat{X} \rangle^2} = \langle (\hat{a}^\dagger + \hat{a})^2 \rangle = \langle \hat{a}^\dagger \hat{a}^\dagger \rangle + \langle \hat{a}^\dagger \hat{a} \rangle + \langle \hat{a} \hat{a}^\dagger \rangle + \langle \hat{a} \hat{a} \rangle \tag{2.14}$$

where $\langle \hat{a}\hat{a}^\dagger \rangle$ can be solved using the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$ [1], resulting in

$$V = \langle \hat{a}^\dagger \hat{a}^\dagger + 2\hat{a}^\dagger \hat{a} + \hat{a}\hat{a} \rangle + 1 = \langle (\hat{a}^\dagger + \hat{a})^2 \rangle + 1 = 4 \langle \mathbb{X}^2 \rangle + 1 = 4V_{\mathrm{mod}} + 1 = 2 \langle n \rangle + 1, \tag{2.15}$$

which corresponds to the variance of the signal at the output of Alice's system plus the unavoidable shot noise, removing that shot noise contribution and including the effect of the channel transmittance, T, and Bob's receiver's detection efficiency, η, yields the variance of the signal at Bob's input,

$$\mathrm{S} = 2\, T\eta \langle n \rangle . \tag{2.16}$$

The noise variance can be split into noise originating at Bob's side, N_{rx}, and noise originating in the channel N_{ch}

$$\mathrm{N} = N_{\mathrm{ch}} + N_{\mathrm{rx}}. \tag{2.17}$$

The noise originating in the channel is assumed to be injected at the channel input, i.e. Alice's side, which corresponds to the worst case scenario, and is thus subjected to attenuation by both the channel transmittance and Bob's receiver quantum efficiency,

$$N_{\mathrm{ch}} = T\eta\epsilon, \tag{2.18}$$

with ϵ corresponding to the variance of any noise that travels through the channel. Some of this noise might actually originate in Alice's transmitter system, for example from noise in the output of her DAC or from her laser's Random Intensity Noise (RIN) [7], or arise accidentally from other signals sharing the same optical fibre, for example due to Raman scattering [7], rather than being due to the action of a spy, but since Eve has full access to the channel, all noise that travels through it cannot be trusted and thus is treated as if it was inserted by her. Meanwhile, Eve is assumed to have no control over Bob's apparatus, so the noise added at Bob's receiver is assumed to be trusted noise and has contributions from Bob's laser's shot noise, taking unit value, and from his receiver's thermal noise, ϵ_{th}, in SNU,

$$N_{\mathrm{rx}} = 2 + 2\epsilon_{\mathrm{th}}, \tag{2.19}$$

where both contributions are here doubled due to contributions from the image band that occur due to the heterodyne detection scheme employed [16]. Recalling now (2.11), we can write the classical mutual information between Bob and Alice as

$$I_{BA} = \log_2 \left(1 + \frac{2T\eta \langle n \rangle}{2 + T\eta\epsilon + 2\epsilon_{\mathrm{th}}} \right). \tag{2.20}$$

Having thus defined the mutual information between Bob and Alice, it remains to obtain the quantum mutual information between Bob and Eve, again assuming that the noise introduced in the channel is all due to Eve's tampering.

Eve has no restriction to the detection method she can implement, so the information she is able to obtain is only bounded by quantum laws. We assume that Eve will perform a collective attack. Asymptotically, this limitation does not give Alice and Bob an advantage, as collective attacks have been shown to be optimal [6]. From a mathematical point of view, it is easier to tackle the impact of a collective attack on an Entanglement-Based (E-B) technique than on a Prepare and Measure (P&M) one [6]. Consequently, we will assess the security of an E-B system that would yield the same results as our P&M one. In this equivalent system, Alice generates a pair of entangled states, performs some prospective measurement on one of them and sends the other to Bob. The state received by Bob will have collapsed to one of the $|\alpha_k\rangle$ states due to the measurement performed by Alice on the twin state. In this situation, the mutual information between Eve and Bob can be written in function of the individual, S_{AB}, and conditional, $S_{AB|B}$, von Neumann entropies [6]

$$\chi_{BE} = S_{AB} - S_{AB|B}, \tag{2.21}$$

where S_{AB} is the von Neumann entropy of a bipartite entangled state shared by Alice and Bob and $S_{AB|B}$ is the conditional von Neumann entropy of that same bipartite state given Bob's measurement. S_{AB} and $S_{AB|B}$ are defined, respectively, as [6, 17]

$$S_{AB} = \sum_{i=1}^{2} \left(\frac{\mu_i^{AB}+1}{2}\right) \log_2 \left(\frac{\mu_i^{AB}+1}{2}\right) - \left(\frac{\mu_i^{AB}-1}{2}\right) \log_2 \left(\frac{\mu_i^{AB}-1}{2}\right), \tag{2.22}$$

$$S_{AB|B} = \sum_{i=1}^{2} \left(\frac{\mu_i^{AB|B}+1}{2}\right) \log_2 \left(\frac{\mu_i^{AB|B}+1}{2}\right) - \left(\frac{\mu_i^{AB|B}-1}{2}\right) \log_2 \left(\frac{\mu_i^{AB|B}-1}{2}\right), \tag{2.23}$$

where $\mu_{1,2}^{AB}$ are the symplectic eigenvalues of the covariance matrix that describes the entangled state shared by Alice and Bob and $\mu_{1,2}^{AB|B}$ are the symplectic eigenvalues of the covariance matrix that describes the system after Bob's prospective measurement. These are used because they remain invariant under Eve's collective attack [6]. The symplectic eigenvalues of a matrix Σ with dimensions $2N \times 2N$ can be obtained from the modulus of the eigenvalues of the matrix

$$\tilde{\Sigma} = i\Omega\Sigma, \tag{2.24}$$

where i is the imaginary constant and

$$\Omega = \bigoplus_{i=1}^{N} \omega, \qquad \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{2.25}$$

where $\bigoplus_{i=1}^{N}$ signifies an N-fold direct addition of the ω matrices. $\tilde{\Sigma}$ will have $2N$ eigenvalues, which will be grouped in positive-negative pairs, since we take only the modulus of the eigenvalues, there will only be N unique eigenvalues. These N unique eigenvalues are the symplectic eigenvalues of Σ. With this in mind, we now proceed to develop the system's covariance matrices [6].

We start by defining the density operator of some M-symbol discrete constellation [18],

$$\hat{\rho} = \sum_{k=1}^{M} p_k \left|\alpha_k\right\rangle \left\langle\alpha_k\right|, \tag{2.26}$$

where p_k is the probability that the $|\alpha_k\rangle$ is chosen by Alice from an arbitrary constellation with some arbitrary probabilistic distribution. For simplicity, we assume that the constellation is symmetric in relation to the x-axis of the Argand plane, which is a realistic assumption when working with common constellations. $\hat{\rho}$ can be interpreted as the mixture of states seen by Bob at the input of his receiver system. The average number of photons per symbol for any given constellation is given by

$$\langle n\rangle = \sum_{k=1}^{M} p_k |\alpha_k|^2 \tag{2.27}$$

We now proceed to derive an entangled state that generates the same state mixture as $\hat{\rho}$. We begin by rewriting $\hat{\rho}$ as a function of Gaussian states $|\phi_k\rangle$

$$\hat{\rho} = \sum_{k=1}^{M} \lambda_k |\phi_k\rangle \langle\phi_k| \,. \tag{2.28}$$

We choose to express the system with Gaussian states because all operations on these states using linear optical components can be described as Gaussian operations, greatly simplifying our work. With these states we can now introduce the purified entangled state that Alice could have generated [6]

$$|\Phi\rangle = \sum_{k=1}^{M} \sqrt{\lambda_k}\, |\phi_k\rangle_A |\phi_k\rangle_B \,, \tag{2.29}$$

which corresponds to the ensemble of the entangled states generated at Alice's output, with $|\phi_k\rangle_A$ being the state kept and measured by Alice and $|\phi_k\rangle_B$ the state transmitted to Bob. The exact values of the λ_k parameters will depend on the constellation generated by Alice. By further introducing the states [18]

$$|\varphi_k\rangle = \sqrt{p_k}\hat{\rho}^{-\frac{1}{2}} |\alpha_k\rangle \,, \tag{2.30}$$

we can rewrite (2.29) as [18]

$$|\Phi\rangle = \sum_{k=1}^{M} \sqrt{p_k}\, |\varphi_k\rangle_A |\alpha_k\rangle_B \,, \tag{2.31}$$

it becomes obvious that to generate the mixture observed by Bob, Alice needs to perform the prospective measurement $|\varphi_k\rangle \langle\varphi_k|$ on the half of the entangled state that she keeps in order for Bob to receive the corresponding coherent state, i.e. Bob receives state $|\alpha_1\rangle$ when Alice performs the measurement $|\varphi_1\rangle \langle\varphi_1|$, state $|\alpha_2\rangle$ when she performs the measurement $|\varphi_2\rangle \langle\varphi_2|$ and so on.

The covariance matrix describing the state shared by Alice and Bob before Bob's prospective measurement [18, 19]

$$\gamma_{\text{AB}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}Z\sigma_Z \\ \sqrt{T}Z\sigma_Z & (TV+1-T+T\epsilon)\mathbb{I}_2 \end{bmatrix} = \begin{bmatrix} \gamma_A & \gamma_C \\ \gamma_C & \gamma_B \end{bmatrix}, \tag{2.32}$$

where $\mathbb{I}_2$ is the 2×2 identity matrix and $\sigma_Z = \text{diag}(1,-1)$ and Z is given by

$$Z = 2\text{tr}(\hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{\frac{1}{2}}\hat{a}^\dagger) - \sqrt{2\epsilon W}, \tag{2.33}$$

and where in turn

$$W = \sum_{k=1}^{M} p_k(\langle\alpha_k| \hat{a}_\rho^\dagger \hat{a}_\rho |\alpha_k\rangle - |\langle\alpha_k| \hat{a}_\rho |\alpha_k\rangle|^2), \tag{2.34}$$

where, finally,

$$\hat{a}_\rho = \hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{-\frac{1}{2}}. \tag{2.35}$$

To the best of our knowledge, it isn't possible to compute the value of Z analytically, however, its value can be estimated numerically. This numerical estimation starts by describing the coherent states in their Fock basis

$$|\alpha_k\rangle = e^{-\frac{1}{2}|\alpha_k|^2}\sum_{n=0}^{+\infty}\frac{\alpha_k^n}{\sqrt{n!}}|n\rangle \tag{2.36}$$

and then capping the sum at some dimension D, resulting in a column vector of the type

$$|\alpha_k\rangle \rightarrow \begin{bmatrix} e^{-\frac{1}{2}|\alpha_k|^2}\frac{\alpha_k^0}{\sqrt{0!}} & e^{-\frac{1}{2}|\alpha_k|^2}\frac{\alpha_k^1}{\sqrt{1!}} & \cdots e^{-\frac{1}{2}|\alpha_k|^2}\frac{\alpha_k^D}{\sqrt{D!}}\end{bmatrix}^{\mathrm{T}}. \tag{2.37}$$

D is chosen high enough so that the contribution of the number states with photon numbers higher than it are negligible. We can then define the creation operator as a matrix of the result of the application of $\hat{a}$ to the number states in (2.36), resulting in

$$\hat{a} \rightarrow \begin{bmatrix} 0 & \sqrt{1} & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & \sqrt{2} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \sqrt{k} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & \sqrt{D} \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 \end{bmatrix}. \tag{2.38}$$

Taking into account that $\langle\alpha_k|$ and $\hat{a}^\dagger$ are obtainable by complex transposing (2.37) and (2.38), respectively, computing $\hat{\rho}$, $\hat{\rho}^{\frac{1}{2}}$, $\hat{\rho}^{-\frac{1}{2}}$, W, $\hat{a}_k$, $\hat{a}_k^\dagger$ and, ultimately, Z is a more or less trivial affair.

The covariance matrix that describes Bob's projective measurement, $\gamma_{\mathrm{AB—B}}$, is obtained from γ_{AB} in the following manner:

1. Expand matrix γ_{AB} by appending to it the modes corresponding to Bob's detector electronic noise, which is modelled by an EPR state with variance [14]

   $$\Xi_{\mathrm{rx}} = 1 + \frac{2\epsilon_{\mathrm{th}}}{1-\eta}. \tag{2.39}$$

   This will result in

   $$\gamma_{\mathrm{ABF_0G}} = \gamma_{\mathrm{AB}} \oplus \gamma_{\mathrm{F_0G}}, \tag{2.40}$$

   where

   $$\gamma_{\mathrm{F_0G}} = \begin{bmatrix} \Xi_{\mathrm{rx}}\mathbb{I}_2 & \sqrt{\Xi_{\mathrm{rx}}^2 - 1}\sigma_Z \\ \sqrt{\Xi_{\mathrm{rx}}^2 - 1}\sigma_Z & \Xi_{\mathrm{rx}}\mathbb{I}_2 \end{bmatrix}. \tag{2.41}$$

   The $\oplus$ in (2.40) signifies direct addition of the matrices. The resulting matrix will be

   $$\gamma_{\mathrm{ABF_0G}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}Z\sigma_Z & 0 & 0 \\ \sqrt{T}Z\sigma_Z & (TV+1-T+T\epsilon)\mathbb{I}_2 & 0 & 0 \\ 0 & 0 & \Xi_{\mathrm{rx}}\mathbb{I}_2 & \sqrt{\Xi_{\mathrm{rx}}^2 - 1}\sigma_Z \\ 0 & 0 & \sqrt{\Xi_{\mathrm{rx}}^2 - 1}\sigma_Z & \Xi_{\mathrm{rx}}\mathbb{I}_2 \end{bmatrix}, \tag{2.42}$$

   where 0 is a 2×2 matrix of zeros;

2. Act on the combined state $\gamma_{\mathrm{ABF_0G}}$ with a beam-splitter state (symbolizing the quantum efficiency of the detectors)

$$\gamma_{\mathrm{ABFG}} = (Y_{\mathrm{BS}})^T(\gamma_{\mathrm{ABF_0G}})Y_{\mathrm{BS}}, \tag{2.43}$$

   where

$$Y_{\mathrm{BS}} = \mathbb{I}_2 \oplus Y_{\mathrm{BS}}^{\mathrm{B_1F_0}} \oplus \mathbb{I}_2, \tag{2.44}$$

   and where in turn

$$\mathrm{Y}_{\mathrm{BS}}^{\mathrm{B_1F_0}} = \begin{bmatrix} \sqrt{\eta}\mathbb{I}_2 & \sqrt{1-\eta}\mathbb{I}_2 \\ -\sqrt{1-\eta}\mathbb{I}_2 & \sqrt{\eta}\mathbb{I}_2 \end{bmatrix}; \tag{2.45}$$

3. Reorder the rows and columns of γ_{ABFG}, changing the second row to now be the fourth row and changing the second column to now be the fourth column. Note that since each entry to the matrix is a 2 × 2 matrix, each "line" and "column" here will actually be two lines and columns;

4. Partition matrix γ_{AFGB} into four submatrices such that

$$\gamma_{\mathrm{AFGB}} = \begin{bmatrix} \gamma_{\mathrm{AFG}} & \sigma_{\mathrm{AFGB}}^T \\ \sigma_{\mathrm{AFGB}} & \gamma_{\mathrm{B}} \end{bmatrix}, \tag{2.46}$$

   where

$$\gamma_{\mathrm{AFG}} = \begin{bmatrix} V\mathbb{I}_2 & 0 & \sqrt{(1-\eta)T}Z\sigma_Z \\ 0 & \Xi_{\mathrm{rx}}\mathbb{I}_2 & \sqrt{\eta(\Xi_{\mathrm{rx}}^2-1)}Z\sigma_Z \\ \sqrt{(1-\eta)T}Z\sigma_Z & \sqrt{\eta(\Xi_{\mathrm{rx}}^2-1)}Z\sigma_Z & [(1-\eta)(TV+1-T+T\epsilon)+\eta\Xi_{\mathrm{rx}}]\mathbb{I}_2 \end{bmatrix}, \tag{2.47}$$

$$\sigma_{\mathrm{AFGB}} = \begin{bmatrix} \sqrt{T\eta}Z\sigma_Z & -\sqrt{(1-\eta)(\Xi_{\mathrm{rx}}^2-1)}Z\sigma_Z & [(TV+1-T+T\epsilon)-\Xi_{\mathrm{rx}}]\sqrt{\eta(1-\eta)}\mathbb{I}_2 \end{bmatrix}, \tag{2.48}$$

   and

$$\gamma_{\mathrm{B}} = [\eta(TV+1-T+T\epsilon)+(1-\eta)\Xi_{\mathrm{rx}}]\mathbb{I}_2; \tag{2.49}$$

5. Obtain the covariance matrix of Bob's projective measurement by computing

$$\gamma_{\mathrm{AB—B}} = \gamma_{\mathrm{AFG}} - \sigma_{\mathrm{AFGB}}^T(\gamma_{\mathrm{B}}+\mathbb{I}_2)^{-1}\sigma_{\mathrm{AFGB}}. \tag{2.50}$$

Finally, we can take matrices γ_{AB} and $\gamma_{\mathrm{AB—B}}$, compute matrices $\tilde{\gamma}_{\mathrm{AB}}$ and $\tilde{\gamma}_{\mathrm{AB—B}}$ through (2.24) and take the modulus of the eigenvalues of the resulting matrices. Matrix $\tilde{\gamma}_{\mathrm{AB}}$ will return two unique eigenvalues, μ_1^{AB} and μ_2^{AB}. Meanwhile, $\tilde{\gamma}_{\mathrm{AB—B}}$ will return three unique eigenvalues, however one of them will always be equal to 1, since patching $\mu_i^{AB|B} = 1$ into (2.23) would result in a $0\log_2(0)$ term, which is not well defined but can be shown to be 0 through limits, that eigenvalue is discarded and only the non-unit eigenvalues are taken, $\mu_1^{AB|B}$ and $\mu_2^{AB|B}$. Plugging μ_1^{AB} and μ_2^{AB} into (2.22) and $\mu_1^{AB|B}$ and $\mu_2^{AB|B}$ into (2.23), subsequently the two von Neumann entropies are then plugged into (2.21), thus obtaining the mutual information between Eve and Bob, χ_{BE}. Putting this mutual information into (2.4), where it is subtracted from the information shared between Bob and Alice, I_{BA}, obtained through (2.20), scaled by the reconciliation efficiency β, which depends on the error correction code and is always smaller or equal to 1, yields the amount of secure bits obtained per symbol transmitted.

To illustrate the results above, we are going to show the dependency of the mutual informations with multiple different parameters for a system using an 8 symbol Phase Shift Keying (PSK) constellation format. Unless where otherwise noted, the parameters assumed are: $T = 0.15849$ (corresponding to a 40 km standard fibre with 0.2 dB/km of attenuation), $\eta = 0.90$, $\beta = 0.95$, $|\alpha|^2 = 0.2$ photons, $\epsilon = 0.005$ SNU and $\epsilon_{\text{th}} = 0.3$ SNU. The values for η, β and ϵ were chosen in due to them being quite common in the literature, while the values for T and ϵ_{th} were chosen due to them agreeing with the experimental parameters presented later in this work. In Figure 2.4 the dependency of I_{BA}, χ_{BE} and K with the average number of photons per symbol is presented. Both I_{BA} and χ_{BE} increase with $\langle n \rangle$, with I_{BA} initially growing faster than χ_{BE} but eventually being overtaken. I_{BA} tends to 0 as $\langle n \rangle$ tends to 0, which is predictable as in this situation no states are shared, however χ_{BE} tends to some positive value, this is due to Eve having some information on Bob's received excess noise. For this particular combination of parameters, the maximum key rate is 4.402×10^{-3} bits/symbol at a mean number of photons per symbol of ~ 0.22. Furthermore, no secure bits can be recovered with less than ~ 0.041 or more than ~ 0.48 photons per symbol in average.

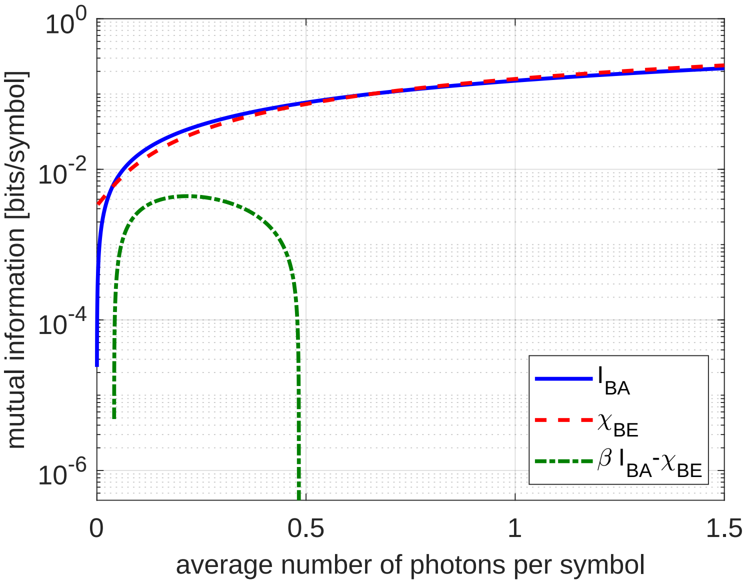
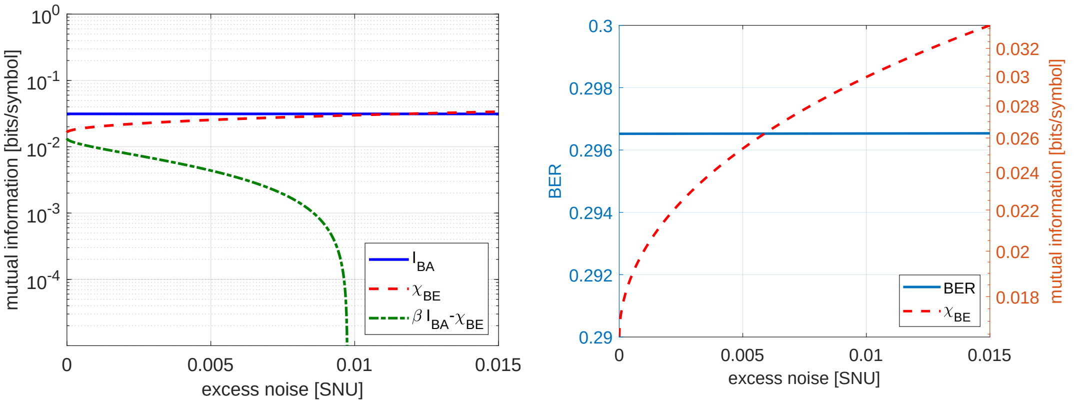


Figure 2.4: Mutual information between Bob and Alice, between Bob and Eve and corresponding key rate in function of the average number of photons per symbol, for an 8-PSK constellation.

In Figure 2.5a the dependency of I_{BA}, χ_{BE} and K with the excess channel noise is presented. As the channel excess noise increases, χ_{BE} increases sharply, this is to be expected, as the more Eve tampers with the signal, the more information she can extract from it and the more noise she adds. Note that some excess noise may originate in Alice's transmitter setup, but as this noise passes through the channel it cannot be trusted and must be included in the excess noise. For this particular combination of parameters, no secure bits can be recovered with an excess noise of more than ~ 0.0098 SNU. To illustrate the impact of the



(a) Mutual information between Bob and Alice, between Bob and Eve and corresponding key rate in function of excess noise.

(b) Bit Error Rate and mutual information between Bob and Eve in function of channel excess noise.

Figure 2.5: Impact of excess noise on the performance of a CV-QKD system using an 8-PSK constellation.

excess noise on the system, in Figure 2.5b the dependency of the Bit Error Rate (BER) and χ_{BE} with excess noise is plotted for two different transmission values. The BER in function of SNR for an M-PSK constellation is given by [20]

$$\mathrm{BER} = \frac{1}{\log_2(\mathrm{M})} \mathrm{erfc}\left[\sqrt{\mathrm{SNR}\log_2(\mathrm{M})} * \sin\left(\frac{\pi}{\mathrm{M}}\right)\right], \tag{2.51}$$

where erfc() is the complementary error function. We see that an increase of the excess noise will result in an increase of the mutual information between Bob and Eve, but that increase is not reflected in any appreciable alteration of the BER. From this result we observe that Eve's action would not be noticed through an impact on the system performance itself, as the BER remains almost unchanged, unless Alice and Bob specifically monitor the channel excess noise.

In Figure 2.6 the dependency of I_{BA}, χ_{BE} and K with the transmission distance is presented. I_{BA} decreases with decreasing transmission, this is explained by the fact that with decreasing transmission the signal that reaches Bob is increasingly weaker while his internal sources of noise remain the same, degrading his SNR and in turn the mutual information I_{BA}. χ_{BE} also decreases with decreasing transmission, this is explained as Bob's internal noise has an ever increasing influence on his results, thus degrading the information she has on them. However, χ_{BE} decreases at a slower rate than I_{BA}, as such it will eventually overtake it, resulting in a maximum secure transmission distance, which for this particular combination of parameters occurs at around 78 km.

Rx thermal noise and photons per symbol are established prior to communication, that leaves excess noise and channel transmission as the channel parameters to be estimated. In Figure 2.7 the sensitivity of the security bounds to small deviations of the channel parameters is shown. Figure 2.7a shows the key rate in function of excess noise for a transmittance of 0.1585, corresponding to a 40 km standard fibre with 0.2 dB/km, and transmission distances 10% above and below that, while Figure 2.7b shows the key rate in function of transmission distance for an excess noise of 0.005 SNU and with deviations of 10% above and below. From

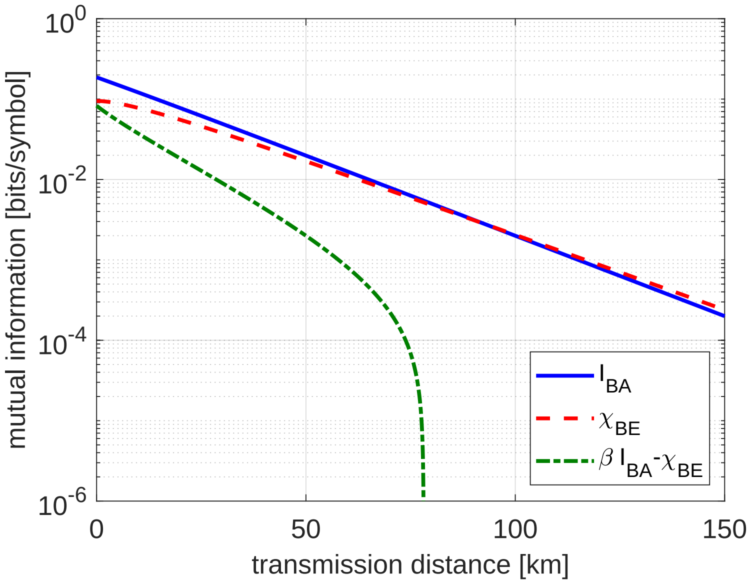


Figure 2.6: Mutual information between Bob and Alice, between Bob and Eve and corresponding key rate in function of transmission distance, assuming a standard fibre with 0.2 dB/km of attenuation.

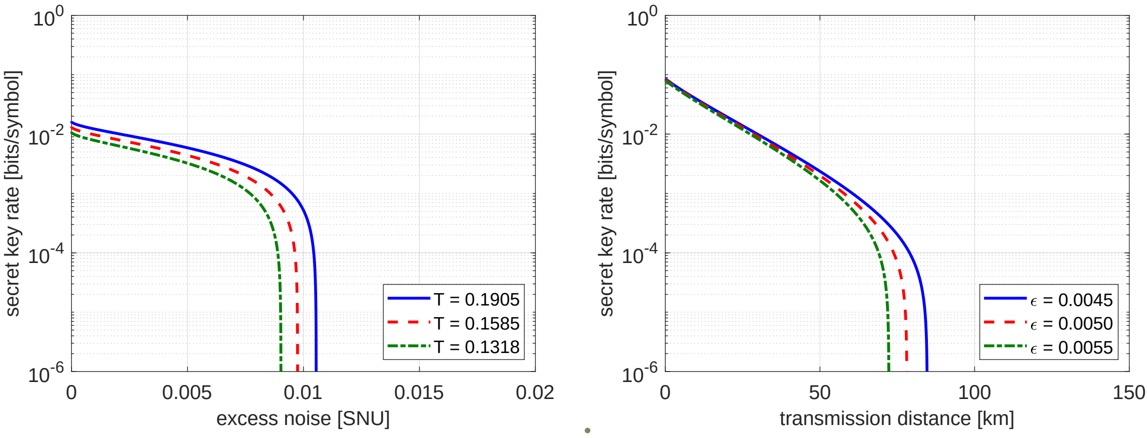
these figures we see that the security limits are more sensitive to excess noise fluctuations than to transmission. Due to this sensitivity, an accurate estimation of the channel parameters is very important for the function of any CV-QKD system.

2.3.1 Parameter estimation

The mutual informations and, subsequently, key rate obtained in the previous section assumed a perfect knowledge of the channel and receiver parameters. In the case of an experimental system these parameters need to be continuously estimated, and those estimations will naturally have an associated uncertainty. One more factor to take into consideration is the fact that in the process of estimating these parameters a subset of the bits in the raw key will have to be shared through an open channel, these will be revealed and thus must be discarded from the generated key. Computing the key rate with these considerations in mind means that the system is functioning in the finite size scenario, in opposition to the asymptotic one, where Alice and Bob have access to infinitely many samples to use in parameter estimation. The impact that including these considerations has on the performance of the system is usually dubbed Finite Size Effects (FSE) The effect of sharing this subset can be easily included in the secure key rate (2.4) as:

$$K = \frac{n}{N}\left(\beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}} - \Delta^{\mathrm{PA}}\right), \tag{2.52}$$

where N is the length of the raw key, $n = N - k$ is the remaining key after the subset of length k as been openly shared [6] and Δ^{PA} is a parameter describing the amount of information



(a) Key rate in function of excess noise for multiple values of transmission distance.

(b) Key rate in function of transmission distance for multiple values of excess noise.

Figure 2.7: Plot of the key rate in function of excess noise (left) and transmission distance (right).

lost due to the privacy amplification stage, given by [21]

$$\Delta^{\mathrm{PA}} = 7\sqrt{\frac{\log_2\left(\frac{2}{\bar{\epsilon}}\right)}{n}} + \frac{2}{n}\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right), \tag{2.53}$$

where $\bar{\epsilon}$ is a smoothing parameter and ϵ_{PA} is the failure probability of the privacy amplification step.

To estimate the channel transmission and excess noise we start by considering that Alice and Bob share a couple of correlated variables a and b, corresponding to the states generated by Alice and those received by Bob, respectively. Both variables are assumed to be expressed in Shot Noise Units (SNU), for a this is accomplished simply by using the definitions for the constellation points α_k, while for b it is done by having Bob divide the output of his DSP stage by the shot noise variance. a and b are related by the normal linear model [6]:

$$b = ta + z, \tag{2.54}$$

where $t = \sqrt{\eta T}$ and z is the noise contribution, following a normal distribution with null mean and variance

$$\sigma^2 = 2 + 2\epsilon_{\mathrm{th}} + \eta T\epsilon. \tag{2.55}$$

We can estimate t through:

$$\tilde{t} = \frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{a_i b_i^*}{|a_i|^2}\right\} = \frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{a_i(ta_i)^*}{|a_i|^2}\right\} + \frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{a_i z_i^*}{|a_i|^2}\right\}, \tag{2.56}$$

where Re() signifies the real component of the argument. Since z has zero mean, the second term in (2.56) will cancel out, yielding

$$\tilde{t} = t\frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{|a_i|^2}{|a_i|^2}\right\} = t. \tag{2.57}$$

Meanwhile, σ^2 can be estimated through

$$\tilde{\sigma}^2 = \frac{1}{k}\sum_{i=1}^{k}(b_i - \tilde{t}a_i)^2 = \frac{1}{k}\sum_{i=1}^{k}(z_i)^2, \tag{2.58}$$

taking again into account that z has zero mean, this last term is basically the definition for the variance of z.

In order to obtain the channel parameters we need first to have an estimation of the receivers' thermal and shot noise variance. The formula for the $(1-\varepsilon)$ confidence interval of a variance estimate, s^2, done with recourse to a sufficiently large number of samples, k, is given by the inequalities

$$s^2\left(1 - z_{\varepsilon/2}\sqrt{\frac{2}{k}}\right) \leq \sigma^2 \leq s^2\left(1 + z_{\varepsilon/2}\sqrt{\frac{2}{k}}\right), \tag{2.59}$$

where $z_{\varepsilon/2}$ is the $100(1-\frac{\varepsilon}{2})$th percentile of a standard normal distribution. In order to ensure security with certain degree of confidence ε, the worst case scenario value, i.e. the values that give the most advantage to Eve, for each value in the given confidence interval needs to be taken. For the case of the thermal noise, this corresponds to using the lower bound of the confidence interval, as any noise not attributed to the receiver thermal noise will be in turn attributed to the eavesdropper, thus degrading the performance of the system. Meanwhile, for the case of the shot noise, this corresponds to obtaining the channel transmission estimation using the upper bound of the shot noise estimation to convert Bob's DSP output to SNU, and to obtaining the excess noise estimation using the lower bound. In doing this, we are splitting the linear model (2.54) in two

$$b_{\text{upper}} = t_{\text{upper}}a + z_{\text{upper}}, \tag{2.60}$$

$$b_{\text{lower}} = t_{\text{lower}}a + z_{\text{lower}}, \tag{2.61}$$

and computing $\tilde{T}$ from the upper one and $\tilde{\epsilon}$ from the lower one (while using the channel transmission estimation obtained previously).

