POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Practical Implementation of Discrete and Continuous Variable Quantum Key Distribution in Passive Optical Networks

Tesi di Laurea Magistrale in Telecommunication Engineering - Ingegneria delle Telecomunicazioni

Author: **Francesco Fumagalli**

Student ID: 248764
Advisor: Prof. Alberto Gatto
Co-advisors: Dr. Alessandro Gagliano
Academic Year: 2024-2025

Abstract

The imminent advent of quantum computing threatens classical cryptography, making Quantum Key Distribution (QKD) essential to guarantee the unconditional security of future networks. This thesis compares the Discrete-Variable (DV) and Continuous-Variable (CV) paradigms within access infrastructures, specifically Passive Optical Networks (PONs). Their coexistence with classical channels is hindered by severe Spontaneous Raman Scattering (SpRS) noise which, combined with the losses introduced by optical splitters, drastically degrades system performance. The study rigorously evaluates both architectures in the finite-key regime, overcoming idealized asymptotic assumptions to quantify the real statistical uncertainties of practical transmissions. Through a dedicated MATLAB simulator equipped with a Graphical User Interface (GUI), the Secret Key Rate (SKR) was evaluated as a function of the transmitted block size, spectral allocation and distance. The results highlight a clear technological trade-off. The DV approach, although limited to narrower bands due to its sensitivity to Raman noise, emerges as the most robust solution for high-density networks, supporting up to 32 users over 20 km. A critical exception is represented by the XG-PON standard, where such performance collapses. Conversely, the CV approach leverages coherent detection to filter Raman interference, providing significantly higher generation rates and requiring a notably smaller transmitted block size to initiate secure transmission. Ultimately, DV-QKD confirms itself as the optimal choice for networks with a high number of users, whereas CV-QKD dominates the XG-PON and low number of users scenarios.

Keywords: Quantum Key Distribution, Secret Key Rate, Finite-key regime, Spontaneous Raman Scattering, Discrete Variable, Continuous Variable, Passive Optical Networks

Abstract in lingua italiana

L'imminente avvento della computazione quantistica minaccia la crittografia classica, rendendo la Distribuzione di Chiave Quantistica essenziale per garantire la sicurezza incondizionata delle reti future. Questa tesi confronta i paradigmi a Variabile Discreta e a Variabile Continua all'interno delle infrastrutture di accesso, nello specifico le reti ottice passive. La loro coesistenza con i canali classici è ostacolata dal severo rumore di Scattering Raman Spontaneo che, combinato con le perdite introdotte dagli splitter ottici, degrada drasticamente le prestazioni del sistema. Lo studio valuta rigorosamente entrambe le architetture nel regime a chiave finita, superando le idealizzate assunzioni asintotiche per quantificare le reali incertezze statistiche delle trasmissioni pratiche. Tramite un simulatore MATLAB dedicato, dotato di interfaccia grafica, è stato valutato il tasso di generazione della chiave segreta in funzione della dimensione del numero di stati inviati, dell'allocazione spettrale e della distanza. I risultati evidenziano un netto compromesso tecnologico. L'approccio a Variabile Discreta, seppur limitato a bande più ristrette per la sensibilità al rumore Raman, emerge come la soluzione più robusta per reti ad alta densità, supportando fino a 32 utenti su 20 km. Un'eccezione critica è rappresentata dallo standard XG-PON, dove tali prestazioni collassano. Al contrario, la Variabile Continua sfrutta la rivelazione coerente per filtrare l'interferenza Raman, fornendo tassi di generazione nettamente superiori e richiedendo una dimensione del blocco inviato notevolmente inferiore per avviare la trasmissione sicura. In definitiva, la Variabile Discreta si conferma la scelta ottimale per le reti con elevato numero di utenti, mentre la Variabile Continua domina gli scenari XG-PON e con ridotto numero di utenti.

Parole chiave: Distribuzione di Chiave Quantistica, tasso di generazione della chiave segreta, regime a chiave finita, rumore Raman Spontaneo, Variabile Discreta, Variabile Continua, Reti Ottiche Passive

Contents

Introduction

[1] Cryptography plays a fundamental role in modern digital security, ensuring data confidentiality and user privacy across global communication networks. While the discipline has evolved significantly since its historical origins, contemporary cryptographic standards fundamentally rely on the computational hardness of complex mathematical problems, such as large integer factorization and discrete logarithms. Although these algorithms remain robust against classical computational paradigms, the advent of quantum computers poses a fatal threat to their security, threatening to render current encryption protocols obsolete. To address this vulnerability, the field of Quantum Information has advanced two primary countermeasures: Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). While PQC aims to secure communications through novel mathematical algorithms presumed to be resistant to quantum attacks, offering a highly deployable software-based solution, QKD leverages the fundamental laws of quantum physics to guarantee unconditional, information-theoretic security at the physical layer. This thesis focuses exclusively on the latter. Based on the fundamental laws of quantum mechanics, QKD enables a symmetric key exchange between legitimate parties guaranteeing perfect secrecy. Historically, the first approach to QKD, introduced by Bennett and Brassard in 1984, relied on the transmission of quantum states chosen into a limited and discrete set (Discrete Variable QKD - DV-QKD), encoding the information into the properties of single photons generated by highly attenuated laser sources and detected by suitable single-photon detectors. Conversely, the more recent Continuous-Variable (CV-QKD) approach encodes information into the amplitude and phase quadratures of the electromagnetic field, advantageously exploiting standard coherent telecommunication receivers. While early practical implementations of QKD relied on dedicated dark fibers, the current strategic focus has shifted toward the integration of quantum channels into existing classical communication infrastructures to avoid prohibitive deployment costs. This thesis specifically investigates this coexistence scenario within access networks, utilizing Passive

[1] Editorial Note: To refine the clarity and linguistic consistency of this manuscript, the author used Google Gemini language model as a writing assistant. The tool was employed exclusively for grammar correction, style refinement and improving textual fluency. All scientific concepts, theoretical models, analyses, results and discussions remain entirely the original work of the author.

Optical Networks (PONs) as the reference architecture. Deploying QKD over PONs is significantly more challenging than standard point-to-point links. The coexistence of fragile quantum states multiplexed with high-power classical data streams requires to cope with severe non-linear effects, most notably Spontaneous Raman Scattering (SpRS). During propagation, classical photons undergo inelastic scattering, generating a continuous flux of noise photons at both higher (Stokes region) and lower (anti-Stokes region) wavelengths. This phenomenon severely impairs the quantum channel, acting as indistinguishable background noise that particularly cripples single-photon transmission, whereas the intrinsic spatial and spectral filtering properties of coherent receivers make CV-QKD naturally more resilient. Furthermore, PON architectures rely on passive optical splitters, which broadcast the incoming signal to multiple users. These components act as severe attenuators, introducing a massive, localized loss penalty that scales directly with the number of served ports. To comprehensively evaluate and compare the performance of DV-QKD and CV-QKD under these severe architectural constraints, the Secret Key Rate (SKR) serves as the primary performance indicator. In this thesis, a rigorous evaluation of both DV- and CV-QKD approaches in the finite-key regime is carried out. By surpassing the idealized asymptotic assumption, this work properly accounts for the statistical uncertainties and fluctuation penalties inherent in practical parameter estimation, always present in real-world implementations. To perform this comparative analysis, a suitable MATLAB simulator, equipped with a Graphical User Interface (GUI), has been developed. Firstly, the analysis focuses on the direct impact of the finite-key regime by evaluating the SKR as a function of the total number of transmitted symbols, thereby rigorously quantifying the physical penalties induced by finite block sizes. Then, it enables the precise identification of the optimal quantum spectral bands for both approaches—minimizing SpRS noise interference—across various next-generation PON standards and user splitting. Finally, the simulator is employed to assess the SKR against the overall transmission distance, providing a definitive comparison of the maximum reachable secure distance and the architectural scalability of each paradigm in a realistic coexistence scenario.

The thesis is organized as follows:

Chapter 1 presents the state of the art of Quantum Key Distribution, detailing the fundamental characteristics of both Discrete-Variable (DV) and Continuous-Variable (CV) approaches. It provides a comprehensive description of the most prominent protocols for each paradigm, establishing the theoretical baseline for the thesis.

Chapter 2 details the Passive Optical Network (PON) architecture, reviewing the principal existing standards (GPON, XG-PON, NG-PON2 and HS-PON) alongside their specific characteristics, i.e. spectral allocations and launch powers. Moreover, a rigorous

analyis of the primary physical impairments in classical-quantum coexistence, namely fiber attenuation and Spontaneous Raman Scattering (SpRS), is presented.

Chapter 3 derives the theoretical Secret Key Rate (SKR) formulations for both DV and CV-QKD within the finite-key regime. These mathematical models are subsequently implemented, analyzed and computationally optimized in a baseline point-to-point dark fiber scenario to benchmark their ideal cryptographic performance.

Chapter 4 presents the developed MATLAB simulation tool and its Graphical User Interface (GUI). It outlines the underlying multi-layered software architecture designed to seamlessly integrate the theoretical quantum cryptographic models with the physical parameters of the PON infrastructure.

Chapter 5 leverages the developed software to conduct a comprehensive comparative analysis between DV- and CV-QKD in an integrated PON environment. It systematically evaluates the protocols' performance against the finite block size, identifying optimal quantum spectral allocations and assessing the SKR across varying transmission distances.

Chapter 6 summarizes the main findings of the comparative study, drawing final conclusions on the viability and scalability of DV- and CV-QKD in access networks. Finally, it outlines potential future developments and research directions in the field of quantum-classical coexistence.

1 | Cryptography and Quantum Key Distribution

1.1. Classical Security

Cryptography (from the Greek *kryptós*, "hidden", and *gráphein*, "to write") is the branch of mathematics dedicated to the study of techniques designed to render information unintelligible to unauthorized third parties [1]. Its primary objective is to guarantee the confidentiality of the original message, denoted as the plaintext (m), protecting it from any adversary, often referred to as an *eavesdropper*, capable of intercepting the communication. Although historically encryption techniques were the almost exclusive domain of the military sector, in the current digital era cryptography has become an essential pillar for the security of personal, financial and sensitive data in daily communications. Through the years, many encoding techniques have been developed, which can be distinguished into two main categories [2]:

- *Symmetric key cryptography (or Private-key)*: the two communicating parties (Alice and Bob) share the same secret key k, utilized for both encryption and decryption. Although computationally efficient, it requires that the parties have previously established a secure channel to exchange the key.
- *Asymmetric key cryptography (or Public-key)*: each user possesses a pair of keys: a *public key*, known to everyone, used for encryption and a *private key*, kept secret, used for decryption. This resolves the key exchange problem but entails a significantly higher computational cost.

1.1.1. Symmetric Cryptography

Focusing on symmetric cryptography, the formal theoretical framework was introduced by Claude Shannon in 1949 [3]. As illustrated in Figure 1.1, the system is defined by a triple of algorithms (Gen, Enc, Dec):

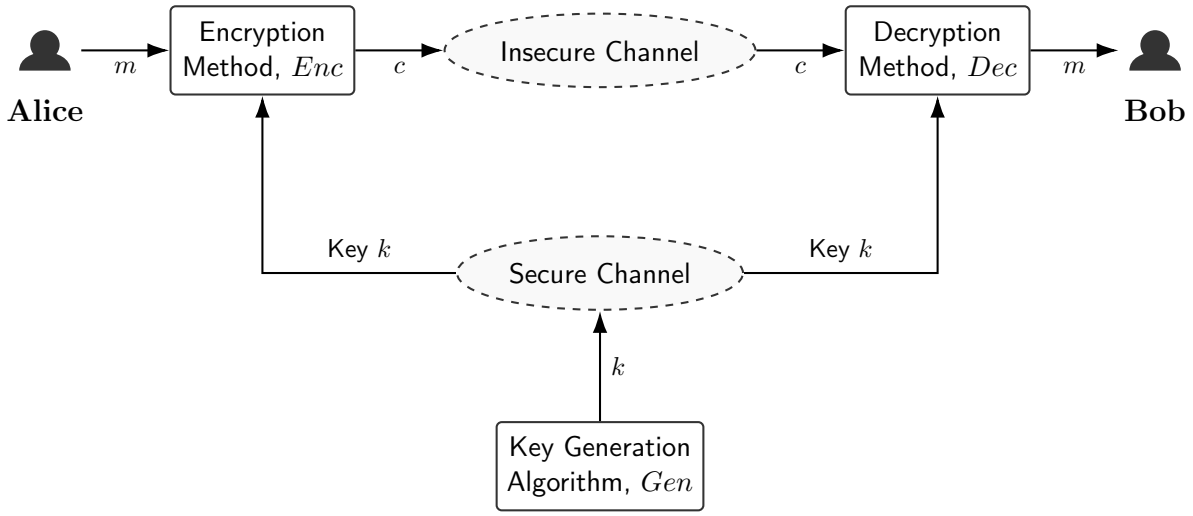


Figure 1.1: Schematic representation of a symmetric cryptography system.

1. *Gen*: a probabilistic algorithm that chooses a key k uniformly at random from the key space $\mathcal{K}$.