Furthermore, the uncertainty of the channel parameter estimations themselves need to be taken into account. The confidence interval for the variance of z will follow the same behavior as shown in (2.59), meanwhile the channel transmission estimate will have the confidence interval:

$$\tilde{t} - z_{\varepsilon/2}\sqrt{\frac{\tilde{\sigma^2}}{k}} \leq t \leq \tilde{t} + z_{\varepsilon/2}\sqrt{\frac{\tilde{\sigma^2}}{k}} \tag{2.62}$$

For the channel parameters, the worst case scenarios correspond to the lower bound of the channel transmission and the upper bound of the excess noise.

$$t_{\min} \approx \tilde{t} - z_{\varepsilon/2}\sqrt{\frac{\tilde{\sigma}^2}{k}}, \tag{2.63}$$

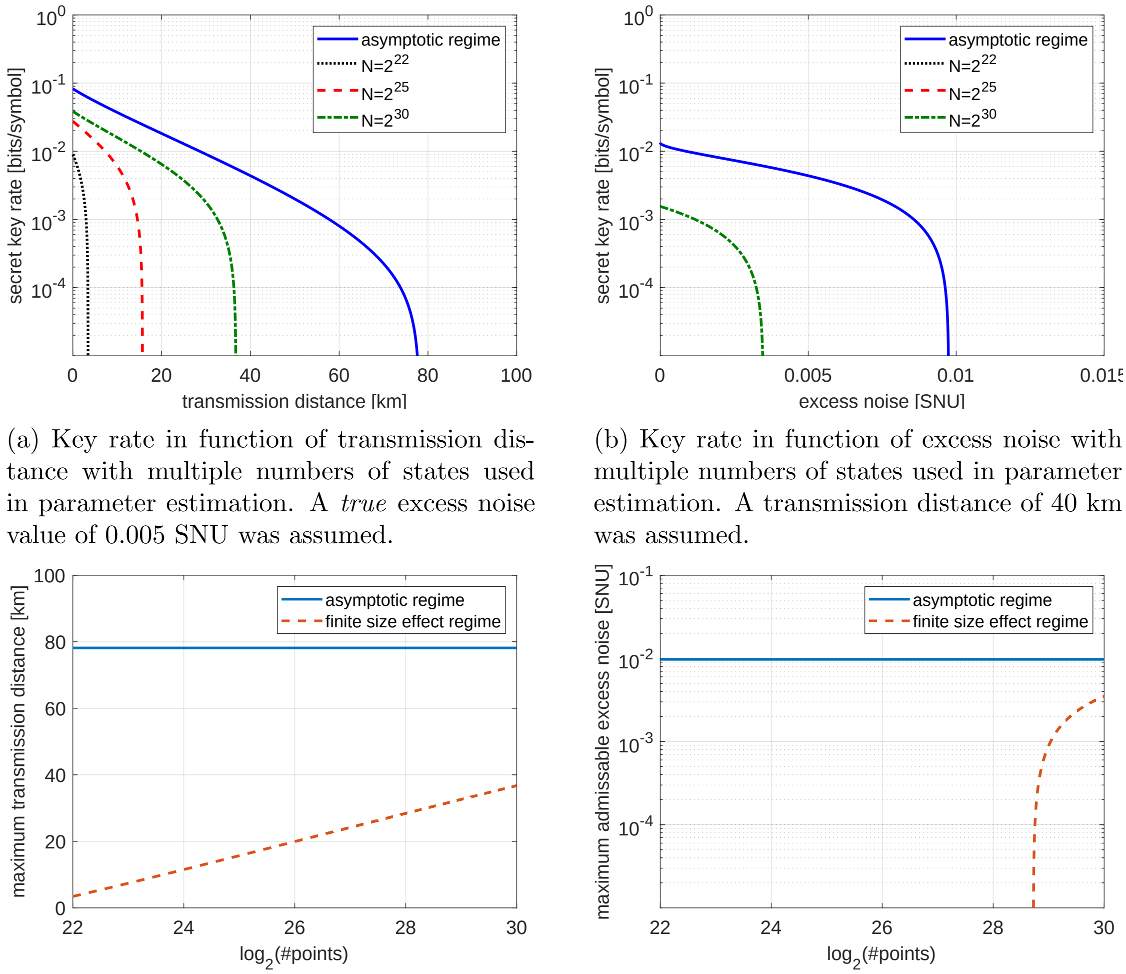
$$\sigma^2_{\max} \approx \tilde{\sigma}^2 + z_{\varepsilon/2}\frac{\tilde{\sigma}^2\sqrt{2}}{\sqrt{k}}, \tag{2.64}$$

The corresponding transmission and excess noise parameters are obtained through

$$T_{\min} = \frac{1}{\eta}t^2_{\min}, \tag{2.65}$$

$$\epsilon_{\text{max}} = \frac{\sigma^2_{\text{max}} - 1 - \epsilon_{\text{ele, min}}}{T_{\text{min}}}. \tag{2.66}$$

In Figure 2.8 we present results showing the impact of the finite size effect on the performance of a CV-QKD system, obtained from (2.52). For these results we assumed $\beta = 0.95$ and $\frac{n}{N} = \frac{1}{2}$, in Figures 2.8a and 2.8c the *true* value of ϵ was taken as 0.005 and in Figures 2.8b and 2.8d the transmission distance was set at 40 km. To allow for comparison, the asymptotic performance of the system is presented as a full blue line, obtained through (2.4). In Figure 2.8a we trace the key rate, obtained from (2.52), for 3 different numbers of symbols shared and for the asymptotic scenario. We see that there is a very steep performance decrease in the maximum achievable distance, once FSE are taken into account. Even in the scenario where the largest amount of states considered are shared, 2^{30} to be exact, the maximum achievable distance is effectively halved. The dependency of the achievable distance with the number of symbols shared is more clearly seen in Figure 2.8c, where we can see that it climbs linearly with the logarithm of the number of symbols used. The situation is even worse when considering the impact of FSE on the excess noise resistance of the system. In Figure 2.8b we see that, at a transmission distance of 40 km, no key can be generated using either 2^{22} or 2^{25} symbols during parameter estimation, and even for the 2^{30} symbol scenario the excess noise resistance is very poor, with the key rate being almost an order of magnitude below that of the asymptotic regime and not even reaching 0.005 SNU of excess noise resistance. This effect is again seen in Figure 2.8d, where we see that under $\sim 2^{27}$ symbols used in estimation, no key is generated. As a rule of thumb, the longer the distance and the higher the excess noise, the more symbols are necessary to generate a secure key. However, using more symbols in the estimation is not always feasible, as practical considerations (stability time of the channel, limitations of the digital post-processing stage, among others) usually put a maximum ceiling on the number of symbols that can be used in parameter estimation.



(a) Key rate in function of transmission distance with multiple numbers of states used in parameter estimation. A *true* excess noise value of 0.005 SNU was assumed.

(b) Key rate in function of excess noise with multiple numbers of states used in parameter estimation. A transmission distance of 40 km was assumed.

(c) Maximum achievable distance in function of number of points used in the parameter estimation. A *true* excess noise value of 0.005 SNU was assumed.

(d) Maximum admissible excess noise in function of number of points used in the parameter estimation. A transmission distance of 40 km was assumed.

Figure 2.8: Impact of FSE on the performance of a CV-QKD system. A standard fibre with 0.2 dB/km attenuation was assumed.

2.4 Summary

In this Chapter we have presented the framework of CV-QKD. We began by establishing the first principles in play, then went on to describe the functioning of a generalized QKD protocol. We then narrowed our study, describing a more detailed CV-QKD system, the security of which we established following the methodology of [18]. We show how, under the right, somewhat optimistic, circumstances, CV-QKD systems using 8-PSK constellations are capable of achieving distances of almost 80 km in the asymptotic regime, thus being suitable for medium-range, inter-city links. We finished this chapter with an exploration of the impact of uncertainties in the estimated channel and receiver parameters on the security of a CV-QKD system. From this last study we observe that, to achieve the transmission distances observed in the asymptotic regime, well over 2^{30} symbols have to be transmitted, requiring a large amount of storage and processing power and, depending on the symbol rate of the system, a long stability channel time.

Bibliography

[1] Rodney Loudon. *The quantum theory of light.* OUP Oxford, 2000.

[2] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[3] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999.

[4] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2):022309, 2000.

[5] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv preprint quant-ph/0204127*, 2002.

[6] Anthony Leverrier. *Theoretical study of continuous-variable quantum key distribution.* PhD thesis, Télécom ParisTech, 2009.

[7] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[8] Fabian Laudenbach and Christoph Pacher. Analysis of the trusted-device scenario in continuous-variable quantum key distribution. *Advanced Quantum Technologies*, 2(11):1900055, 2019.

[9] Xiangyu Wang, Yi-Chen Zhang, Zhengyu Li, Bingjie Xu, Song Yu, and Hong Guo. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *arXiv preprint arXiv:1703.04916*, 2017.

[10] Hossein Mani, UL Andersen, T Gehring, C Pacher, S Forchhammer, JM Mateo, and M Vicente. Error reconciliation protocols for continuous-variable quantum key distribution. *Ph. D. dissertation, Technical University of Denmark*, 2021.

[11] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[12] Claude E Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[13] DSP related. Filtered white noise. Online Resource, April 2020. https://www.dsprelated.com/freebooks/sasp/Filtered_White_Noise.html.

[14] A Becir, FAA El-Orany, and MRB Wahiddin. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10(01):1250004, 2012.

[15] Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher, Michael Hentschel, Chi-Hang Fred Fung, Fotini Karinou, Andreas Poppe, Momtchil Peev, and Hannes Hübel. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*, 3:193, 2019.

[16] Heng Fan, Dechao He, and Sheng Feng. Experimental study of a phase-sensitive heterodyne detector. *JOSA B*, 32(10):2172–2177, 2015.

[17] John Von Neumann. *Mathematical foundations of quantum mechanics.* Number 2. Princeton university press, 1955.

[18] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 2021.

[19] Margarida Almeida. Practical security limits of continuous-variable quantum key distribution. Master's thesis, University of Aveiro, 2021.

[20] Andrea Goldsmith. *Wireless communications.* Cambridge university press, 2005.

[21] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

Chapter 3

Numerical and Experimental Implementation

In this Chapter results pertaining to the numerical and experimental implementation of the Continuous Variables Quantum Key Distribution (CV-QKD) system described previously in Chapter 2 are presented. The content in this Chapter aims to carefully describe the experimental system as well as the Digital Signal Processing (DSP) routine used for the results in this thesis.

This Chapter begins with a description of and results from the simulated implementation of the system detailed in Chapter 2, presented in Section 3.1. These simulation results are also used to detail the functioning of the DSP stage in a controlled environment. Then follows a detailed description of the experimental implementation of the protocol, presented in Section 3.2, where we also showcases the robustness of our receiver system in the presence of very high polarization drift. The chapter concludes with a short description of the field trial experiment, presented in Section 3.3.

3.1 Simulation of Continuous Variables Quantum Key Distribution

The simulation platform under development, dubbed *netxpto*, intends to be a basis for simulating point-to-point links, both classical and quantum, allowing for the performance of experimental setups to be tested via simulation before being assembled in the laboratory. The platform is being coded in C++ and consists of a multi person effort, in which the results presented in this report insert themselves. The results shown here intend to present the functioning of the DSP stage mentioned previously in Figure 2.3.

The simulations are composed of blocks and signals. Blocks are self contained sections of code that either act on or generate signals, attempting to closely replicate physical components (photodiodes, optical amplifiers, etc.) when applicable. Whenever quantum properties of components need to be simulated, this is done through the use of appropriate statistical models. Signals are vectors which simulate either time sampled physical signals or logical sequences, allowing for interaction between individual blocks. Signals can take multiple types, the ones of most interest to us are now enumerated:

- Binary signals, used to contain the encoding basis to the signals or the decoding results;

- Real valued signals, used to model (among others) electrical signals, in either voltage or amperage;
- Bandpass complex optical signals, simulating either single or double polarization optical signals in bandpass representation.

For optical signals, for example with a wavelength of 1550 nm, typical for coherent communications, a sampling rate of $\sim$ 400 THz is necessary in order to avoid aliasing. This frequency is many orders of magnitude above the bit rate utilized in optical transmissions and would thus generate a large number of unnecessary samples for each symbol. In order to avoid this we take advantage of the bandpass representation of optical signals, which consists of down-converting the signal from a high frequency f_c to a base frequency. Thus, to sample an optical signal with bandwidth $B = f_2 - f_1$, all that is necessary is a sampling frequency $\omega_s \geq 2B$ [1].

The architecture of the simulation follows the one presented in Figures 2.2 and 2.3. A detailed block diagram of the transmitter and channel stages of the simulation is presented in Figure 3.1. The simulation begins by taking a binary key, encoding it in an 8-PSK constellation, thus converting it into a complex signal, and filling the transition points between each constellation state following a Root Raised Cosine (RRC) modulation format with a bandwidth of 38.4 MHz. We again adopt RRC modulation because of the possibility of using matched filtering at the receiver without inter-symbol interference [2], thus allowing for optimum Gaussian white-noise minimization. At this point the sampling rate is set at 307.2 MHz, corresponding to 16 samples per symbol. This rate is chosen to allow us some room to perform upconversion and will be used for the remainder of the system. This RRC modulated signal is then multiplied by a complex exponential of the form $e^{i2\pi 38.4e6 t_k}$, this accomplishes the upconversion of the signal to an intermediate frequency of 38.4 MHz. Furthermore, another complex exponential, this time of the form $e^{i2\pi 153.6e6 t_k}$, is added to the signal, thus inserting a pilot tone at the intermediate frequency 153.6 MHz. This signal is then used to modulate the real and imaginary parts of a bandpass represented optical signal, which is simulated

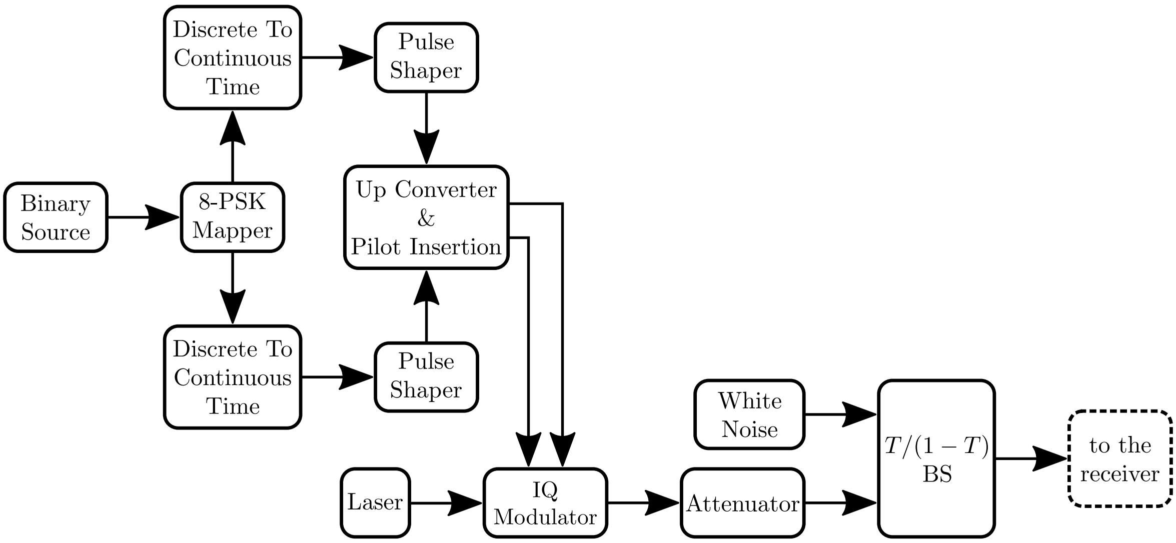


Figure 3.1: Block diagram of the transmitter and channel stages of the simulation.

with a power of 0 dBm. At each simulation time instant t_k, the simulated laser signal has an instantaneous phase given by [3]:

$$\phi_{t_k} = \phi_{t_{k-1}} + \Delta\phi, \tag{3.1}$$

where $\Delta\phi$ is a Gaussian random variable with null mean and variance $2\pi\Delta\nu|t_k - t_{k-1}|$, where, in turn, $\Delta\nu$ is the laser linewidth, which was set at 10 kHz, and $t_k - t_{k-1}$ is effectively the sampling time, Δt. Given the sampling rate mentioned previously, $\Delta t = \frac{1}{307.2\times 10^6} \sim 3.2552$ ns. This modulated signal is attenuated to $\sim$ 0.5 µW, corresponding to 0.2 photons per symbol, and then output from the transmitter stage and injected into the fibre. In Figure 3.2 is shown the signal at the output of the transmitter stage of the simulation, both as a spectrum and as a snapshot of the time domain signal. At this point the signal is assumed to be noiseless, thus the quantum signal in the spectrum in Figure 3.2 is clearly visible. Meanwhile, the transmission channel is modelled as a Beam Splitter (BS) with a transmission coefficient of T. This model is used for convenience, as from Bob's perspective it is indistinguishable from a lossy channel and it gives us an easy way to add excess noise is to the signal, by connecting a white-noise generating block, generating random values extracted from a Gaussian distribution with null mean and variance $\frac{T}{1-T}\epsilon$, to the open port of the BS block. The variance of the Gaussian distribution is chosen so as to cause the channel excess noise, ϵ, to be referred to the channel input. For the results presented here, ϵ=0.005 Shot Noise Units (SNU) was used.

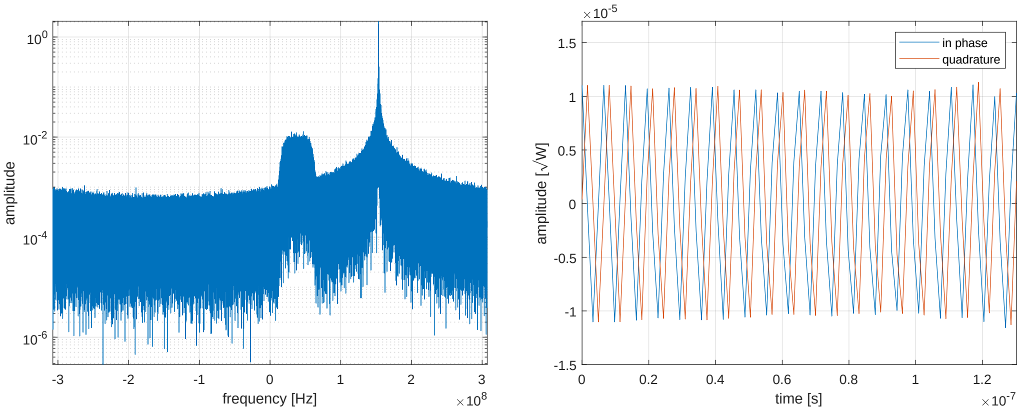


Figure 3.2: Spectral and time domain snapshot of the simulated optical signal at the output of the transmitter show in Figure 2.2.

A detailed block diagram of the receiver stage is presented in Figure 3.3. The noisy signal

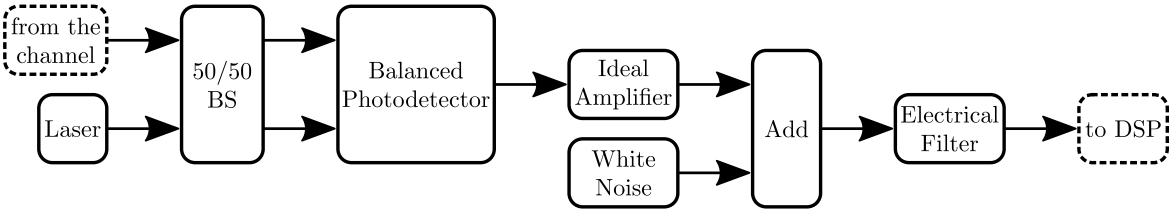


Figure 3.3: Block diagram of the receiver stage of the simulation.

from the fibre is mixed with a reference laser tone in a 50/50 BS block, the outputs of which are evaluated by a balanced photodiode pair. The photodiode pair block also adds shot noise to the signal. The energy in each time cell k of the simulation with mean optical power $\bar{P}_k$, is given by:

$$E_k = \bar{P}_k \Delta t, \tag{3.2}$$

the corresponding mean photon number is then given by:

$$\bar{n}_k = \frac{\bar{P}_k \Delta t \lambda}{hc}. \tag{3.3}$$

The photon number n of a coherent state follows a Poisson distribution with mean $\bar{n}$. It can be shown that the square root of a random variable with Poissonian distribution is a normally distributed random variable with standard deviation 1/2 [4], therefore the square root of the photon number can be modelled as:

$$\sqrt{n_k} = \sqrt{\frac{\bar{P}_k \Delta t \lambda}{hc}} + \frac{1}{2}x, \tag{3.4}$$

where x is a normally distributed random variable with zero mean and unitary standard deviation. This variable is the one responsible for the introduction of the shot noise into the optical signal. Thus, the optical power of the time cell k, with shot noise included, can be written as:

$$P_k = \bar{P}_k + \sqrt{\frac{\bar{P}_k hc}{\Delta t \lambda}}x + \frac{hc}{4\Delta t \lambda}x^2. \tag{3.5}$$

This signal is then amplified in a noiseless ideal amplifier, with thermal noise being added to the amplified signal by another white-noise generating block, generating random values extracted from a Gaussian distribution with null mean and variance $\epsilon_{\text{th}} = 0.3$ SNU. This amplified and noisy signal is then passed through a low-pass filter, with a cut-off frequency of 1.6 GHz, which serves to emulate the bandwidth of the Thorlabs receivers we will be using in our practical implementation. The signal at the output of the simulated receiver is presented in Figure 3.4, both as a spectrum and as a snapshot of the time domain signal. Due to the

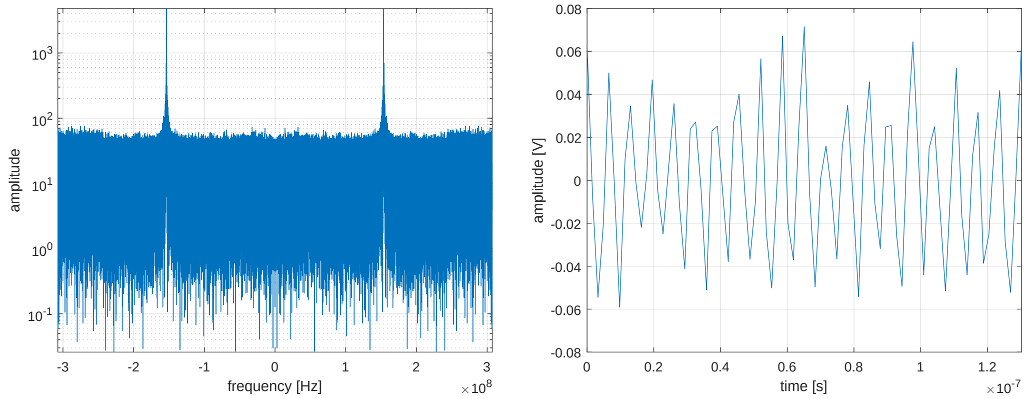


Figure 3.4: Spectral and time domain snapshot of the simulated electrical signal at the output of the receiver show in Figure 2.3.

addition of shot and thermal noise, the quantum signal is no longer visible in Figure 3.4, with only the pilot tone appearing above the noise floor. Given the relatively low sampling frequency of the simulation, the effect of the low-pass filter is not visible in Figure 3.4.

A detailed block diagram of the DSP stage of the simulation is presented in Figure 3.5, where simplified representations of the spectra at multiple stages of the DSP are included. The DSP stage starts by performing frequency recovery, where four copies of the input signal are taken and a tight digital pass-band filter, centered at $\tilde{f}_P = f_P + f_S$, is applied to one of them. Extracting the phase from this filtered signal and fitting it against a time-vector will yield an estimation for $\tilde{f}_P$. One of the other copies from the original signal is then downconverted by multiplying it by the complex oscillator $e^{-i2\pi \tilde{f}_P t_k}$, where t_k is a time-vector, thus placing the pilot signal close to base band. This signal will later be used for phase noise compensation. The third copy of the original signal is downconverted by another complex oscillator of the form $e^{-i2\pi\left(\tilde{f}_P + \frac{f_Q}{2}\right)t_k}$, which will cause the pilot to be located at roughly $\frac{f_Q}{2}$. This signal will later be used for clock recovery and aid in the Constant Modulus Algorithm (CMA) step. The fourth and final copy of the original signal is downconverted by a third complex oscillator of the form $e^{-i2\pi\left(\tilde{f}_P + \Delta f\right)t_k}$, where $\Delta f = f_Q - f_P$, resulting in the oscillator taking the explicit form $e^{-i2\pi\left(f_Q + f_S\right)t_k}$, this places the quantum signal at close to base band. Note

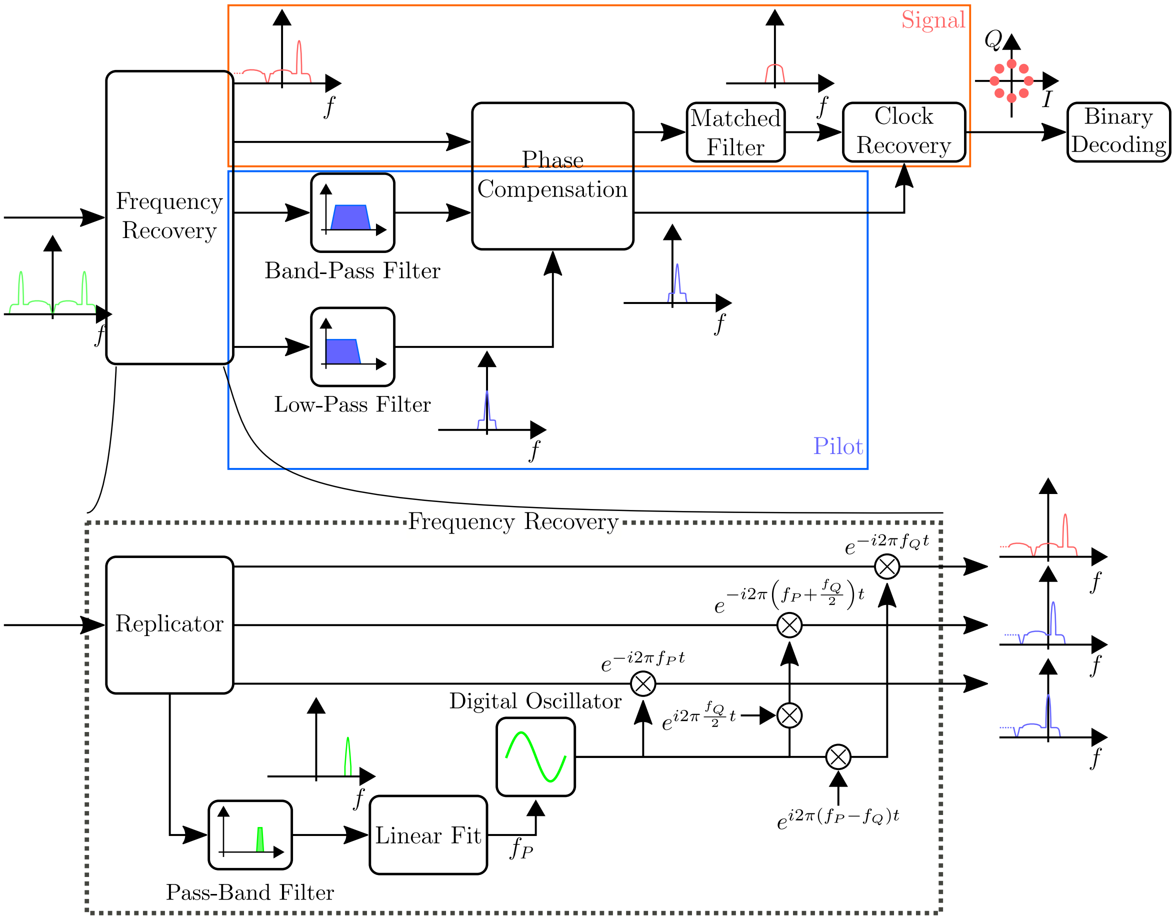
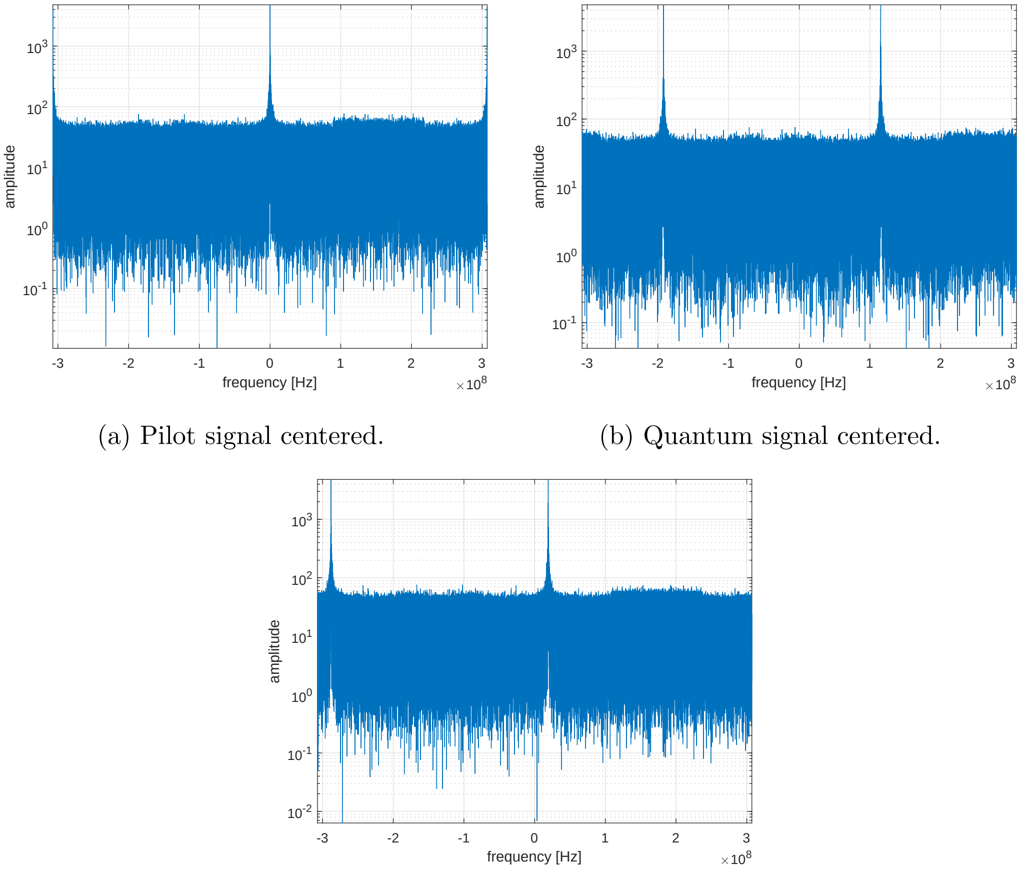


Figure 3.5: Block diagram of the DSP stage of the simulation

that the estimation of $\tilde{f}_P$ is assumed to contain errors. The outputs of the frequency recovery DSP step are presented in Figure 3.6. The action of the down converter can be observed by



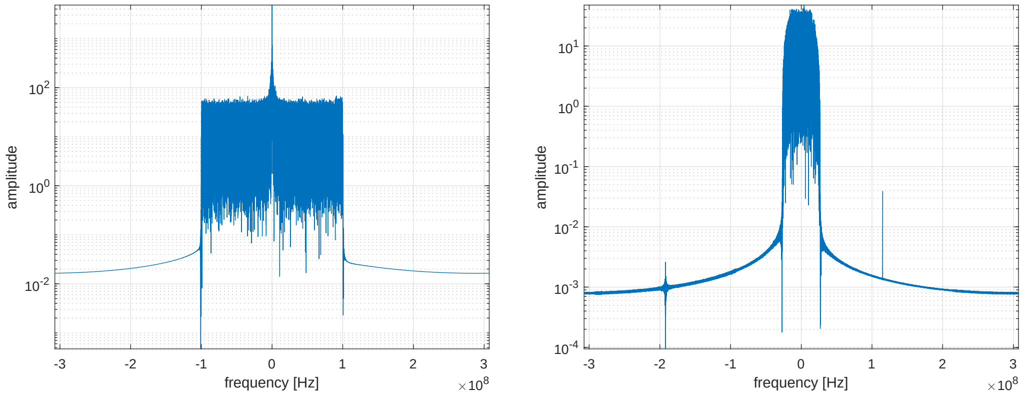
(a) Pilot signal centered.

(b) Quantum signal centered.

(c) Pilot downcoverted to serve as clock.

Figure 3.6: Spectra of the output from the down-converter block.

the relative position of the pilot tone, which is the only visible component of the signal. The frequency compensated pilot and clock signals are then passed through a low-pass and a band-pass filter, respectively. This filtering step will both reduce the noise present in the signals and isolate them from each other. The spectrum of the pilot signal after down conversion and filtering is presented in Figure 3.7a. The phase of the filtered pilot signal, which is equal to the phase mismatch between the two lasers apart from a constant value, which in turn is obtained during an initial calibration stage, is then extracted and used to compensate for the phase noise in both the quantum signal and the clock. Since the pilot and signal are sampled at the same instant, the phase mismatch estimated from the former will equal that of the latter, thus residual phase noise will arise mainly from amplitude noise degrading the accuracy of the estimation [5]. The phase compensated quantum signal is then passed through its own matched filter. The filtering stage on the quantum signal is postponed until after the phase compensation step, this is done because small errors in the frequency estimate can be corrected by the phase noise compensation and application of the matched filter on the signal while it is not at base band may cause distortion in the final obtained constellation. The



(a) Pilot signal after filtering.

(b) Spectrum of the filtered quantum signal.

Figure 3.7: Spectra of the filtering stage outputs.

quantum signal after filtering is presented in Figure 3.7b. Finally, the filtered clock is used to re-sample both itself and the filtered quantum signal to one sample per symbol, with one sample being taken of each for every 0 of the imaginary component of the clock signal. The final constellation obtained from the simulation is presented in Figure 3.8, where the different states are identified by different colours.

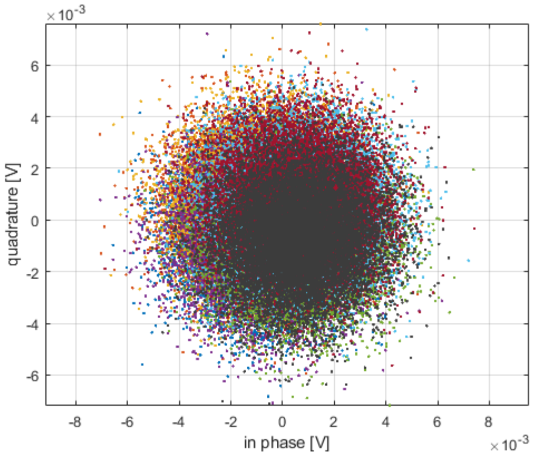


Figure 3.8: Final constellation recovered from the simulation.

3.2 Experimental implementation of Continuous Variables Quantum Key Distribution

Having successfully prototyped the CV-QKD system in a simulation environment, we now proceed to an experimental implementation of the same. There are some experimental impairments that, due to them not being implemented in the simulation platform, were not taken into account. The main such impairment is time dependent random polarization drift.

Random polarization drift occurs naturally in fibres subjected to vibrations, temperature fluctuations, and other perturbations [6]. Misalignments between the polarizations of the two laser fields interfering in the coherent detection scheme will severely reduce the efficiency of the detection scheme employed [5, 7]. In CV-QKD communication systems, polarization drift is typically avoided, during a limited time window, by manually aligning the polarization of the signal with that of the LO [5, 8]. This may be appropriate in a laboratory environment, where stability times are typically in the range of hours [7]. However, in field deployed fibres, especially aerially deployed ones, this stability will be on the order of minutes [6]. A CV-QKD system using an electronic polarization controller coupled with a dynamic feedback system was proposed in [7], using a transmitted LO design. However, this solution increases cost and introduces experimental complexity. Conversely, in classical communications, random polarization drift is compensated for by detecting both polarizations of the incoming light field and then compensating for the time-evolving drift in DSP [2]. A system employing DSP aided polarization mismatch recovery was presented in [9], using two optical hybrids coupled with four balanced coherent receivers.

We endeavoured to tackle this problem by implementing a polarization diverse receiver setup employing true heterodyne detection, for use in CV-QKD applications, is presented, requiring only two balanced receivers. The use of heterodyne detection allows us to use half the number of balanced coherent receivers than the system presented in [9], effectively halving the power requirements of the receiver. This is, to the best of our knowledge, the first demonstration of a true heterodyne polarization diverse receiver for CV-QKD systems. The presented system is able to achieve secure transmissions even in very adverse random polarization drift scenarios.

3.2.1 Polarization diverse receiver description

A block diagram of our system is presented in Figure 3.9. Alice starts by modulating the

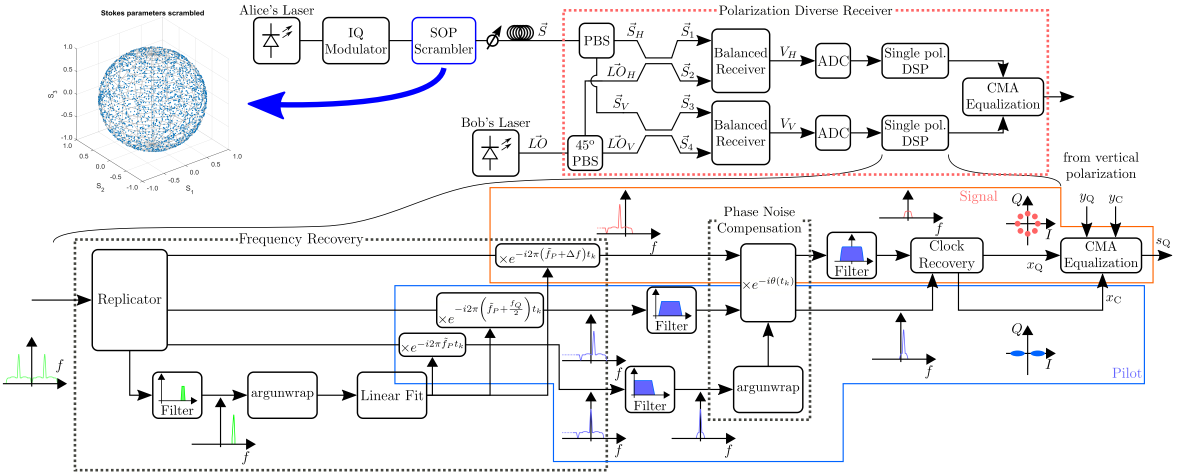


Figure 3.9: Block diagram of the experimental system, the polarization diverse receiver system is highlighted.

optical signal that she extracts from her local coherent source, which consists of a Yenista OSICS Band C/AG TLS laser, tuned to 1550.006 nm. RRC modulation is chosen because of the possibility of using matched filtering at the receiver without inter-symbolic interference [2], thus allowing for optimum Gaussian white-noise minimization. The symbol rate was set at 38.4 MBd (i.e. 38.4 million symbols per second), with an 8-phase-shift keying (8-PSK) constellation, the security of which, in the asymptotic regime, was established in [10] and has since been updated in [11]. In order to avoid the high levels of noise present in the low frequency part of the electromagnetic spectrum [12], the RRC signal is up-converted in the transmitter to an intermediate frequency, $f_Q = 38.4$ MHz. Furthermore, this signal is frequency multiplexed with a DC pilot tone, i.e. $f_P = 0$ Hz, which will be used for frequency and phase recovery at the receiver. This signal is fed into a Texas Instruments DAC39J84EVM digital to analog converter (DAC), which in turn drives a u2t Photonics 32 GHz single polarization IQ modulator coupled with a SHF807 RF amplifier and a YYLabs software bias controller. The single polarization modulated signal is first passed through a Thorlabs PL100S State Of Polarization (SOP) Locker/Scrambler, which allows us to scramble the polarization state of the signal. The action of the SOP Locker/Scrambler in scrambled mode is visible in the Poincaré sphere included as an inset. The results for this sphere were taken during 2 minute period. Note that the SOP Locker/Scrambler is used in order to emulate the polarization drift that would be observed in the field, thus it is not an integral part of the system and during normal operation it would not be included. After scrambling, the signal is then attenuated using a Thorlabs EVOA1550F variable optical attenuator until the signal has, on average 0.33 photons, per symbol. This value is calibrated by connecting the system in a back-to-back configuration and estimating the channel transmission. As in a back-to-back configuration the channel transmission is 1, any deviation from that value is actually a deviation from the desired output channel power. In a field implementation, this could be accomplished by having a copy of the receiver architecture at Alice's side or by using an optical spectral analyser. The signal is then sent through a single-mode fibre spool with a length of 40 km before arriving at the receiver. At the receiver side, the signal is first passed through a PBS, splitting its polarizations and sending each to different 50/50 BS, where they are mixed with the LO. The LO consists of a Yenista OSICS Band C/AG TLS laser tuned to 1549.999 nm, in this situation the signals have a frequency shift of $f_S \approx 1$ GHz, a value chosen to coincide with the flattest region of the balanced detectors' frequency response. The LO is also passed through a PBS, this one with its fast-axis shifted 45° in relation to the polarization alignment of the laser, effectively sending half the power to each individual 50/50 BS. Both 50/50 BS are polarization maintaining, ensuring that the polarization of both the signal and LO mixed in each match. The outputs of each 50/50 beam-splitter are fed into a pair of Thorlabs PDB480C-AC balanced optical receivers, connected to the inputs of a Texas Instruments ADC32RF45EVM ADC board, which is running at a sample rate of 2.4576 GS/s. A photo of our system assembled in laboratory is presented here in Figure 3.10. The two lasers of the system share the same OSICS mainframe and are located at the center of the setup in Figure 3.10. The IQ modulator is located at the extreme left of the setup in Figure 3.10, with the DAC and VOA placed on top of it. The 40 km single-mode fibre spool can be seen in Figure 3.10 on the upper shelf of the bench, above and slightly to the right of the OSICS mainframe. Meanwhile, the receiver assembly is located at the right of the photo in Figure 3.10, with the polarization diverse assembly placed just to the right of the OSICS mainframe, the optical receivers are at the back and the ADC at the far right.

The digitized signal is then fed into the DSP stage, which is also presented in Figure 3.9. The bulk of the DSP is performed independently for each polarization, before the recovered constellations from each polarization are combined in a CMA step. Finally, the filtered clock

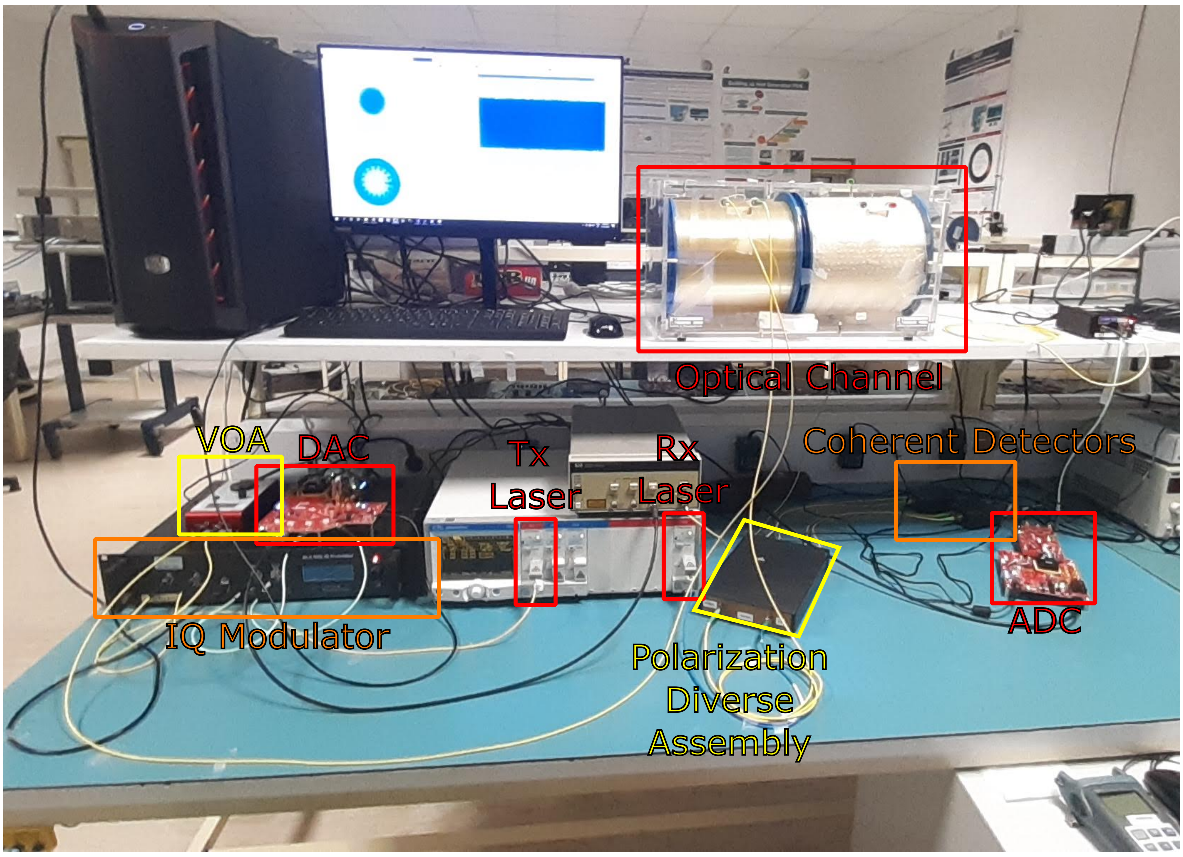


Figure 3.10: Photo of our experimental CV-QKD system assembled at our laboratory. Main components are highlighted and identified.

is used to re-sample both itself and the filtered quantum signal to one sample per symbol, with one sample being taken of each for every 0 of the imaginary component of the clock signal. At the end of this clock recovery step we are in the possession of four constellations, two corresponding to the clock constellations of the clock signal, x_{C} and y_{C}, and two to the quantum signal ones , x_{Q} and y_{Q}.

These four constellations are then fed into the CMA algorithm, which follows a modified version of the method presented in [2]. Sliding blocks of N samples of each of the four constellations are isolated, taking the form of the column vectors

$$\vec{x}_{\mathrm{Ci}}(n) = [x_{\mathrm{C}}(n)\ x_{\mathrm{C}}(n-1)\ ...\ x_{\mathrm{C}}(n-N)]^T, \tag{3.6}$$

$$\vec{y}_{\mathrm{Ci}}(n) = [y_{\mathrm{C}}(n)\ y_{\mathrm{C}}(n-1)\ ...\ y_{\mathrm{C}}(n-N)]^T, \tag{3.7}$$

$$\vec{x}_{\mathrm{Qi}}(n) = [x_{\mathrm{Q}}(n)\ x_{\mathrm{Q}}(n-1)\ ...\ x_{\mathrm{Q}}(n-N)]^T, \tag{3.8}$$

$$\vec{y}_{\mathrm{Qi}}(n) = [y_{\mathrm{Q}}(n)\ y_{\mathrm{Q}}(n-1)\ ...\ y_{\mathrm{Q}}(n-N)]^T. \tag{3.9}$$

At the start of the algorithm, i.e. blocks $\vec{x}_{\mathrm{Ci,Qi}}(0)/\vec{y}_{\mathrm{Ci,Qi}}(0)$, the vectors are composed of all zeros except for the first element, which will consist of the first element of the corresponding constellation. The other elements of the sliding blocks are then progressively filled up. The blocks for each signal are concatenated, resulting in the input column vectors [2]

$$\vec{u}_{\mathrm{Ci}}(n) = [\vec{x}_{\mathrm{Ci}}(n);\ \vec{y}_{\mathrm{Ci}}(n)], \tag{3.10}$$

$$\vec{u}_{\mathrm{Qi}}(n) = [\vec{x}_{\mathrm{Qi}}(n);\ \vec{y}_{\mathrm{Qi}}(n)]. \tag{3.11}$$

Two N-tap filters are created, $\vec{h}_{\mathrm{x}}$ and $\vec{h}_{\mathrm{y}}$, consisting also of column vectors. At the start of the algorithm the first element of $\vec{h}_{\mathrm{x}}$ and $\vec{h}_{\mathrm{y}}$ is set to $\frac{1}{\sqrt{2}}$, with all the others being 0. These two filters are concatenated,

$$\vec{h} = [\vec{h}_{\mathrm{x}};\ \vec{h}_{\mathrm{y}}], \tag{3.12}$$

with the resulting filter being applied to the input column vectors following

$$s_{\mathrm{C}}(n) = \vec{h}^{\dagger} \cdot \vec{u}_{\mathrm{Ci}}(n), \tag{3.13}$$

$$s_{\mathrm{Q}}(n) = \vec{h}^{\dagger} \cdot \vec{u}_{\mathrm{Qi}}(n), \tag{3.14}$$

which correspond to the clock and quantum output constellations, respectively. Note that both $\vec{h}$ and $\vec{u}_{\mathrm{Ci,Qi}}(n)$ are $2N \times 1$ column vectors, so for each of the inner products in (3.13) and (3.14), one output constellation point will be generated. After each step n, the "error", ε, of the algorithm is computed through [2]

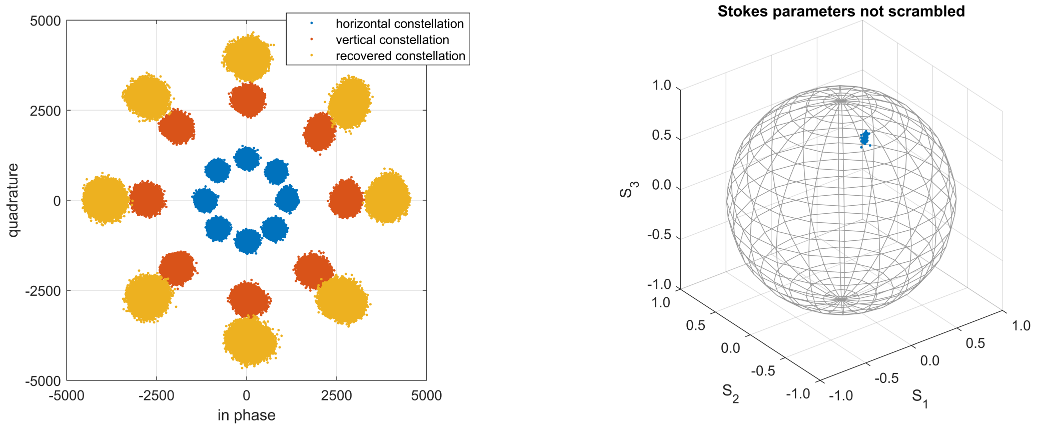
$$\varepsilon = \mathrm{E}[|\vec{x}_{\mathrm{C}}|] + \mathrm{E}[|\vec{y}_{\mathrm{C}}|] - s_{\mathrm{C}}(n), \tag{3.15}$$

which measures the distance of the amplitude of the latest output point of the clock constellation to the expected clock constellation amplitude. This "error" is then used to update the filter $\vec{h}$ through [2]

$$\vec{h} = \vec{h} + \mu\varepsilon s_{\mathrm{C}}^{*}(n)\vec{u}_{\mathrm{C}}(n) \tag{3.16}$$

The output clock constellation can then be discarded, while the quantum output constellation is carried forward. Due to our CMA algorithm working based on the pilot tone, more precisely the clock constellation, it is agnostic, i.e. applicable to any constellation that may be chosen for the quantum signal.

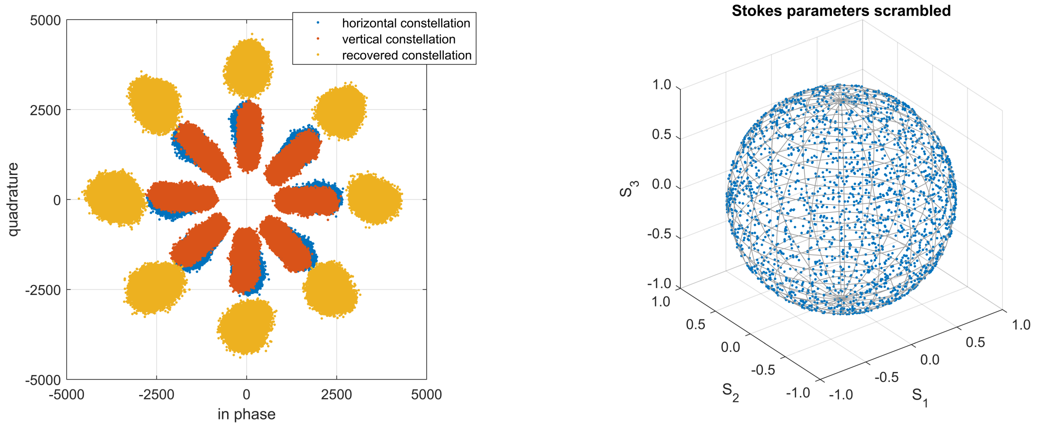
In order to show the performance of our polarization diverse system, we present here two sets of results obtained at a high power level, one with the SOP Locker/Scrambler set to lock the output polarization, presented in Figure 3.11, and one set to scramble the output polarization, presented in Figure 3.12. In both figures we show the constellations near the end of the DSP, showing the individual polarization constellations and the one recovered from the summation of the two, alongside a figure of the corresponding Stokes' parameters plotted on a Poincaré sphere. The scrambling of the polarization is clearly visible by the evolution of the Stokes parameters shown in Figures 3.11b and 3.12b. In the non-scrambled scenario (Figure 3.11b) the Stokes parameters remain roughly in the same point of the Poincaré sphere, whereas in the scrambled scenario (Figure 3.12b) the Poincaré sphere is almost completely filled due to the random polarization drift imposed by the SOP Locker/Scrambler. We can see from Figure 3.11a that, under low polarization noise scenarios, our system is capable of recovering the 8-PSK constellation without the need of any polarization adjustment (manual or electronic), maximizing SNR. Conversely, under a large polarization noise scenario, such as the one presented in Figure 3.12a, we can see that our system allows us to recover from the amplitude noise observed in the individual polarization constellations. For reference,



(a) Constellations.

(b) Stokes parameters.

Figure 3.11: Results obtained with SOP Locker set to lock.



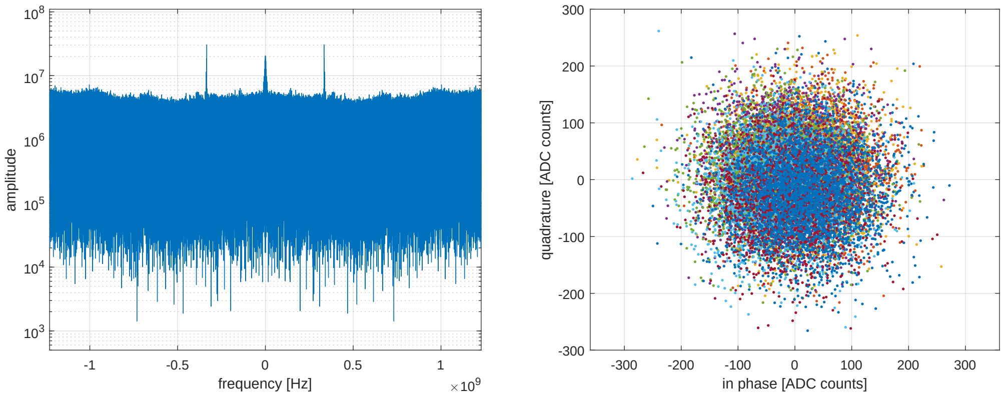
(a) Constellations.

(b) Stokes parameters.

Figure 3.12: Results obtained with SOP Locker set to scrambled.

in Figure 3.13 is shown the spectrum of the obtained electrical signal and the final obtained constellation obtained after the application of the DSP. In the spectrum shown in Figure 3.13a, the pilot is clearly seen at roughly 300 MHz, low frequency noise is also clearly visible as the band around 0 Hz. At this power level, the signal itself is not clearly visible in the spectrum. The constellation presented in Figure 3.13b, where the different states are identified by different colours, has an associated Bit Error Rate (BER) of 0.42, being well within the limits of the LDPC [13, 14].

The next step in the system is to estimate Bob's receiver noise. The shot and thermal noise estimations were made with recourse to a capture of the receiver output with the transmitter laser turned off and with both lasers turned off, respectively. To obtain precise shot and thermal noise figures, the same DSP that was applied to the quantum signal was applied to the shot and thermal noise captures obtained previously, with the noise captures being down converted, phase compensated, using the same frequency and phase recovery values utilized previously for the quantum constellation, and filtered before their variance was computed.



(a) Spectrum.

(b) Constellation.

Figure 3.13: Results obtained in the lab using 0.5 photons per symbol.

This was necessary because both are highly dependent on their spectral position, as can be seen in their spectra, shown here in Figure 3.14. To better illustrate the dominance of the shot noise over the thermal noise in our receiver, we also show in Figure 3.14 the spectrum of the shot to thermal noise clearance. Furthermore, we indicate the bandwidth utilized for data transmission in this experiment with two vertical lines. Since we cannot measure the shot noise without also including the thermal noise, the latter was obtained first and its value was subtracted from the variance of the former, yielding an estimate for the true shot noise. The variance of the shot and thermal noise signals, named here σ^2_{shot} and $\sigma^2_{\text{thermal}}$ respectively, are both expressed in ADC counts. Thermal noise is converted to Shot Noise Units (SNU) by dividing it by the shot noise estimate σ^2_{shot}, explicitly

$$\epsilon_{\text{thermal}} = \frac{\sigma^2_{\text{thermal}}}{\sigma^2_{\text{shot}}}. \tag{3.17}$$

The signal output by Bob's DSP is also converted to SNU, this in turn is accomplished by dividing the ADC count output by $\sqrt{\sigma^2_{\text{shot}}}$. Following the methods described in Section 2.3.1, Bob and Alice can then proceed to estimate the channel parameters and, subsequently, the security of the transmission. Note that, since the objective of this part of the work is to evaluate the capabilities of the polarization diverse receiver system, Finite Size Effects (FSE) are not taken into account during security evaluation.

3.2.2 Security impact of polarization drift

Protocol security is evaluated following the methodology presented previously in Section 2.3. In the following development we assume an ideal scenario, where the polarization beam-splitters split the polarizations with a perfect separation of $\frac{\pi}{2}$ and both employed receivers exhibit the same quantum efficiency and gain. Recall that the achievable secret key rate is given by

$$K = \beta I_{\text{BA}} - \chi_{\text{BE}}, \tag{3.18}$$

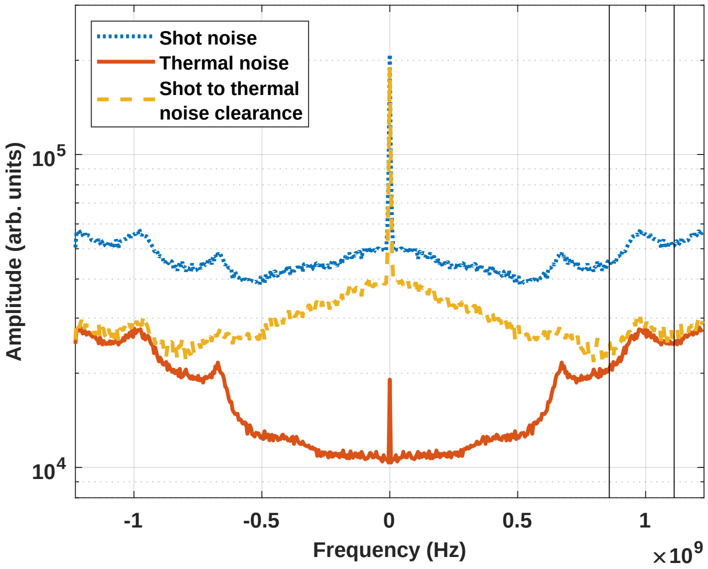


Figure 3.14: Spectra of the thermal and shot noise snapshots taken from the experimental system. The spectral region occupied by the data snapshots in this work are delimited by the vertical black lines.

---

where β is the reconciliation efficiency, I_{BA} is the mutual information between Bob and Alice, given by [10]

$$I_{\text{BA}} = \log_2\left(1 + \frac{2T\eta\,\langle n\rangle}{2 + T\eta\epsilon + 2\epsilon_{\text{thermal}}}\right). \tag{3.19}$$

The mutual information between Alice and Bob for each polarization channel can be obtained by taking (3.19) and scaling the transmission by the angle projection

$$I_{\text{BA,H}} = \log_2\left(1 + \frac{2T\cos^2(\theta)\eta\,\langle n\rangle}{2 + T\cos^2(\theta)\eta\epsilon + 2\epsilon_{\text{thermal}}}\right), \tag{3.20}$$

$$I_{\text{BA,V}} = \log_2\left(1 + \frac{2T\sin^2(\theta)\eta\,\langle n\rangle}{2 + T\sin^2(\theta)\eta\epsilon + 2\epsilon_{\text{thermal}}}\right), \tag{3.21}$$

where θ is the angle between the polarization of the quantum signal at the output of the fibre and that of the LO. In (3.18), χ_{BE} describes the Holevo bound that majors the amount of information that Eve can gain on Bob's recovered states, being obtained through [10].

$$\chi_{\text{BE}} = \sum_{i=1}^{2} G\left(\frac{\mu_i - 1}{2}\right) - \sum_{i=3}^{4} G\left(\frac{\mu_i - 1}{2}\right), \tag{3.22}$$

where

$$G(x) = (x+1)\log_2(x+1) - x\log_2(x). \tag{3.23}$$

In (3.22), $\mu_{1,2}$ are the symplectic eigenvalues of the covariance matrix describing the states shared by Alice and Bob while $\mu_{3,4}$ are the non-unitary symplectic eigenvalues of the covariance matrix that describes Bob's projective measurement.

For this development, we assume that Alice modulates only the horizontal polarization. The covariance matrix of the two-mode system at the output of Alice's system is given by [10]

$$\gamma_{\mathrm{A}} = \begin{bmatrix} V\mathbb{I}_2 & Z\sigma_Z \\ Z\sigma_Z & V\mathbb{I}_2 \end{bmatrix}, \tag{3.24}$$

where V is the variance of the signal at the output of the transmitter, Z is a measure of the covariance between the mode Alice keeps and the one she sends to the fibre, $\mathbb{I}_2$ is the 2×2 identity matrix and $\sigma_Z = \mathrm{diag}(1, -1)$. In order to study the effects of polarization drift, we expand γ_A by adding another mode, corresponding to the channel's vertical polarization

$$\gamma_{\mathrm{A,MP}} = \begin{bmatrix} V\mathbb{I}_2 & Z\sigma_Z & 0 \\ Z\sigma_Z & V\mathbb{I}_2 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \tag{3.25}$$

Note that, in these matrices of matrices, the 0 represent a 2×2 matrix of zeros. The matrix that describes the channel's polarization rotation by θ degrees is defined as [15]

$$J_{\mathrm{Ch}} = \begin{bmatrix} \cos(\theta)\mathbb{I}_2 & \sin(\theta)\mathbb{I}_2 \\ -\sin(\theta)\mathbb{I}_2 & \cos(\theta)\mathbb{I}_2 \end{bmatrix}, \tag{3.26}$$

where we have included the identity matrices, $\mathbb{I}_2$, to separate the effect along the real and imaginary parts of the signal, we assume that the polarization rotation does not cause cross-talk between the two. Combining this matrix with that of a beam-splitter with transmission coefficient T, yields the matrix that describes the full channel's action, both transmission and a polarization rotation, given by

$$\Lambda_{\mathrm{Ch}} = \begin{bmatrix} \sqrt{T} J_{\mathrm{Ch}} & \sqrt{1-T} J_{\mathrm{Ch}} \\ \sqrt{1-T} J_{\mathrm{Ch}} & \sqrt{T} J_{\mathrm{Ch}} \end{bmatrix}. \tag{3.27}$$

The full system with the unmixed noise mode is represented by the following covariance matrix

$$\gamma_N = \gamma_A \oplus \begin{bmatrix} (1 + \frac{T}{1-T}\epsilon)\mathbb{I}_2 & 0 \\ 0 & 0 \end{bmatrix}. \tag{3.28}$$

We assume here that the excess noise at the input of the channel is contained only in the horizontal polarization and that this noise will be distributed by the channel, alongside the signal. This corresponds to assuming that Eve has access to the signal at Alice's system output, before any polarization drift has occurred, and that she then causes the polarization rotation. Applying the channel transmission matrix to (3.28) as

$$\gamma_N' = (\mathbb{I}_2 + \Lambda_{\mathrm{Ch}})^T \gamma_N (\mathbb{I}_2 + \Lambda_{\mathrm{Ch}}), \tag{3.29}$$

where $\cdot^T$ indicates the transpose matrix. Equation (3.29) returns the modes at the output of the transmission channel, and selecting Alice's and Bob's modes returns

$$\gamma_{\mathrm{AB,MP}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}\cos(\theta)Z\sigma_Z & \sqrt{T}\sin(\theta)Z\sigma_Z \\ \sqrt{T}\cos(\theta)Z\sigma_Z & \cos^2(\theta)V_B\mathbb{I}_2 & \cos(\theta)\sin(\theta)V_B\mathbb{I}_2 \\ \sqrt{T}\sin(\theta)Z\sigma_Z & \cos(\theta)\sin(\theta)V_B\mathbb{I}_2 & \sin^2(\theta)V_B\mathbb{I}_2 \end{bmatrix}, \tag{3.30}$$

where

$$V_B = TV + 1 - T + T\epsilon. \tag{3.31}$$

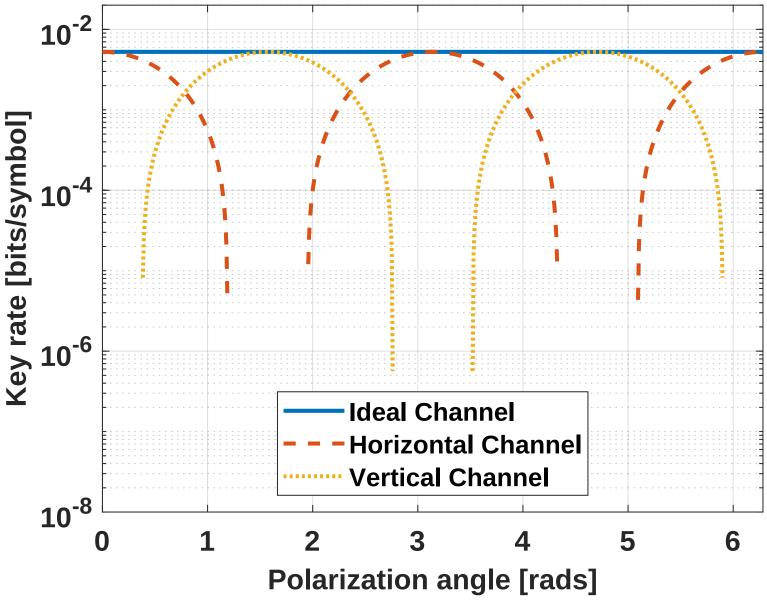


Figure 3.15: Key rate in function of the polarization angle for the vertical and horizontal polarization "channels". These key rates are not independent from each other, rather they are the key rates that would be observed if Bob were to monitor only one of the polarization channels. Parameters assumed were $\beta = 0.95$, $T = 0.1585$, $\epsilon = 0.03$ SNU, $\epsilon_{\text{th}} = 0.35$ SNU, $\langle n \rangle = 0.33$

By choosing either Bob's horizontal or vertical polarization, we obtain the covariance matrix for each channel individually

$$\gamma_{\text{AB,H}} = \begin{bmatrix} (V_{\text{A}} + 1)\mathbb{I}_2 & \sqrt{T}\cos(\theta) Z\sigma_Z \\ \sqrt{T}\cos(\theta) Z\sigma_Z & \cos^2(\theta) V_B \mathbb{I}_2 \end{bmatrix}, \tag{3.32}$$

$$\gamma_{\text{AB,V}} = \begin{bmatrix} (V_{\text{A}} + 1)\mathbb{I}_2 & \sqrt{T}\sin(\theta) Z\sigma_Z \\ \sqrt{T}\sin(\theta) Z\sigma_Z & \sin^2(\theta) V_B \mathbb{I}_2 \end{bmatrix}. \tag{3.33}$$

Following the methodology described in Chapter 2 to obtain $\mu_{1,2,3,4}$, we can obtain the mutual information between Eve and Bob for each polarization channel. From these mutual informations obtained from both (3.20)-(3.21) and (3.32)-(3.33), we can define the key rates that would be obtained if Bob were to monitor only one of the polarization channels

$$K_{\text{H}} = \beta I_{\text{BA,H}} - \chi_{\text{BE,H}}, \tag{3.34}$$

$$K_{\text{V}} = \beta I_{\text{BA,V}} - \chi_{\text{BE,V}}. \tag{3.35}$$

We can now trace both key rates in function of the polarization angle, results shown here in Figure 3.15, alongside the key rate expected from a channel without polarization drift. From the results in Figure 3.15, we can see the key rate's dependence on the polarization drift angle, with the key rate of each individual polarization channel exhibiting a maximum when the signal's polarization is aligned to it (polarization angles of $n\pi$ for the horizontal channel and of $(2n + 1)\pi$ for the vertical channel, $n \in \mathbb{N}$), and decreasing until it reaches a negative value as it misaligns. The maximum value corresponds to the key rate of the ideal, non-rotating channel. Note that these key rates should not be understood as independent from each other, but rather as the key rates that would be observed if Bob were to monitor only one of the polarization channels.