2. *Enc*: the encryption algorithm which, given a message m and the key k, produces the *ciphertext* c:

$$c = Enc_k(m) \tag{1.1}$$

3. *Dec*: the deterministic decryption algorithm which retrieves the original message:

$$m = Dec_k(c) \tag{1.2}$$

Shannon defined the concept of *perfect secrecy* (or *unconditional security*): in this scenario, it is assumed that the attacker has unbounded computational resources but is purely passive, meaning they are interested only in confidentiality and not in forging messages. A cipher enjoys perfect secrecy if the ciphertext reveals no information about the plaintext. Mathematically, this implies that the probability of observing a certain cryptogram c is identical regardless of the message sent (m_0 or m_1):

$$\Pr[Enc_k(m_0) = c] = \Pr[Enc_k(m_1) = c] \tag{1.3}$$

Historically, one of the earliest implementation attempts was the Caesar Cipher, used in the Roman era to protect military strategies [1]. It is a simple monoalphabetic substitution cipher where the key $k \in [0, 25]$ represents the shift of the alphabet letters. However, a fundamental step towards modern cryptography and the realization of Shannon's theo-

retical model occurred in 1917 with Gilbert Vernam and his *One Time Pad* (OTP). The OTP operates on binary strings by applying the logical XOR operation ($\oplus$) between the bits of the message and those of the key:

$$c = m \oplus k \tag{1.4}$$

The OTP is the practical implementation of perfect secrecy, but to be valid it must satisfy stringent conditions: the key must be purely random, at least as long as the message and used only once. These conditions make the OTP impractical for mass telecommunications: if a secure channel is capable of transmitting keys as long as the messages existed, it could be used to send the messages directly. Nevertheless, the OTP remains the theoretical benchmark for absolute security, a concept central to Quantum Key Distribution (QKD). Since perfect secrecy is difficult to achieve in standard classical networks, modern cryptography relies on *semantic security* (or *computational security*). In this framework, it is assumed that the adversary has limited (polynomial) computational resources. A system is defined as secure if the adversary's advantage in distinguishing between two encrypted messages is negligible, which specifically means lower than a minimum threshold ϵ:

$$Adv = |\Pr[Exp(0) = 1] - \Pr[Exp(1) = 1]| \leq \epsilon \tag{1.5}$$

where the experiment $Exp(b)$ represents a cryptographic game in which the adversary attempts to guess which message was encrypted. To realize this in practice, two main approaches are used. The first are *stream ciphers*, which attempt to approximate the OTP using a short key (the seed) expanded by a deterministic algorithm called a *Pseudorandom Generato*r (PRG). The PRG produces a long stream of bits (keystream) that appears random, which is then XORed with the message. While they do not offer perfect secrecy, they are extremely fast and hardware-efficient. The second approach involves *block ciphers*, which operate by dividing the plaintext into fixed-size blocks (e.g., 128 bits). The key controls a complex permutation function that transforms the input block into the output. According to Shannon's principles, a good block cipher must guarantee:

- *Confusion*: the relationship between the key and the ciphertext must be complex.
- *Diffusion*: changing a single bit of the plaintext should modify, on average, half of the ciphertext bits (avalanche effect).

The most widespread current standard for this category is the *Advanced Encryption Standard* (AES), which supports key sizes of 128, 192 and 256 bits.

1.1.2. Asymmetric Cryptography

The second fundamental category of encryption schemes is asymmetric cryptography, also known as public-key cryptography. As illustrated in Figure 1.2, the architectural model differs significantly from the symmetric approach. In this framework, rather than sharing a single secret, a pair of mathematically related keys is generated for each user:

- A public key (pk): widely distributed and accessible to all users, used to encrypt messages intended for the key's owner;
- A secret key (sk) (or private key): kept exclusively by the owner and never shared, used to decrypt the received ciphertexts.

The encryption and decryption processes are described formally by the following equations:

$$c = Enc_{pk}(m) \tag{1.6}$$

$$m = Dec_{sk}(c) \tag{1.7}$$

Regarding the distribution channels, the requirements change compared to the symmetric model. The secret key is generated locally and must be stored securely, never requiring transmission across the network. The public key, conversely, can be sent over an insecure channel, provided that the channel is authenticated to prevent active attacks, ensuring that the key belongs to the legitimate entity. This scheme was first introduced by Whitfield Diffie and Martin Hellman in 1975 [4], revolutionizing the field. Its primary advantages are the simplified key management and distribution: in a network of N users, each user only needs to manage their own key pair, rather than establishing $N(N-1)/2$ shared secrets. However, this scalability comes at a cost: asymmetric algorithms are sig-

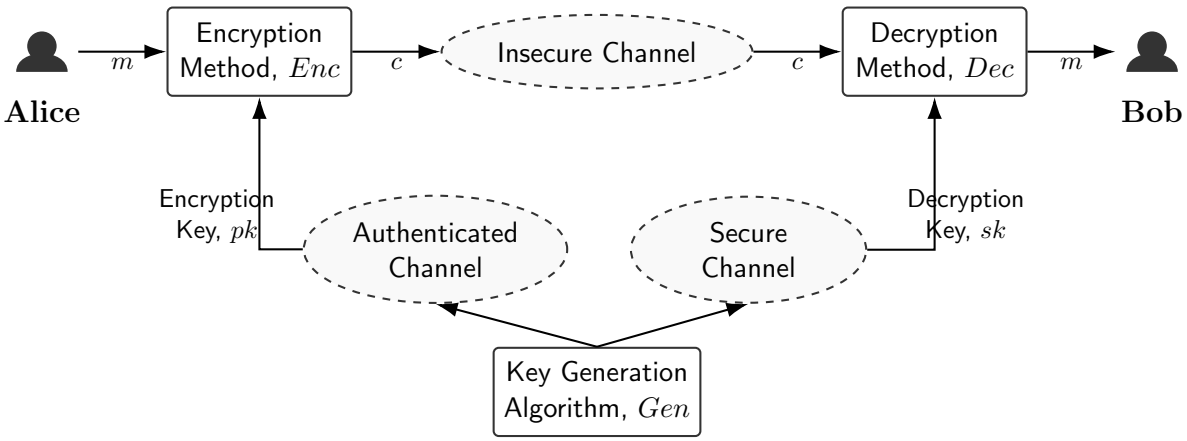


Figure 1.2: Schematic representation of an asymmetric (public-key) cryptography system.

nificantly more computationally intensive and slower than their symmetric counterparts. The security of this paradigm relies on computational complexity. It is based on one-way trapdoor functions: mathematical operations that are easy to compute in one direction (encryption) but computationally infeasible to reverse (decryption) without the special "trapdoor" information contained in the secret key. Historically, the security of systems like RSA, taking the name from its inventors R.L. Rivest, A. Shamir and L. Adleman [5], was based on the integer factorization problem (the difficulty of decomposing large integers into prime factors). However, as computing power has increased and factorization algorithms have improved, larger key sizes have become necessary to maintain security. Consequently, modern cryptography has increasingly shifted towards problems based on Discrete Logarithms, specifically leading to the adoption of the Diffie-Hellman Key Exchange (DHKE) and Elliptic Curve Cryptography (ECC), which offer equivalent security with smaller key sizes.

1.2. Introduction to Quantum Key Distribution

Since the development of the theoretical model for the universal computer by John von Neumann and Alan Turing, computational power has experienced exponential growth. This trend was empirically observed in 1965 by Gordon Moore, whose law stated that the number of transistors in a dense integrated circuit—and consequently computational power—would double approximately every two years. However, as transistors shrink to atomic dimensions, classical computing encounters physical boundaries dictated by quantum mechanics. Rather than viewing these quantum effects as detrimental limitations, the scientific community began to theorize a new computational paradigm that actively exploits them: quantum computing.

Unlike classical computers, which encode information in binary digits (bits) strictly confined to mutually exclusive states of either 0 or 1, quantum computers operate using quantum bits, or *qubits* [6]. Governed by the principles of quantum mechanics, a qubit can exist in a coherent superposition of both states simultaneously. Furthermore, multiple qubits can be linked through quantum entanglement, a property that exponentially increases the state space of the system with each additional qubit. This fundamental shift in information representation allows quantum processors to perform highly parallel computations, evaluating massive amounts of possibilities concurrently. While this architecture holds unprecedented potential for scientific advancement, it also poses a fatal threat to current cryptographic standards. In 1994, Peter Shor demonstrated that a sufficiently powerful quantum computer could exploit this quantum parallelism to solve the integer factorization and discrete logarithm problems in polynomial time [7]. Shor's algorithm

effectively breaks the foundational security of widely used public-key cryptosystems, such as the RSA and Diffie-Hellman protocols. To address this impending vulnerability, two main research directions have emerged:

- *Post-Quantum Cryptography*: this approach focuses on developing new classical algorithms based on mathematical problems that are believed to be hard even for quantum computers [8]. Its security still relies on computational complexity assumptions.
- *Quantum Key Distribution* (QKD): this method guarantees secure key exchange based on the fundamental laws of quantum mechanics, offering information-theoretic security independent of the adversary's computational power.

This thesis focuses on the second approach. In the realm of Quantum Information, the qubit is described as a linear combination of two computational basis states, denoted in Dirac notation as $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.8}$$

where α and β are complex numbers known as probability amplitudes that must satisfy the probabilistic condition:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.9}$$

The phenomenon for which the qubit follows a probabilistic distribution between the states 0 and 1 is known as the *Quantum Superposition Principle*. However, the superposition exists only until a measurement is performed. A fundamental postulate of quantum mechanics states that measuring a qubit forces it to "collapse" irreversibly into one of the basis states: the outcome will be $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. Once measured, the quantum information is lost, and the qubit behaves like a classical bit. One of the most important laws of quantum mechanics is rooted in the *no-cloning theorem*, which asserts that it is impossible to create an identical copy of an arbitrary unknown quantum state. In the context of key distribution, this implies that an eavesdropper (Eve) cannot copy the key transmitted through the quantum channel between the legitimate parties (Alice and Bob). Any attempt by Eve to measure or clone the qubits in transit will inevitably perturb the quantum states. This disturbance introduces errors (noise) into the transmission, revealing the presence of the eavesdropper to Alice and Bob. As classified in literature [9], QKD protocols fall into two primary categories based on the nature of the quantum states used:

- *Discrete-Variable* (DV-QKD): these protocols encode information into discrete properties of single photons, such as polarization or phase.

- *Continuous-Variable* (CV-QKD): these protocols encode information into continuous variables of the electromagnetic field, specifically the quadrature components of the quantized electro-magnetic modes of light.

The choice between DV and CV architectures involves a trade-off. DV-QKD is currently a more mature technology, capable of achieving long-haul transmissions with high stability. However, it typically requires expensive single-photon detectors (SPDs) and specialized hardware. Instead, CV-QKD offers the advantage of compatibility with standard telecommunication components (using homodyne and heterodyne detection instead of SPDs) and can sustain higher secret-key rates over short-to-medium distances. However, its security analysis is generally more complex due to the analog nature of the signal and channel noise. Given this landscape, the development of flexible, multi-protocol QKD devices represents a significant step forward [10]. Such versatility is particularly valuable in scenarios like free-space optical (FSO) links and satellite communications, where hardware cannot be easily modified after deployment. While fiber-based networks constitute the backbone of QKD, free-space applications are gaining traction for establishing global quantum networks.

Regardless of the specific architecture (DV or CV), a typical QKD session consists of two distinct phases:

1. *Quantum transmission*: the initial phase of any QKD protocol relies on the transmission of quantum states on a quantum channel to establish a shared sequence of correlated data. This stage is typically implemented through one of two primary architectural frameworks:

    - *Prepare-and-Measure* (P&M) scheme: in this approach, the quantum communication is strictly unidirectional. Alice generates a classical random variable, denoted as a, and encodes it onto a set of non-orthogonal quantum states. These prepared states are subsequently transmitted through a quantum channel to Bob. Upon reception, Bob performs specific quantum measurements to extract his own classical random variable, b. Due to the probabilistic nature of quantum measurements and the presence of channel noise or potential eavesdropping, Bob's variable b exhibits only a partial correlation with Alice's original variable a. By iteratively repeating this transmission and measurement process, the two parties accumulate a vast dataset of partially correlated symbols, collectively referred to as the raw key.

    - *Entanglement-Based* (E-B) scheme: conversely, this scenario relies on the physical distribution of quantum entanglement. In this configuration, a bipartite

entangled quantum state is generated. Alice retains and measures one half of the entangled pair, thereby collapsing the state and obtaining her classical random variable a. The complementary half of the entangled pair is propagated through the quantum channel to Bob, who performs corresponding measurements on his subsystem to derive his variable b. It is important to note that, from Bob's operational perspective, his measurement procedure in the E-B scheme is entirely indistinguishable from that in the P&M scheme. Ultimately, the inherent nonlocal correlations of the shared bipartite state guarantee that Alice and Bob's measurement outcomes are statistically linked, providing the necessary mathematical foundation for the generation of the secret key.

2. *Classical post-processing:* Alice and Bob communicate over a classical, authenticated public channel to distill a secure key from their raw data. This phase includes subprotocols such as *sifting* (basis reconciliation), *error correction* (to fix transmission errors) and *privacy amplification* (to eliminate any information Eve might have gained).

It is important to note that, for the purposes of this thesis, all subsequent numerical simulations and performance evaluations will focus exclusively on the Prepare-and-Measure (P&M) architecture. This methodological choice is driven by its higher technological maturity and its direct compatibility with the standard optical access networks investigated in the following chapters.

While the distinction between P&M and E-B architectures defines the physical layer of the implementation, a crucial methodological dichotomy exists in the theoretical security analysis: the assumption of the available data block size. Historically, the majority of QKD security proofs rely on the asymptotic assumption. In this idealized regime, it is assumed that the communicating parties exchange an infinitely long sequence of quantum signals. Under this hypothesis, statistical fluctuations in the parameter estimation vanish, allowing Alice and Bob to determine the channel characteristics with absolute precision. While mathematically convenient for deriving upper bounds on performance, this approach inevitably overestimates the achievable key transmission rate in real-world scenarios, where transmission time is finite and data blocks are necessarily limited in size. In contrast, a *finite-key* analysis considers the realistic constraint where the total number of transmitted pulses is finite. In this regime, the statistical estimation of channel parameters is subject to unavoidable fluctuations. To guarantee unconditional security, these uncertainties must be rigorously accounted for by applying worst-case estimators, which effectively penalize the raw key rate to compensate for the potential information leakage due to finite sampling. Crucially, this thesis departs from the standard asymptotic ide-

alization to focus strictly on the finite-key regime. By incorporating the finite block size effects directly into the numerical models for both Discrete-Variable (DV) and Continuous-Variable (CV) protocols, this study provides a *practical implementation* perspective. This approach ensures that the resulting performance evaluations are not merely theoretical upper bounds but represent reliable, achievable benchmarks for real-world deployment.

1.3. Discrete-Variable - QKD

The Discrete-Variable QKD (DV-QKD) represents the historical and most mature approach to quantum communications. The fundamental principle relies on the encoding of information into discrete properties of single *quanta* of light, typically the polarization state or the phase of single photons. In practical experimental setups, due to the technological complexity of ideal single-photon emitters, this is typically achieved by generating Weak Coherent Pulses (WCP) from standard laser sources, which are heavily attenuated to ensure a mean photon number per pulse strictly lower than one [11], [12].