The application of a CMA-like algorithm to achieve full random drift polarization compensation can be described by the rotator matrix

$$\Lambda_{\text{CMA}} = \begin{bmatrix} h_{xx}\mathbb{I}_2 & h_{xy}\mathbb{I}_2 \\ h_{yx}\mathbb{I}_2 & h_{yy}\mathbb{I}_2 \end{bmatrix}, \tag{3.36}$$

to the multi-polarization covariance matrix (3.30). Parameters h_{xx} and h_{xy} are analogous to the vectors $\vec{h}_{\text{x}}$ and $\vec{h}_{\text{y}}$ from (3.12). Since we wish to recover the signal onto one of the polarizations, we can simplify (3.36) to

$$\Lambda_{\text{CMA}} = \begin{bmatrix} h_{xx}\mathbb{I}_2 & h_{xy}\mathbb{I}_2 \\ 0 & 0 \end{bmatrix}. \tag{3.37}$$

Since Bob controls this process, he can force h_{yx} and h_{yy} to be 0. Applying this rotator to (3.30) we get

$$\begin{aligned} \gamma'_{\text{AB,MP}} &= (\mathbb{I}_2 \oplus \Lambda_{\text{CMA}})^T \gamma_{\text{AB,MP}} (\mathbb{I}_2 \oplus \Lambda_{\text{CMA}}) \\ &= \begin{bmatrix} l(V_{\text{A}}+1)\mathbb{I}_2 & \sqrt{T}(h_{xx}\cos(\theta) + h_{yx}\sin(\theta))Z\sigma_Z & 0 \\ \sqrt{T}(h_{xx}\cos(\theta) + h_{yx}\sin(\theta))Z\sigma_Z & (h_{xx}\cos(\theta) + h_{yx}\sin(\theta))^2 V_{\text{B}}\mathbb{I}_2 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \end{aligned} \tag{3.38}$$

Note that the noise present in the two input polarization modes now appears in the recovered polarization mode. By discarding the empty polarization modes from (3.38), and setting $h_{xx} = \cos(\theta)$ and $h_{yx} = \sin(\theta)$, we obtain the final covariance matrix

$$\gamma_{\text{AB}} = \begin{bmatrix} (V_{\text{A}}+1)\mathbb{I}_2 & \sqrt{T}Z\sigma_Z \\ \sqrt{T}Z\sigma_Z & V_{\text{B}}\mathbb{I}_2 \end{bmatrix}, \tag{3.39}$$

which corresponds directly to the covariance matrix in [11], apart from $\sqrt{T}$ having been put in evidence. From this development we see that, assuming an ideal performance of the DSP stage, our CMA implementation is transparent to the covariance matrix, thus having no effect on security. A non-ideal performance of the CMA DSP step would result in the h_{xx} and h_{yx} parameters not equalling $\cos(\theta)$ and $\sin(\theta)$, respectively, but rather to follow some other angle ϕ. This would result in a degradation of the observed channel transmission, described here by the parameter $\eta_{\text{DSP}} = \cos(\phi)\cos(\theta) + \sin(\phi)\sin(\theta)$, from which definition it can be shown that $|\eta_{\text{DSP}}| \leq 1$. Since the same CMA DSP that is applied to the signal is then applied to the shot and thermal noise figures, the effect of the non-ideal application of the DSP will also be present in the shot noise estimate, thus its contribution in (3.31) will still be read as 1 and (3.39) becomes

$$\gamma_{\text{AB, non ideal}} = \begin{bmatrix} (V_{\text{A}}+1)\mathbb{I}_2 & \sqrt{\eta_{\text{DSP}}T}Z\sigma_Z \\ \sqrt{\eta_{\text{DSP}}T}Z\sigma_Z & (\eta_{\text{DSP}}TV + 1 - \eta_{\text{DSP}}T + \eta_{\text{DSP}}T\epsilon)\mathbb{I}_2 \end{bmatrix}, \tag{3.40}$$

from which we see that a non-ideal application of the CMA step will result in a degradation of the observed channel transmission. This degradation does not give any advantage to Eve, but rather reduces the system's performance.

3.2.3 System performance

The system was run freely for a half hour in scrambled mode and, for comparison purposes, fifteen minutes in unscrambled mode, with 2 ms snapshots taken every 10 seconds. The usage of the SOP Locker/Scrambler in the scrambled mode allows us to emulate the polarization drift that would be observed during an hours or days long experiment in minutes. This effect can also be observed in the Poincaré sphere included as an inset in Figure **??**, for which we monitored the SOP of the signal prior to the attenuation for only 2 minutes. In this work 200 snapshots were taken in the scrambled scenario and 100 in the unscrambled one, each snapshot containing 65536 symbols. Snapshots of the thermal and excess noises were obtained immediately before the data snapshots. The behaviour for the channel transmissions of both the single polarization and the recovered channels, in the scrambled scenario, are presented here in Table 3.1. From the results in Table 3.1 we can see that the single polarization channels exhibit a much lower average transmission and much higher variance of the transmission estimates, when compared to the values observed for the recovered channel. The average estimated transmission obtained from the constellations is also very close to the transmission that was measured a-priori, which took into account both the transmission of the 40 km spool and losses in the receiver. In Figure 3.16 we present the values of the estimated excess noise in the recovered channel observed for each of the 200 results taken in the scrambled mode. Situations where a secure key was able to be transmitted are highlighted with green asterisks. We can see that our system was able to recover secure keys for the duration of the experiment, with the excess noise being close to 0, apart from some deviations caused by failures in signal recovery. Some situations exhibit negative excess noise, these are not present in Figure 3.16 due to the use of a logarithmic scale, these can be attributed to the low number of samples used in this estimation. The average width of the 99% confidence interval for the excess noise estimates is roughly 3.5 SNU, while the average excess noise observed in our system is approximately 0.5 SNU. Nevertheless, negative excess noise estimations are not unheard off, having been reported in [5], and a contributing factor may be time-evolving imbalances of the optical components, a topic that is further explored in Chapter 5. Further optimization of the noise calibration step could improve the overall efficiency of the system. Finally, we show the experimentally observed secure key rates in function of channel transmission in Figure 3.17, alongside with the corresponding theoretical curve, for which the average values of the observed excess noise and thermal noise were used. Data from both scrambled and unscrambled polarization scenarios is included. We can see that our experimental results closely adhere to the theoretical curve and that the system performs equally in both situations. We see that, in both scenarios, we were able to achieve secure key rates of roughly 0.004 bits/symbol, slightly below that reported in [5], albeit using more accessible components. As mentioned before, the reduced number of symbols utilized, coupled

Table 3.1: Channel Transmissions for Single Polarization and Recovered Channels

Channel	$\mathrm{E}\left[\tilde{T}\right]$	$\mathrm{Var}\left[\tilde{T}\right]$
Horizontal	0.088	0.0064
Vertical	0.068	0.0047
Recovered Channel	0.113	0.0014
Actual Transmission	**0.116**	

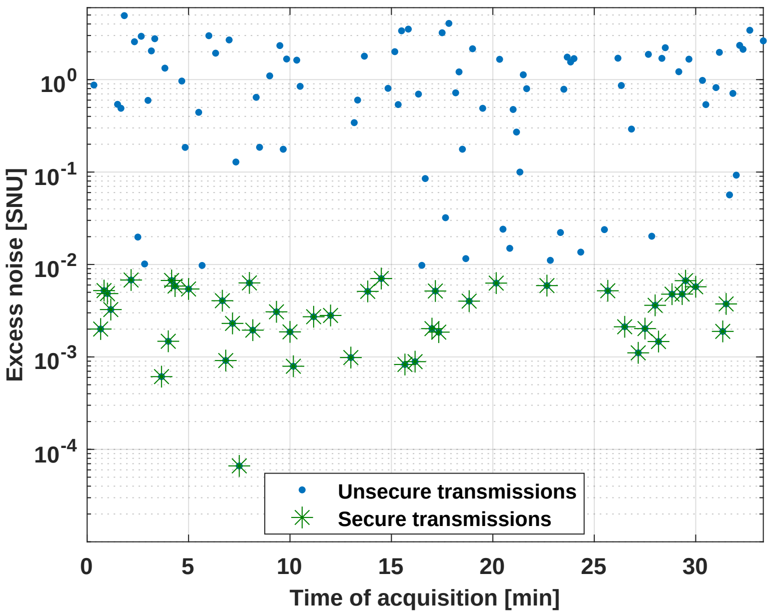


Figure 3.16: Evolution of the estimated excess noise for the 200 results taken. Situations where the a secure key was able to be transmitted are highlighted with green asterisks. Results taken in the scrambled scenario.

with the fact that post-processing is done offline, means that the security of our system remains a proof of concept one. No secure transmissions were observed for the individual polarization channels.

3.3 Lisbon field-trial

Having tested our system in the lab, we then proceeded to perform a field trial in Lisbon. The system described in Section 3.2 was used to connect the *Estado Maior General das Forças Armadas* building in Belém, where the transmitter stage was set up, to the *Centro de Manutenção Electrónica* in Monsanto, roughly 3 km away, where the receiver was located. A map pointing out the two locations connected is shown in Figure 3.18. The connection between the two buildings was done over an already deployed optical fibre. Photos of the transmitter and receiver stages of the communication system *in situ* are presented in Figure 3.19

A total of 4 C++ routines, 2 at the transmitter and 2 at the receiver, were written that allowed it to update the key being transmitted and recovered. The first routine at the transmitter side would generate a binary key of length 65538, where the first 3000 bits were a predetermined bit sequence known at both the transmitter and receiver sides and the remaining 62538 were a random sequence obtained using the default C++ *rand()* function. This binary key was then encoded, using the *netxpto* simulation environment, in a Root Raised Cosine (RRC) modulated signal, upconverted to 38.4 MHz and had a pilot added at 153.6 MHz. This modulated signal was then saved in a .csv file, with the second C++ routine loading and transmitting the file to the DAC board at the rate of one file per minute. This rate was chosen as to allow for synchronization between the transmitter and receiver stages. The first routine at the receiver side would command the ADC board to capture a snapshot of the

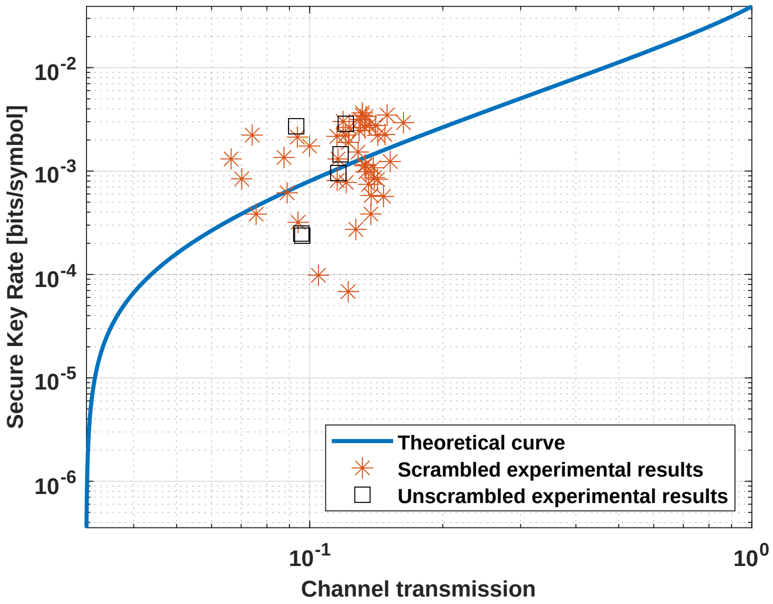


Figure 3.17: Achievable key rate, given by (3.18), for our polarization diverse receiver, with $\beta = 0.95$.

electrical signal being outputted by the two balanced receivers once per minute, then saving that capture to a .csv file. Synchronization with the transmitter stage was accomplished by starting the routine once a 10 MHz reference tone, used to synchronize the clocks of the DAC and ADC boards, was detected. This 10 MHz reference tone was shared by amplitude modulating a 1300 nm laser and sending it to the receiver through an auxiliary optical fiber, where it was evaluated using a PP-10G Nortel PIN Preamp Receiver. The second receiver routine consisted of the application of the DSP stage to the .csv files generated by the first routine. The DSP used the topology shown in Figure 3.9 and was followed by a decoding of the recovered constellation back to binary. This recovered binary was then subjected to a frame synchronization sub-routine, using the shared 3000 bits included in the transmitted signal to find the start of the random sequence, this random sequence was then outputted by the routine as a raw key.

The system was able to share raw keys autonomously for the full duration of the demonstration (which took around 2 hours), and was previously observed to work consistently for the entire afternoon of the previous day. The raw keys were sifted into symmetric keys using a Low Density Parity Check (LDPC) algorithm functioning in a reverse reconciliation mode (the transmitter keys where corrected to include the errors of the keys at the receiver), provided by Margarida Almeida, at the time with the Department of Physics of the University of Aveiro, and were then used to feed an encrypted text communication channel, provided by Ricardo Chaves from IT-Lisboa. Photographs of the communication windows at the transmitter and receiver systems are shown in Figure 3.20.

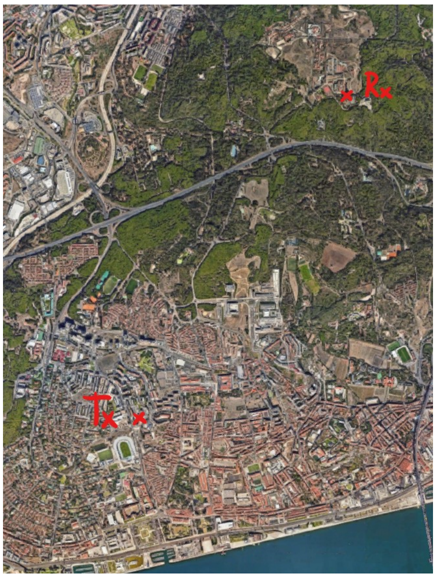
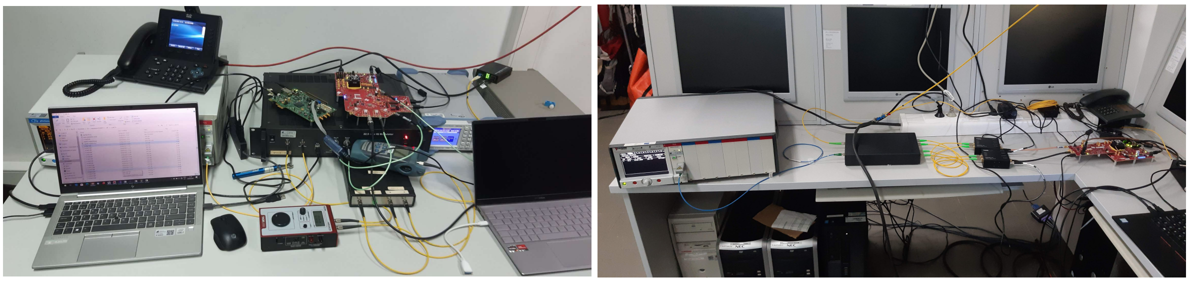


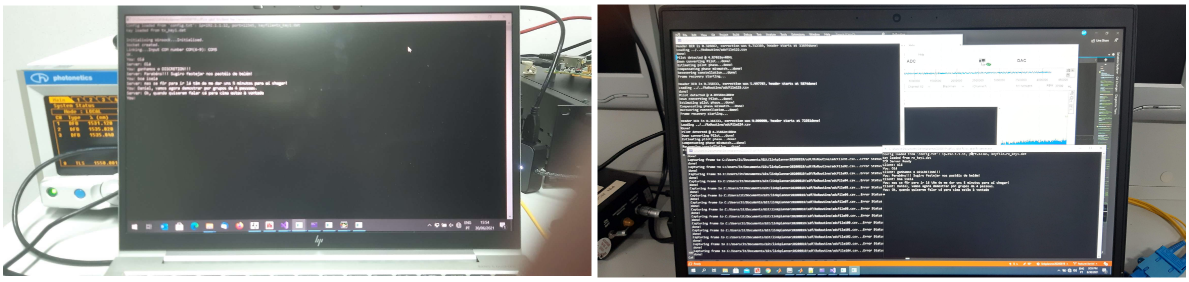
Figure 3.18: Map of the Belém and Monsanto region of Lisbon, pointing the two buildings connected in the field trial.



(a) Transmitter system.

(b) Receiver system.

Figure 3.19: Photos of the transmitter and receiver stages during the field trial in Lisbon.



```
Config loaded from 'config.txt': ip=192.1.1.12, port=12345, keyfile=tx_key1.dat
Key loaded from tx_key1.dat

Initialising Winsock...Initialised.
Socket created.
Linking...Input COM number COM(6-9): COM5
OK.
You: Olá
Server: Olá
You: ganhamos o DISCRETION!!!
Server: Parabéns!!! Sugiro festejar nos pastéis de belém!
You: boa ideia
Server: mas se fôr para ir lá têm de me dar uns 5 minutos para aí chegar!
You: Daniel, vamos agora demonstrar por grupos de 4 pessoas.
Server: Ok, quando quiserem falar cá para cima estao à vontade
You:
```

```
Header BER is 0.326667, correction was 4.712389, header starts at 33699done!
Loading ../../RxRoutine/adcFile122.csv
done!
Pilot detected @ 4.87032e+08Hz
Down converting Pilot...done!
Estimating pilot phase...done!
Compensating phase mismatch...done!
Recovering constellation...done!
Frame recovery starting...

Header BER is 0.350333, correction was 5.497787, header starts at 5874done!
Loading ../../RxRoutine/adcFile123.csv
done!
Pilot detected @ 4.89502e+08Hz
Down converting Pilot...done!
Estimating pilot phase...done!
Compensating phase mismatch...done!
Recovering constellation...done!
Frame recovery starting...

Header BER is 0.361333, correction was 0.000000, header starts at 72351done!
Loading ../../RxRoutine/adcFile124.csv
done!
Pilot detected @ 4.35662e+08Hz
Down converting Pilot...done!
Estimating pilot phase...done!
Compensating phase mismatch...done!
```

```
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile91.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile92.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile93.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile94.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile95.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile96.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile97.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile98.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile99.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile100.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile101.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile102.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile103.csv...Error Status
done!
Capturing frame to C:/Users/it/Documents/Git/linkplanner20200819/sdf/RxRoutine/adcFile104.csv...Error Status
done!
```

```
Config loaded from 'config.txt': ip=192.1.1.11, port=12345, keyfile=rx_key1.dat
Key loaded from rx_key1.dat
TCP Server Ready
Client: Olá
You: Olá
Client: ganhamos o DISCRETION!!!
You: Parabéns!!! Sugiro festejar nos pastéis de belém!
Client: boa ideia
You: mas se fôr para ir lá têm de me dar uns 5 minutos para aí chegar!
Client: Daniel, vamos agora demonstrar por grupos de 4 pessoas.
You: Ok, quando quiserem falar cá para cima estão à vontade
```

(a) Encrypted text channel at the transmitter side.

(b) Encrypted text channel at the receiver side.

Figure 3.20: Photos of the secure text link established between the transmitter and receiver stages during the field trial in Lisbon.

3.4 Summary

In this Chapter we started by presenting our simulated implementation of the system described previously in Chapter 2, where we also take care to showcase our developed DSP stage. We then proceeded to present a polarization diverse receiver architecture that avoids the need for manual calibration or complex feedback loops to recover from random polarization drift. Our proposed system works by detecting both polarizations independently and, after application of the DSP routine presented and tested previously in simulation, performing a modified CMA routine. We study the impact of polarization drift on security and show that our system, under an ideal scenario, is capable of fully mitigating it. We validated our proposed system experimentally both with an high-power classical signal and a low-power, quantum signal. Our system was capable of working for an indefinite period of time at a transmission distance compatible with metro network connections, and was able to generate 50 secure keys, in the asymptotic regime, from our 300 snapshots, with an average key rate of $\sim$0.001 bits/symbol. Finally, we presented some results from our Lisbon field trial, the first such trial of a CV-QKD system in Portugal. During the field trial the system was capable of sharing an updated key at a rate of one key per minute, being limited in this regard by the capability of the computer performing the DSP.

Bibliography

[1] Govind P Agrawal. *Fiber-optic communication systems*, volume 222. John Wiley & Sons, 2012.

[2] Md Saifuddin Faruk and Seb J Savory. Digital signal processing for coherent transceivers employing multilevel formats. *Journal of Lightwave Technology*, 35(5):1125–1141, 2017.

[3] R Paschotta. Phase noise.

[4] Norman L Johnson, Adrienne W Kemp, and Samuel Kotz. *Univariate discrete distributions*, volume 444. John Wiley & Sons, 2005.

[5] Sebastian Kleis, Max Rueckmann, and Christian G Schaeffer. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics letters*, 42(8):1588–1591, 2017.

[6] Rende Liu, Hao Yu, Jiye Zan, Song Gao, Liwei Wang, Mulan Xu, Jun Tao, Jianhong Liu, Qing Chen, and Yong Zhao. Analysis of polarization fluctuation in long-distance aerial fiber for qkd system design. *Optical Fiber Technology*, 48:28–33, 2019.

[7] Wenyuan Liu, Yanxia Cao, Xuyang Wang, and Yongmin Li. Continuous-variable quantum key distribution under strong channel polarization disturbance. *Physical Review A*, 102(3):032625, 2020.

[8] Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher, Michael Hentschel, Chi-Hang Fred Fung, Fotini Karinou, Andreas Poppe, Momtchil Peev, and Hannes Hübel. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*, 3:193, 2019.

[9] Tao Wang, Peng Huang, Shiyu Wang, and Guihua Zeng. Polarization-state tracking based on kalman filter in continuous-variable quantum key distribution. *Opt. Express*, 27(19):26689–26700, Sep 2019.

[10] A Becir, FAA El-Orany, and MRB Wahiddin. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10(01):1250004, 2012.

[11] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 2021.

[12] Robert B Tomer. *Getting the most out of Vacuum tubes: electron tubes valves*, volume 2. BOOK GEEK, 1960.

[13] Xiangyu Wang, Yi-Chen Zhang, Zhengyu Li, Bingjie Xu, Song Yu, and Hong Guo. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *arXiv preprint arXiv:1703.04916*, 2017.

[14] Hossein Mani, UL Andersen, T Gehring, C Pacher, S Forchhammer, JM Mateo, and M Vicente. Error reconciliation protocols for continuous-variable quantum key distribution. *Ph. D. dissertation, Technical University of Denmark*, 2021.

[15] Dennis H Goldstein. *Polarized light.* CRC press, 2017.

Chapter 4

Performance Optimization

In this Chapter the efforts made to further improve the performance of the Continuous Variables Quantum Key Distribution (CV-QKD) system described in Chapter 3 are presented.

This Chapter begins with an exploration on why performance improvements on CV-QKD systems are necessary and how these may be accomplished, presented in Section 4.1. In Section 4.2 we describe how the performance of a CV-QKD can be greatly improved using high-cardinality constellations coupled with Probabilistic Constellation Shaping (PCS). In Sub-Section 4.2.1 we present experimental results in which we show how our polarization diverse system was easily converted to these new constellation formats. The chapter concludes with a short description of how we tackled improving the Digital Signal Processing (DSP) performance by adding an auxiliary signal, presented in Section 4.3.

4.1 High performance CV-QKD

As was shown in Section 2.3, the performance of CV-QKD is highly dependent on the channel parameters [1]. Different modulation parameters have different security limits, thus a careful choice of modulation scheme is of high importance. CV-QKD can be grouped into Gaussian Modulation (GM) or Discrete Modulation (DM) [1] methods. GM-CV-QKD based systems allow for maximizing the transmitted information, as a result exhibiting an optimal theoretical secure key rate and resistance to excess noise [1]. However, GM-CV-QKD protocols have historically exhibited low reconciliation efficiency [2, 3], put an extreme burden on the transmitter's random number source [4] and tend to be more susceptible to imperfect state preparation [5]. As a result, the majority of experimental work done in CV-QKD uses DM [2]. DM-CV-QKD started by using Phase Shift Keying (PSK) constellations, 2-PSK and 4-PSK at first [1], followed quickly by the adoption of 8-PSK, the format that we have been using in this work so far. This increase in constellation order is done because it brings the performance of DM implementations closer to that of GM ones [6]. However we can see from the results presented in Figure 2.7 that the maximum admissible excess noise limits, even in the asymptotic regime, are quite low. In fact due to these limits, the experimental system we presented in Section 3.2 was only able to generate secure keys 25% of the time, while operating in the asymptotic regime. This is only exacerbated when finite size effects are taken into account, as is shown in Figure 2.8. For example, for the parameters used in Section 3.2, with a symbol frequency of 38.4 MBd (i.e. 38.4 million symbols per second), in order to even approach the transmission distance of 40 km utilized, symbols would have to be acquired during a time-frame of roughly one minute. This poses a very high a practical challenge, not only because the memory and processing required to accumulate and process so large a number of symbols is very high, but also because the stability times of the channel and receiver parameters are usually on the order of seconds [7]. This means that performance improvements again need to be explored through novel constellation formats. Further increasing the order of the PSK constellation does not produce an appreciable improvement [8], however, better results have been obtained by using M-symbol quadrature amplitude modulation (M-QAM) coupled with PCS [9]. M-symbol Amplitude and Phase Shift Keying (APSK) constellations can have the same number of symbols while using a smaller number of amplitude levels, thus exhibiting a peak-to-average power ratio 1.5 dB lower than that of an equivalent M-QAM constellation [10]. M-APSK constellations, also coupled with PCS, have been proposed for use in CV-QKD [3, 11]. Another avenue that can be explored to improve the performance of CV-QKD is the improvement of DSP performance, allowing for high numbers of symbols to be used in the parameter estimation stage and for the finite size performance to approach the asymptotic one as much as possible.

4.2 CV-QKD with high cardinality constellations

For this study we have chosen to look at the 128-APSK regular 16 (reg16), and 128-APSK irregular (ireg) constellations. To evaluate their performance, we will be comparing them with the 8-PSK constellation we have been using up until now, as well as the optimal Gaussian constellation. The states for these constellations are chosen from the alphabet [3]:

$$\chi = \left\{ \frac{p}{R} \alpha e^{ik\frac{2\pi}{M_p}},\ k = 0, 1, ..., M_p - 1,\ p = 1, 2, ...R \right\}, \tag{4.1}$$

where p is the ring's index (counting from the innermost to the outermost ring), α is the amplitude of the outer ring, k is the state's index within ring p and M_p is the number of states within ring p. Diagrams of the two constellations are presented here in Figure 4.1. The 128-APSK(ireg) constellation, which can be seen in Figure 4.1a, consists of 5 rings containing 4, 12, 16, 32 and 64 states, counting from the innermost to the outermost ring, while the 128-APSK(reg16) constellation, which can be seen in Figure 4.1b, consists of 8 rings, each with 16 states. The constellations' rings follow a binomial distribution, which means that a constellation with Q amplitude levels, $A_i, i \in \{1, ..., Q\}$, the probability of each amplitude i is given by [3]:

$$P_i = \frac{1}{2^{2Q-1}} \binom{2Q-1}{Q-i}. \tag{4.2}$$

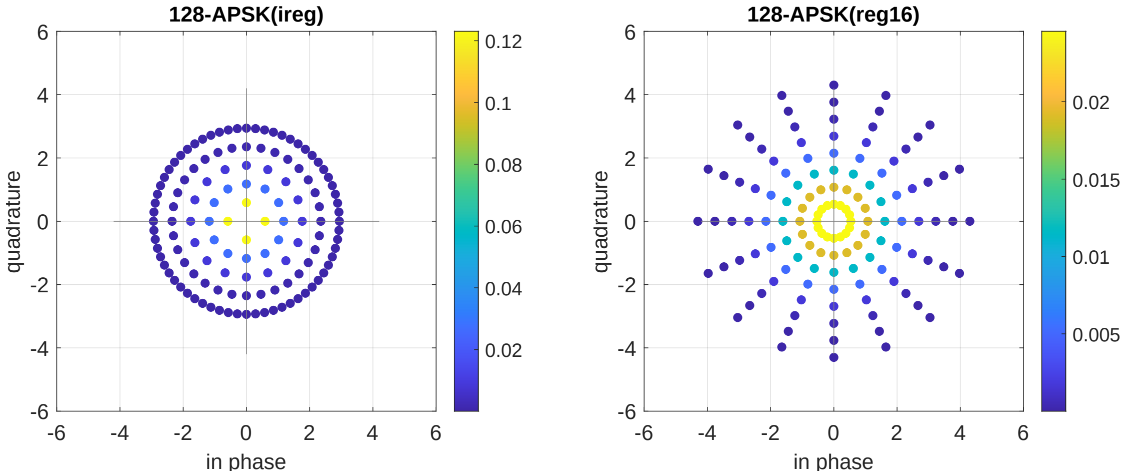
Within any given amplitude level, each state is equiprobable.

Recall that the achievable secret key rate is given by

$$K = \beta I_{\text{BA}} - \chi_{\text{BE}}, \tag{4.3}$$

where β is the reconciliation efficiency, I_{BA} is the mutual information between Bob and Alice, given by [6]

$$I_{\text{BA}} = \log_2(1 + \text{SNR}) = \log_2 \left(1 + \frac{2T\eta \langle n \rangle}{2 + T\eta\epsilon + 2\epsilon_{\text{thermal}}} \right), \tag{4.4}$$



(a) Scatter diagram of the irregular 128-APSK constellation with binomial distribution of the amplitudes. Individual state probability identified by color.

(b) Scatter diagram of the 16-state, regular 128-APSK constellation with binomial distribution of the amplitudes. Individual state probability identified by color.

Figure 4.1: Scatter diagrams of the irregular and regular 128-APSK constellations, coupled with binomial distribution of the amplitudes.

and χ_{BE} describes the Holevo bound that majors the amount of information that Eve can gain on Bob's recovered states, being obtained through [6]

$$\chi_{\mathrm{BE}} = \sum_{i=1}^{2} G\left(\frac{\mu_i - 1}{2}\right) - \sum_{i=3}^{4} G\left(\frac{\mu_i - 1}{2}\right), \tag{4.5}$$

where

$$G(x) = (x+1)\log_2(x+1) - x\log_2(x). \tag{4.6}$$

In (4.4), SNR stands for Signal to Noise Ratio, T is the channel transmission, $\langle n \rangle$ is the average number of photons per symbol, η is the quantum efficiency of the photodetectors, ϵ is the channel excess noise and $\epsilon_{\mathrm{thermal}}$ is the receiver's electronic noise. In (4.5), $\mu_{1,2}$ are the symplectic eigenvalues of the covariance matrix describing the states shared by Alice and Bob

$$\gamma_{\mathrm{AB}} = \begin{bmatrix} (2\langle n \rangle + 1)\mathbb{I}_2 & \sqrt{T}Z\sigma_Z \\ \sqrt{T}Z\sigma_Z & (2T\langle n \rangle + 1 + T\epsilon)\mathbb{I}_2 \end{bmatrix}. \tag{4.7}$$

while $\mu_{3,4}$ are the non-unitary symplectic eigenvalues of the covariance matrix that describes Bob's projective measurement, the method through which this last matrix can be obtained is described in detail in Section 2.3. In (4.7), $\mathbb{I}_2$ is the 2×2 identity matrix, $\sigma_Z = \mathrm{diag}(1, -1)$ and the Z parameter is a measure of the correlation between the states at the transmitter and receiver, being given by

$$Z = 2\mathrm{tr}(\hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{\frac{1}{2}}\hat{a}^{\dagger}) - \sqrt{2\epsilon W}, \tag{4.8}$$

where $\hat{\rho}$ is the density operator for the M-symbol discrete constellation defined by

$$\hat{\rho} = \sum_{k=1}^{M} p_k \left|\alpha_k\right\rangle \left\langle\alpha_k\right|, \tag{4.9}$$

and [8]

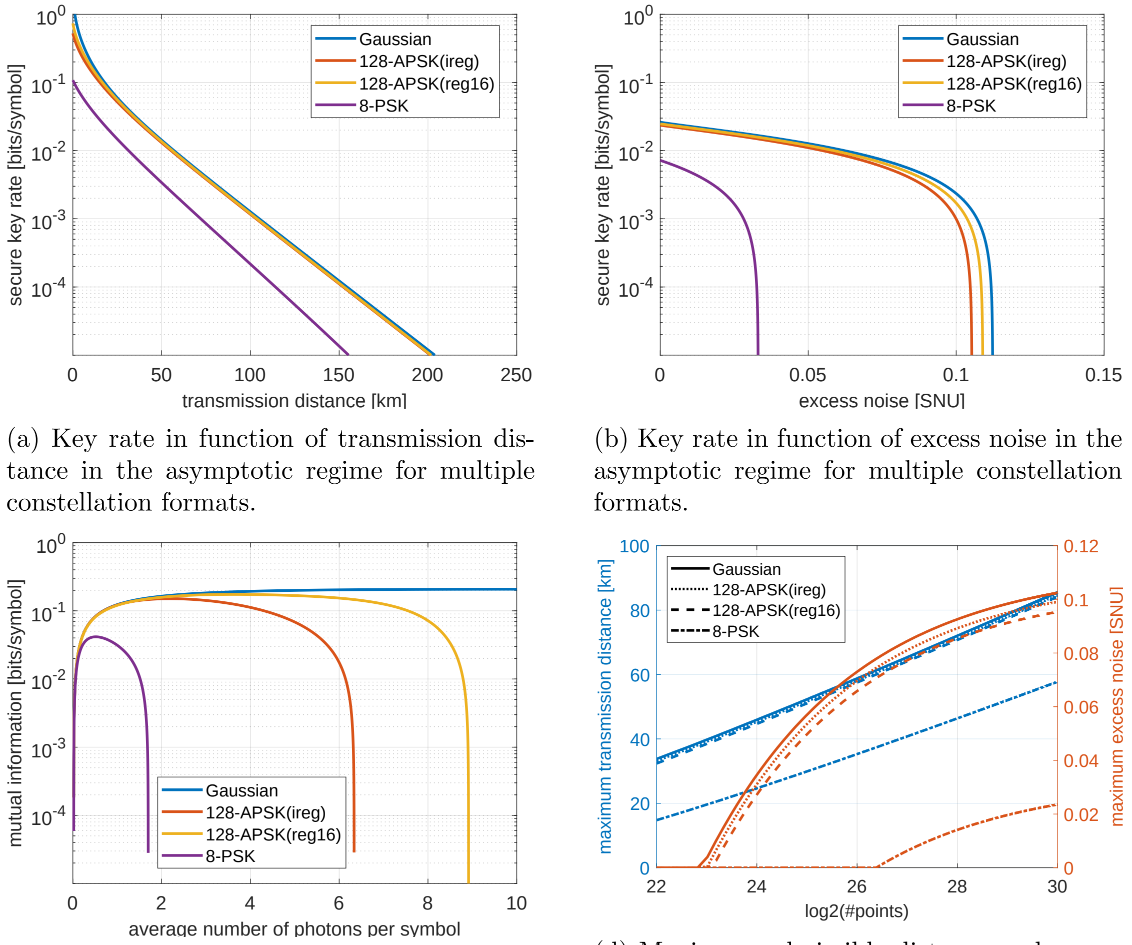
$$W = \sum_{k=1}^{M} p_k(\langle\alpha_k|\, \hat{a}_\rho^\dagger \hat{a}_\rho \,|\alpha_k\rangle - |\, \langle\alpha_k|\, \hat{a}_\rho \,|\alpha_k\rangle \,|^2) \tag{4.10}$$

and, finally,

$$\hat{a}_\rho = \hat{\rho}^{\frac{1}{2}} \hat{a} \hat{\rho}^{-\frac{1}{2}}. \tag{4.11}$$

The exact methodology to compute χ_{BE} can be found in [8]. The method for obtaining the symplectic eigenvalues is explored in depth in Section 2.3.

In Figure 4.2 we present results comparing the performance of different constellation formats. For these results, and unless otherwise noted, the parameters assumed are: $T = 0.15849$, $\eta = 0.90$, $\beta = 0.95$, $\epsilon = 0.005$ SNU, $\epsilon_{\text{th}} = 0.3$ SNU and $\langle n \rangle$ was optimized for each situation. Figure 4.2a shows the key rate in function of the transmission distance for the multiple con-



(a) Key rate in function of transmission distance in the asymptotic regime for multiple constellation formats.

(b) Key rate in function of excess noise in the asymptotic regime for multiple constellation formats.

(c) Key rate in function of the average number of photons per symbol in the asymptotic regime for multiple constellation formats.

(d) Maximum admissible distance and excess noise in function of number of symbols used for multiple constellation formats.

Figure 4.2: Performance and security limit comparisons between different constellation formats of a CV-QKD system. Unless when under study, a transmission distance of 40 km and a *true* excess noise value of 0.005 SNU were assumed.

stellation formats assumed, in the asymptotic regime. We can see that there is a considerable performance improvement, with an increase of ~50 km in maximum achievable distance, from the 8-PSK to the 128-APSK constellations, with the latter constellations exhibiting, for the parameters assumed here, almost the same performance as the optimal, Gaussian one. Figure 4.2b shows the key rate in function of the channel excess noise for the multiple constellation formats assumed, in the asymptotic regime. Again we see a dramatic improvement in performance from the 8-PSK to the 128-APSK constellations, with the maximum admissible noise jumping from under 0.01 SNU to over 0.10 SNU, with the Gaussian constellation exhibiting a slightly higher excess noise resistance. Figure 4.2c shows the key rate in function of the photon number, in the asymptotic regime. We see that the 8-PSK constellation not only has a considerably lower performance, but also can only use a very limited number of photons per symbol, generating no key for $\langle n \rangle > 1.7$. Meanwhile, the 128-APSK(ireg) and 128-APSK(reg16) can use up to 6.3 and 8.9 photons per symbol. Taking into account that the SNR is proportional to the number of photons per symbol and recalling from (2.3) that the reconciliation efficiency, β, depends on the SNR, which in turn scales linearly with the number of photons, $\langle n \rangle$, the ability to use of a higher number of photons carries a great advantage. Finally, Figure 4.2d shows the maximum achievable transmission distance and maximum admissible excess noise in the finite size scenario, described in Section 2.3.1, for a confidence interval of 10^{-10} in function of the number of samples used in the estimation. We see a dramatic improvement in for the maximum values of both parameters, with the 128-APSK constellations being able to reach a maximum distance roughly 20 km greater than the 8-PSK one while using the same number of symbols, and being able to work with a much higher excess noise, for example resisting an excess noise of 0.02 SNU using only $\sim 2^{-6} = 1.5\%$ as many symbols. This dramatic drop in the the number of samples required greatly simplifies practical implementations, as both the processing power for the DSP and channel stability time requirements are drastically reduced.

The general approach of the performance of the 128-APSK constellations to that of the Gaussian one can be understood as arising from these constellations looking more and more like a two dimensional Gaussian distribution. This improvement in performance is achievable by simply performing slight changes to the pre- and post-processing of the system, making this solution highly desirable.

4.2.1 Experimental verification

We then proceeded to implement the new constellation formats explored here in the experimental system described in Section 3.2. A block diagram of the system used for this trial is presented in Figure 4.3. Alice starts by modulating the optical signal that she extracts from her local coherent source, which consists of a Yenista OSICS Band C/AG Tuneable Laser Source (TLS), tuned to 1550.004 nm. We again adopt Root Raised Cosine (RRC) modulation because of the possibility of using matched filtering at the receiver without inter-symbol interference [12], thus allowing for optimum Gaussian white-noise minimization, and set the symbol rate was at 153.6 MBd. The RRC signal is then up-converted in the transmitter to an intermediate frequency, $f_Q = 153.6$ MHz, and frequency multiplexed with a DC pilot tone, i.e. $f_P = 0$ Hz, which will be used for frequency and phase recovery at the receiver. This signal is fed into a Texas Instruments DAC39J84EVM Digital to Analog Converter (DAC), which in turn drives a u2t Photonics 32 GHz IQ modulator coupled with a SHF807 RF amplifier. The modulated signal is then attenuated using a Thorlabs EVOA1550F variable

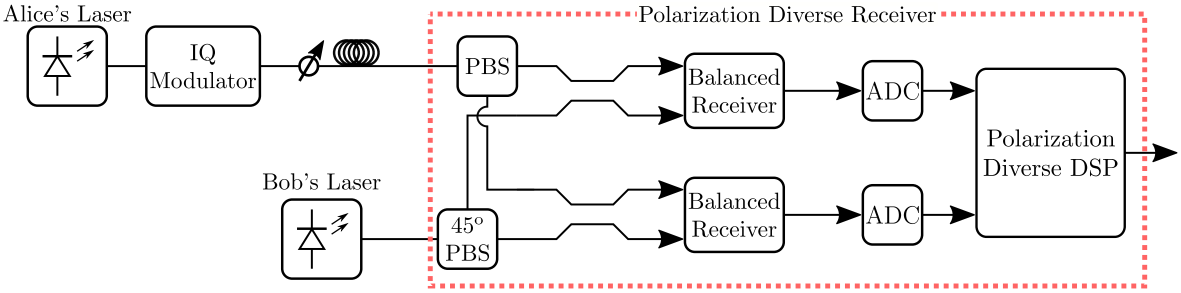


Figure 4.3: Block diagram of the experimental system. An in depth description on the applied DSP is presented in Chapter 3.

optical attenuator until the signal has, on average, 1.29 photons per symbol for the irregular and 1.91 photons per symbol for the regular constellation. The signal is then sent through a single-mode fibre spool with length 40 km before arriving at the receiver. At the receiver side, the signal is fed into a polarization diverse receiver, where it is mixed with the Locally generated Local Oscillator (LLO). The LLO consists of a Yenista OSICS Band C/AG TLS tuned to 1549.999 nm. In this situation, the signals have a frequency shift of $f_S \approx 800$ MHz. The mixed optical signals are evaluated by a pair of Thorlabs PDB480C-AC balanced optical receivers, connected to the inputs of a Texas Instruments ADC32RF45EVM Analog to Digital Converter (ADC) board, which is running at a sample rate of 2.4576 GS/s. The digitized signals are then fed into the digital signal processing (DSP) stage, where they are subjected to frequency, phase and clock recovery, steps which are aided by the pilot tone inserted at f_P, and matched filtering. For a more detailed description of the polarization diverse receiver, see Section 3.2. The state sequences present at the transmitter and receiver were synchronized through the use of a known header of 3000 states inserted at the start of the sequence by Alice, with Bob computing a the Error Vector Magnitude (EVM) of a sliding window of the states he recovers from the channel, with the sequences being synchronized when the BER is minimum.

As stated previously, for the results presented in this work $\langle n \rangle$ was set at 1.29 photons per symbol for the 128-APSK(ireg) scenario and at 1.91 photons per symbol for the 128-APSK(reg16) scenario. Meanwhile, $\tilde{\epsilon}$ and $\epsilon_{\text{thermal}}$ were dynamically estimated for each experimental measurement run. The shot and thermal noise estimations were made with recourse to captures of the receiver output with the transmitter laser turned off and with both lasers turned off, respectively. To obtain precise shot and thermal noise figures, the same DSP that was applied to the quantum signal was applied to the data collected for the shot and thermal noise estimation, being down converted, phase compensated and filtered before their variance was computed. Meanwhile, the values of $\tilde{\epsilon}$ and $\epsilon_{\text{thermal}}$ used for the theoretical curves in Figures 4.5 and 4.6 were the average of the experimentally observed ones. Lastly, η was measured as 0.72.

Recall that Alice's and Bob's constellations, a and b respectively, are related by the normal linear model [1]:

$$b = ta + z, \tag{4.12}$$

where $t = \sqrt{\eta T}$ and z is the noise contribution, following a normal distribution with null mean and variance

$$\sigma^2 = 2 + 2\epsilon_{\text{th}} + \eta T \epsilon. \tag{4.13}$$

We can estimate t through:

$$\tilde{t} = \frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{a_i b_i^*}{|a_i|^2}\right\} = \frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{a_i (t a_i)^*}{|a_i|^2}\right\} + \frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{a_i z_i^*}{|a_i|^2}\right\}, \tag{4.14}$$

since z has zero mean, the second term in (4.14) will cancel out, yielding

$$\tilde{t} = t\frac{1}{k}\mathrm{Re}\left\{\sum_{i=1}^{k}\frac{|a_i|^2}{|a_i|^2}\right\} = t. \tag{4.15}$$

Meanwhile, σ^2 can be estimated through

$$\tilde{\sigma}^2 = \frac{1}{k}\sum_{i=1}^{k}(b_i - \tilde{t}a_i)^2 = \frac{1}{k}\sum_{i=1}^{k}(z_i)^2. \tag{4.16}$$

This topic is further explored in Section 2.3.1. Note that for the results presented in this Section, the finite size effect is not taken into consideration due to memory limitations. The experimental system was run continuously for roughly one hour and a half, with 7 ms snapshots taken every 30 seconds. The time between acquisitions was due to the limitations of the ADC available in our laboratory. A total of 200 snapshots were taken, each containing 1048576 symbols. In order to achieve security in the finite size scenario with our constellation formats, approximately 8 times as many symbols would have had to have been captured in order to achieve security with a 10^{-10} confidence level [13], which is not possible due to our post-processing hardware capabilities. This, coupled with the fact that post-processing is done offline, means that our system remains a proof of concept one, albeit one with very promising results.

In Figure 4.4 we present the evolution of the excess noise as a function of the acquisition time. The theoretical excess noise limits for a secure transmission using 8-PSK, irregular and regular PCS-128-APSK and Gaussian constellations, at a transmission distance of 40km, are also included, as a dashed line, a dotted line, a dash-dot line and a full line, respectively. For the theoretical limits of the Gaussian and 8-PSK constellations, 2.40 and 0.33 photons per symbol were assumed, respectively. When a point is located bellow a certain line, it would mean a transmission in those conditions would be secure. We can see that there is a considerable increase from the security limit of the 8-PSK to that of the irregular PCS-128-APSK, meaning that the system is able to transmit secure keys 1.9x more often than if it were using an 8-PSK constellation, all while using the same, fully telecom-grade equipment. Meanwhile, switching to a GM system would only lead to a 1.1x increase over the irregular PCS-128-APSK constellation in the number of secure keys, a less dramatic increase. Note that the system was not finely tuned beforehand, so we believe that this experiment decently approximates a real-world scenario. Crucially, our system was able to generate secure keys for the duration of the acquisition time. We also perform a comparative study between the irregular and regular PCS-128-APSK constellations, also shown in Figure 4.4, where a graphic inset shows the region immediately around the security limit in greater detail. For the situation presented in this work, the use of a regular constellation would lead to only a 0.5% increase in the number of transmitted keys. However small this increase, it is achieved with only a small alteration in the pre- and post-processing algorithms and both retain the same advantage in ease of implementation when compared to the GM case. Again, in this scenario our system was able to generate secure keys for the duration of the experiment.

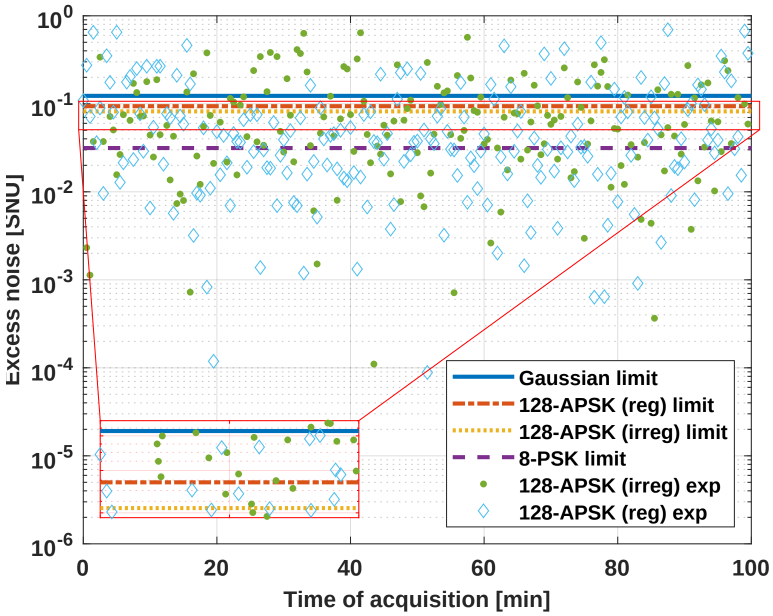


Figure 4.4: Evolution of the estimated excess noise for the 200 snapshots taken of both the irregular and regular 128-APSK constellations. Theoretical limits for the 8-PSK, 128-APSK, irregular and regular, and Gaussian constellations are included. A zoomed inset, showing the region between the theoretical limits of the 128-APSK constellations and the Gaussian one, is also included.

In Figure 4.5, the secure key rate, obtained through (4.3), as a function of the observed excess noise is presented. Experimental results, using instantaneous measurements of the channel transmission, excess noise and thermal noise, are presented as dots and squares, for the irregular and regular PCS-128-APSK constellations, respectively. The trend lines for the irregular PCS-128-APSK, regular PCS-128-APSK and Gaussian constellations are presented as a dashed line, a dash-dot line and a full line, respectively. In obtaining these theoretical trend lines, the average observed channel transmission, $\tilde{T} = 0.142$, and the average observed thermal noise, $\epsilon_{\text{thermal}} = 0.35$ SNU, are used. From Figure 4.5, we can see that the regular constellation has a slightly higher resistance to excess noise when compared to the irregular one, and that in both cases the performance of our system as a function of excess noise is quite close to that of an equivalent GM system, when sufficiently far away from the noise limit value, with the advantage of a simpler key reconciliation stage.

In Figure 4.6 we present the secure key rate as a function of the transmission distance. The mean experimental result for the regular PCS-128-APSK constellation is presented as a star, with its theoretical line consisting of a dash-dot line, the mean experimental result for the irregular PCS-128-APSK constellation is presented as a square, with its theoretical line consisting of a dashed line, and the theoretical curve for a Gaussian constellation is presented as a full line. The average excess noise in each experiment, 0.035 SNU in the irregular and 0.026 SNU in the regular one, was used for their corresponding theoretical curve, while for the GM curve the average of the two excess noises was used. For all of these, the asymptotic regime was assumed. Here we see that, under the observed experimental parameters, the regular PCS-128-APSK constellation would theoretically be able to reach distances of upwards of 185 km,

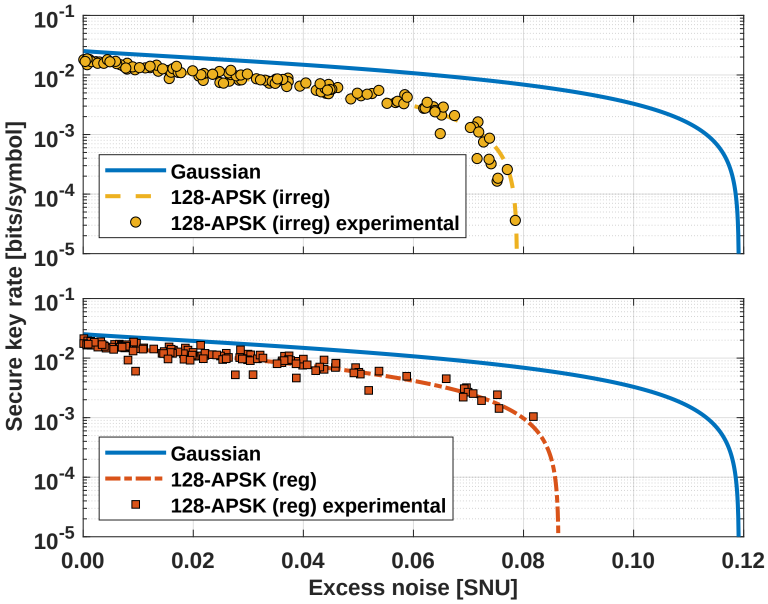


Figure 4.5: Secure key rate, given by (4.3) with $\beta = 0.95$, as a function of excess noise. Experimental results identified as dots and squares, lines indicate the theoretical secure key rate for the PCS-128-APSK irregular, PCS-128-APSK regular and Gaussian constellations. The trend lines for the 128-APSK and Gaussian constellations use the mean transmission and electrical noise observed experimentally.

while the irregular would only reach 129 km, albeit requiring the use of roughly 2^{53} symbols during parameter estimation in order to achieve security under a finite size scenario [13], this would necessitate data transmission for much longer than the channel parameters can be considered to remain stable. This indicates that, in a practical scenario, considering finite size effects and assuming a channel stability time on the order of seconds, achievable distances of around 60 km are expected. We see here that the experimental performance of the regular constellation approaches that of the GM one, achieving 79% of the latter's performance, while the irregular constellation achieves only 58% of the GM system's performance. These discrepancies are in part due to the different mean excess noise observed in each scenario. However, even when under the same channel parameters, regular constellations exhibit better performance than irregular ones with the same cardinality [11].

4.3 Frame synchronization and parameter estimation

Despite the drastic improvements in performance obtained by changing to a 128-APSK constellation, due to the memory and processing power limitations of our hardware, we still weren't able to operate in the finite size regime. Because of this, we endeavoured to reduce the weight of the DSP used in our CV-QKD system. By far the slowest DSP step in the systems presented in Sections 4.2 and 3.2 is the sequence synchronization step, a visualization of which is presented in Figure 4.7. The particular results shown in Figure 4.7 are taken from one of the snapshots taken for the results in Section 4.2.1, chosen at random This step would use a header of k symbols that was inserted at the start of each sequence and would compute a

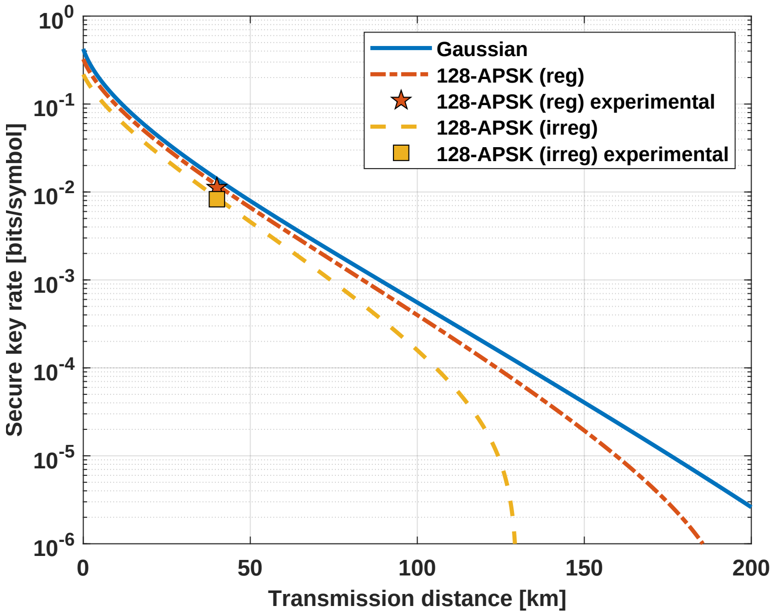


Figure 4.6: Secure key rate, given by (4.3) with $\beta = 0.95$, as a function of the transmission distance. Mean experimental result indicated as a star for the regular and as a square for the irregular 128-APSK scenario. The theoretical results for the 128-APSK constellations use the mean excess noise observed experimentally in each scenario, with the Gaussian results using the average of the noise observed in the other two.

modified Error Vector Magnitude (EVM) using a sliding window scheme over the full received sequence with length N. The EVM computed for each position i is given by

$$\mathrm{EVM}(i) = \frac{1}{k}\sum_{l=1}^{k} \frac{b(i+l) - \mathrm{header}(l)}{|\mathrm{header}(l)|}, \tag{4.17}$$

The sequences were deemed synchronized at the point in which the EVM would be minimum, the location of the minimum in Figure 4.7 is highlighted by a red circle. This technique is not very efficient, requiring that k comparisons, each comparison comprising of a complex-number subtraction and a division, be done $N - k$ times. For the particular results presented in Figure 4.7, the main DSP (excluding frame synchronization) stage took 117 seconds, while the frame synchronization alone took 170 seconds. Taking into account the high number of states required to function in the finite size regime, which can be seen in Figure 4.2d, this means that this technique is woefully inadequate and presents a big limit to the system's performance. With this in mind we endeavoured to develop an alternative approach.

In Figure 4.8 we present a block diagram illustrating the method developed for easier state sequence synchronization. In Figure 4.8 we also represent the hardware necessary for Bob to perform real-time estimation of his receiver's shot and thermal noise. This method consists of frequency multiplexing a relatively high intensity Quadrature Phase Shift Keying (QPSK) auxiliary channel with the same symbol rate as the quantum signal, carrying a m bit counter and of generating the states for channel parameter estimation using a deterministic Pseudo Random Number Generator (PRNG). The QPSK auxiliary channel can also be used to share other useful and open information. Alice generates a random seed with her Quantum

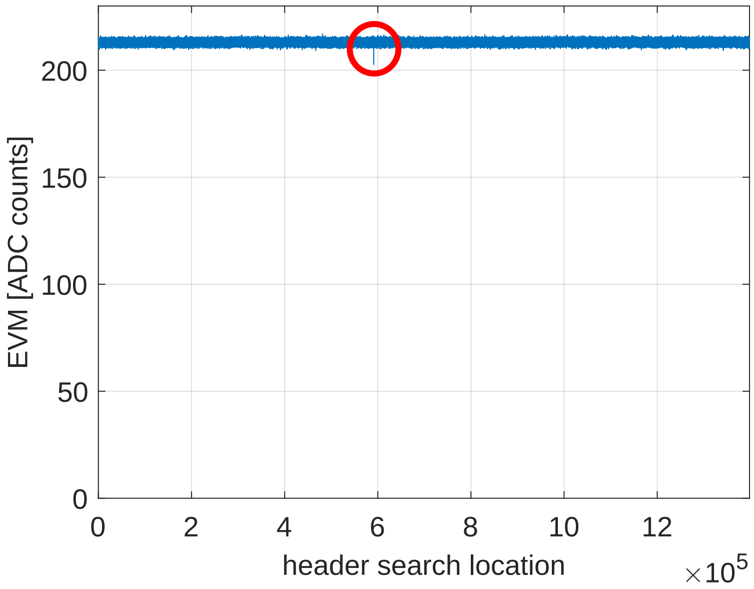


Figure 4.7: Visualization of the sequence synchronization DSP step. Header start location identified by a red circle.

Random Number Generator (QRNG), with which she feeds her PRNG, which consists of a 64-bit linear-feedback shift register, described by the code

```
class LFSRand
{
private:
        uint64_t g_wlfsr;

public:
        void seed(uint64_t uSeed)
        {
                g_wlfsr = uSeed;
        }
        uint64_t rand64()
        {
                uint64_t bit;
                uint64_t dwOut;
                bit = ((g_wlfsr >> 0) ^ (g_wlfsr >> 1) ^ (g_wlfsr >> 3) ^
 ↪  (g_wlfsr >> 4)) & 1;
                g_wlfsr = (g_wlfsr >> 1) | (bit << 63);

                return g_wlfsr;
        }
        void discard(uint32_t discardLength)
        {
                for (uint32_t i = 0; i < discardLength; i++)
                {
```

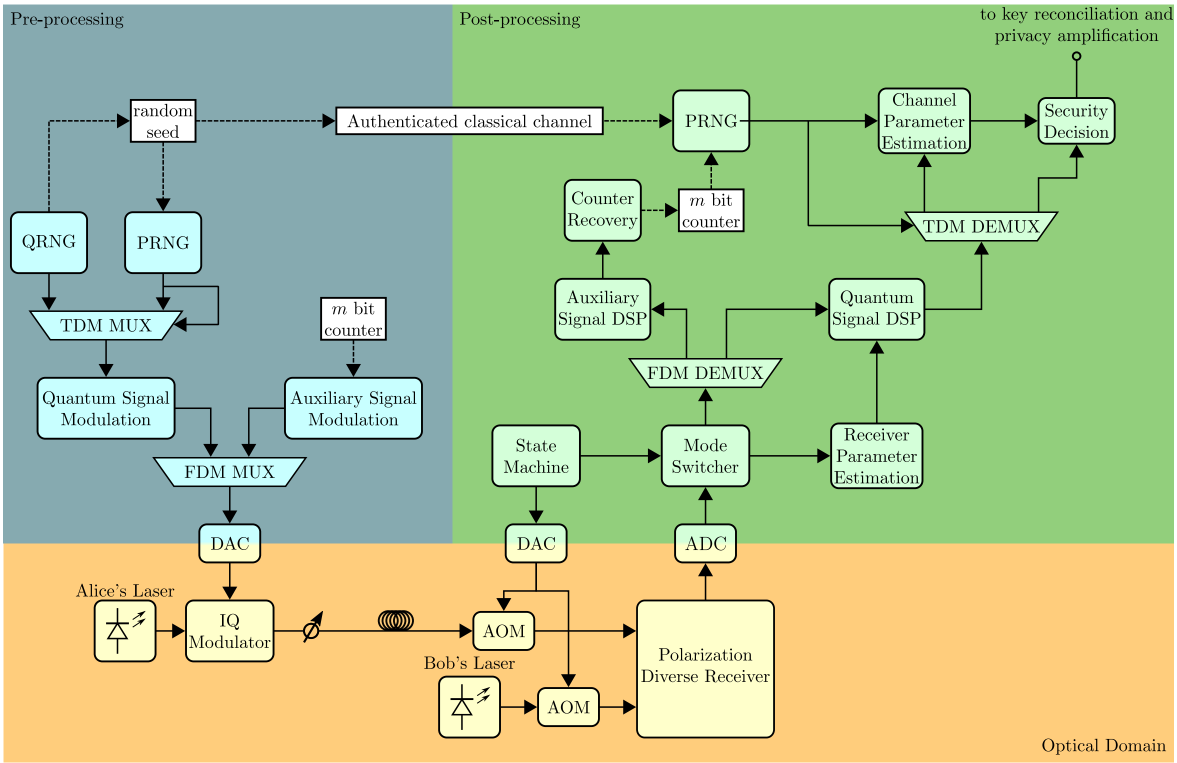


Figure 4.8: Block diagram of the system showing the function of the proposed sequence recovery, as well as the receiver and channel parameter estimation schemes.

```
                                rand64();
                    }
          }
};
```

Alice then uses the output of this PRNG both to generate the states for estimation and to control the location of those states, by using one bit to control the Time Division Multiplexing (TDM). The TDM signal is then modulated following the same methodology described in Chapter 3, following which it is combined with the m-bit counter carrying auxiliary signal through Frequency Division Multiplexing (FDM).