This technology remains the benchmark for long-distance secure communication, with recent research focusing on extending the reach of repeater-less links and enhancing co-existence in high-capacity networks. The current distance record for fiber-based QKD is held by protocols based on Twin-Field (TF-QKD), which have successfully demonstrated secure key exchange over 1002 km of ultralow-loss optical fiber in laboratory settings [13]. This was achieved by suppressing system noise to extreme levels and optimizing the *sending-or-not-sending* (SNS) protocol variants. In real-world field deployments, significant progress has been made in 2025. A notable experiment in Germany demonstrated TF-QKD over a 254 km deployed fiber link between cities, achieving stable key rates without the need for cryogenic cooling, marking a step forward for practical long-haul backbones [14]. On a larger scale, 2026 saw the announcement of large-scale networks based on integrated photonic quantum chips, with network topologies capable of spanning thousands of kilometers, highlighting the maturity of chip-based DV-QKD for massive user scaling.

The historical and paradigmatic example of DV-QKD is the BB84 protocol, introduced by Bennett and Brassard in 1984.

1.3.1. BB84 Protocol Description

The protocol operates in two main phases [15]:

1. *Quantum transmission*: the process begins with Alice generating a random string

of classical bits (0s and 1s) and an equally long sequence of random polarization bases. She chooses between two conjugate bases:

- Rectilinear (R or +), consisting of Vertical (90°) and Horizontal (0°) polarizations.
- Diagonal (D or ×), consisting of 45° and 135° polarizations.

Alice encodes each bit into a single photon according to her chosen basis. For instance, she might map a binary 0 to 0° or 45°, and a binary 1 to 90° or 135°. She then transmits this train of photons to Bob via a quantum channel (optical fiber). Upon receiving the photons, Bob—who has no knowledge of Alice's choices—independently selects a random basis (Rectilinear or Diagonal) to measure each incoming photon. If Bob measures in the same basis Alice used to transmit, he will deterministically measure the correct polarization and correctly interpret the bit (assuming a noiseless channel). If Bob measures in the wrong basis (e.g., measuring a diagonal photon using a rectilinear filter), the result is fundamentally random. He has a 50% chance of recording a 0 or a 1, resulting in the loss of the original information.

2. *Public discussion (sifting and error estimation)*: subsequent steps occur over a classical public channel, which may be monitored by an eavesdropper (Eve) but cannot be altered.

   - *Sifting*: Alice and Bob publicly exchange the sequence of bases they used (e.g., "I used Rectilinear for photon 1"). They discard all instances where their bases did not match. The remaining bits, where bases were identical, form the *sifted key*.
   - *Error detection*: since the primary objective of QKD is to counteract potential attackers aiming to breach confidentiality, detecting the presence of an eavesdropper (Eve) is of paramount importance. To achieve this, a random subset of corresponding bits from the sifted key is selected and publicly compared to estimate the Quantum Bit Error Rate (QBER). For the selected sample, the QBER is defined as:

$$QBER = \frac{\text{number of wrong compared bits}}{\text{total number of compared bits}} \tag{1.10}$$

   Assuming the sample is statistically representative, the estimated error rate is

extended to the entire sifted key as follows:

$$QBER \approx \frac{\text{number of wrong bits in the sifted key}}{\text{total number of sifted key bits}} \tag{1.11}$$

- *Final key generation*: security proofs establish a theoretical upper bound for this error rate. If the calculated QBER exceeds the threshold of 11%, the key exchange is considered insecure against external attacks. Consequently, the key is immediately discarded, and the procedure must be repeated [16], [17]. If the error rate in the sample is below this threshold, the parties conclude the channel is secure. They discard the revealed test bits and perform error correction and privacy amplification procedures on the remaining bits to produce the final secret key.

The theoretical framework described above is summarized in the step-by-step execution example reported in Table 1.1. The table clearly outlines the complete operational flow, from the initial transmission of the quantum states to the derivation of the final key.

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↖	↔	↕	↕	↔	↔	↖	↗	↕	↖	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1	1	1	0	1	0	0	0	1	1	1	1	0	0	1
PUBLIC DISCUSSION															
Bob reports bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Alice checks bases			OK	OK	OK			OK	OK			OK	OK	OK	OK
Shared information (sifted key)			1	0	1			0	1			1	0	0	1
Bob reveals sample bits					1							1		0	
Alice confirms sample					OK							OK		OK	
OUTCOME															
Final secret key			1	0				0	1				0		1

Table 1.1: Example of the BB84 QKD protocol execution. The table illustrates the states sent by Alice, the measurements performed by Bob and the sifting process to derive the shared secret key.

1.3.2. DV-QKD Transmission Model

The BB84 protocol theoretically exploits the transmission of single-photon Fock states to guarantee the unconditional secrecy of the key. In practice, however, the implementation of a pure single-photon source is technologically challenging. Consequently, an alternative

solution has been widely adopted: the use of a highly attenuated laser source that outputs Weak Coherent Pulses (WCPs) via properly calibrated attenuators. In these pulses, the photon number statistics follows a Poisson probability distribution. This implies that the number of photons in each pulse is probabilistic, leading to the potential generation of multi-photon signals. The coherent state $|\alpha\rangle$ can be expressed in terms of Fock states using the following expansion, where α is a complex amplitude, $\mu = |\alpha|^2$ is the mean photon number, and n is the number of photons per pulse:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{1.12}$$

Since the photon number per pulse is probabilistic, the probability $P(n, \mu)$ of finding exactly n photons in a coherent state, given the average number μ, is defined in Eq. (1.13). Furthermore, the conditional probability of generating multi-photon pulses, assuming a non-empty pulse, is derived in Eq. (1.14):

$$P(n, \mu) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} = \frac{\mu^n}{n!} e^{-\mu} \tag{1.13}$$

$$P(n > 1|n > 0, \mu) = \frac{1 - P(0, \mu) - P(1, \mu)}{1 - P(0, \mu)} = \frac{1 - e^{-\mu}(1 + \mu)}{1 - e^{-\mu}} \simeq \frac{\mu}{2} \tag{1.14}$$

Since the objective is to maximize the number of single-photon pulses, the probability of multi-photon states is mitigated by lowering the mean photon number μ. However, for very small values of μ, the probability of generating vacuum states increases as shown in Eq. (1.15). In other words, while small μ values reduce multi-photon events, they simultaneously enhance the probability of transmitting empty pulses.

$$P(n = 0) \approx 1 - \mu \tag{1.15}$$

Since the detectors remain active for all incoming slots, a high rate of empty pulses induces a low Signal-to-Noise Ratio (SNR), as vacuum events carry no information and only noise (dark counts) is detected. In the literature, a standard value of $\mu = 0.1$ is frequently adopted, which translates to a conditional multi-photon probability of $P(n > 1|n > 0, \mu) \approx 0.05$. Despite this convention, other works demonstrate the possibility of computing an optimal μ tailored to the specific experimental setup, with a particular focus on transmission losses [18].

1.3.3. Photon Number Splitting Attacks and Decoy Method

The technological absence of deterministic single-photon transmitters, and the consequent reliance on Weak Coherent Pulses (WCPs), exposes the system to a specific class of eavesdropping threats known as Photon Number Splitting (PNS) attacks [19]. In this scenario, Eve is assumed to possess the capability to perform a Quantum Non-Demolition (QND) measurement to resolve the photon number of each pulse without disturbing its quantum state. If a pulse contains multiple photons, Eve can split the beam, retaining one photon for herself while forwarding the remaining ones to Bob through a lossless channel to maintain the expected detection rate. By storing her copy in a quantum memory and waiting for the public basis reconciliation (sifting) phase, Eve can measure her photon in the correct basis and acquire the bit value with certainty. Conversely, Eve blocks all single-photon pulses, as they cannot be split without introducing detectable errors. In doing so, the intrinsic security guaranteed by single-photon measurements is compromised. The threat posed by PNS attacks is non-negligible, as it fundamentally undermines the unconditional security proof of QKD. To address this vulnerability, Hwang proposed the Decoy-State Method in 2003 [20]. The core concept relies on the random modulation of the laser source intensity. In its simplest form, two intensities are exploited: a *Signal* state and a *Decoy* state. Since Eve cannot distinguish between signal and decoy pulses during transmission (as they only differ in their average photon number, not their spectral or temporal properties), her attack must affect both types of pulses equally based on their actual photon content. However, because the decoy states are typically prepared with a different intensity, the statistical distribution of multi-photon pulses differs from that of the signal states. If Eve selectively targets multi-photon pulses, she inevitably alters the yield (detection probability) of the decoy states in a way that does not match the theoretical prediction. This discrepancy allows Alice and Bob to detect her presence by estimating the upper bound on the multi-photon yield. Let Δ be the upper bound on the signal state multi-photon counts, with μ' representing the decoy state intensity and μ the signal state intensity. The bound can be approximated as:

$$\Delta = \frac{\mu e^{-\mu}}{\mu' e^{-\mu'}} \tag{1.16}$$

where μ is usually optimized around 0.4-0.7 photons/impulse, while μ' must be critically lower to statistically analyze the channel, usually around 0.05-0.1. While this two-state protocol provides a solution, it can be further optimized. It has been theoretically demonstrated that using an infinite number of decoy intensities would provide the tightest estimation of channel parameters, though this remains just an ideal solution [21]. For

practical implementations, a three-intensity protocol [22] using a Signal state (μ_1), a weak Decoy state (μ_2) and a Vacuum state (μ_3) is widely considered the standard for secure key generation. The role of these intensities is distinct:

- Vacuum state ($\mu_3 \approx 0$): it allows Alice and Bob to strictly estimate the background noise and dark count rates of the detectors.
- Weak Decoy state (μ_2): it enables the precise lower-bounding of the yield of single-photon pulses ($s_{X,1}$), which are the only secure contributors to the key.

During the classical post-processing phase, Alice announces the intensity setting used for each pulse (rather than the probabilistic photon number). This allows Bob to classify his detection events corresponding to Signal, Decoy and Vacuum states separately, thereby calculating the error rates and yields necessary to unmask any PNS attempt.

1.4. Continuous-Variable - QKD

Continuous-Variable Quantum Key Distribution (CV-QKD) represents a paradigm shift from the discrete photon-counting approach of DV-QKD. Instead of encoding information into the polarization or time-bin of single photons, CV-QKD utilizes the continuous amplitude and phase quadratures of the quantized electromagnetic field. The fundamental advantage of this architecture lies in its hardware compatibility: it employs standard telecommunication components, such as coherent receivers and homodyne detectors, eliminating the need for specialized single-photon transmitters/detectors.

CV-QKD has recently achieved significant milestones, particularly regarding high-speed generation rates and integration into existing telecommunication infrastructures. In the context of *finite-size* security, which is critical for practical deployments, recent experiments have pushed the boundaries of both distance and secret key rate (SKR). A major breakthrough in 2025 demonstrated a 10 GHz symbol rate using a multi-carrier (MC) modulation scheme based on Orthogonal Frequency Division Multiplexing (OFDM) [23]. This system achieved a Secret Key Rate in the order of Gbps over 10 km and maintained Mbps-level rates over 100 km, significantly outperforming previous setups limited to the MHz range. Regarding transmission distance, which has historically been a limitation for CV protocols due to their sensitivity to channel excess noise, recent implementations have successfully extended the reach. A record transmission distance of 120 km was achieved in the asymptotic regime (100 km in the finite-size regime) while coexisting with fully populated Coarse Wavelength Division Multiplexing (CWDM) classical channels, demonstrating the effectiveness of local oscillator (LO) mode filtering against Raman noise [24].

Furthermore, advancements in photonic integration are paving the way for cost-effective mass deployment. In 2026, researchers demonstrated a QPSK-based CV-QKD system integrated on glass-based photonic chips, achieving stable secure key generation over simulated fiber links, thus validating the feasibility of compact, chip-scale CV transceivers for access networks [25]. Commercial field trials in metro networks have also confirmed that CV-QKD can seamlessly coexist with classical data in the C-band without requiring dedicated dark fibers, leveraging standard off-the-shelf components. It is also important to address the computational overhead. CV-QKD necessitates sophisticated Digital Signal Processing (DSP) algorithms and complex post-processing stages, including parameter estimation, error correction, and privacy amplification. These operations are computationally intensive and often constrained by hardware memory and processing speed, thereby imposing limitations on the real-time performance of the system.

1.4.1. Continuous-Variable Quantum System, Fock States and Coherent States

A Continuous-Variable quantum system is canonically defined as an infinite-dimensional system comprising an ensemble of N bosonic modes, described by observables holding a continuous spectrum of eigenvalues. This system is described by a global Hilbert space $\mathcal{H}$, constructed as the tensor product of N infinite-dimensional Fock spaces $\mathcal{H}_m$:

$$\mathcal{H} = \bigotimes_{m=1}^{N} \mathcal{H}_m \tag{1.17}$$

Each component Fock space $\mathcal{H}_m$ corresponds to a specific optical mode and is spanned by the orthonormal basis set $\{|0\rangle, \ldots, |n\rangle, \ldots\}$, where the ket $|n\rangle$ denotes a Fock state containing exactly n indistinguishable photons. These number states are intrinsically linked to the fundamental ladder operators: the *annihilation operator* $\hat{a}$ and the *creation operator* $\hat{a}^\dagger$. For a single-mode field, the states $|n\rangle$ are the eigenstates of the photon number operator $\hat{n} = \hat{a}^\dagger \hat{a}$, satisfying:

$$\hat{a}^\dagger \hat{a}|n\rangle = n|n\rangle \tag{1.18}$$

Physically, this relationship signifies the presence of n quanta within the specific mode. The state $|0\rangle$ is defined as the vacuum state (a field with zero photons) and the action of the ladder operators on the number states is defined as:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \tag{1.19}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{1.20}$$

Consequently, an arbitrary Fock state $|n\rangle$ can be generated by iteratively applying the creation operator to the vacuum state:

$$|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n|0\rangle \tag{1.21}$$

While Fock states represent quantum states with a precisely defined number of photons, their experimental generation for $n > 2$ remains technically challenging. In practical CV-QKD implementations [26], the sender (Alice) does not prepare pure Fock states; rather, she prepares a sequence of coherent states generated by a stable laser source. Formally, a coherent state $|\alpha_j\rangle$ is a quantum state where the photon number is not precisely determined. It is defined as the eigenstate of the non-Hermitian annihilation operator $\hat{a}$:

$$\hat{a}|\alpha_j\rangle = \alpha_j|\alpha_j\rangle \tag{1.22}$$

Because the annihilation operator can be expressed as a function of the continuous quadrature operators $\hat{q}$ and $\hat{p}$, the eigenvalue equation can be rewritten as:

$$\frac{1}{2}(\hat{q} + i\hat{p})|\alpha_j\rangle = (q_j + ip_j)|\alpha_j\rangle \tag{1.23}$$

$$|\alpha_j\rangle = |q_j + ip_j\rangle \tag{1.24}$$

where the complex eigenvalue α_j represents the state's position in the phase space (or phasor plane), as shown in Figure 1.3. Alternatively, a coherent state can be described as a displaced vacuum state, generated by applying the unitary displacement operator $\hat{D}(\alpha_j) = e^{\alpha_j\hat{a}^\dagger - \alpha_j^*\hat{a}}$ to the vacuum state $|0\rangle$. Unlike Fock states, which possess a completely random phase, coherent states exhibit a well-defined phase, but their photon number probability $P(n)$ is governed by a Poisson distribution. The quadrature operators themselves can be expressed as functions of the annihilation and creation operators:

$$\hat{q} = \hat{a} + \hat{a}^\dagger \tag{1.25}$$

$$\hat{p} = -i(\hat{a} - \hat{a}^\dagger) \tag{1.26}$$

Their canonical commutation relation can be derived directly from $[\hat{a}, \hat{a}^\dagger] = 1$:

$$[\hat{q}, \hat{p}] = -i([\hat{a}, \hat{a}] - [\hat{a}, \hat{a}^\dagger] + [\hat{a}^\dagger, \hat{a}] - [\hat{a}^\dagger, \hat{a}^\dagger]) = 2i \neq 0 \tag{1.27}$$

Since the two variables do not commute, they cannot be simultaneously measured with arbitrary precision in a practical implementation.

To understand the physical limits of the system, it is essential to compute the expected value (first moment) and the variance (second moment) of these operators when applied to Alice's local coherent state $|\alpha_j\rangle$:

$$\langle \hat{q} \rangle = \langle \alpha_j | \hat{q} | \alpha_j \rangle = 2\mathrm{Re}(\alpha_j) = 2q \tag{1.28}$$

$$\langle \hat{p} \rangle = \langle \alpha_j | \hat{p} | \alpha_j \rangle = 2\mathrm{Im}(\alpha_j) = 2p \tag{1.29}$$

The second moments evaluate to:

$$\langle \hat{q}^2 \rangle = \langle \alpha_j | (\hat{a} + \hat{a}^\dagger)^2 | \alpha_j \rangle = 4q^2 + 1 \tag{1.30}$$

$$\langle \hat{p}^2 \rangle = 4p^2 + 1 \tag{1.31}$$

This leads directly to the variance computation:

$$V(\hat{q}) = \langle \Delta \hat{q}^2 \rangle = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2 = 1 \tag{1.32}$$

$$V(\hat{p}) = \langle \Delta \hat{p}^2 \rangle = \langle \hat{p}^2 \rangle - \langle \hat{p} \rangle^2 = 1 \tag{1.33}$$

This result, $V = 1$, represents the minimum variance in Shot Noise Units (SNU), often referred to simply as shot noise. In a coherent state, both quadratures carry the exact same uncertainty, satisfying the minimum bound of the Heisenberg uncertainty relation in SNU:

$$\delta \hat{q} \cdot \delta \hat{p} \geq 1 \tag{1.34}$$

In the context of QKD, Alice modulates these states. Assuming q is a realization of a random variable Q distributed as $Q \sim \mathcal{N}(0, V^e_{mod})$, we can relate the modulation variance of the component to the variance of the overall operator:

$$V(\hat{q}) = \langle \hat{q}^2 \rangle = 4\langle Q^2 \rangle + 1 = 4V^e_{mod} + 1 = V_{mod} + 1 \tag{1.35}$$

where V^e_{mod} is the quadrature component's variance and $V_{mod} = 4V^e_{mod}$ is the operator's

variance. The shot-noise variance plays an essential role here: even if the modulation variance V_{mod} is null, the total variance is non-zero. The overall variance of the modulated ensemble is thus defined as:

$$V(\hat{q}) = V(\hat{p}) = V = V_{mod} + 1 \tag{1.36}$$

The boson-number operator $\hat{n} = \hat{a}^\dagger \hat{a}$ can be expressed in terms of the quadrature operators:

$$\hat{n} = \frac{1}{4}(\hat{q}^2 + \hat{p}^2 - 2) \tag{1.37}$$

The expectation value (mean photon number) of $\hat{n}$ for a single coherent state $|\alpha_j\rangle$ is simply:

$$\langle \hat{n} \rangle = |\alpha_j|^2 = q_j^2 + p_j^2 \tag{1.38}$$

However, while theoretically each coherent state is randomly sampled from an ideal continuous Gaussian distribution, practical implementations typically employ discrete modulation formats, such as 256-QAM, to approximate this behavior. Regardless of the chosen modulation scheme, it remains crucial to calculate the mean photon number of the entire ensemble state:

$$\langle n \rangle = \langle Q^2 \rangle + \langle P^2 \rangle = 2V_{mod}^e \tag{1.39}$$

Combining this with our previous variance definitions, the mean photon number for the ensemble state can be expressed purely as a function of the operator's modulation variance:

$$\langle n \rangle = \frac{1}{2}(V - 1) = \frac{V_{mod}}{2} \tag{1.40}$$

This formulation is essential for computing excess noise in later stages of the protocol. After preparing these states, Alice transmits them across a Gaussian quantum channel towards Bob. Upon reception, Bob performs either homodyne or heterodyne detection. In a homodyne setup, Bob performs a projective measurement on the received mode to perfectly extract the eigenvalue of a single chosen quadrature (either $\hat{q}_B$ or $\hat{p}_B$). Conversely, heterodyne detection requires a 50:50 beam splitter to divide the incoming mode into two distinct modes (B_1 and B_2); Bob then performs projective measurements with orthogonal quadrature operators on each split mode, allowing him to simultaneously retrieve noisy estimates of both q and p.

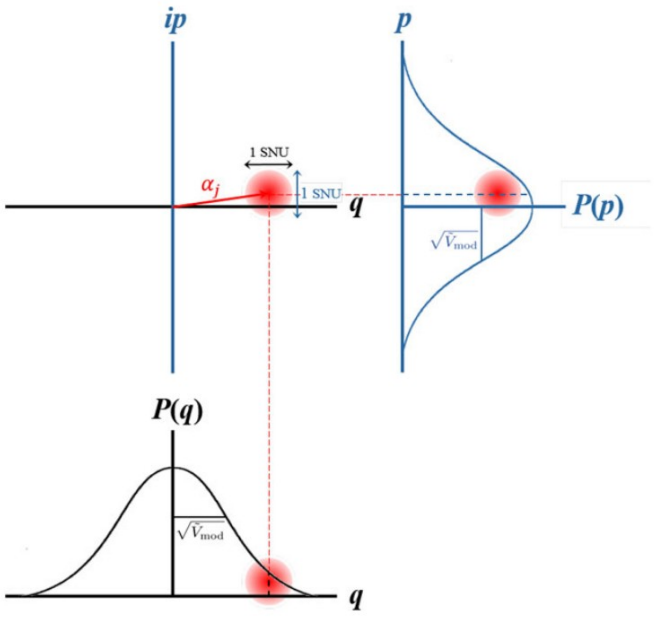


Figure 1.3: Gaussian-modulated coherent states [26].

1.4.2. GG02 Protocol Description

Currently, the landscape of Continuous-Variable Quantum Key Distribution (CV-QKD) is populated by numerous protocols under active study and implementation. The vast majority of these modern schemes are theoretically and practically derived from the foundational GG02 protocol, originally introduced by Grosshans and Grangier in 2002 [28]. Figure 1.4 illustrates the general architecture of a CV-QKD protocol employing dual quadrature measurements. The complete operational procedure can be detailed as follows:

1. *State preparation*: the protocol initiates with Alice generating a sequence of N complex symbols, denoted as $x_1, \ldots, x_N \in \mathbb{C}$. Each symbol x_i is defined by its two quadrature components, the in-phase (I) and quadrature (Q) terms:

$$x_i = x_i^{(I)} + i x_i^{(Q)} \tag{1.41}$$

The statistical distribution of these symbols depends on the chosen modulation format. In the case of Gaussian modulation, the symbols x_i are drawn from a continuous bivariate Gaussian distribution centered at zero, i.e., $x_i \sim \mathcal{N}(0, V_{mod})$. Here, V_{mod} represents the modulation variance, which directly determines the signal energy and the average photon number per state, $\langle n \rangle$, according to Eq. 1.40. Alternatively, for discrete modulation schemes, the symbols x_i are selected from a finite

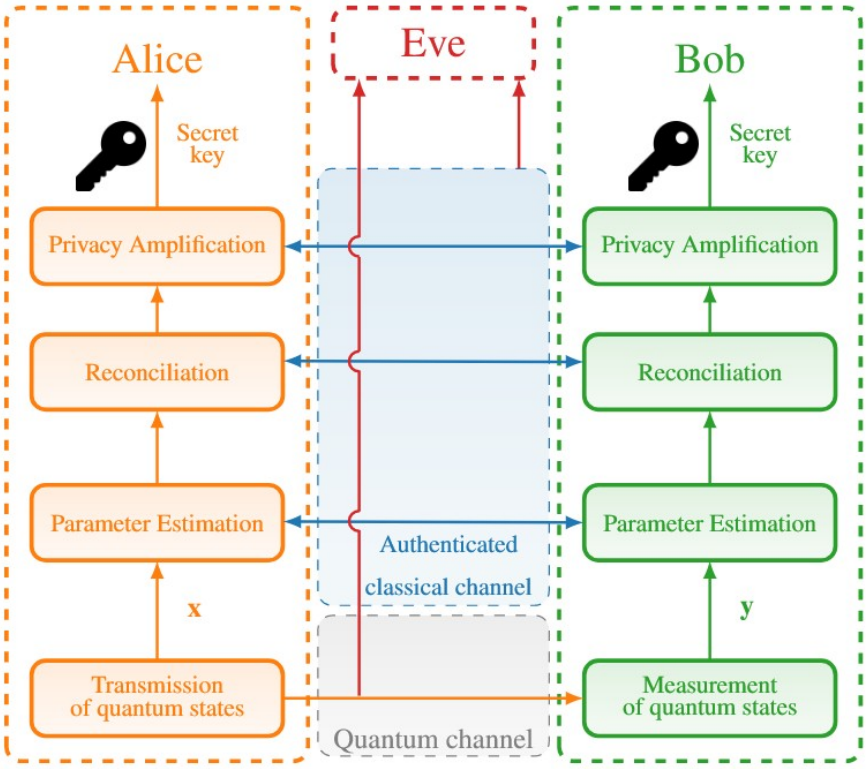


Figure 1.4: Simplified schematic of a CV-QKD protocol for the generation of secret keys [27].

constellation in the phase space. A common example is Quaternary Phase-Shift Keying (QPSK), where the symbols take values from the set $x_i \in \{\pm\alpha, \pm i\alpha\}$. Once generated, Alice encodes these classical symbols onto optical coherent states and transmits them to Bob through the quantum channel.

2. *Measurement*: upon receiving the optical states, Bob performs a dual quadrature measurement—typically utilizing a heterodyne or coherent detection scheme—on each incoming signal. This process yields a sequence of complex measurement results $y_1, \ldots, y_N$. Mirroring the structure of Alice's preparation, each of Bob's measurement outcomes y_i corresponds to the simultaneous detection of both quadratures:

$$y_i = y_i^{(I)} + i y_i^{(Q)} \tag{1.42}$$

Due to channel attenuation and detection noise, these values represent a noisy version of the original symbols sent by Alice.

3. *Parameter estimation*: to assess the security of the link, Alice and Bob randomly select a subset of their data with length $N_{PE} < N$. They publicly reveal the as-

sociated input-output pairs $(x_1, y_1), \ldots, (x_{N_{PE}}, y_{N_{PE}})$ via an authenticated classical channel. By analyzing the correlations within this sample, they perform parameter estimation to characterize the physical properties of the link. Specifically, this step allows them to quantify the channel transmittance T and the excess noise ξ. These parameters are crucial, as they allow the parties to calculate the theoretical Secret Key Rate (SKR) and determine whether the session is secure enough to proceed or if the keys must be discarded.

4. *Information reconciliation*: following a successful parameter estimation, Alice and Bob share correlated continuous-variable sequences. The goal of information reconciliation is to agree on a common binary sequence from these analog measurements. This is achieved by exchanging error-correction information (syndromes) over the authenticated classical channel. Imperfect correlations caused by quantum channel noise and receiver electronic noise are corrected using high-performance Error Correction Codes (ECC), such as Low-Density Parity-Check (LDPC) or multi-edge type LDPC codes, which typically achieve efficiencies ranging between 93% and 97% of the Shannon limit [29].

5. *Privacy amplification*: in the final stage, Alice and Bob apply privacy amplification algorithms (typically based on universal hashing functions) to their reconciled bit strings. The objective of this step is to shrink the key slightly to eliminate any partial information that an eavesdropper (Eve) might have gained during the quantum transmission or the classical reconciliation process. The result is a pair of identical, final secret keys known only to the legitimate parties.

1.4.3. QKD Security Analysis

The modern standard for cryptographic security is the *Universally Composable (UC) framework* introduced by Renner [30]. This framework defines security in terms of the trace distance between the actual protocol output and an ideal "perfect" key. A perfect key is defined as one that is identical for Alice and Bob (correctness), uniformly distributed (randomness), and completely independent of the adversary (secrecy). In a realistic QKD protocol, the joint state of the generated key S and the eavesdropper's quantum system E can be expressed as:

$$\rho_{SE} = \sum_{s \in \mathcal{S}} p_S(s) |s\rangle\langle s| \otimes \rho_E^s \tag{1.43}$$

where $p_S(s)$ is the probability distribution of the key S, $\{|s\rangle\}$ forms an orthonormal basis for the key space $\mathcal{H}_S$, and ρ_E^s is the density matrix describing Eve's state in the Hilbert

space $\mathcal{H}_E$, conditioned on the key value $S = s$. This conditional state encapsulates all quantum and classical information available to Eve, including the public transcripts exchanged during the protocol. The key S is defined as ε-secure with respect to $\mathcal{H}_E$ if:

$$\frac{1}{2}\|\rho_{SE} - \rho_S \otimes \rho_E\|_1 \leq \varepsilon \tag{1.44}$$

where $\| \cdot \|_1$ denotes the trace norm, ρ_E is an arbitrary state of Eve's system, and $\rho_S = \sum s \in \mathcal{S} \frac{1}{|\mathcal{S}|} |s\rangle\langle s|$ represents the maximally mixed state (uniform distribution) in $\mathcal{H}_S$. This condition implies that the shared key is indistinguishable from a perfect key with probability at least $1-\varepsilon$. For practical cryptographic applications, a typical security parameter is $\varepsilon \approx 10^{-10}$ [31], [32].