At Bob's side the signal is passed through an Acousto-Optic Modulator (AOM), which allows Bob to switch off of the signal from the fibre in order to perform receiver parameter characterization measurements. During the receiver characterization stage both the shot noise and thermal noise of Bob's receiver will be estimated, this noise is deemed to be trusted, the latter of which being performed when both AOMs are set to shut off the signal. The topic of receiver parameter estimation is further explored in Chapters 2 and 3. The AOMs are controlled by a state machine which controls the immediate functioning mode of the system, commanding the DSP to either perform the full DSP on the signal or to estimate the receiver parameters. We consider that the three different states, thermal noise estimation, shot noise estimation and signal reception, all have the same duration and are used cyclically. In Figure 4.9 we present the output of one of the coherent receivers of the polarization diverse receiver system described in Chapter 3. The system described in depth in Chapter 3 was

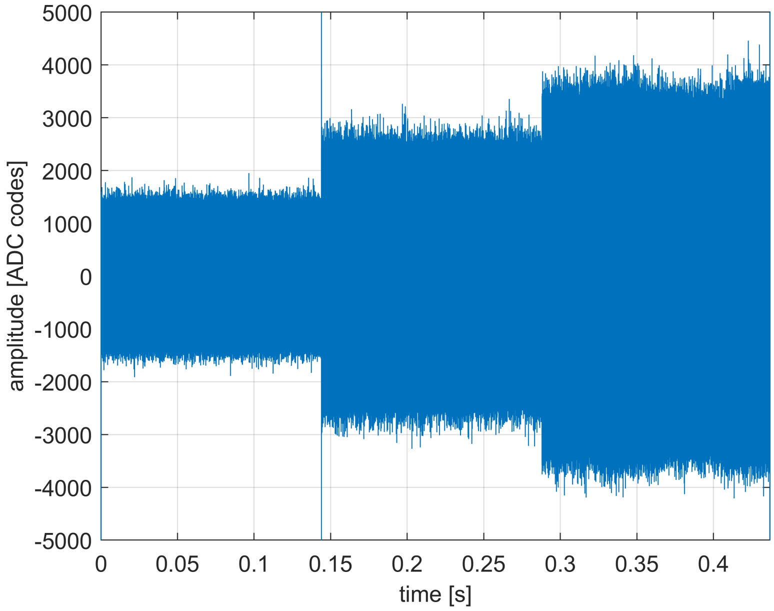


Figure 4.9: Output of the horizontal coherent receiver showing the three operation states of Bob's system in Figure 4.8. From left to right, the states are:thermal noise estimation, shot noise estimation and signal reception.

altered by the addition of two AOMs in the positions described in Figure 4.8. The top AOM, controlling the signal from the fibre, consisted of a Gooch & Housego MLP035 modulator, coupled with a R26035 driver also from Gooch & Housego, while the bottom AOM, controlling the LO, consisted of an Aerodiode 1550-AOM-2, coupled with a RFAOM-T-200 driver also from Aerodiode. Both drivers where in turn driven by a Transistor-Transistor Logic (TTL) signal generated by an Arduino Due board, which cycled through the three states with a frequency of 2.3 Hz. The three states are clearly distinguishable in Figure 4.9, identifiable by the varying variance levels, with the first state corresponding to the thermal noise estimation, the second one shot noise estimation and the third state to signal reception. In the transition into and out of the thermal noise estimation stage we observe and sudden transient spike, which reveals to us that a small gap around the state transitions should be cut out during signal processing. When both AOMs are set to pass, Bob demultiplexes the auxiliary from the quantum signal and processes both independently, subjecting each to a DSP stage identical to the one described in Chapter 2. The information recovered within each cycle we dub a *data frame*. From the auxiliary channel Bob will recover a simple binary sequence containing the encoded m-bit counter, however he cannot be sure at what point in the binary description of the number his sequence starts. To circumvent this, he decodes the binary in m-bit blocks into the corresponding decimal number, delaying the start position of the decoding by 2 bits until he finds one that recovers the sequence as consecutive integers. An example of a counter-based synchronization recovery is presented in Table 4.1. Due to size constraints, an 8-bit counter is assumed. For the example in Table 4.1 the sequence of succeeding integers is found in the third iteration. Taking into account the data structure assumed here and that the QPSK constellation encodes 2 bits per symbol, only $\frac{m}{2}$ start positions need to be tested recover the sequence synchronization. An 8-bit counter would only be able to index $2^8 \times 4 = 1024$ states before it repeats, due to the high number of states that need to be shared to work in the

Table 4.1: 8-bit counter based synchronization recovery

Recovered binary	10	01	00	10	10	10	00	10	10	11	00	10	11	00	00	10	11	01
$i = 1$	146				162				178				194				...	
$i = 2$	...	74				138				203				13				...
$i = 3$	...		42				43				44				45			

finite-size regime, the bit width m used for the counter will have to be higher. The max number of states for each m is presented for reference in Table 4.2. However, choosing a too high value for m will result in a single QPSK state, the one encoding the bits 00, to be sent much more frequently than the others, as a result the smallest value m for the desired number of states being shared per data frame. Once Bob recovers the counter, Alice can share the random seed she used to drive her PRNG through the authenticated classical channel. Since Bob possesses the same 64-bit linear-feedback shift register PRNG as Alice does, and now is in possession of the seed used by Alice and the knows at which point in the PRNG sequence his recovered data starts, he can generate the states that Alice TDM multiplexed into the quantum signal for channel parameter estimation and knows their positions. In order to mitigate the impact of errors in the QPSK channel, Bob can choose a relatively large number of bits to decode and set the pass-fail decision as based on a percentage of the recovered integers being consecutive. For example, Bob might set his pass-fail percentage as 99% and decode a total of 3000 integers, corresponding to 3000 × m bits, he deems to have recovered the counter once he finds 2970 or more consecutive integers in his decoded sequence. Now in the possession of the channel parameters, Bob can evaluate the security of the shared key and choose whether to proceed to key reconciliation and privacy amplification. Once the seed is shared, Alice extracts a new one from her QRNG, resets the m-bit counter and the process repeats.

Table 4.2: Max number of states counted for different counter bit widths, m.

counter bit width, m	8	16	32	64	...
max number of states	1024	262144	17179869184	73786976294838206464	...

4.4 Summary

In this Chapter we have presented methods through which the performance of CV-QKD systems may be improved. We first show how the performance of our DM-CV-QKD communication system can be improved, while using the same telecom-grade components as before, by transitioning to PCS-128-APSK constellation formats. This change to our previously presented system greatly improves on the capability of 8-PSK based systems, allowing for an extra 50 km for transmission distance, a 10 fold increase in excess noise resistance and at least a 3-fold increase in the allowable photon-number. The capability to withstand much worse channel parameters also has the knock-on effect of enabling the updated system to, in the finite size scenario, reach the same performance as the 8-PSK one while using 95% fewer samples, greatly reducing the post-processing hardware requirements. We present results from our experimental system where we show that, after the conversion to the PCS-128-APSK constellation formats, our average key rate rose by a factor of 10 to ∼0.01 bits/symbol, corresponding to 79% of the performance of an equivalent GM-CV-QKD system. Our experimental system was tested with a fiber channel of 40 km and would be suitable to work in the finite size regime in both metro network connections and some short- to medium-range inter-city connections, provided that a substantial but ultimately manageable increase in the block size is performed. Furthermore, we show that, in the asymptotic regime, our system is capable of reaching distances in excess of 185 km, and, as a result, is compatible with medium- to long-range inter-city connections. We also present a full system diagram of how our system can be updated to perform sequence synchronization as well as receiver and channel parameter estimation efficiently. Through the use of an auxiliary QPSK channel we are able to recover sequence synchronization using only a fraction of the number of symbols required by our previous, header-based technique in a manner that scales well with increasing block sizes.

Bibliography

[1] Anthony Leverrier. *Theoretical study of continuous-variable quantum key distribution.* PhD thesis, Télécom ParisTech, 2009.

[2] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[3] Margarida Almeida, Daniel Pereira, Nelson Muga, Margarida Facão, Armando N Pinto, and Nuno A Silva. Secret key rate of multi-ring m-apsk continuous variable quantum key distribution. *Optics Express*, 10 2021.

[4] Eneet Kaur, Saikat Guha, and Mark M Wilde. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A*, 103(1):012412, 2021.

[5] Wenyuan Liu, Xuyang Wang, Ning Wang, Shanna Du, and Yongmin Li. Imperfect state preparation in continuous-variable quantum key distribution. *Physical Review A*, 96(4):042312, 2017.

[6] A Becir, FAA El-Orany, and MRB Wahiddin. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10(01):1250004, 2012.

[7] Hans Brunner, Lucian Comandar, Fotini Karinou, Stefano Bettelli, David Hillerkuss, Fred Fung, Dawei Wang, Spiros Mikroulis, Yi Qian, Maxim Kuschnerov, Andreas Poppe, Changsong Xie, and Momtchil Peev. A low-complexity heterodyne cv-qkd architecture. pages 1–4, 07 2017.

[8] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 2021.

[9] François Roumestan, Amirhossein Ghazisaeidi, Jérémie Renaudier, Luis Trigo Vidarte, Eleni Diamanti, and Philippe Grangier. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In *2021 European Conference on Optical Communication (ECOC)*, pages 1–4. IEEE, 2021.

[10] Marco Baldi, Franco Chiaraluce, Antonio de Angelis, Rossano Marchesani, and Sebastiano Schillaci. A comparison between apsk and qam in wireless tactical scenarios for land mobile systems. *EURASIP Journal on Wireless Communications and Networking*, 2012(1):1–14, 2012.

[11] Margarida Almeida. Practical security limits of continuous-variable quantum key distribution. Master's thesis, University of Aveiro, 2021.

[12] Md Saifuddin Faruk and Seb J Savory. Digital signal processing for coherent transceivers employing multilevel formats. *Journal of Lightwave Technology*, 35(5):1125–1141, 2017.

[13] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

Chapter 5

Impact of Device Imperfections

In this Chapter we present the theoretical and numerical models used to describe the impact of device imperfections on the performance and security of a Continuous Variables Quantum Key Distribution (CV-QKD) system using Discrete Modulation (DM). The results in this Chapter aim to study how the use of realistic, imperfect devices will affect the performance of a system whose theoretical security proof assumed to be composed of balanced, ideal devices.

This Chapter begins in Section 5.1 with a short introduction, where the fact that the security proofs for CV-QKD, including the proof presented in this work in Chapter 2, assume ideal, balanced components, is explored. The introduction is followed by a study on the impact of modulator device imperfections on the security and performance of Continuous Variables Quantum Key Distribution (CV-QKD) systems, presented in Section 5.2, followed by a further study on the impact of generic constellation deformations on the same parameters, presented in Section 5.2.2. This Chapter then concludes with a study on the impact of receiver imbalances on the performance of Continuous Variables Quantum Key Distribution (CV-QKD) systems, presented in Section 5.3.

5.1 CV-QKD with imperfect devices

We previously established the security of DM-CV-QKD in Chapter 2. However, in this development it was assumed that the experimental components employed were balanced [1–5], something that in real-life implementations can not always be trusted. This was also the case for the security evaluations of the systems presented in Chapters 3 and 4. In Chapter 4 we also looked at how the performance of CV-QKD may be improved by the employment of more complex constellation formats, with the more the constellations approaches the Gaussian one (usually done by increasing cardinality), the better the performance [4, 5]. However, Gaussian constellations, due to their continuous nature, tend to be more susceptible to imperfect state preparation [6], as no modulation stage has the infinite resolution required to faithfully recreate the necessary bi-variate Gaussian distribution, and choosing a too high cardinality constellation will again cause distortions in the modulation stage to become apparent. The formalism presented in Section 2.3 allows us to evaluate the inherent security of an arbitrary constellation.Another approach is to treat these imbalances as deviations from the ideal system and seeing the impact of these imperfections on the parameters that can be measured by Alice and Bob, assuming that a balanced system would yield the true performance, any deviation from it would result in either lost performance or a partially insecure key being generated. This possible double impact of loss of performance or loss of security shows that an in depth study on the impact of device imperfections of the CV-QKD system is paramount.

For these studies it is helpful to consider a simplified CV-QKD system, such as the one presented in Figure 5.1, which will be used as a basis for the work in this Chapter. The transmitter stage is comprised of a laser source, which generates a coherent signal that is then modulated in a generic modulation stage. The modulated signal is then transmitted through a Single Mode Fibre (SMF) with a transmission coefficient of T. At the receiver assembly, the modulated signal is evaluated with the help of a reference tone extracted from a local laser source, with which it is mixed in a coherent detection assembly, which may consist of an intradyne or heterodyne receiver. The output of the balanced receiver is subjected to a Digital Signal Processing (DSP) stage, at the end of which the transmitted constellation is recovered. The information measured at the receiver can be used to estimate the channel parameters, which is a fundamental step to obtain the secure key rate.

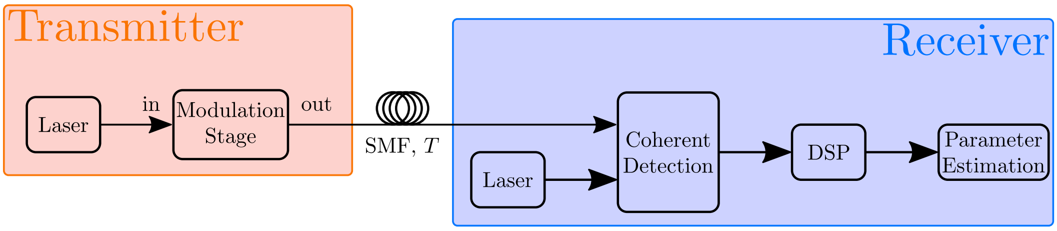
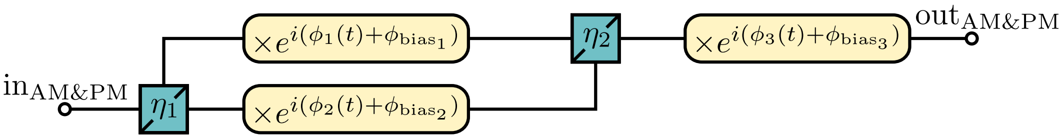


Figure 5.1: High level block diagram of a coherent state CV-QKD system.

5.2 Modulation device imperfections

In this section, we describe the theoretical model used to describe the role of modulation stage imperfections on the performance of a DM-CV-QKD system. We present the impact of those imbalances on the shape a 256-Quadrature Amplitude Modulation (QAM) constellation in order to illustrate the problem. The 256-QAM constellation is chosen because it has a high-cardinality and, being square, deformations to it are quite easy to identify. The modulation stage mentioned in Figure 5.1 can take different forms, for the purposes of this work two different modulation methods are assumed: (1) an Amplitude Modulator (AM) connected in tandem with a Phase Modulator (PM); (2) a single In-phase and Quadrature (IQ) Modulator. Both modulation methods can be fully described as systems of Beam Splitter (BS) and PMs. For the diagrams presented in this work, the BS are presented as teal squares and labeled by their transmission coefficient, η_i, while the PMs are presented as yellow rectangles with rounded corners and labelled by the complex exponential that describes their action on the signal, $e^{i(\phi_i(t)+\phi_{\text{bias}_i})}$, where $\phi_i(t)$ is the time-varying phase that is intended to be imparted on the signal and ϕ_{bias_i} is a constant factor that sets the phase added to the signal when $\phi_i(t) = 0$.

A low-level block diagram of an AM&PM pair is presented in Figure 5.2, assuming the AM to be in a push-pull configuration. The input signal is first split in the η_1 BS, with the reflected component having the phase $\phi_1(t) + \phi_{\text{bias}_1}$ imparted on it and the transmitted one the phase $\phi_2(t) + \phi_{\text{bias}_2}$. After these individual phase modulations, the two resulting signals are combined again in the second BS with transmission coefficient η_2. The interference that



$\mathrm{in}_{\mathrm{AM\&PM}}$
η_1
$\times e^{i(\phi_1(t)+\phi_{\mathrm{bias}_1})}$
$\times e^{i(\phi_2(t)+\phi_{\mathrm{bias}_2})}$
η_2
$\times e^{i(\phi_3(t)+\phi_{\mathrm{bias}_3})}$
$\mathrm{out}_{\mathrm{AM\&PM}}$

Figure 5.2: Low level block diagram of an Amplitude- and Phase-modulator based modulation stage.

occurs at this combination is what accomplishes the amplitude modulation. The amplitude modulated signal is then subjected to one last phase rotation of $\phi_3(t) + \phi_{\mathrm{bias}_3}$. The in-out relations of a generic AM&PM pair can be described as

$$\mathrm{out}_{\mathrm{AM\&PM}} = \Big[\sqrt{\eta_1(1-\eta_2)}e^{i(\phi_1(t)+\phi_{\mathrm{bias}_1})}+ \sqrt{(1-\eta_1)\eta_2}e^{i(\phi_2(t)+\phi_{\mathrm{bias}_2})}\Big] e^{i(\phi_3(t)+\phi_{\mathrm{bias}_3})}\mathrm{in}_{\mathrm{AM\&PM}}. \quad (5.1)$$

Note that, from a theoretical point of view, the relative position of the AM and PM is arbitrary, as the resulting in-out relations will be the same. In an ideal, balanced scenario, we would have $\eta_1 = \eta_2 = 0.5$, $\phi_1(t) = -\phi_2(t)$, $-\phi_{\mathrm{bias}_1} = \phi_{\mathrm{bias}_2} = \pi/2$ and $\phi_{\mathrm{bias}_3} = 0$. In this scenario, (5.1) would simplify to

$$\mathrm{out}_{\mathrm{AM\&PM}} = \sin(\phi_1(t))e^{i\phi_3(t)}\mathrm{in}_{\mathrm{AM\&PM}}. \quad (5.2)$$

A further factor is that, in order for the desired constellation to be faithfully recreated, $\phi_1(t)$ should contain the arcsin of the desired amplitude levels, in order to prevent the appearance of non-linearities in the AM, and the PM should be fully driven, i.e. $\phi_3(t)$ should make a full rotation from $-\pi$ to π.

The deformation of a regular 256-QAM constellation, taking into account different imbalance types, in the AM&PM scenario is presented in Figure 5.3. Figure 5.3 (a) is a schematically represented, ideal regular 256-QAM constellation, included for comparison. Figure 5.3 (b) shows the constellation generated when the internal BS are imbalanced, for this particular constellation $\eta_1 = 0.6$ and $\eta_2 = 0.5$ were assumed. In this situation, the signals in each arm of the AM will have different amplitudes, thus impacting the interference that occurs at the η_2 BS, inhibiting the destructive interference. Note that if $\eta_1 \neq 0.5$ and $\eta_2 \neq 0.5$ but $\eta_1 + \eta_2 = 1$, the output constellation will appear with a lower amplitude but otherwise unaffected, having no effect on system performance. Figure 5.3 (c) shows the constellation generated when the bias points of the individual PMs of the AM are incorrectly set, for this particular constellation $\phi_{\mathrm{bias}_1} = -\frac{2\pi}{5}$ and $\phi_{\mathrm{bias}_2} = \frac{\pi}{2}$ were assumed. Again, the interference that occurs at the η_2 BS is impacted, as the signals at each arm are no longer in phase opposition. Figure 5.3 (d) shows the constellation generated when the signals driving the two individual PMs of the AM have different amplitudes, for this particular constellation $\phi_1(t) = -1.2\phi_2(t)$. In this situation we observe deformation from the non-linear nature of complex exponentials. Finally, Figures 5.3 (e) and (f) show the constellation generated when the PM is either over- or under-driven, i.e. $\phi_3(t)$ is not contained in or is not capable of filling the $]-\pi, \pi]$ domain. In Figure 5.3 (e) we assume that the PM is over-driven by a factor of 20%, this results in the constellation points of the 2nd and 3rd quadrants to overlap. Conversely, in Figure 5.3 (f) we assume that the PM is under-driven by a factor of 20%, which results in a slice of the 2nd and 3rd quadrants to not be reachable, causing the constellation

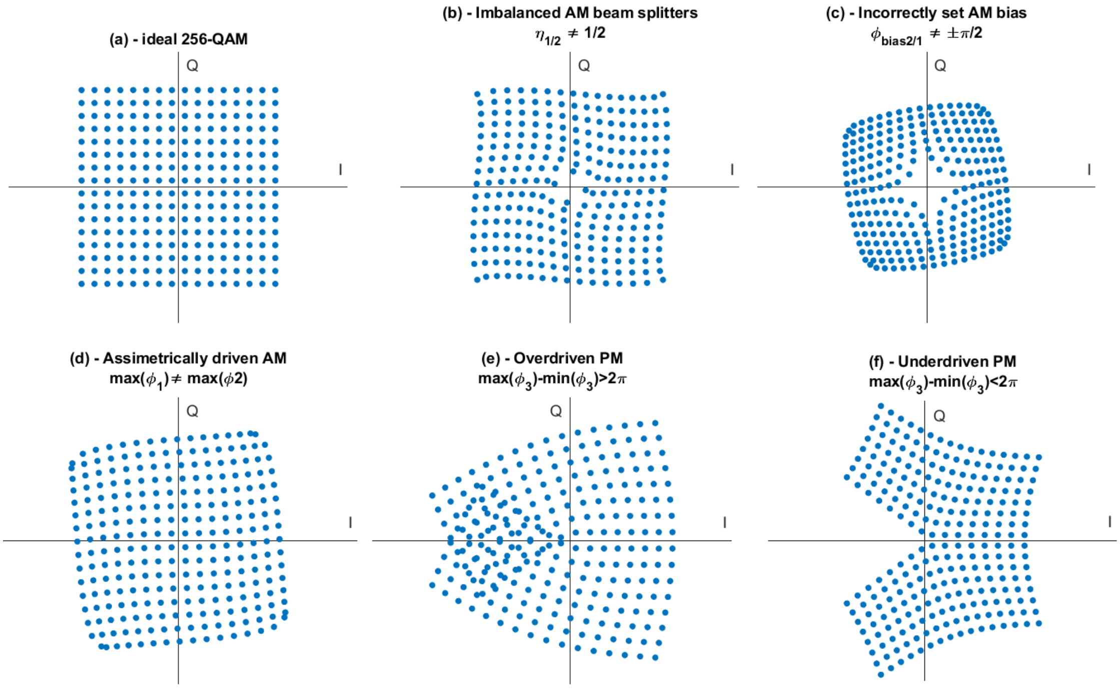


Figure 5.3: Exemplary deformed 256-QAM constellations for multiple imbalanced AM&PM scenarios.

to have an open region. An incorrectly set ϕ_{bias_3} will result in a simple rotation of the whole constellation, since this can be easily compensated in DSP [7] this effect is not considered further in this work.

A low-level block diagram of an IQ Modulator is present in Figure 5.4. An IQ Modulator

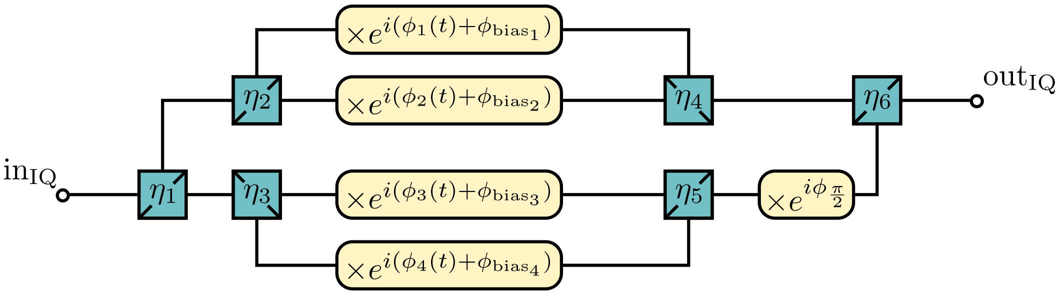

$\times e^{i(\phi_1(t)+\phi_{\text{bias}_1})}$
$\eta 2$
$\times e^{i(\phi_2(t)+\phi_{\text{bias}_2})}$
$\eta 4$
$\eta 6$
out_{IQ}
in_{IQ}
$\eta 1$
$\eta 3$
$\times e^{i(\phi_3(t)+\phi_{\text{bias}_3})}$
$\eta 5$
$\times e^{i\phi_{\frac{\pi}{2}}}$
$\times e^{i(\phi_4(t)+\phi_{\text{bias}_4})}$

Figure 5.4: Low level block diagram of an IQ-modulator based modulation stage.

can be seen as a pair of nested AMs, with one modulating the in-phase and the other the quadrature component of the signal. To accomplish this, the input signal is first split in the η_1 BS, with each output of being subjected to the same amplitude modulation process described previously in the AM&PM scenario. The output of the lower AM in Figure 5.4 is then subjected to a phase rotation of $\phi_{\frac{\pi}{2}}$ before it is combined with the output of the upper

AM. The in-out relations of a generic IQ Modulator can be described as

$$\begin{aligned}\mathrm{out}_{\mathrm{IQ}} = \Big\{ & \sqrt{\eta_1(1-\eta_6)}\left[\sqrt{(1-\eta_2)(1-\eta_4)}e^{i(\phi_1(t)+\phi_{\mathrm{bias}_1})} + \sqrt{\eta_2\eta_4}e^{i(\phi_2(t)+\phi_{\mathrm{bias}_2})}\right] \\ & + \sqrt{(1-\eta_1)\eta_6}\left[\sqrt{\eta_3\eta_5}e^{i(\phi_3(t)+\phi_{\mathrm{bias}_3})} + \sqrt{(1-\eta_3)(1-\eta_5)}e^{i(\phi_4(t)+\phi_{\mathrm{bias}_4})}\right]\Big\}\,\mathrm{in}_{\mathrm{IQ}} \qquad (5.3)\end{aligned}$$

In an ideal, balanced scenario, we would have $\eta_{1,2,3,4,5,6} = 0.5$, $\phi_{1,3}(t) = -\phi_{2,4}(t)$, $-\phi_{\mathrm{bias}_{1,3}} = \phi_{\mathrm{bias}_{2,4}} = \pi/2$ and $\phi_{\frac{\pi}{2}} = \frac{\pi}{2}$. In this scenario, (5.3) would simplify to

$$\mathrm{out}_{\mathrm{IQ}} = [\sin(\phi_1(t)) + i\sin(\phi_3(t))]\mathrm{in}_{\mathrm{IQ}}. \qquad (5.4)$$

Again, a further factor is that $\phi_1(t)$ and $\phi_3(t)$ should contain the arcsin of the desired amplitude levels.

The deformation of the constellation caused by different imbalances in the IQ scenario is presented in Figure 5.5. Again we include an ideal regular 256-QAM constellation for comparison, presented in Figure 5.5 (a). Figure 5.5 (b) shows the constellation generated when the external BS (external in relation to the nested AMs, i.e. η_1 and η_6) of the IQ are imbalanced, for this particular constellation $\eta_1 = 0.6$ and $\eta_6 = 0.5$ were assumed. In this situation, the signals in each nested AM will have different amplitudes, resulting in the output constellation having *stretched out* appearance. Note that, analogously to what occurs in the AM+PM scenario, if $\eta_1 = \eta_6$, the output constellation will appear with a lower amplitude but otherwise unaffected, having no effect on system performance. Figure 5.5 (c) shows the constellation generated when internal BSs are imbalanced, for this particular constellation

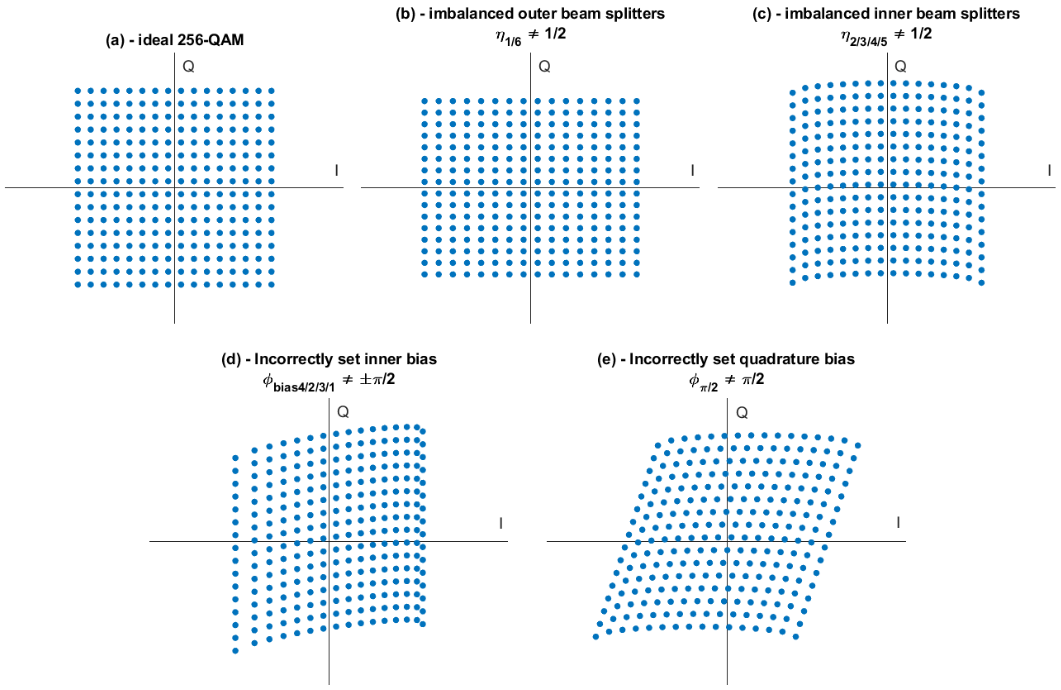


Figure 5.5: Exemplary deformed 256-QAM constellations for multiple imbalanced IQ scenarios.

$\eta_2 = 0.6$ and $\eta_3 = \eta_4 = \eta_5 = 0.5$ were assumed. This causes a slight *bowing* of the output constellation in the direction of the quadrature being modulated by the imbalanced AM. Figure 5.5 (d) shows the constellation generated when the bias points of the internal PMs deviate from $\pm\frac{\pi}{2}$, for the particular constellation shown $\phi_{\text{bias}_1} = -\frac{2\pi}{5}$ and $\phi_{\text{bias}_2} = -\phi_{\text{bias}_3} = \phi_{\text{bias}_4} = \frac{\pi}{2}$ were assumed. In this situation, an asymmetric *bowing* of the constellation is now seen, again affecting the quadrature being modulated by the now imbalanced AM. Finally, Figure 5.5 (e) shows the constellation generated when the quadrature bias point is incorrectly set, i.e. $\phi_{\frac{\pi}{2}} \neq \frac{\pi}{2}$, for this particular constellation $\phi_{\frac{\pi}{2}} = \frac{2\pi}{5}$. When this occurs, the two signals being modulated in each nested AM are no longer separated by $\frac{\pi}{2}$, resulting in the constellation now being slanted diagonally.

In all the imbalanced scenarios shown previously, the deformation of the constellation will impact the true performance of the system, as the set of states now being generated deviates from that of the ideally generated constellations. If Alice and Bob assume the constellation was correctly generated, it will cause the channel parameters estimated in the receiver to degrade.

5.2.1 Performance impact of Imperfect Modulation Stage Devices

In this section, we describe how to compute the channel parameters and subsequent secure key rate and show the impact of transmitter device imperfections on the performance of a DM-CV-QKD system.

For this work we will be studying the impact of modulation imbalances on the performance of systems using 5 different constellation formats: 1024-QAM, 256-QAM, 64-QAM and regular 256-APSK with 32 states per ring and 64 states per ring. The amplitude levels of the constellations studied in this work follow a Maxwell-Boltzmann distribution. For a constellation with Q amplitude levels, $A_i, i \in \{1, ..., Q\}$, the probability of each amplitude i is given by

$$P_i = \frac{e^{-\nu A_i^2}}{\sum_{n=1}^{Q} P_n}, \tag{5.5}$$

where the ν parameter needs to be optimized for each scenario. The probability, q_k, of a given state, $|\alpha_k\rangle$, with amplitude $|\alpha_k| = A_i$, in a given constellation, can be readily computed by dividing the amplitude probability by the total number of states with the same amplitude. All constellations are generated with the same initial maximum amplitude of 1, with new amplitude levels being added progressively closer to the origin. After deformation, the final amplitude of the constellations was set so that

$$\langle n \rangle = \sum_{k=1}^{M} q_k |\alpha_k|^2, \tag{5.6}$$

where $\langle n \rangle$ is the average number of photons per symbol. For the results in this work, $\langle n \rangle$ was optimized for each constellation format, with Alice assuming that her constellation is faithfully recreated in the optical domain, i.e. that the modulation system is balanced and that the constellation points are correctly positioned. The value of $\langle n \rangle$ was kept constant regardless of the degree of the constellation deformation.

Recall from Chapter 2 that the transmitter, a, and receiver, b, constellations are related by the normal linear model [7]:

$$b = ta + z, \tag{5.7}$$

where $t = \sqrt{2 \langle n \rangle \eta_d \tilde{T}}$ and z is the noise contribution, which follows a normal distribution with null mean and variance

$$\sigma^2 = 2 + \eta_d \tilde{T} \tilde{\epsilon} + 2\epsilon_{\text{thermal}}. \tag{5.8}$$

In the t and σ^2 parameters, $\tilde{T}$ is the estimate for the channel transmission, η_d is the quantum efficiency of Bob's detection system, $\tilde{\epsilon}$ is the estimate for the excess channel noise and $\epsilon_{\text{thermal}}$ is the receiver thermal noise, these last two being both expressed in shot noise units (SNU). Recall also that t and σ^2 can be estimated through [7]:

$$\tilde{t} = \frac{1}{N} \text{Re} \left\{ \sum_{i=1}^{N} \frac{a_i b_i^*}{|\alpha_i|^2} \right\}, \qquad \tilde{\sigma}^2 = \frac{\sum_{i=1}^{N} |b_i - \tilde{t} a_i|^2}{N}. \tag{5.9}$$

The transmission and excess noise are then estimated through:

$$\tilde{T} = \frac{\tilde{t}^2}{2 \langle n \rangle \eta_d}, \qquad \tilde{\epsilon} = \frac{\tilde{\sigma}^2 - 2 - 2\epsilon_{\text{thermal}}}{\eta_d \tilde{T}}. \tag{5.10}$$

We previously explored the security of DM-CV-QKD against collective attacks in Chapter 2, following the methodology presented in [8]. Recall that the achievable secure key rate is given by:

$$K = \beta I_{\text{BA}} - \chi_{\text{BE}}, \tag{5.11}$$

where β is the reconciliation efficiency, given by

$$\beta = 2 \frac{R}{I_{\text{BA}}}, \tag{5.12}$$

where R is the rate of the reconciliation code being employed. Meanwhile, I_{BA} is the mutual information between Bob and Alice, given by [3]:

$$I_{\text{BA}} = \log_2 \left(1 + \frac{2\tilde{T}\eta_d \langle n \rangle}{2 + \tilde{T}\eta_d \tilde{\epsilon} + 2\epsilon_{\text{thermal}}} \right) = \log_2 (1 + \text{SNR}), \tag{5.13}$$

where SNR stands for Signal to Noise Ratio. As β is dependent on I_{BA}, it will be indirectly dependent on the SNR, in fact, a given code rate R is limited by the minimum SNR it requires to function, with the higher the rate, the higher the minimum SNR required. For this work we assume a Multi Edge Type Low Density Parity Check (MET-LDPC) reconciliation method, with the code rates and corresponding SNR limits being presented in Table 5.1 [9, 10]. The

Table 5.1: Code rates and respective minimum SNR requirements of different MET-LDPC matrices [9, 10].

R	Minimum SNR
0.25	0.4162
0.10	0.1549
0.05	0.0741
0.02	0.0286
0.01	0.0141

value of β was computed for each scenario, with the optimal code rate being chosen for each.