The security analysis is conducted on specific assumptions regarding the adversary's capabilities. Eve is assumed to be able to prepare arbitrary ancillary states that interact with the signals transmitted by Alice. Furthermore, she possesses a quantum memory capable of storing these ancillas to perform measurements at optimal times, specifically after learning the classical information exchanged during post-processing. Three primary classes of attacks are typically analyzed:

- *Individual attack:* Eve performs independent and identically distributed (i.i.d.) interactions with each transmitted quantum signal. She prepares separable ancillary states, each interacting with a single signal pulse. These ancillas are stored in quantum memory and measured individually before the post-processing phase. The maximum information Eve can extract is bounded by the Shannon mutual information between her results and the raw key (I_{BE} for reverse reconciliation or I_{AE} for direct reconciliation), derived from the Csiszár-Körner bound [33]. The secret key fraction for reverse reconciliation is given by:

$$K_{ind} = I(A:B) - I(B:E) \tag{1.45}$$

  where $I(A:B)$ is the mutual information between Alice and Bob.

- *Collective attack:* similar to the individual attack, Eve interacts with each signal using independent and separable probes. However, she stores the ancillary states in a quantum memory and performs an optimal collective measurement on the entire ensemble of stored states. This measurement can be deferred until after the classical post-processing phase. Under collective attacks, Eve's information is bounded by

the Holevo quantity χ [34], as established by the Devetak-Winter bound [35]:

$$\chi(B:E) = S(\rho_E) - \sum_b p(b) S(\rho_{E|b}) \tag{1.46}$$

where $S(\cdot)$ is the von Neumann entropy, b denotes Bob's measurement outcomes, and $\rho_{E|b}$ is Eve's state conditioned on b. The achievable secret key rate is:

$$K_{coll} = I(A:B) - \chi(B:E) \tag{1.47}$$

- *Coherent attack:* this represents the most general and powerful attack strategy. Eve is not restricted to independent interactions; she may prepare a global entangled ancillary state that interacts with the entire sequence of transmitted pulses. Like in the collective attack, she can store the system and perform an optimal collective measurement after post-processing.

In the theoretical framework, the security of CV-QKD is typically derived assuming a Gaussian Modulation (GM) of the signal states. In the ideal GG02 protocol, Alice modulates the quadratures of coherent states $|\alpha\rangle$ according to a continuous bivariate Gaussian distribution centered at zero. This approach maximizes the mutual information between legitimate parties and simplifies the security proof, as Gaussian attacks are proven to be optimal for the eavesdropper. However, experimental implementations often face practical constraints in generating perfect continuous distributions due to the finite resolution of Digital-to-Analog Converters (DACs) and the complexity of error correction at low Signal-to-Noise Ratios (SNRs). Consequently, recent advancements have focused on Discrete-Modulation (DM) CV-QKD, where the Gaussian distribution is approximated using finite constellations, such as Quadrature Phase Shift Keying (QPSK) or Quadrature Amplitude Modulation (16-QAM or 64-QAM). While discrete modulation significantly relaxes the hardware requirements and digital signal processing load, it requires specific security proofs to account for the deviation from the ideal Gaussian statistic. This thesis will analyze the system performance considering both the asymptotic Gaussian limit and practical finite constellation schemes.

Security proofs can be derived in two distinct regimes: the asymptotic limit - where the number of transmitted signals $N \to \infty$ - and the finite-size regime, where N is finite and fixed. While the asymptotic assumption simplifies the theoretical derivation of bounds (allowing the assumption that parameter estimation is perfect), realistic implementations are inherently finite. In the finite-size regime, statistical fluctuations in parameter es-

timation must be accounted for, as they significantly reduce the extractable key length compared to the asymptotic upper bound. This thesis adopts a specific methodology, following [27]: it utilizes the security proof for discrete-modulation CV-QKD derived in the asymptotic regime and adapts it to the finite-size setting. This adaptation is achieved by employing statistical worst-case estimators for the channel parameters (excess noise and transmittance) and incorporating finite-size penalties associated with privacy amplification, under the assumption of a Gaussian linear channel. A detailed derivation of the SKR will be provided in Chapter 3.

2 | Passive Optical Networks

Fiber-to-the-Home (FTTH) represents the state-of-the-art solution for the "last mile" of telecommunication networks, designed to meet the increasing demand for high bandwidth, scalability, and network efficiency. Historically, two primary architectures have been proposed for optical access [36]: Point-to-Point (P2P), which dedicates a direct fiber link from the Central Office (CO) to each user, and the Passive Optical Network (PON), which utilizes a point-to-multipoint topology.

The term *passive* refers to the exclusive use of unpowered optical components within the distribution network. This absence of active elements is crucial for QKD, as it avoids signal regeneration and noise amplification that would otherwise severely limit the achievable secret-key rate. Moreover, PONs offer a cost-effective alternative to the deployment of dedicated *dark fibers* by allowing infrastructure sharing. This architecture naturally supports the coexistence of classical and quantum channels—a scenario where CV-QKD is particularly advantageous due to its high compatibility with standard telecommunication hardware compared to DV-QKD. Driven by these economic and technical benefits, PONs have become the dominant standard for FTTH deployments. The following sections will detail the internal structure of PONs and their standardization protocols.

2.1. PON Architecture

A Passive Optical Network is made of three main building blocks, as illustrated in Figure 2.1:

- *Optical Line Terminal* (OLT);
- *Optical Distribution Network* (ODN);
- *Optical Network Units* (ONUs).

The Optical Line Terminal (OLT) is located at the Central Office (CO), acting as the interface between the access network and the metro backbone. The OLT serves as the network master, managing traffic scheduling, bandwidth allocation and buffer control to

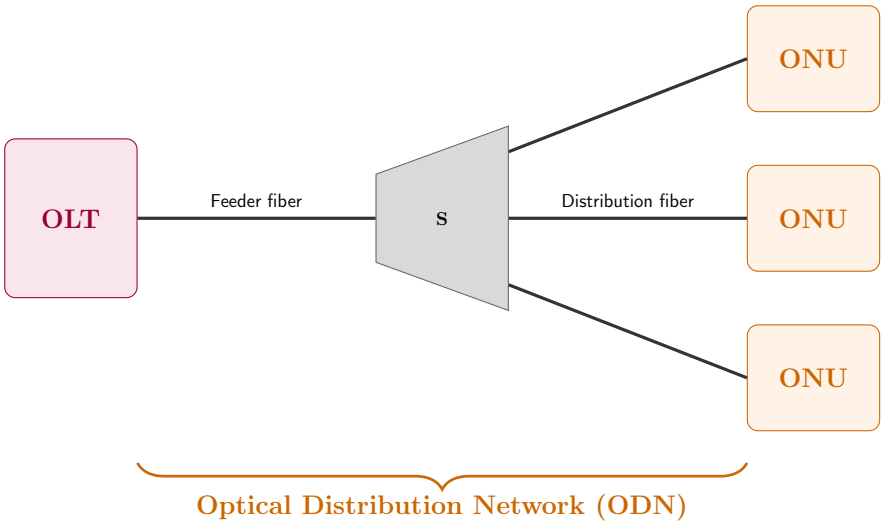


Figure 2.1: Passive Optical Network architecture.

coordinate the multiple users connected to the network. These end-users utilize Optical Network Units (ONUs), located at the customer premises. Connecting the OLT and ONUs is the Optical Distribution Network (ODN), a segment composed entirely of passive elements such as single-mode optical fibers, connectors and passive splitters.

The fundamental characteristic of the PON architecture is its point-to-multipoint topology, enabled by passive optical splitters. In the downstream (DS) direction (OLT to ONU), the signal is broadcast to all connected users; the optical power is physically divided among the output ports according to the splitting ratio, leading to significant attenuation. Since splitters are passive devices unable to route traffic selectively, every ONU receives the entire data stream, filtering only the packets addressed to it. This broadcast nature raises security concerns [37], as a malicious actor could potentially eavesdrop on the communication, highlighting the need for robust encryption methods like QKD. Conversely, in the upstream (US) direction (ONU to OLT), data from multiple users converge onto a single fiber. To prevent collisions, this direction requires a Multiple Access scheme. Although Wavelength Division Multiplexing (WDM) assigns unique frequencies to users to avoid interference, current standard deployments largely rely on time-domain techniques. Specifically, downstream transmission typically utilizes Time Division Multiplexing (TDM), while upstream transmission relies on Time Division Multiple Access (TDMA). In TDMA, the OLT assigns specific time slots to each ONU, ensuring that users transmit only within their authorized windows.

Regarding the integration of QKD, placing single-photon detectors—which are costly and bulky—at the user side (ONU) is economically unfeasible. Therefore, to minimize

A	B	C	C+	N1	N2	E1	E2
(dB)	(dB)	(dB)	(dB)	(dB)	(dB)	(dB)	(dB)
5 - 20	10 - 25	15 - 30	17 - 32	14 - 29	16 - 31	18 - 33	20 - 35

Table 2.1: ODN classes according to channel losses.

deployment costs, this thesis focuses on an upstream quantum channel configuration for both DV-QKD and CV-QKD, where the complex receiver hardware is centralized at the OLT. Finally, the ODN topology analyzed in this thesis employs a single-stage splitting architecture. This divides the fiber infrastructure into two main segments: the *feeder fiber* (from OLT to the splitter) and the *distribution fiber* (from the splitter to the ONUs). The lengths of these segments are critical factors in the total link loss budget, which directly impacts the feasibility of quantum signal transmission. The propagation losses, summed with the losses induced by the optical splitters, lead to a detailed ODN classification, as reported in Table 2.1.

2.2. PON Standards

As depicted in Figure 2.2, the history of PON standardization is extensive, involving up to nine different protocols defined by the IEEE (Institute of Electrical and Electronics Engineers) and, most notably, the ITU-T (International Telecommunication Union - Telecommunication Standardization Sector).
Each standard is defined by specific physical layer parameters: upstream (US) and downstream (DS) bitrates, splitting ratios, maximum logical reach, launch power and spectral occupancy. This thesis focuses on the four most relevant ITU-T standards for current and future access networks:

- *Gigabit PON* (GPON), defined in ITU-T G.984 series.
- *10-Gigabit PON* (XG-PON), defined in ITU-T G.987 series.
- *Next Generation PON 2* (NG-PON2), defined in ITU-T G.989 series.
- *Higher Speed PON* (HS-PON), defined in ITU-T G.9804 series.

The choice of the standard dictates the spectral availability for the quantum channel and directly influences the achievable secret-key rate. It is assumed that these standards operate within a typical access network range of approximately 20 km. Furthermore, this analysis considers ODN classes C or N1 (depending on the specific standard's budget), as

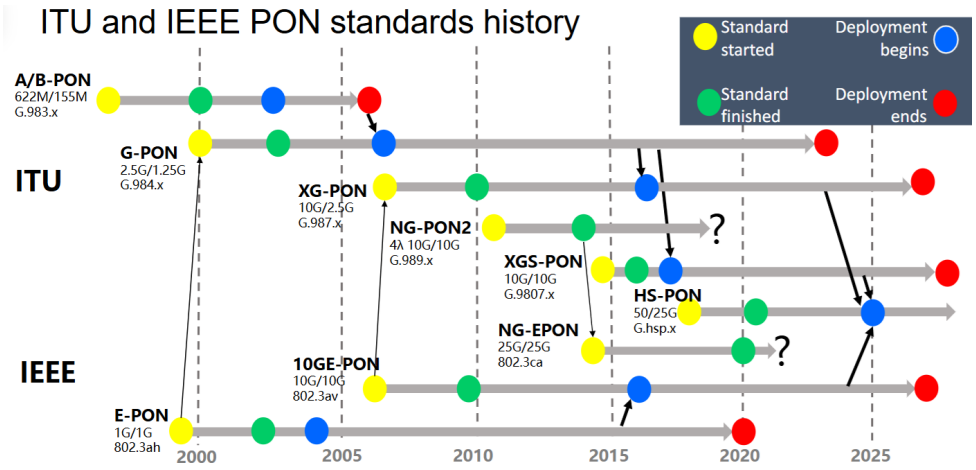


Figure 2.2: PON's standards history scheme [38].

detailed in Table 2.1.

GPON represents the first widely deployed gigabit-class standard. Due to the technological limitations of early optical components, it requires relatively wide spectral bands: the upstream channel is allocated between 1290 nm and 1330 nm, while the downstream occupies the 1480–1500 nm range (Table 2.2). The launch powers are calculated to tolerate a total link loss of approximately 30 dB, supporting splitting ratios up to 1:64. In terms of performance, GPON provides asymmetric speeds of 2.5 Gbps in downstream and 1.25 Gbps in upstream [39], [40], [41], [42].

GPON	**Bandwidth** [nm]	**Launch Power** [dBm]
US	1290 - 1330	2 - 7
DS	1480 - 1500	3 - 7

Table 2.2: GPON standard with bandwidth and launch power specifications, depending on the direction (upstream or downstream).

The XG-PON standard was designed to increase capacity to 10 Gbps (DS) and 2.5 Gbps (US) [43], [44], [45]. A key design requirement for ITU-T is backward compatibility; therefore, XG-PON operates on spectral bands distinct from GPON to allow coexistence on the same fiber. Specifically, the upstream channel is shifted to 1260–1280 nm, and the downstream to 1575–1580 nm [46]. The typical ODN loss class considered for XG-PON is N1. The typical launch power ranges are reported in Table 2.3.