In (5.11), χ_{BE} describes the Holevo bound that majors the amount of information that Eve can gain on Bob's recovered states, being obtained through the methodology presented in Chapter 2, where the key parameter of interest to us the Z parameter, which is a measure of the correlation between the states at the transmitter and receiver, being given by

$$Z = 2\mathrm{tr}(\hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{\frac{1}{2}}\hat{a}^{\dagger}) - \sqrt{2\epsilon W}. \tag{5.14}$$

where $\hat{\rho}$ is the density operator for the M-symbol discrete constellation, defined by [8]

$$\hat{\rho} = \sum_{k=1}^{M} p_k \left|\alpha_k\right\rangle \left\langle\alpha_k\right|, \tag{5.15}$$

and [8]

$$W = \sum_{k=1}^{M} p_k(\left\langle\alpha_k\right| \hat{a}_{\rho}^{\dagger}\hat{a}_{\rho} \left|\alpha_k\right\rangle - |\left\langle\alpha_k\right| \hat{a}_{\rho} \left|\alpha_k\right\rangle|^2) \tag{5.16}$$

and, finally,

$$\hat{a}_{\rho} = \hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{-\frac{1}{2}}. \tag{5.17}$$

The exact methodology to compute χ_{BE} can be found in [8] and is reproduced here in Chapter 2.

In order to evaluate the impact of the constellation deformations, we look at two different security scenarios:

- The **real** scenario, in which the value of Z in (2.32) is calculated for each individual deformed constellation and the deformations themselves are assumed to be taken into account during parameter estimation, i.e. the deformation does not affect the estimated channel parameters. This value will correspond to the actual key rate of the deformed constellations.

- The **naive** scenario, which consists of the key rate that Alice and Bob estimate by assuming that the transmitter system is balanced, using the value of Z computed for the ideal constellation and attributing all deviations from the ideal constellation to reduced transmission and excess channel noise.

The system parameters assumed in this work were $T = 0.1585$ (corresponding to the transmission coefficient of a standard 40 km SMF), $\eta = 0.9$, $\epsilon_{\mathrm{thermal}} = 0.3$ SNU and $\epsilon = 0.01$ SNU. In the naive scenario, the noise introduced by the deformation of the constellations is added to ϵ.

The performance of the imbalanced AM&PM modulation stage (see Figure 5.2), measured in terms of the secret key rate, given by (5.11), for a combination of 3 different constellations with 256 cardinality, is presented in Figure 5.6. Figure 5.6 (a) shows the key rate in function of the different values of the AM BS. We see that, for the 3 constellations assumed, the real value of the key rate decreases slowly as the value deviates from equilibrium, while the naively estimated value decreases much more sharply, as the excess noise induced by the deformation takes it toll. Meanwhile, in Figure 5.6 (b) we show the key rate in function of the bias point of the internal PM of the AM. This time around, both the real and naive values of key rate decrease very quickly as the value deviates from equilibrium. In both the previous scenarios

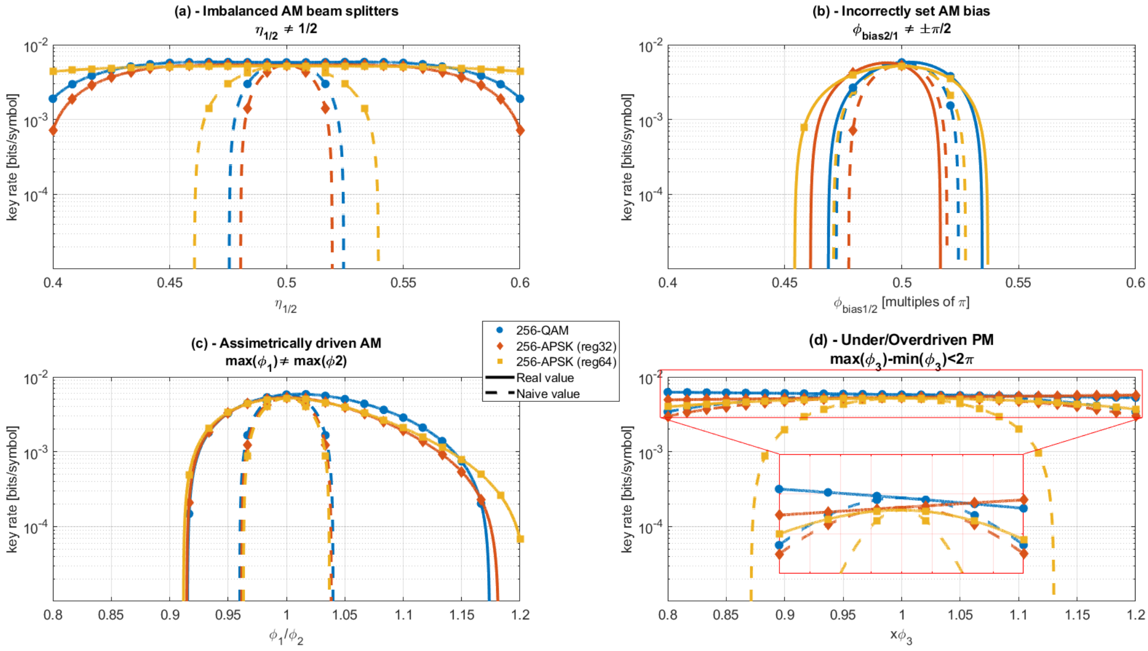


Figure 5.6: Real (full line) and naively (dashed line) estimated secret key rates for an imbalanced AM&PM modulation stage. Shapes and colours indicate the different constellation formats, blue circles indicate the 256-QAM constellation, orange diamonds indicate the 256-APSK with 32 states per ring and yellow squares indicate the 256-APSK with 64 states per ring. The parameters assumed were $T = 01585$, $\nu = 0.9$, $\epsilon_{\text{thermal}} = 0.3$ SNU and $\epsilon = 0.01$ SNU, in the naive scenario to this excess noise is added the contribution of the deformation of the constellations.

we see that the 256-APSK (reg64) constellation, the one that places its lowest amplitude states the farthest away from the origin, is the one whose performance, both in the real and naive scenarios, decreases the slowest. This is due to imbalances in the AM degrading its ability to perform destructive interference, causing the lower amplitude states to be shifted, which will be read as excess noise. Figure 5.6 (c) shows the key rate in the situation of an asymmetrically driven AM, where the amplitude of $\phi_1(t)$ is multiplied by a constant factor while $\phi_2(t)$ remains unchanged. This time around, the real value of the key rate decreases faster when $\phi_1(t)/\phi_2(t) < 1$ than in the opposite scenario, while the naively estimated value decreases much more sharply and roughly at the same rate for the 3 constellations studied. Finally, Figure 5.6 (d) shows the key rate in the situation of an under/overdriven PM. The real value of the key rate decreases very slowly as the value deviates from equilibrium, while from in the naive scenario only the 256-APSK (reg64) constellation sees a considerable reduction in performance. This is due to the 256-APSK (reg64) constellation placing the most points close the x-axis, and as a result will have more points deviated from their optimal position. For all the results in Figure 5.6, we see that the performance estimated by Alice and Bob in the naive scenario is lower than its corresponding real value.

The performance of the imbalanced IQ modulation stage (see Figure 5.4), measured in terms of the secret key rate, given by (5.11), and for a combination of 3 different QAM constellations, is presented in Figure 5.7. Figure 5.7 (a) shows the key rate in function of the

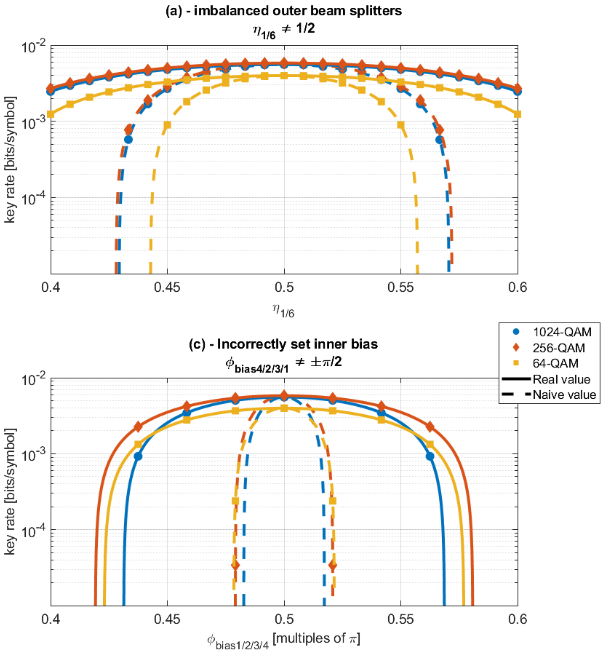


Figure 5.7: Real (full line) and naively (dashed line) estimated secret key rates for an imbalanced IQ modulation stage. Shapes and colours indicate the different constellation formats, blue circles indicate the 1024-QAM constellation, orange diamonds indicate the 256-QAM constellation and yellow squares indicate the 64-QAM constellation. The parameters assumed were $T = 01585$, $\nu = 0.9$, $\epsilon_{\text{thermal}} = 0.3$ SNU and $\epsilon = 0.01$ SNU, in the naive scenario to this excess noise is added the contribution of the deformation of the constellations.

different values of the outer BSs of the IQ modulator. We see that, for the 3 constellations assumed, the real value of the key rate decreases slowly as the value deviates from equilibrium, while the naively estimated value decreases much more sharply, with the 1024- and 256-QAM constellations exhibiting almost the same performance and the 64-QAM one exhibiting a noticeably lower one. Figure 5.7 (b) shows the key rate in function of the different values of the inner BSs of the IQ modulator. Again, the naive value of the key rate decrease much faster than the real one, with the detail that the 64-QAM constellation being slightly more resistant to the drop in performance than the other, higher-cardinality constellations. Figure 5.7 (c) shows the key rate in function of the bias point of the internal PMs of the IQ modulator. Once more, the naive value of the key rate decreases much faster than the real one, with the 1024-QAM constellation being slightly more affected and exhibiting a higher performance drop than the other two considered. Lastly, Figure 5.7 (d) shows the key rate in function of the bias point of the IQ modulator's quadrature bias. Similar results to the case of Figure 5.7 (a) are seen, with the real value of the key rate decreasing slower than the naive one, with the 1024- and 256-QAM constellations exhibiting almost the same performance and the 64-QAM exhibiting a noticeably lower one. Similarly to the AM&PM scenario, for all the results in Figure 5.7, the performance estimated by Alice and Bob in the naive scenario is lower than its corresponding real value.

5.2.2 Impact of Finite Extinction Ratio (FER) on CV-QKD

It can prove useful to look at the isolated impact of the Finite Extinction Ratio (FER) on the performance of the system. The extinction ratio of a modulator describes the ratio between the maximum and minimum powers its output signal can achieve, and is usually indicated in dB. Assuming a modulator without gain, the maximum output power is, at most, equal to the power at its input, as a result, the ER is governed by the minimum output power, i.e. how effective the modulator is in *extinguishing* the signal [6]. In order to be able to fully extinguish the input optical signal, the extinction ratio of the modulator would have to be infinite, as a result its inability to achieve this is attributed to its FER. In terms of the output constellation, this effect will be seen as the inability to place points at or near the origins of the complex plane.

In Figure 5.8 we present a pictogram depicting this phenomena, where the FER is indicated by the shaded areas. Figure 5.8 also contains a simplified block diagram of a transmitter in a CV-QKD transmission link employing an IQ modulator. Each one of the nested AM of the IQ modulator will have some finite extinction ratio, which we assume to be equal to each other. Due to the FER of modulator, the modulation stage is unable to place constellations points in the shaded area, as a result the actually generated constellation points are shifted to the closest available region. Assuming the modulator does not have gain, as constellation formats add more and more amplitude levels, this is achieved by placing these levels closer to the origins. Eventually these points will be placed in the unreachable region, with the result being a deformed constellation.

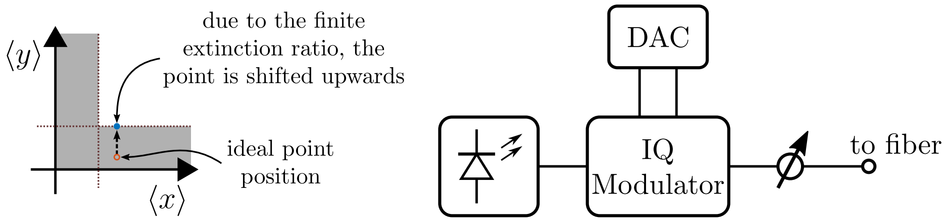
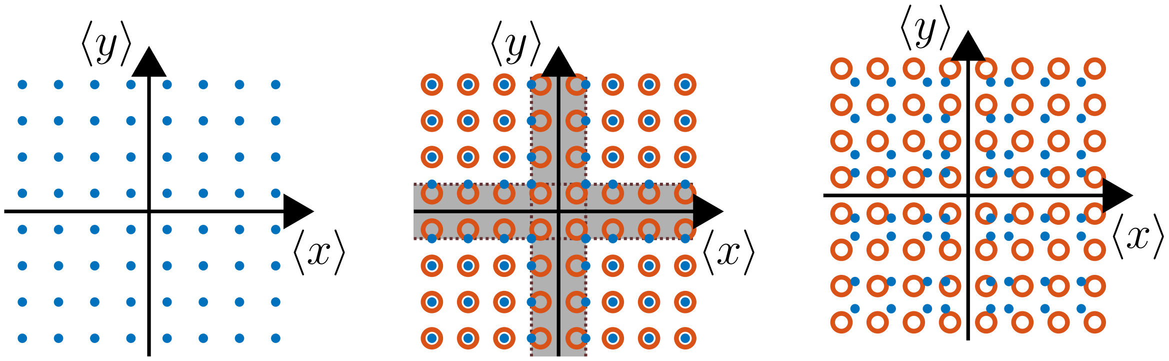


Figure 5.8: Left: pictogram depicting the impact of finite extinction ratio on the position of constellation points; right: simplified block diagram of a CV-QKD transmitter.

Again we assume that the constellations follow a Maxwell-Boltzmann distribution as described in (5.5). For the results in this section, we consider that Alice estimates the optimal ν parameter assuming that her constellation is not deformed. Note that, in general, the innermost points in Probabilistic Constellation Shaping (PCS) constellations are much more likely to be chosen [4, 5].

The *evolution* of the constellation as it progresses through the transmitter is presented in Figure 5.9. Again, for the purposes of this work, we assume that Alice acts naively, i.e. when modulating her signal she considers the output constellation of her modulator is ideal. The FER of the IQ modulator shifts the constellation points that are closest to the quadrature axis away from them, this can be seen in Figure 5.9b. Meanwhile, when Alice is calibrating her output photon number, and because the innermost points of the constellation are the most common ones, she will in essence pull all constellation points towards the origin, thus resulting in a deformed output constellation of the sort shown as blue dots in Figure 5.9c, where the ideal output constellation is also included as orange circles. From this we can see that the impact of the FER will be that the higher amplitude states will contaminate the



(a) Original constellation at DAC output.

(b) FER shifts lower constellation points.

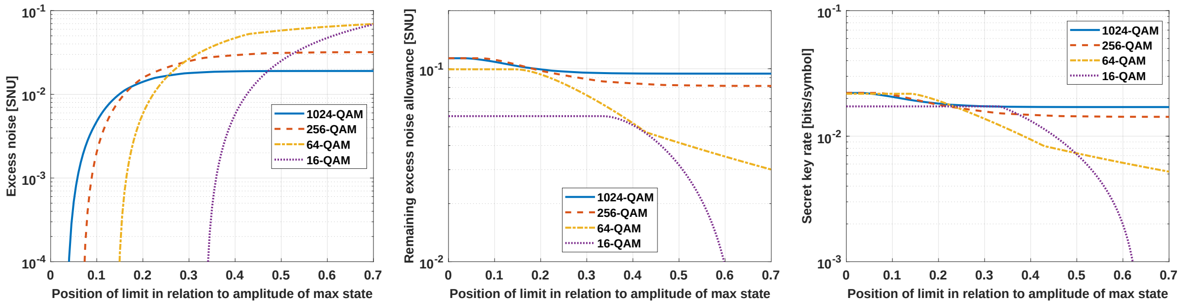
(c) After $\langle n \rangle$ calibration, the output constellation is deformed.

Figure 5.9: Pictogram depicting the impact of finite extinction ratio on a 64-QAM constellation, presenting the constellation as it would look after exiting the DAC, then after exiting the IQ-Modulator and then after being attenuated to the desired photon-number. Where useful, ideal point positions are presented as orange circles, while their actual positions are presented as blue dots.

lower amplitude ones.

Security impact of FER

For these results we assume only the naive scenario. Since the modulation signals used in CV-QKD often include high amplitude auxiliary channels in conjunction with the quantum signal itself, we have chosen to express the FER according to its position in relation to the higher amplitude point of the constellation. This means that if the relative position is expressed as 0.5, the position of points whose amplitude are less than half that of the highest amplitude point will be shifted according to the process described in Figure 5.8. In Figure 5.10 we present the dependence of the system performance on the relative position of the FER limit for 4 QAM constellations of different cardinality, namely 1024-, 256-, 64- and 16-QAM. We can see from Figure 5.10a that the FER will start introducing excess noise



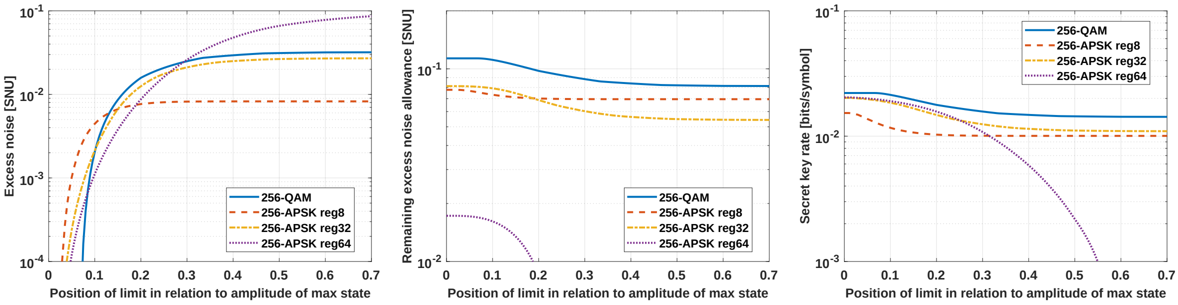
(a) Excess noise in function of FER limit position.

(b) Remaining noise resistance after induced noise is subtracted.

(c) Key rate in function of FER limit position.

Figure 5.10: Performance of the CV-QKD link in function of the position of the FER limit. 4 different cardinality QAM constellations were assumed.

progressively earlier as the constellation's cardinality increases. This is understandable, as the higher the number of states in the constellation, the larger will be number of amplitude levels and the closer the lowest amplitude states will be to the origins. However, we see that the induced excess noise eventually levels out to a more or less constant value, with the higher cardinality constellations leveling out at a lower value than the lower cardinality ones. This is due to the fact that, due to the employed PCS, the more amplitude levels the constellation has, the lower the likelihood will be that states of higher amplitude will be chosen, this means that the "contamination" by the higher amplitude states will be lower. Higher cardinality constellations also exhibit a higher resistance to excess noise [4, 11], so a better measure of the impact of FER on the performance of the system is the remaining excess noise allowed before no secure key can be generated, this is shown in Figure 5.10b. We see that, despite FER only impacting them later, the two lower cardinality constellations consistently exhibit a lower excess noise allowance, owing to their initial lower noise resistance. Meanwhile, the 256-QAM briefly exhibits a higher noise allowance than the 1024-QAM one, before dropping back down as the stabilization level of its induced excess noise becomes higher. In Figure 5.10c we present the system secret key rate in function of FER while assuming the only contribution to excess noise is the constellation distortion. In this scenario we see that the best performing constellation format varies considerably, with the 1024-QAM constellation being the best performing at the start, before being surpassed by the 64-QAM constellation. The 1024-QAM constellation's performance eventually stabilizes to roughly the performance of the ideal 16-QAM constellation, with the two becoming the best performing formats before the FER starts to affect the latter one. Moreover, at high values of the relative position of the FER limit, the higher the cardinality of the constellation, the better performing it will be. In Figure 5.11 we present the dependence of the system performance on the FER for three 256-APSK regular constellations, with 8, 32 and 64 states per ring, and for a 256-QAM constellation. Besides that, our goal for this work was also to compare 4 constellation formats



(a) Excess noise in function of FER limit position.

(b) Remaining noise resistance after induced noise is subtracted.

(c) Key rate in function of FER limit position.

Figure 5.11: Performance of the CV-QKD link in function of the position of the FER limit. 3 different cardinality APSK constellations were assumed, with a 256-QAM constellation included for comparison.

of the same cardinality and test which is best performing under these non-ideal conditions. We can see from Figure 5.11a that the FER introduces excess noise earlier for the APSK constellations, this is due to, in our definition of the APSK constellations, there being states placed directly at the quadrature origins, as a result these immediately start to be deviated from their position. However, for higher values of the relative position of the FER limit, the APSK constellations start to exhibit a lower induced excess noise than the 256-QAM constellation, with only the 256-APSK reg64 constellation eventually surpassing the induced excess noise of the 256-QAM constellation. Noting that the more states per ring for the APSK constellation of a given cardinality has, the less rings and thus less amplitude levels it will have, the order of the values at which the induced excess noise stabilizes is very analogous to the ones in Figure 5.10a, with the constellations organizing in accordance to the number of amplitude levels, occurring for the reason expanded on previously. From Figure 5.11b we see that the APSK constellations with more amplitude levels perform better at high levels of the relative position of the FER limit, again similar to what was seen for the QAM constellations. In terms of secret key rate, shown in Figure 5.11c, we see that the 256-QAM constellation consistently exhibits the best performance, with the best APSK format constellation at the start being the reg64 one, before being surpassed by the reg32 one.

5.3 Receiver device imperfections

A simplified block diagram of the CV-QKD system assumed in this work is presented in Fig. 5.12. Alice's setup is composed by an optical laser signal (coherent state), represented by the annihilation operator $\hat{a}_{0\mathrm{A}}(t)$, and an IQ-modulator for constellation generation. The action of $\hat{a}_{0\mathrm{A}}(t)$ on the coherent state obtained from Alice's laser is given by

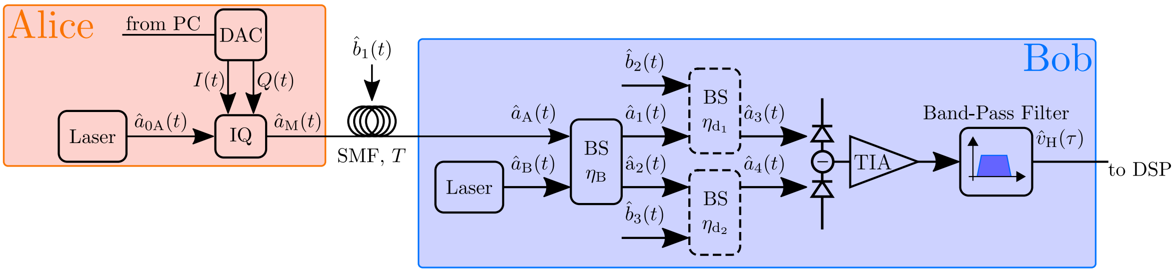


Figure 5.12: Block diagram of the locally generated local oscillator CV-QKD communication system.

$$\hat{a}_{0\mathrm{A}}(t)\left|\alpha_{\mathrm{A}}(t)\right\rangle = \alpha_{\mathrm{A}}(t)\left|\alpha_{\mathrm{A}}(t)\right\rangle, \tag{5.18}$$

where

$$\alpha_{\mathrm{A}}(t) = |\alpha_{\mathrm{A}}|e^{i(\omega_{\mathrm{A}}t+\phi_{\mathrm{A}}(t))}, \tag{5.19}$$

and $|\alpha_{\mathrm{A}}|$ represents the amplitude of Alice's laser such that $|\alpha_{\mathrm{A}}|^2$ is the photon-flux, ω_{A} is the optical frequency of the laser and $\phi_{\mathrm{A}}(t)$ is the unknown optical phase of the laser at instant t. The IQ modulator is driven by signals $I(t)$ and $Q(t)$, generated by a PC controlled Digital to Analog Converter (DAC). The DM constellation assumed for this study consists of an 8-Phase Shift Keying (PSK) with Root Raised Cosine (RRC) pulse shaping and is inserted at an intermediate frequency f_Q. A frequency multiplexed pilot tone is also included in the modulation, consisting of a complex sine-wave inserted at an intermediate frequency f_P, chosen to be outside of the bandwidth of the quantum signal. The modulated laser signal is thus given by

$$\hat{a}_{\mathrm{M}}(t) = \hat{a}_{0\mathrm{A}}(t)M(t), \tag{5.20}$$

where $M(t)$ is the modulation applied to Alice's signal, given by

$$M(t) = q(t)e^{i2\pi f_Q t} + Pe^{i2\pi f_P t} + \epsilon_{\mathrm{Mod}}, \tag{5.21}$$

with $q(t)$ being the 8-PSK RRC signal, P the amplitude of the pilot tone and ϵ_{Mod} a noise parameter that accounts for imperfections in the modulation. Modulation imperfections may arise due to noise in the driving signals or due to an improper balancing of the modulator itself.

In Fig. 5.12, the optical fibre is modelled as a beam-splitter with a transmission coefficient of T, where it is mixed with the vacuum state at port $\hat{b}_1(t)$. The fibre output signal is in that case given by

$$\hat{a}_{\mathrm{A}}(t) = \sqrt{T}\hat{a}_{\mathrm{M}}(t) + \sqrt{1-T}\hat{b}_1(t). \tag{5.22}$$

At Bob's side, the quantum signal $\hat{a}_{\mathrm{A}}(t)$ is sent to a beam-splitter with transmittance η_{B}, where it is mixed with Bob's LLO, $\hat{a}_{\mathrm{B}}(t)$. The beam-splitter outputs are described by

$$\hat{a}_1(t) = \sqrt{\eta_{\mathrm{B}}}\hat{a}_{\mathrm{A}}(t) + \sqrt{1-\eta_{\mathrm{B}}}\hat{a}_{\mathrm{B}}(t), \tag{5.23}$$

$$\hat{a}_2(t) = \sqrt{1-\eta_{\mathrm{B}}}\hat{a}_{\mathrm{A}}(t) - \sqrt{\eta_{\mathrm{B}}}\hat{a}_{\mathrm{B}}(t). \tag{5.24}$$

Note that this beam-splitter ideally would have $\eta_{\mathrm{B}} = \frac{1}{2}$. The action of $\hat{a}_{\mathrm{B}}(t)$ on the coherent state extracted from Bob's laser is given by

$$\hat{a}_{\mathrm{B}}(t) \left|\alpha_{\mathrm{B}}(t)\right\rangle = \alpha_{\mathrm{B}}(t) \left|\alpha_{\mathrm{B}}(t)\right\rangle, \tag{5.25}$$

where

$$\alpha_{\mathrm{B}}(t) = |\alpha_{\mathrm{B}}|e^{i(\omega_{\mathrm{B}}t+\phi_{\mathrm{B}}(t))}, \tag{5.26}$$

and $|\alpha_{\mathrm{B}}|$ represents the amplitude of Bob's laser such that $|\alpha_{\mathrm{B}}|^2$ is the photon-flux, ω_{B} is the optical frequency of the laser and $\phi_{\mathrm{B}}(t)$ is the unknown optical phase of the laser at instant t. The beam-splitter outputs, $\hat{a}_1(t)$ and $\hat{a}_2(t)$, are then detected by a pair of photodiodes. The quantum efficiency of each photodiode, η_{d1} and η_{d2}, is modelled by a virtual beam-splitter with a transmission coefficient equal to the quantum efficiency of the real photodiode followed by an ideal photodiode [12]. As a result, the signals are mixed with the vacuum states at ports $\hat{b}_2(t)$ and $\hat{b}_3(t)$, resulting in the outputs

$$\hat{a}_3(t) = \sqrt{\eta_{\mathrm{d}_1}}\hat{a}_1(t) + \sqrt{1-\eta_{\mathrm{d}_1}}\hat{b}_2(t), \tag{5.27}$$

$$\hat{a}_4(t) = \sqrt{\eta_{\mathrm{d}_2}}\hat{a}_2(t) + \sqrt{1-\eta_{\mathrm{d}_2}}\hat{b}_3(t). \tag{5.28}$$

Ideally, the quantum efficiencies of the two photodetectors would be equal, but experimentally this may not be the case. The pair of optical signals in (5.27) and (5.28) is then converted to an electrical current according to

$$\hat{I}_1(t) = q_e\hat{a}_3^{\dagger}(t)\hat{a}_3(t), \tag{5.29}$$

$$\hat{I}_2(t) = q_e\hat{a}_4^{\dagger}(t)\hat{a}_4(t), \tag{5.30}$$

where q_e is the elementary electron charge.

The two currents in (5.29) and (5.30) are subtracted and the thermal noise, $\hat{n}_{\mathrm{th}}$, is added to the resulting current

$$\hat{I}(t) = \hat{I}_2(t) - \hat{I}_1(t) + \hat{n}_{\mathrm{th}}(t), \tag{5.31}$$

where $\hat{n}_{\text{th}}(t)$ is a Gaussian distributed random variable with null mean and variance $\varepsilon_{\text{th}}^2$. This subtraction current is then passed through a trans-impedance amplifier in which process it is filtered by a bandpass filter, resulting in

$$\hat{v}_{\text{H}}(\tau) = g_{\text{TIA}} \left(h_{\text{BP}}(t) * \hat{I}(t) \right) (\tau), \tag{5.32}$$

where g_{TIA} is the gain of the trans-impedance amplifier, $h_{\text{BP}}(t)$ represents the impulse response of the bandpass filter and the $*$ symbol represents convolution. This amplified signal is then digitized and fed into a DSP system that allows for frequency and phase recovery. For the purposes of this work, we assume this DSP to be ideal, not introducing any extra noise.

5.3.1 Impact of imbalances

In this section, we describe the impact of devices imperfections at Bob's detection system on the expected value and variance of the measured voltage. Moreover, we also consider the role of those imperfections on the estimation of the channel's transmission coefficient, excess noise and secret key rate.

The expected value of the output voltage $\hat{v}_{\text{H}}(\tau)$ of the coherent receiver in Fig. 5.12 is given by (5.33).

$$\begin{aligned} \langle \hat{v}_{\text{H}}(\tau) \rangle = {} & g_{\text{TIA}} q_e [\eta_{\text{d}_1} \eta_{\text{B}} - \eta_{\text{d}_2}(1 - \eta_{\text{B}})] T |\alpha_{\text{A}}|^2 (h_{\text{BP}}(t) * |M(t)|^2)(\tau) \\ & + g_{\text{TIA}} q_e [\eta_{\text{d}_1}(1 - \eta_{\text{B}}) - \eta_{\text{d}_2} \eta_{\text{B}}] |\alpha_{\text{B}}|^2 (h_{\text{BP}}(t) * 1)(\tau) \\ & + 2 g_{\text{TIA}} q_e (\eta_{\text{d}_1} + \eta_{\text{d}_2}) \sqrt{\eta_{\text{B}}(1 - \eta_{\text{B}}) T} |\alpha_{\text{A}}| |\alpha_{\text{B}}| \\ & \quad \{ h_{\text{BP}}(t) * \cos[(\omega_{\text{A}} - \omega_{\text{B}}) t + \phi_{\text{A}}(t) - \phi_{\text{B}}(t)] \text{Re}[M(t)] \}(\tau), \end{aligned} \tag{5.33}$$

In (5.33), the first and second terms are due to an imperfect subtraction of Alice's and Bob's average power, respectively, and the last term is due to the interference between Alice's modulated signal and Bob's local oscillator. The $(h_{\text{BP}}(t) * 1)(\tau)$ term in (5.33) is due to the constant power nature of Bob's laser signal.