XG-PON	Bandwidth [nm]	Launch Power [dBm]
US	1260 - 1280	2 - 7
DS	1575 - 1580	2 - 6

Table 2.3: XG-PON standard with bandwidth and launch power specifications, depending on the direction (upstream or downstream).

NG-PON2 introduces a paradigm shift by implementing Time and Wavelength Division Multiplexing (TWDM). This architecture allows for multiple wavelength channels—typically four downstream channels of 10 Gbps each—reaching an aggregate capacity of 40 Gbps (expandable to 80 Gbps with 8 channels) [47], [48]. In downstream, each user is assigned to a specific fixed wavelength, requiring tunable filters at the ONU side to select the correct data stream. In upstream, the wavelength allocation is flexible and can be dynamically tuned (TDM/TWDM) to optimize spectral usage [49], [50]. The spectral windows are 1524–1544 nm for upstream and 1596–1603 nm for downstream [51]. Notably, NG-PON2 can exploit the C-band, which benefits from the lowest attenuation in silica fibers—a critical factor for power budget analysis.

NG-PON2	Bandwidth [nm]	Launch Power [dBm]
US	1524 - 1544	4 - 9
DS	1596 - 1603	3 - 7

Table 2.4: NG-PON2 standard with bandwidth and launch power specifications, depending on the direction (upstream or downstream).

Finally, the Higher Speed PON (HS-PON) pushes single-channel rates to 25 Gbps or 50 Gbps [52], [53], [54] and the ODN loss class is N1. The spectral allocation for HS-PON is highly dependent on the coexistence scenario. In downstream, the band is fixed at 1340–1344 nm. In upstream, three options exist to avoid interference:

- Coexistence with XG-PON: 1260–1280 nm.
- Coexistence with GPON only: 1284–1288 nm.
- Standalone: 1290–1310 nm.

HS-PON	Bandwidth [nm]	Launch Power [dBm]
US	1260 - 1280; 1284 - 1288; 1290 - 1310	4 - 9
DS	1340 - 1344	5.5 - 11

Table 2.5: HS-PON standard with bandwidth and launch power specifications, depending on the direction (upstream or downstream).

The spectral analysis of these standards is a prerequisite for identifying a suitable wavelength for the quantum channel. While the unassigned spectral regions might theoretically host the QKD signal, the choice is constrained by physical impairments. In particular, the Raman scattering generated by the high-power classical channels described above can spill into the quantum band, acting as a dominant noise source. These impairments will be analyzed in detail in the following section.

2.3. Impact of Classical-Quantum Coexistence Impairments on Optical Channels

The primary goal of QKD is to guarantee secure key exchange between legitimate parties through a quantum channel. To avoid the prohibitive costs associated with deploying dedicated dark fibers, the coexistence of quantum and classical signals within the same optical infrastructure is often required. However, this spectral integration introduces significant impairments due to the simultaneous propagation of strong classical signals and weak quantum states. These impairments can be categorized into linear effects-such as attenuation and linear crosstalk-and non-linear effects, including Spontaneous Raman Scattering, Stimulated Raman Scattering, Stimulated Brillouin Scattering, Kerr Effect and Four-Wave Mixing [55] [56]. This thesis specifically focuses on the analysis of the most critical phenomena affecting performance.

2.3.1. Propagation Attenuation

The most significant linear impairment in optical fiber transmission is propagation attenuation. This phenomenon manifests as an exponential decay of the signal intensity as it travels through the medium, intrinsically limiting the maximum reach of the communication link. Beyond a certain threshold distance, the signal power falls below the receiver's sensitivity limit, making detection impossible. Mathematically, the residual signal power

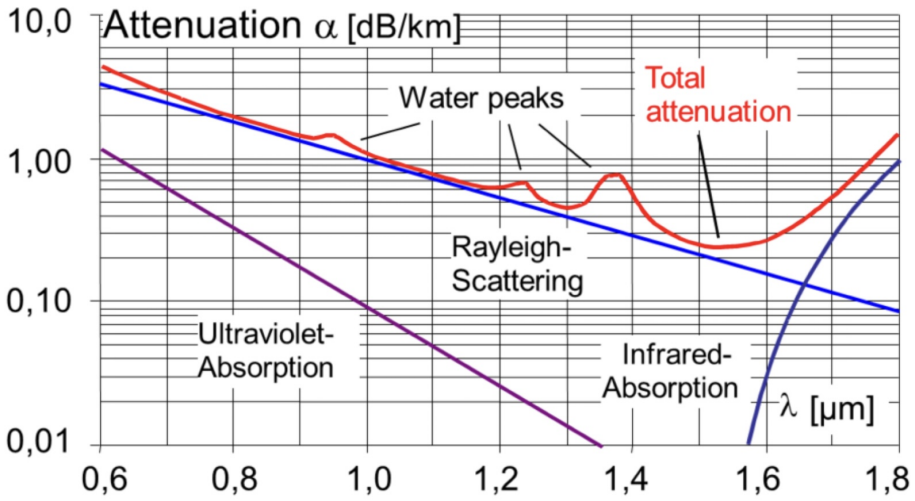


Figure 2.3: Typical fiber loss spectrum as a function of wavelength. The contributions of various physical effects are also shown separately [57].

$P(L)$ at a distance L is related to the input power $P(0)$ by the Beer-Lambert law:

$$P(L) = P(0) \cdot e^{-\alpha L} \tag{2.1}$$

where α represents the *linear attenuation coefficient*. The magnitude of α is strongly dependent on the signal's wavelength, as illustrated in Figure 2.3. The attenuation profile is shaped by several physical mechanisms, primarily Rayleigh scattering—caused by elastic collisions between photons and silica molecules—and absorption peaks due to ultraviolet and infrared resonances. Additionally, extrinsic factors such as waveguide imperfections and micro-bending can contribute to the overall loss. A notable feature in standard silica fibers is the *water peak* around 1400 nm, an abrupt increase in attenuation caused by the absorption of hydroxyl ions (OH^-) trapped within the glass matrix. While modern manufacturing processes have produced *Low Water Peak* (LWP) fibers that effectively eliminate this impairment, this thesis considers standard fibers, therefore the spectral region around 1400 nm is treated as unusable. Despite these losses, it is worth noting that optical fibers offer a significantly lower attenuation coefficient compared to other transmission media, such as copper coaxial cables, which justifies their dominance in telecommunications. To maximize transmission distance, optical systems are designed to operate in specific low-loss spectral regions, historically classified into three main *windows*:

- *First window* (∼800 nm): exploited in the early days of optical communications due to the availability of GaAs LED sources and silicon detectors.

- *Second window* (∼1300 nm): developed to take advantage of the zero-dispersion region of silica fibers and the advent of laser diodes.
- *Third window* (∼1550 nm): corresponds to the absolute minimum of fiber attenuation. The development of Erbium-Doped Fiber Amplifiers (EDFAs) and passive WDM components in this window enabled modern long-haul communications.

The third window spans approximately 15 THz. According to ITU-T standards, this bandwidth is organized into a grid where channels are typically spaced by 100 GHz (approx. 0.8 nm). This standardization is the foundation of Wavelength Division Multiplexing (WDM), a technique that allows multiple signals to propagate simultaneously within the same fiber by assigning them distinct, non-interfering carrier frequencies. Unlike Time Division Multiplexing (TDM), which separates users in the time domain, WDM treats signals as an orthogonal set of carriers. As discussed in later sections, increasing the channel number enhances network capacity and the served users, but inevitably increases the impact of non-linear effects.

Currently, the ITU-T divides the optical spectrum into six distinct bands (as shown in Table 2.6). The O-band (Original band), characterized by an attenuation of $\alpha \approx 0.3$ dB/km, was historically the first to be exploited. However, the C-band (Conventional band) is now the industry standard for long-distance transmission, as it benefits from the minimum attenuation coefficient of $\alpha \approx 0.2$ dB/km. The S-band (Short-wavelength band) serves as an intermediate region with attenuation values falling between those of the O and C bands. This spectral segmentation is particularly relevant for the coexistence of classical and quantum signals in Passive Optical Networks (PONs), where different standards are allocated to specific bands to minimize interference, as detailed in the previous Sections.

Since the objective of this thesis is to analyze QKD performance within a PON architecture, it is necessary to define a cumulative parameter that synthesizes the total system

Band	**$\Delta\lambda$ [nm]**	**Band**	**$\Delta\lambda$ [nm]**
O-band	1260 - 1360	C-band	1530 - 1565
E-band	1360 - 1460	L-band	1565 - 1625
S-band	1460 - 1530	U-band	1625 - 1675

Table 2.6: Telecommunication bands classification and associated wavelength span.

loss. We define the transmittance T as:

$$T = S \cdot e^{-\alpha_q L} \tag{2.2}$$

where α_q is the fiber attenuation coefficient at the quantum signal wavelength, L is the total fiber length and S represents the splitting ratio of the optical splitter in the analyzed PON ODN. The parameter T represents a critical variable in the computation of the SKR for both DV- and CV-QKD protocols.

2.3.2. Spontaneous Raman Scattering

Having addressed the linear constraints of propagation, the analysis must now extend to the non-linear phenomena that arise from the interaction between high-intensity optical fields and the silica medium. These impairments can be categorized into Kerr-induced non-linearities—arising from the refractive index modulation, such as Self-Phase Modulation, Cross-Phase Modulation and Four-Wave Mixing—and inelastic scattering processes. The latter group primarily includes Stimulated Brillouin and Raman Scattering. In the specific context of QKD coexistence within PONs, the dominant and most detrimental impairment is undoubtedly Spontaneous Raman Scattering (SpRS). This phenomenon arises whenever an intense optical signal propagates through a fiber and becomes a critical noise source in coexistence scenarios, particularly when weak quantum signals share the medium with strong classical traffic.

When an optical pulse travels through an optical fiber, photons interact with the molecular vibrations (phonons) of the silica structure. This interaction results in scattering, which alters the photon's direction and, potentially, its frequency and can be of two types:

- *Rayleigh scattering*: if the scattering is elastic, the photon's wavelength remains unchanged. This is the most probable event and primarily dictates the fiber's attenuation profile.
- *Raman scattering*: if the scattering is inelastic, an energy exchange occurs, changing the photon's frequency.

In a coexistence scenario, Raman scattering represents the dominant impairment because the non-elastically scattered photons can take on a wide range of frequencies. The most significant risk arises when the wavelength of these scattered photons randomly coincides with that of the quantum channel, creating in-band noise.
Denoting f_0 as the frequency of the original classical signal, two distinct spectral regions are identified:

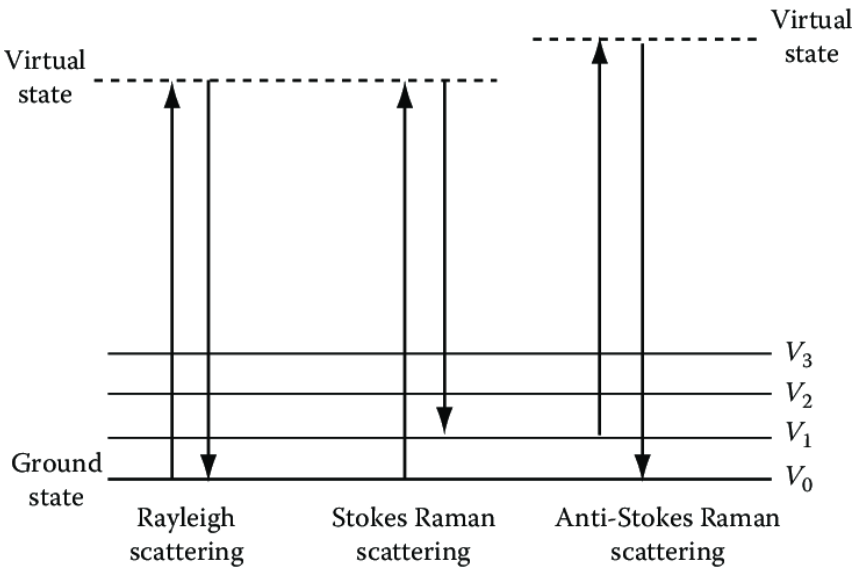


Figure 2.4: Transitions between vibrational energy levels, which lead to Rayleigh scattering and to either Stokes or anti-Stokes Raman scattering [58].

- *Stokes region*: scattered photons possess a lower frequency (longer wavelength) than f_0.
- *Anti-Stokes region*: scattered photons possess a higher frequency (shorter wavelength) than f_0.

The microscopic mechanism involves a silica phonon initially in a specific vibrational energy level (rest state). Upon interaction with an incoming photon, the energy is absorbed, and the system transitions to a *virtual* excited state—so named because it is not an eigenstate of the molecule [59]. This state is unstable and the system quickly decays, emitting a new photon. If the system decays to a vibrational level higher than the initial one, the emitted photon has less energy (Stokes shift). Conversely, if it decays to a lower energy level, the emitted photon has higher energy (anti-Stokes shift). It is important to note that anti-Stokes scattering is typically orders of magnitude weaker than Stokes scattering. Due to its higher intensity, the Stokes region is utilized for signal amplification in long-haul transmissions [60], while the Anti-Stokes region is often exploited in sensor technology for monitoring temperature, strain and pressure [61]. Because the temperature strictly dictates the thermal population of vibrationally excited energy levels, the intensity of the anti-Stokes scattering is inherently temperature-dependent. By accurately measuring this scattered signal, the distributed temperature profile along the entire optical fibre can be mapped.
To properly understand these dynamics, it is crucial to distinguish between Spontaneous Raman Scattering (SpRS) and Stimulated Raman Scattering (SRS). SpRS is a baseline

scattering process that occurs continuously at any optical power level, generated by the random thermal vibrations of the silica molecules. It scatters a fraction of the incident light into a broad spectrum encompassing both the Stokes and anti-Stokes regions. Conversely, SRS is a nonlinear optical effect that manifests only when the optical power exceeds a specific threshold, causing the incident light to coherently stimulate further scattering and effectively transferring energy from shorter to longer wavelengths.
In the context of QKD coexistence, Raman Scattering is an unavoidable drawback rather than an advantage. Consequently, allocating the quantum channel in the anti-Stokes region is generally preferred, as the noise floor generated by the classical channels is naturally lower in this spectral band.