The performance of the CV-QKD system can be assessed through the estimation of the excess noise added to the measured voltage in (5.33). To quantify that, we must calculate the signal variance at Bob's detection system. This variance will have to be computed using a time-sampled numerical code with sampling time dt, in which situation the Dirac delta function is defined as [13]

$$\delta(t) = \begin{cases} \frac{1}{dt}, & 0 < t \leq dt, \\ 0, & \text{otherwise.} \end{cases} \tag{5.34}$$

The variance for $\hat{v}_{\text{H}}(\tau)$ is given by (5.35), where $\text{RIN}_{\Delta f}^{\text{A}}$ and $\text{RIN}_{\Delta f}^{\text{B}}$ are, respectively, the power spectral densities of Alice's and Bob's lasers Random Intensity Noise (RIN).

$$
\begin{aligned}
&\langle \hat{v}_{\mathrm{H}}(\tau)^2 \rangle - \langle \hat{v}_{\mathrm{H}}(\tau) \rangle^2 = g_{\mathrm{TIA}}^2 \varepsilon_{\mathrm{th}}^2 \\
&+ g_{\mathrm{TIA}}^2 q_e^2 [\eta_{\mathrm{d}_1} \eta_{\mathrm{B}} - \eta_{\mathrm{d}_2}(1-\eta_{\mathrm{B}})]^2 T^2 \frac{1}{dt} |\alpha_{\mathrm{A}}|^4 \mathrm{RIN}_{\Delta f}^{\mathrm{A}} (h_{\mathrm{BP}}^2(t) * |M(t)|^4)(\tau) \\
&+ g_{\mathrm{TIA}}^2 q_e^2 [\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) - \eta_{\mathrm{d}_2} \eta_{\mathrm{B}}]^2 \frac{1}{dt} |\alpha_{\mathrm{B}}|^4 \mathrm{RIN}_{\Delta f}^{\mathrm{B}} (h_{\mathrm{BP}}^2(t) * 1)(\tau) \\
&+ g_{\mathrm{TIA}}^2 q_e^2 [\eta_{\mathrm{d}_1} \eta_{\mathrm{B}} + \eta_{\mathrm{d}_2}(1-\eta_{\mathrm{B}})] \frac{1}{dt} T |\alpha_{\mathrm{A}}|^2 (h_{\mathrm{BP}}^2(t) * |M(t)|^2)(\tau) \\
&+ g_{\mathrm{TIA}}^2 q_e^2 [\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) + \eta_{\mathrm{d}_2} \eta_{\mathrm{B}}] \frac{1}{dt} |\alpha_{\mathrm{B}}|^2 (h_{\mathrm{BP}}^2(t) * 1)(\tau) \\
&+ 2 g_{\mathrm{TIA}}^2 q_e^2 (\eta_{\mathrm{d}_1} - \eta_{\mathrm{d}_2}) \sqrt{\eta_{\mathrm{B}}(1-\eta_{\mathrm{B}}) T} \frac{1}{dt} |\alpha_{\mathrm{A}}| |\alpha_{\mathrm{B}}| \\
&\qquad \{ h_{\mathrm{BP}}^2(t) * \cos[(\omega_{\mathrm{A}} - \omega_{\mathrm{B}})t + \phi_{\mathrm{A}}(t) - \phi_{\mathrm{B}}(t)] \mathrm{Re}[M(t)] \}(\tau),
\end{aligned}
\tag{5.35}
$$

In (5.35), the first term is the noise variance due to the thermal noise of the receiver, whereas the second and third terms represent the noise variance due to the RIN from Alice's and Bob's lasers, respectively. The fourth and fifth terms correspond, respectively, to Alice's and Bob's shot noise. The sixth and final term in (5.35) is the shot noise of the interference between Alice's modulated signal and Bob's LO. The final term in (5.35) will take a negative value when $\eta_{\mathrm{d}_1} < \eta_{\mathrm{d}_2}$, this however is not an instance of negative noise but rather a correction to the fourth and fifth terms of the equation. In fact, the last three terms of (5.35) can be rewritten as

$$
\begin{aligned}
&g_{\mathrm{TIA}}^2 q_e^2 \frac{1}{dt} \eta_{\mathrm{d}_1} \left\{ h_{\mathrm{BP}}^2(t) * \left| \sqrt{\eta_{\mathrm{B}} T} \alpha_{\mathrm{A}}(t) M(t) + \sqrt{1-\eta_{\mathrm{B}}} \alpha_{\mathrm{B}}(t) \right|^2 \right\} (\tau) \\
&+ g_{\mathrm{TIA}}^2 q_e^2 \frac{1}{dt} \eta_{\mathrm{d}_2} \left\{ h_{\mathrm{BP}}^2(t) * \left| \sqrt{(1-\eta_{\mathrm{B}}) T} \alpha_{\mathrm{A}}(t) M(t) - \sqrt{\eta_{\mathrm{B}}} \alpha_{\mathrm{B}}(t) \right|^2 \right\} (\tau),
\end{aligned}
\tag{5.36}
$$

where it becomes clear that the combination of the shot noises from both lasers with the interference variance will always have a positive value.

Both channel parameters, transmission, T, and excess noise, ϵ, can be estimated from (5.33) and (5.35). Bob can estimate T through his measured average voltage via [14]

$$
\tilde{T} = \left(\frac{\langle \hat{v}_{\mathrm{H}}(\tau) \rangle}{2 g_{\mathrm{TIA}} q_e \eta_{\mathrm{d}} |\alpha_{\mathrm{A}}| |\alpha_{\mathrm{B}}| \{ h_{\mathrm{BP}}(t) * \cos[(\omega_{\mathrm{A}} - \omega_{\mathrm{B}})t + \phi_{\mathrm{A}}(t) - \phi_{\mathrm{B}}(t)] \mathrm{Re}[M(t)] \}(\tau)} \right)^2, \tag{5.37}
$$

where $\eta_{\mathrm{d}} = \frac{\eta_{\mathrm{d}_1} + \eta_{\mathrm{d}_2}}{2}$ is the mean value of the quantum efficiency of the two photodiodes. In this definition, the transmittance is effectively estimated from the average value of the constellation. Bob can estimate the thermal noise of his receiver by turning off both the signal from the fibre and his receiver laser and then estimate the noise added by his laser by turning on his receiver laser and subtracting the previously observed thermal noise variance from the now observed variance. However, Bob will not be able to distinguish between his laser's shot noise and RIN, as a result his estimation for the shot noise will be given by

$$
\begin{aligned}
\tilde{\Sigma} = &\, g_{\mathrm{TIA}}^2 q_e^2 [\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) - \eta_{\mathrm{d}_2} \eta_{\mathrm{B}}]^2 \frac{1}{dt} |\alpha_{\mathrm{B}}|^4 \mathrm{RIN}_{\Delta f}^{\mathrm{B}} (h_{\mathrm{BP}}^2(t) * 1)(\tau) \\
&+ g_{\mathrm{TIA}}^2 q_e^2 [\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) + \eta_{\mathrm{d}_2} \eta_{\mathrm{B}}] \frac{1}{dt} |\alpha_{\mathrm{B}}|^2 (h_{\mathrm{BP}}^2(t) * 1)(\tau).
\end{aligned}
\tag{5.38}
$$

The excess noise measured by Bob, expressed in shot noise units (SNU), will then correspond to the total variance without Bob's thermal and laser noises (shot noise and RIN) and divided by $\tilde{\Sigma}$. Since the security model assumes that the excess noise is added at the channel input, the variance originating from this subtraction will have to be divided by the estimated channel transmission. In that scenario, the excess noise is estimated by

$$\tilde{\epsilon} = \frac{\langle \hat{v}_{\mathrm{H}}(\tau)^2 \rangle - \langle \hat{v}_{\mathrm{H}}(\tau) \rangle^2 - (g_{\mathrm{TIA}}^2 \varepsilon_{\mathrm{th}}^2 + \tilde{\Sigma})}{\tilde{\Sigma}\tilde{T}}. \tag{5.39}$$

The channel parameters $\tilde{T}$ and $\tilde{\epsilon}$ thus obtained can then be used to estimate the secret key rate.

5.3.2 Performance impact of imperfect receiver devices

In this section, we present numerical results illustrating the impact of device imperfections at Bob's detection system on the estimated channel parameters and subsequently on the estimated secret key rate. In Fig. 5.13 (a) we present the evolution of the estimated channel transmission, expressed in (5.37), as a function of the transmission parameter of Bob's beam-splitter, η_{B} in Fig 5.12. From the results in Fig. 5.13 (a) we can see that when the system is balanced, i.e. $\eta_{\mathrm{B}} = 0.5$, the transmission estimated by Bob will coincide with the real transmission. However, as it further imbalances, the estimated transmission will follow the

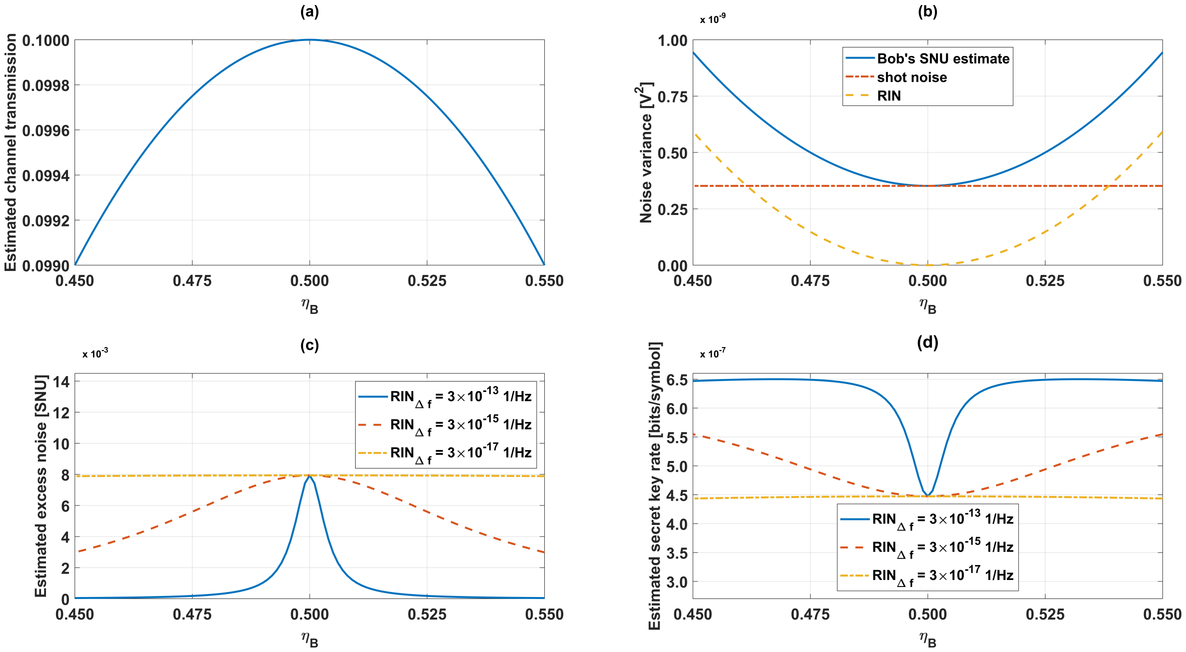


Figure 5.13: Evolution of (a) the estimated channel transmission, given by (5.37), (b) Bob's shot noise estimate, given by (5.38), (c) the estimated excess noise, given by (5.39), and (d) the estimated key rate, given by (5.11), as a function of Bob's beam-splitter transmission coefficient. We have used $T = 0.1$, $g_{\mathrm{TIA}} = 10^4$ V/A, $\varepsilon_{\mathrm{th}} = 1.44 \times 10^{-4}$ Vrms, $|\alpha_{\mathrm{A}}|^2 = 1.25 \times 10^8$ s^{-1}, $|\alpha_{\mathrm{B}}|^2 = 1.56 \times 10^{17}$ s^{-1}, $T_s = 4$ ns, $dt = 31.25$ ps, $\eta_{\mathrm{d}_1} = \eta_{\mathrm{d}_2} = 0.7$ and $\mathrm{RIN}_{\Delta f}^{\mathrm{A}} = \mathrm{RIN}_{\Delta f}^{\mathrm{B}} = 3 \times 10^{-15}$ Hz^{-1}.

curve dictated by $\sqrt{\eta_{\mathrm{B}}(1-\eta_{\mathrm{B}})}$. Note that the first term in (5.33) does not have a major contribution in (5.37), due to the low power of the quantum signal. The second term in (5.33), due to it being a purely DC contribution and DC being filtered out by the bandpass filter $h_{\mathrm{BP}}(t)$, also does not have a major contribution to (5.37).

As stated previously, Bob's shot noise estimate, Σ, will have contributions from both his laser's shot noise and RIN. In Fig. 5.13 (b), we show the dependency of the noise parameters in (5.38) with Bob's beam-splitter transmission coefficient. From the results in Fig. 5.13 (b) we can see that the shot noise contribution remains unchanged with the imbalances, which is to be expected, as the shot noise term in (5.38) is not dependent on η_{B} when $\eta_{\mathrm{d}_1} = \eta_{\mathrm{d}_2}$. Meanwhile, the RIN's contribution rises sharply and rapidly becomes the dominant factor to the global noise at Bob's detection output. The result of the combined shot noise and RIN is an overestimation of the shot noise, which will influence the estimation of the excess noise in relation to it, which can be seen in Fig. 5.13 (c).

In Fig. 5.13 (c), we present the evolution of the estimated excess of noise given by (5.39) in SNU, as a function of Bob's beam-splitter imbalance. The excess noise presented here is due only to Alice's RIN, shot noise and the shot noise of the interference between Alice's modulated signal and Bob's LO, corresponding to the second, fourth and sixth terms of (5.35), respectively. In Fig. 5.13 (c), we can see that, for the different values of RIN, the excess noise will always follow roughly the same behaviour. The estimated excess noise is maximum when the system is balanced and decreases symmetrically around $\eta_{\mathrm{B}} = 0.5$ as it imbalances. This is due to Bob's estimation for the shot noise, Σ, increasing sharply as the system becomes unbalanced, as shown in Fig. 5.13 (b). The higher the RIN, the more pronounced the excess noise underestimation will be. The decrease of the estimated transmission will also have an impact on the estimated excess noise, as the estimated transmission decreases with the increasing imbalance of η_{B}, the estimated excess noise would also increase. However the effect of the increase of $\tilde{\Sigma}$ will be the dominant factor.

The secret key rate can then be estimated for the estimated values of transmission and excess noise following (5.11), yielding the results presented in Fig. 5.13 (d). For the lowest value of RIN the estimated secret key rate will decrease as the η_{B} deviates from 0.5, with this effect being dictated by the decreasing estimated transmission observed in Fig. 5.13 (a). This results in some lost system performance, as usable bits will be discarded. For the other two values of RIN, the underestimation of the excess noise observed in Fig. 5.13 (c) will cause an overestimation of the secure key rate, this poses a security risk as Alice and Bob will distill bits for the key at a rate higher than the channel parameters would allow for a secure key.

In Fig. 5.14 (a), we present the evolution of the estimated channel transmission, defined in (5.37), as a function of the difference between the quantum efficiencies of Bob's photodiodes, identified by η_{d1} and η_{d2} in Fig 5.12, for three different values of η_{B}. From the results in Fig. 5.14 (a) we can see that the estimated transmission follows the curve dictated by $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$, with the different values of η_{B} causing a small vertical shift to the curve. When $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}} > 0$ the transmission will tend to be overestimated, while when $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}} < 0$ it will tend to be underestimated. Furthermore, we can see that equal deviations of η_{B} in either direction, i.e. $\eta_{\mathrm{B}} < 0.5$ and $\eta_{\mathrm{B}} > 0.5$, will result in the same deviation of the estimated channel transmission.

In Fig. 5.14 (b), we show the dependency of $\tilde{\Sigma}$, expressed in (5.38), with the difference between the quantum efficiencies of Bob's photodiodes. We see from Fig. 5.14 (b) that, when $\eta_{\mathrm{B}} = 0.5$, Bob's estimated shot noise has a minimum value, corresponding to the true shot noise, at $\eta_{\mathrm{d1}} = \eta_{\mathrm{d2}}$, and rises as the quantum efficiencies deviate, as the RIN contribution

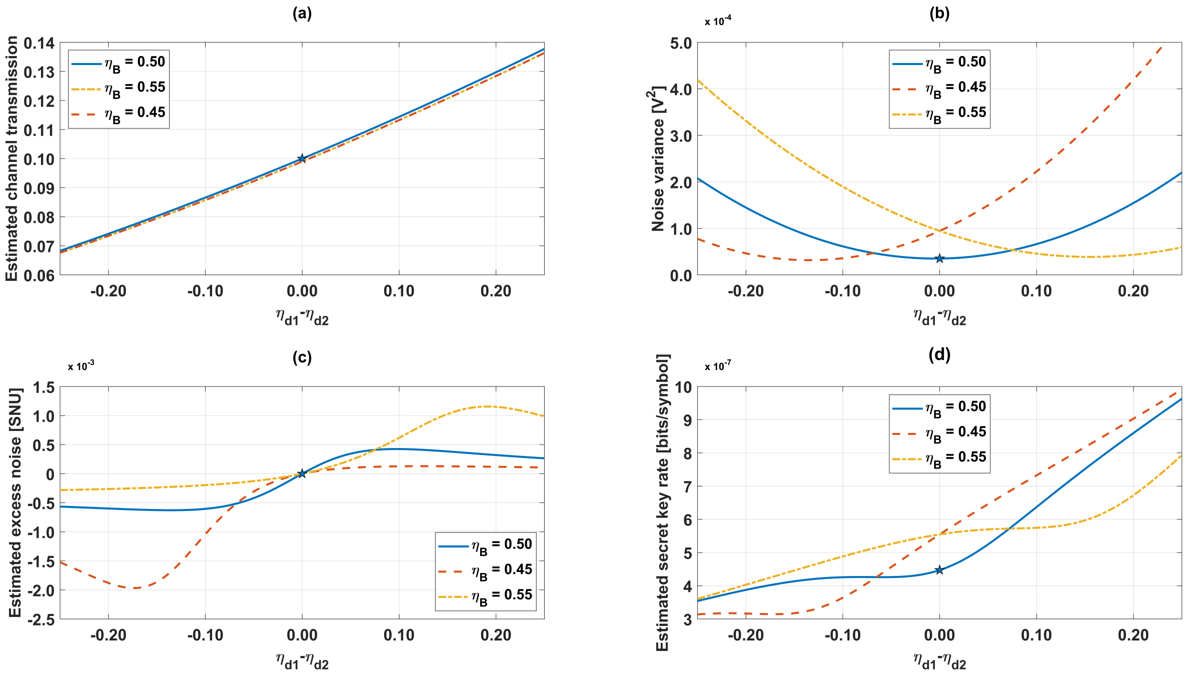


Figure 5.14: Evolution of (a) the estimated channel transmission, given by (5.37), (b) Bob's shot noise estimate, given by (5.38), (c) the estimated excess noise, given by (5.39), and (d) the estimated key rate, given by (5.11), as a function of Bob's photo detector imbalance. We have used $T = 0.1$, $g_{\text{TIA}} = 10^4$ V/A, $\varepsilon_{\text{th}} = 1.44 \times 10^{-4}$ Vrms, $|\alpha_{\text{A}}|^2 = 1.25 \times 10^8$ s^{-1}, $|\alpha_{\text{B}}|^2 = 1.56 \times 10^{17}$ s^{-1}, $T_s = 4$ ns, $dt = 31.25$ ps and $\text{RIN}^{\text{A}}_{\Delta f} = \text{RIN}^{\text{B}}_{\Delta f} = \text{RIN}_{\Delta f} = 3 \times 10^{-15}$ Hz^{-1}. The point corresponding to the balanced system, i.e. the "real" value, is identified by a star.

becomes more and more pronounced. Moreover, in Fig. 5.14 (b), we see that when the value of η_{B} deviates from 0.5, the point at which the value of Bob's estimated shot noise is minimum deviates to negative values of $\eta_{\text{d1}} - \eta_{\text{d2}}$ when $\eta_{\text{B}} < 0.5$ and to positive values of $\eta_{\text{d1}} - \eta_{\text{d2}}$ when $\eta_{\text{B}} > 0.5$. This hints at the fact that imbalances in Bob's beam-splitter may be compensated by tuning the relative values of η_{d1} and η_{d2} and vice versa. Additionally, the value of Bob's estimated shot noise at this minimum point will be slightly below the value observed with the balanced system when $\eta_{\text{B}} < 0.5$ and, conversely, slightly above that value when $\eta_{\text{B}} > 0.5$. This asymmetry is due to the average value of the quantum efficiencies of the photodiodes being lower when $\eta_{\text{d1}} < \eta_{\text{d2}}$ and higher when $\eta_{\text{d1}} > \eta_{\text{d2}}$, causing the second term of (5.38), which corresponds to Bob's laser's shot noise, to increase as the value of $\eta_{\text{d1}} - \eta_{\text{d2}}$ increases.

In Fig. 5.14 (c), we present the evolution of the estimated excess noise, given by (5.39), in SNU, as a function of the difference between the quantum efficiencies of Bob's photodiodes, for three different values of η_{B}. We can see from Fig. 5.14 (c) that all the estimated excess noise curves tend to the same value at $\eta_{\text{d1}} = \eta_{\text{d2}}$, with the excess noise being overestimated when $\eta_{\text{d1}} > \eta_{\text{d2}}$ and underestimated when $\eta_{\text{d1}} < \eta_{\text{d2}}$. When $\eta_{\text{d1}} < \eta_{\text{d2}}$, the estimated excess noise quickly becomes negative, this happens because, in this situation, the excess noise is dominated by the sixth term in (5.35), which itself becomes negative when $\eta_{\text{d1}} < \eta_{\text{d2}}$. Recall that in our case the only excess noise contributions are due to noise originating in Alice's transmission system and due to the interference noise between Alice's signal and Bob's LO, in the presence of other, likely higher, channel noise contributions, the excess noise would not take a negative value, but would rather have a reduced value when compared to a balanced system. Additionally, for $\eta_{\mathrm{B}} = 0.5$, when $\eta_{\mathrm{d1}} < \eta_{\mathrm{d2}}$ the excess noise estimate will decrease until it reaches a minimum and when $\eta_{\mathrm{d1}} > \eta_{\mathrm{d2}}$ it increases until it reaches a maximum. However, this curve is not symmetric, with the minimum value observed not having the same absolute value as the maximum observed value. Meanwhile, when $\eta_{\mathrm{B}} = 0.45$, the excess noise estimate will exhibit a minimum with a lower value and located at a lower value of $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$ and a maximum with a lower value located at a higher value of $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$, when compared to the values for $\eta_{\mathrm{B}} = 0.5$. Conversely, when $\eta_{\mathrm{B}} = 0.55$, the excess noise estimate will exhibit only the maximum observed when $\eta_{\mathrm{d1}} > \eta_{\mathrm{d2}}$, having a higher value and being located at a greater value of $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$, again when compared to the values for $\eta_{\mathrm{B}} = 0.5$. These three curves show a very asymmetric dependency of the excess noise with the photodetector imbalances, this asymmetry is again due to the contribution of the sixth term in (5.35), which is itself asymmetric, and due to the excess noise's dependency on the estimated channel transmission, shown in Fig. 5.14 (a), which will cause the estimated excess noise values when $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}} < 0$ to have a higher absolute value than the ones estimated when $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}} > 0$.

The secret key rate can again be estimated for the estimated values of transmission and excess noise following (5.11), yielding the results presented in Fig. 5.14 (d). We can see from Fig. 5.14 (d) that, for both $\eta_{\mathrm{B}} = 0.5$ and $\eta_{\mathrm{B}} = 0.45$, the estimated secret key rate will, generally, increase as $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$ increases, apart from a short decreasing region. Meanwhile, when $\eta_{\mathrm{B}} = 0.55$, the estimated secret key rate will always increase as $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$ increases. The evolution of the estimated key rate in function of the photodiode imbalance is dominated by the estimated value for the channel transmission, shown in Fig. 5.14 (a), which increases linearly with $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$. The regions where the growth of the estimated key rate slows down, and in the case of $\eta_{\mathrm{B}} = 0.5$ and $\eta_{\mathrm{B}} = 0.45$ stops, are due to the contribution of the excess noise, whose maximum and minimums roughly coincide with these regions. Depending on the exact position in the x-axis, this means that these combined beam-splitter and photodiode quantum efficiencies will result in either an over or under estimation of the secret key rate. In the scenario of an overestimation of the secret key rate, this will pose a security risk as Alice and Bob will distillate bits for the key at a rate higher than the channel parameters would allow for a secure key, while in the case of an underestimation there will be lost performance, as Alice and Bob will discard more bits than they had to.

5.4 Summary

In this Chapter we have studied the impact of device imperfections and imbalances on both the intrinsic key rate available and on the key rate naively estimated by Bob and Alice. We observe that modulation stage imbalances reduce the maximum achievable secure key rate, however, much more impacted is the naively estimated key rate, meaning that there is a considerable loss of performance. However, and rather importantly working in the naive mode with modulator imbalances does not cause the secure key rate to be over-estimated, as a result the security of the generated keys is not impacted. We also see that, under certain imbalance scenarios and for both the real and naive values, the optimal constellation can vary, as a result the choice of constellation to be used in a given system should take possible imbalances in consideration. Additionally, we also performed a detailed study on the impact of receiver imbalances on the channel parameters estimated by Bob and the subsequent impact on the estimated secure key rate. We observe that non-monitored imbalances in the receiver beam-splitter and photodiode quantum efficiencies may pose a security risk, as it will cause Alice and Bob to overestimate their secret key rate. For example, a 2% imbalance of the transmission coefficient of Bob's beam-splitter transmission coefficient will lead up to a 44% overestimation of the key rate. Moreover, receiver imbalances may also lead to a reduced performance of the key distribution system, as the wrongly estimated channel parameters can also lead to a slight underestimation of the secret key rate. For example, in the absence of other receiver imbalances, a 2% deviation between the values of the quantum efficiencies of the photodiodes may lead to either a 3% underestimation or a 4% overestimation of the key rate. However, when the 2% deviation between the values of the quantum efficiencies of the photodiodes is combined with a 5% imbalance of the transmission coefficient of Bob's beam-splitter, the key rate can then be overestimated by 30%, when $\eta_{\mathrm{B}} = 0.45$, or by 25%, when $\eta_{\mathrm{B}} = 0.55$.

All these results clearly indicate that a precise characterization of the experimental system's components should be performed in order correctly estimate the secure key rate and to choose the best constellation.

Bibliography

[1] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[2] A Becir, FAA El-Orany, and MRB Wahiddin. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10(01):1250004, 2012.

[3] Anthony Leverrier. *Theoretical study of continuous-variable quantum key distribution.* PhD thesis, Télécom ParisTech, 2009.

[4] François Roumestan, Amirhossein Ghazisaeidi, Jérémie Renaudier, Luis Trigo Vidarte, Eleni Diamanti, and Philippe Grangier. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In *2021 European Conference on Optical Communication (ECOC)*, pages 1–4. IEEE, 2021.

[5] Margarida Almeida. Practical security limits of continuous-variable quantum key distribution. Master's thesis, University of Aveiro, 2021.

[6] Wenyuan Liu, Xuyang Wang, Ning Wang, Shanna Du, and Yongmin Li. Imperfect state preparation in continuous-variable quantum key distribution. *Physical Review A*, 96(4):042312, 2017.

[7] Sebastian Kleis, Max Rueckmann, and Christian G Schaeffer. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics letters*, 42(8):1588–1591, 2017.

[8] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 2021.

[9] Xiangyu Wang, Yi-Chen Zhang, Zhengyu Li, Bingjie Xu, Song Yu, and Hong Guo. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *arXiv preprint arXiv:1703.04916*, 2017.

[10] Hossein Mani, UL Andersen, T Gehring, C Pacher, S Forchhammer, JM Mateo, and M Vicente. Error reconciliation protocols for continuous-variable quantum key distribution. *Ph. D. dissertation, Technical University of Denmark*, 2021.

[11] Margarida Almeida, Daniel Pereira, Nelson Muga, Margarida Facão, Armando N Pinto, and Nuno A Silva. Secret key rate of multi-ring m-apsk continuous variable quantum key distribution. *Optics Express*, 10 2021.

[12] Rodney Loudon. *The quantum theory of light.* OUP Oxford, 2000.

[13] Paul Adrien Maurice Dirac. *The principles of quantum mechanics.* Number 27. Oxford university press, 1981.

[14] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

Chapter 6

Conclusions and Open Issues

In this Chapter we summarize the conclusions and impact of the results obtained in developing this thesis, where we focused on the implementation and optimization of a Continuous Variables Quantum Key Distribution (CV-QKD) system. However, in the concluding stages of this project, we identified still open questions in the area of CV-QKD.

This Chapter is split into two sections. In Section 6.1 we present a summary of the main conclusions and results obtained in this work. We conclude this thesis with a discussion on the future avenues of research that may follow this work, presented in Section 6.2.

6.1 Conclusions

The topics tackled in this thesis aimed at improving the performance of CV-QKD systems, making them more resilient to real-world practical impairments and showing that both these objectives can be accomplished while maintaining costs of implementation relatively low. We validated our work with experimental results wherever possible, and otherwise endeavored to use realistic values when an experimental verification was not possible.

We first present the theoretical basis for the functioning of CV-QKD systems, establishing the first principles in play and describing a generalized QKD protocol. We then presented an updated proof of security for Discrete Modulation (DM) CV-QKD systems, taking a practical approach at how the security limits may be obtained numerically. We show how, under the right, somewhat optimistic, circumstances, CV-QKD systems using 8-PSK constellations are capable of achieving distances of almost 80 km in the asymptotic regime, thus being suitable for medium-range, inter-city links. We also performed an exploration of the impact of uncertainties in the estimated channel and receiver parameters on the security of a CV-QKD system. From that study we observe that performance in the Finite Size Effects (FSE) regime is greatly reduced, and to achieve the transmission distances observed in the asymptotic regime, well over 2^{30} symbols have to be transmitted, requiring a large amount of storage, processing power and a very stable channel.

We then proceeded to implement our previously explored system, first in simulation and then experimentally. We propose a novel polarization diverse receiver architecture that avoids the need for manual calibration or complex feedback loops to recover from random polarization drift, an unavoidable phenomena in field deployed fibers. Our proposed system works by detecting both polarizations independently using heterodyne detection and then performing a modified Constant Modulus Algorithm (CMA) routine. We performed an in depth study on the impact of polarization drift on the security of CV-QKD and show that our system, under an ideal scenario, is capable of fully mitigating it. We validated our proposed system experimentally both with an high-power classical signal and a low-power, quantum signal. Our system was capable of working for an indefinite period of time at a transmission distance compatible with metro network connections, and was able to generate 50 secure keys, in the asymptotic regime, from our 300 snapshots, with an average key rate of ∼0.001 bits/symbol. We also presented some results from our Lisbon field trial, the first of a CV-QKD system in Portugal. During the field trial the system was capable of sharing an updated key at a rate of one key per minute, being limited in this regard by the capability of the computer performing the post processing.

Avenues for improving the performance of the previously proposed CV-QKD system were then explored. We first looked at how the performance of our DM-CV-QKD communication system can be improved, by transitioning to PCS-128-APSK constellation formats. We showed that this alteration enables us to reach an extra 50 km of transmission distance, a 10 fold increase in excess noise resistance and at least a 3-fold increase in the allowable photon-number, when compared to the 8 symbol Phase Shift Keying (PSK) based system. The capability to withstand much worse channel parameters also enables us to reach the same performance as the 8-PSK one in the finite size scenario while using 95% fewer samples, greatly reducing the post-processing hardware requirements. We presented results from our experimental system where we show that, after the conversion to the PCS-128-APSK constellation formats, our average key rate rose by a factor of 10 to ∼0.01 bits/symbol, corresponding to 79% of the performance of an equivalent GM-CV-QKD system. Our experimental system was tested with a fiber channel of 40 km and would be suitable to work in the finite size regime in both metro network connections and some short- to medium-range inter-city connections, provided that a substantial but ultimately manageable increase in the block size is performed. Furthermore, we show that, in the asymptotic regime, our system is capable of reaching distances in excess of 185 km, and in that regime would be compatible with medium- to long-range inter-city connections. We also presented a technique to allow for our system to perform sequence synchronization as well as receiver and channel parameter estimation efficiently. Through the use of an auxiliary QPSK channel we are able to recover sequence synchronization using only a fraction of the number of symbols required by our previous, header-based technique, in a manner that scales well with increasing block sizes.

We then proceeded to study the impact of device imperfections and imbalances on both the intrinsic key rate available and on the key rate naively estimated by Bob and Alice. We observed that modulation stage imbalances reduce the maximum achievable secure key rate, however, much more impacted was the naively estimated key rate, leading to a considerable loss of performance. However, and rather importantly, working in the naive mode with modulator imbalances does not cause the secure key rate to be over-estimated, as a result the security of the generated keys is not impacted. We also see that, under certain imbalance scenarios and for both the real and naive values, the optimal constellation can vary, as a result the choice of constellation to be used in a given system should take possible imbalances in consideration. Additionally, we also performed a detailed study on the impact of receiver imbalances on the channel parameters estimated by Bob and the subsequent impact on the estimated secure key rate. We observe that non-monitored imbalances in the receiver beam-splitter and photodiode quantum efficiencies may pose a security risk, as it will cause Alice and Bob to overestimate their secret key rate. For example, a 2% imbalance of the transmission coefficient of Bob's beam-splitter transmission coefficient will lead up to a 44% overestimation of the key rate. Moreover, receiver imbalances may also lead to a reduced performance of the key distribution system, as the wrongly estimated channel parameters can also lead to a slight underestimation of the secret key rate. For example, in the absence of other receiver imbalances, a 2% deviation between the values of the quantum efficiencies of the photodiodes may lead to either a 3% underestimation or a 4% overestimation of the key rate. However, when the 2% deviation between the values of the quantum efficiencies of the photodiodes is combined with a 5% imbalance of the transmission coefficient of Bob's beam-splitter, the key rate can then be overestimated by up to 30%.

To conclude, we were able to implement a DM-CV-QKD system using telecom-grade components and managed to achieve performances comparable to that of optimum, Gaussian Modulation (GM) based systems. Our implemented system was shown to be able to function at distances compatible with metro-network connections. We also were able to show that CV-QKD systems are capable of functioning in realistic scenarios, using imperfect devices, provided that those imperfections are accounted for.

6.2 Open Issues

Despite our contributions, this thesis did not exhaust all issues with CV-QKD systems. In fact, a some issues have been uncovered by it. We have identified the following topics that may be interesting to explore:

- Implement the post-processing component of the system in a high-speed platform (for example a Field-Programmable Gate Array (FPGA) and/or a Graphics Processing Unit (GPU)), in order to allow for a real-time implementation of the system;

- Optimize the choice of the constellation format taking into account the limited bandwidth of the authenticated classical channel that is used for key reconciliation;

- Expand the study on the impact of imbalances to the case of the polarization diverse receiver system presented in Chapter 3, considering both imperfections of the experimental components of the receiver as well as inaccuracies in the associated CMA stage;

- Develop methods for estimating experimental device imbalances in real time, to allow for application of the results obtained in Chapter 5. This would provide not only a validation of the obtained results but would also contribute to improving the performance and security of experimental CV-QKD systems at large.