Mathematical Modeling in Passive Optical Networks

Although SpRS is typically characterized for general point-to-point links [62], this thesis addresses the specific architecture of Passive Optical Networks (PONs), following the analysis carried out in [63]. The primary topological difference is the presence of optical splitters, which enable point-to-multipoint communication (in this analysis one splitting level is considered). This splitter fundamentally alters the Raman noise accumulation profile depending on the direction of propagation (upstream or downstream). To model the transition between a multi-user PON and a single-user link, the *Heaviside step function* $\theta(x)$ is employed:

$$\theta(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ 1 & \text{if } x > 0 \end{cases}$$

The Raman power generated in an infinitesimal fiber segment dz is proportional to the Raman efficiency coefficient β (expressed in $[\text{km} \cdot \text{nm}]^{-1}$) and the classical power $P_c(z)$ at that point:

$$dP_{SpRS}(z) = \beta P_c(z) dz \tag{2.3}$$

In a PON architecture, the classical power $P_c(z)$ is attenuated by the fiber loss coefficient α_c and by the presence of splitters along the path. In the case of this thesis, a PON architecture with one splitter S, located at distance $L_S > L$, is analyzed. The power distribution is given by:

$$P_c(z) = P_c(0) \cdot e^{-\alpha_c z} \cdot S^{\theta(L-L_S)\cdot\theta(z-L_S)} \tag{2.4}$$

Here, the term $\theta(L - L_S)$ indicate whether the splitter exists within the total link length L, and $\theta(z - L_S)$ indicates whether the scattering point z occurs after the splitter. If

the arguments is zero, the splitting ratio becomes unity, reverting the model to a point-to-point link. By substituting $P_c(z)$ into the generation equation and accounting for the attenuation of the quantum signal (α_q) as it propagates from z to the receiver at L, we obtain the differential contribution for forward scattering:

$$dP_{SpRS}(z \to L) = \beta \cdot P_c(0) \cdot e^{-\alpha_c z} \cdot e^{-\alpha_q (L-z)} \cdot S^{\theta(L-L_S)} dz \tag{2.5}$$

Integrating the differential contribution over the total fiber length L:

$$P_{SpRS}^{forward} = \int_0^L dP_{SpRS}(z \to L) = \beta P_c(0) S^{\theta(L-L_S)} \int_0^L e^{-\alpha_c z} e^{-\alpha_q (L-z)} dz \tag{2.6}$$

Solving the integral yields:

$$P_{SpRS}^{forward} = \beta P_c(0) S^{\theta(L-L_S)} \frac{1}{\alpha_q - \alpha_c} (e^{-\alpha_c L} - e^{-\alpha_q L}) \tag{2.7}$$

It is necessary to distinguish between two propagation scenarios:

- *Forward Raman*: scattered photons propagate in the same direction as the classical signal.
- *Backward Raman*: scattered photons propagate towards the classical transmitter (counter-propagating).

For backward scattering, the noise is generated at z and travels back to $z = 0$. A crucial difference in PONs is that these backward-traveling photons must pass through the splitter again to reach the receiver (located at the classical source side). This introduces a squared dependence on the splitting ratio (S^2) for the segment beyond the splitter. The differential backward power is:

$$dP_{SpRS}(z \to 0) = \beta P_c(0) e^{-(\alpha_c + \alpha_q) z} S^{2\theta(L-L_S)\theta(z-L_S)} dz \tag{2.8}$$

Integrating over the fiber length L:

$$P_{SpRS}^{backward}(L) = \beta P_c(0) \int_0^L e^{-(\alpha_c + \alpha_q) z} S^{2\theta(L-L_S)\theta(z-L_S)} dz \tag{2.9}$$

This integral can be separated into two distinct sections: the feeder fiber (0 to L_S) and

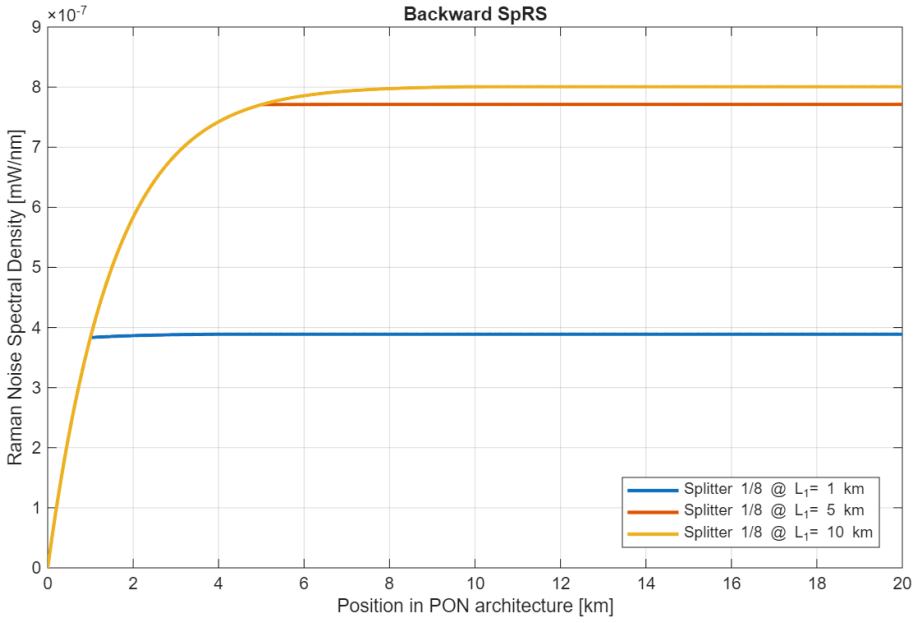
the distribution fiber (L_S to L):

$$P_{SpRS}^{backward}(L) = \beta P_c(0)\left[\int_0^{L_S} e^{-(\alpha_c+\alpha_q)z}dz + S^{2\theta(L-L_S)}\int_{L_S}^{L} e^{-(\alpha_c+\alpha_q)z}dz\right] \tag{2.10}$$

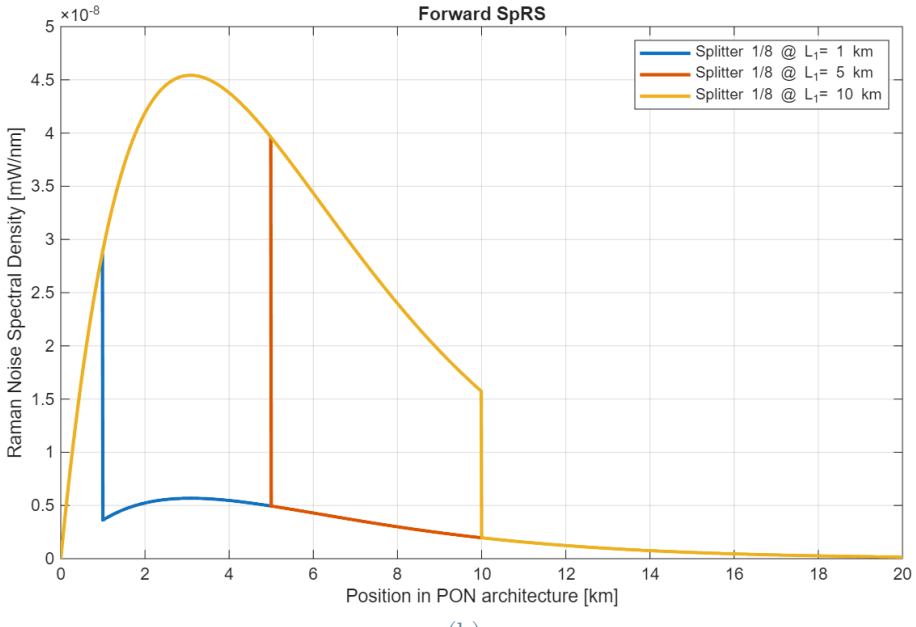
The final analytical expression is:

$$P_{SpRS}^{backward}(L) = \frac{\beta P_c(0)}{\alpha_c+\alpha_q}\left\{1 - e^{-(\alpha_c+\alpha_q)L_s} + S^{2\theta(L-L_S)}\left[e^{-(\alpha_c+\alpha_q)L_S} - e^{-(\alpha_c+\alpha_q)L}\right]\right\} \tag{2.11}$$

A comparison of the two directions reveals that the Backward Raman power density is significantly higher than the Forward Raman power. This disparity is primarily driven by the network topology: in the backward configuration, photons generated in the initial feeder segment (where the classical signal $P_c(z)$ is strongest) travel directly back to the receiver without traversing any splitter. These high-intensity noise photons generated near the source travel a short distance to the detector, minimizing attenuation loss. Conversely, noise generated in the distribution segment is negligible because the classical signal is already attenuated, and any backward-scattered photons must traverse the splitter twice (S^2) to return to the source. Consequently, the backward Raman power curve exhibits a saturation behavior: beyond a certain length, adding more fiber does not increase the noise significantly because the initial feeder contribution dominates. Crucially, as illustrated in Figure 2.5a, the specific saturation level is strictly dependent on the splitter placement: a splitter located further from the source extends the high-power feeder section, resulting in a higher accumulated noise plateau. In contrast, Forward Raman noise must traverse the entire link and all splitters to reach the receiver. Figure 2.5b shows that towards the 20 km mark, the noise values converge to a uniformly low level across all scenarios, heavily suppressed by the significant propagation distance traversed beyond the optical splitters.



(a)



(b)

Figure 2.5: Spatial distribution of the Spontaneous Raman Scattering (SpRS) noise spectral density as a function of the position along the optical fiber link within the PON architecture [64]. (a) Profile of the Backward SpRS. (b) Profile of the Forward SpRS.

3 | Finite-Key SKR Computation and Analysis

The preceding chapters introduced the fundamental principles of Discrete-Variable and Continuous-Variable QKD and outlined the main limitations of Passive Optical Networks. This section digs deeper into the theoretical framework, focusing on the derivation of the Secret-Key Rate (SKR) for both protocols. This quantitative analysis is a prerequisite for a fair performance comparison under identical network conditions. To this end, the derived analytical models are implemented in MATLAB to generate performance curves, which are subsequently analyzed to assess the operational limits and advantages of each approach. It is important to emphasize that this preliminary analysis is conducted assuming a standard point-to-point dedicated fiber link. The specific impairments associated with the PON architecture, such as splitter losses and Raman noise due to coexistence, are not yet included and will be addressed in the subsequent chapters.

3.1. Discrete-Variable Secret Key Rate

In practical QKD implementations, the communication time is necessarily limited, resulting in the generation of finite-length secret keys. Consequently, the asymptotic security assumptions—which rely on infinite data block sizes to perfectly estimate channel parameters—cannot be applied. In a realistic scenario, statistical fluctuations in the parameter estimation can be exploited by an eavesdropper to hide her presence. Therefore, a rigorous security analysis must account for these finite-size effects to guarantee composable security.

3.1.1. Theoretical Derivation of DV-SKR

The analysis in [65] and [66] consider a decoy-state BB84 protocol where Alice uses three intensity levels (μ_1, μ_2, μ_3) to estimate the photon-number-dependent yields and error rates. The length of the secret key ℓ that can be securely extracted from a raw key of

length n_X (being n_X the total number of received states in the X basis), given a failure probability ϵ_{sec} (secrecy) and ϵ_{cor} (correctness), is given by the following Devetak-Winter-like bound, modified for finite-key effects:

$$\ell = \left\lfloor s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6\log_2\left(\frac{21}{\epsilon_{sec}}\right) - \log_2\left(\frac{2}{\epsilon_{cor}}\right)\right\rfloor \tag{3.1}$$

where:

- $s_{X,0}$ is the lower bound on the number of vacuum events (zero-photon pulses) in the raw key.
- $s_{X,1}$ is the lower bound on the number of single-photon events in the raw key.
- ϕ_X is the upper bound on the phase error rate associated with single-photon events.
- $h(x)$ is the binary entropy function.
- λ_{EC} is the amount of information revealed during the error correction process, set to a simple function $f_{EC} \cdot h(e_{obs})$, where f_{EC} is the error-correction efficiency and e_{obs} is the average of the observed error rates in basis X.
- The logarithmic terms represent the penalty due to the finite security parameters ϵ_{sec} and ϵ_{cor}.

The Secret-Key Rate is then defined as $SKR = \ell/N$, where N is the total number of pulses sent by Alice. The relation between N and n_X is given by:

$$n_X = q_X R_X^{avg} N \tag{3.2}$$

where q_X is the probability that Alice will choose the basis X for transmitting a state and R_X^{avg} represents the average detection rate across the three intensity levels employed in the decoy-state protocol. Specifically, the total detection rate for a single transmitted intensity k is given by:

$$R_k = D_k(1 + p_{ap}) \tag{3.3}$$

where p_{ap} denotes the afterpulse probability, which accounts for spurious secondary detection events triggered by charge carriers trapped during a previous avalanche in the Single-Photon Detector (SPD). Furthermore, D_k represents the raw detection probability associated with the intensity k, defined as:

$$D_k = 1 - (1 - 2p_{dc})e^{-\eta_{sys}k} \tag{3.4}$$

In this formulation, p_{dc} is the dark count probability per detector gate, representing false counts generated by thermal or tunneling noise in the complete absence of incident photons and η_{sys} indicates the overall system transmittance.

Crucially, in the finite-key regime, the parameters $s_{X,0}$, $s_{X,1}$ and ϕ_X are not directly observable but must be estimated from the observed detection counts $n_{X,k}$ (number of detections in basis X with intensity k) and error counts $m_{X,k}$. Due to the finite sample size, the observed values deviate from their expected values. The bounds are derived from [65] using statistical inequalities to define a confidence interval. Let n_X be the total block size. The bounds for the statistical fluctuations are integrated into the calculation of expected counts. For a given intensity $k \in \{\mu_1, \mu_2, \mu_3\}$, the expected number of events is bounded by:

$$n^{\pm}_{X,k} := \frac{e^k}{p_k}\left[n_{X,k} \pm \sqrt{\frac{n_X}{2}\ln\frac{21}{\epsilon_{sec}}}\right] \tag{3.5}$$

where p_k is the probability of choosing intensity k.
Using the decoy-state method with the statistical corrections above, the lower bound on vacuum events $s_{X,0}$ contributing to the key is given by:

$$s_{X,0} \geq \tau_0 \frac{\mu_2 n^-_{X,\mu_3} - \mu_3 n^+_{X,\mu_2}}{\mu_2 - \mu_3} \tag{3.6}$$

Similarly, the lower bound on single-photon events $s_{X,1}$ is:

$$s_{X,1} \geq \tau_1 \frac{\mu_1\left(n^-_{X,\mu_2} - n^+_{X,\mu_3} - \frac{\mu_2^2-\mu_3^2}{\mu_1^2}(n^+_{X,\mu_1} - \frac{s_{X,0}}{\tau_0})\right)}{\mu_1(\mu_2-\mu_3) - \mu_2^2 + \mu_3^2} \tag{3.7}$$

where $\tau_n = \sum_{k\in K} e^{-k}k^n\frac{p_k}{n!}$ is the probability that Alice sends a n-photon state. These equations allow the extraction of the secure single-photon contribution, effectively filtering out the multi-photon components that are vulnerable to Photon-Number Splitting (PNS) attacks.

The phase error rate ϕ_X cannot be measured directly on the key generation basis (X) without destroying the key. Instead, it is estimated from the bit error rate observed in the conjugate basis (Z), taking into account the finite-size deviations. The upper bound is derived as:

$$\phi_X \leq \frac{v_{Z,1}}{s_{Z,1}} + \gamma\left(\epsilon_{sec}, \frac{v_{Z,1}}{s_{Z,1}}, s_{Z,1}, s_{X,1}\right) \tag{3.8}$$

where $v_{Z,1}$ is the upper bound on the number of bit errors in single-photon events in the Z basis, and γ is a correction function that accounts for the statistical deviation between

the phase error rate in the X basis and the bit error rate in the Z basis:

$$\gamma(a,b,c,d) \coloneqq \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log_2\left(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}\right)} \tag{3.9}$$

3.1.2. Implementation and Analysis of DV-SKR

To validate the theoretical model and quantify the impact of finite-size effects on system performance, the SKR formula was implemented in a MATLAB simulation environment. The numerical analysis, whose fixed parameters are presented in table 3.1, focuses on two distinct critical aspects for practical deployment. First, we investigate the dependency of the SKR on the postprocessing block size n_X. As indicated by the finite-size corrections in the security bound, the achievable rate is expected to drop significantly for short transmission windows due to wider statistical confidence intervals. For the evaluation, the SKR was numerically optimized-using the MATLAB bult-in function *patternsearch*-over the free parameters of the system:

- q_X: this parameter represents the basis selection probability. It is the probability with which Alice (and Bob) chooses the X basis for state preparation (and measurement), while the Z basis (for channel parameters estimation) is chosen with probability $1 - q_x$.
- μ_1, μ_2: these represent the intensity levels (mean photon numbers) of the laser pulses for signal and decoy states. Alice chooses the intensity for each pulse from a set $K := \{\mu_1, \mu_2, \mu_3\}$. While μ_3 is typically fixed (very low intensity, close to vacuum), μ_1 and μ_2 are free parameters that can be optimized.
- p_{μ_1}, p_{μ_2}: these are the probabilities of selecting the intensity levels μ_1 and μ_2, respectively. The probability of the third intensity, p_{μ_3}, is constrained by the normalization condition $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$.

Figure 3.1 shows that a severe degradation of the rate occurs as n_X decreases. This behavior is directly linked with the statistical correction terms introduced in the security equations: for reduced block sizes, the statistical fluctuations in estimating the number

μ_3	α [dB/Km]	η_{Bob}	p_{dc}	p_{ap}	f_{EC}	e_{mis}	ε_{cor}
$2 \cdot 10^{-4}$	0.2	0.1	$6 \cdot 10^{-7}$	$4 \cdot 10^{-2}$	1.16	$5 \cdot 10^{-3}$	10^{-15}

Table 3.1: DV-QKD fixed parameter values used for numerical simulation.

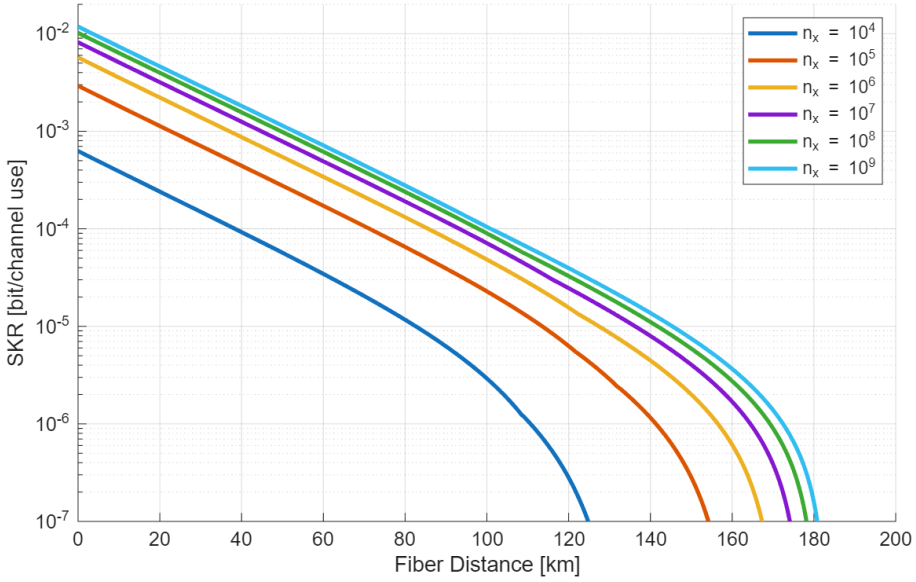


Figure 3.1: DV SKR performance as a function of transmission distance with optimized parameters (dedicated fiber). Numerically optimized secret key rates (in logarithmic scale) are obtained for a fixed postprocessing block size $n_X = 10^s$ with s = 4, 5, ..., 9.

of vacuum and single-photon events are significant, necessitating the adoption of highly conservative worst-case estimates to guarantee security (ϵ_{sec}). Consequently, for low n_X (10^4 or 10^5), not only the maximum rate is reduced, but the maximum reachable distance drops drastically, as the estimated noise rapidly exceeds the security threshold. Other than that, the optimized DV-QKD protocol achieves excellent performance, successfully maintaining a positive SKR for transmission distances up to 180 km.

Second, we address the optimization of the protocol's free parameters. The resulting evolution of these parameters as a function of distance is presented, demonstrating how the system adapts to varying network conditions to maximize the key rate. Several parameters evolutions can be observed from Figure 3.2:

- Basis probability (q_x): for large block sizes (asymptotic-like regime), the optimal q_x approaches 1, consistent with the efficient BB84 protocol where the majority of resources are dedicated to the key generation basis (X). However, as the block size n_x decreases (darker curves), the optimal q_x drops significantly. This is a direct consequence of finite-size corrections: with fewer total signals, the system must allocate a larger proportion of events to the Z-basis (parameter estimation) to keep statistical fluctuations within the required security bounds.
- Intensities (μ_1, μ_2): the signal intensity μ_1 generally sits in the range of $0.4 - 0.6$ photons per pulse, a trade-off between maximizing detection events and minimizing

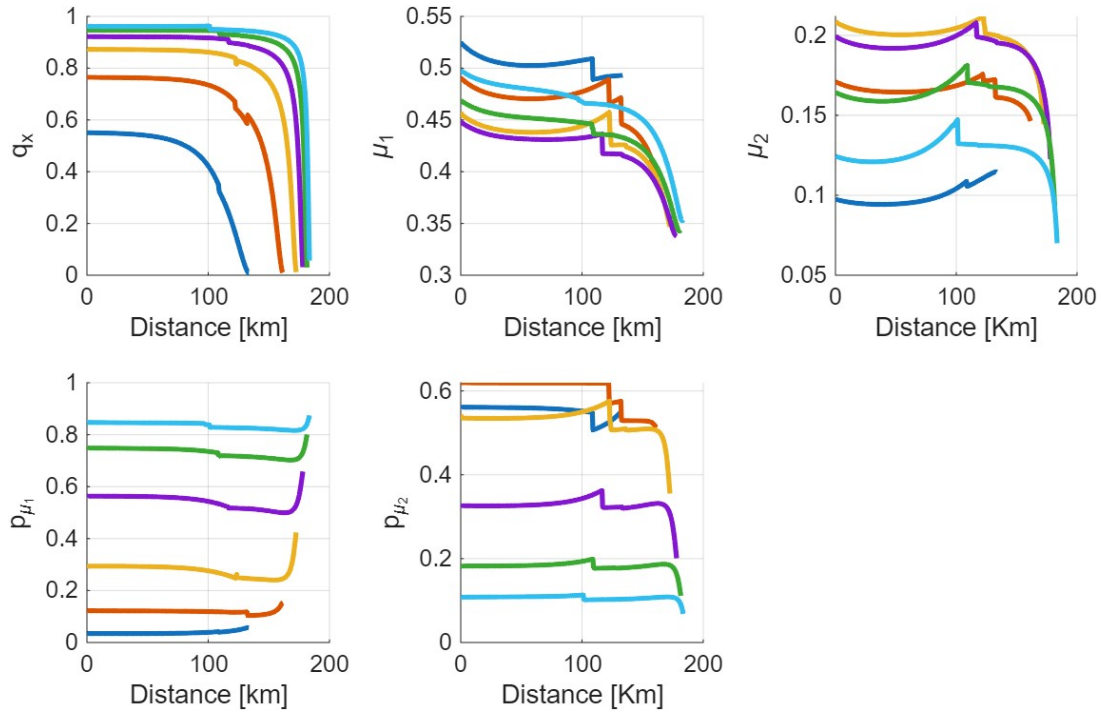


Figure 3.2: Evolution of the optimal DV parameters as a function of the transmission distance.. Numerically optimized parameter values are obtained for a fixed postprocessing block size $n_X = 10^s$ with s = 4,5,...,9. The color scheme follows Figure 3.1.

the multi-photon pulses vulnerable to Photon-Number Splitting (PNS) attacks. The weak decoy intensity μ_2 is maintained at a lower level to effectively estimate the yield of single-photon states.

- High attenuation cut-off: as the channel attenuation increases towards the maximum secure distance (right side of the plots), the parameters exhibit sharp transitions. This point corresponds to the *cut-off* distance where the optimizer fails to find any configuration that satisfies the security criterion (ϵ_{sec}), causing the key rate to vanish.

3.2. Continuous-Variable Secret Key Rate

As previously established, this thesis adopts the finite-size security analysis framework developed in [27]. That work bridges the gap between the asymptotic security proof for discrete-modulation CV-QKD and the realistic finite-block regime by employing statistical worst-case estimators for the critical channel parameters—specifically excess noise (ξ) and transmittance (T)—rather than deriving a full finite-key proof. By incorporating these finite-size penalties associated with privacy amplification, the approach assumes a

Gaussian linear channel and yields tighter, more practical key rate bounds. Consequently, the analytical steps detailed herein strictly follow the methodology established in [27], to derive the final SKR formula that will be later applied to Passive Optical Networks.

3.2.1. Theoretical Derivation of CV-SKR

The derivation begins with the definition of the asymptotic secret key fraction, denoted as $K_{optimal}$. This metric represents the theoretical maximum number of secure bits that can be distilled per transmitted signal in the limit of an infinite key length, assuming perfect error correction and collective attacks. Under the assumption of collective attacks—which are sufficient to prove security against general coherent attacks in the asymptotic limit—the lower bound on the secret key fraction can be formally written as:

$$K_{optimal} = I(X;Y) - \sup_{\mathcal{N}_{A'\to B}} S(E;Y) \tag{3.10}$$

where X and Y denote the classical complex random variables corresponding to the raw data obtained from Alice's and Bob's measurements, respectively.
The first term, $I(X;Y)$, represents the *Shannon Mutual Information*, quantifying the amount of correlated information shared by the legitimate parties before any post-processing. The second term, $S(E;Y)$, is the *Holevo Information* (often denoted as χ_{BE}), which quantifies the maximum information Eve can gain about the classical variable Y stored in her quantum memory E. Since the channel is assumed to be under Eve's control, the supremum indicates that the bound is computed over all possible channel maps $\mathcal{N}_{A'\to B}$ available to Eve. However, this optimization is constrained: the channel must remain compatible with the statistics actually observed by Alice and Bob during the parameter estimation phase of the P&M (Prepare & Measure) protocol [67]. In essence, Eve optimizes her attack to maximize her knowledge, but she cannot violate the parameters measured by the legitimate users.

Given that information is encoded into points within the phase space, the transmission system can be effectively modeled as a discrete-time channel with input symbols x_i and output symbols y_i. A standard classical representation for this interaction is the Additive White Gaussian Noise (AWGN) channel model, where the input-output relation is governed by:

$$y_i = x_i + z_i \tag{3.11}$$

where z_i represents the noise term, modeled as a sequence of independent and identically distributed (i.i.d.) random variables following a complex circular normal distribution.

As established by Claude Shannon, the channel capacity—defined as the maximum achievable information rate—is obtained when the input symbols x_i themselves follow a complex circular normal (Gaussian) distribution. Under this condition, the mutual information $I(X;Y) = H(X) - H(Y|X)$ corresponds to the Shannon capacity limit, expressed in bits per symbol:

$$C = \log_2(1 + \mathrm{SNR}) \tag{3.12}$$

In the specific context of the architecture analyzed here, the Signal-to-Noise Ratio (SNR) is defined as:

$$\mathrm{SNR} = \frac{\eta T V_{mod}}{2 + 2V_{el} + \eta T \xi_{Alice}} \tag{3.13}$$

where η is the detection efficiency, T is the channel transmittance, V_{mod} is the modulation variance, V_{el} represents the electronic noise and ξ_{Alice} accounts for the excess noise generated at the transmitter side.

However, practical constraints often necessitate the use of discrete modulation formats, such as Quadrature Amplitude Modulation (QAM), where the symbols x_i are typically drawn from a uniform distribution over a finite constellation. In this scenario, the achievable mutual information $I(X;Y)$ incurs a shaping penalty compared to the ideal Shannon capacity achievable with Gaussian inputs [68]. To bridge this gap and approach the theoretical limit, techniques such as *Probabilistic Constellation Shaping* (PCS) can be employed, effectively mimicking a Gaussian distribution over the discrete constellation points. In the context of the thesis PCS is employed, thus the mutual information will be computed as in Eq. 3.12.

In real-world implementations, the error correction phase is typically realized using Low-Density Parity-Check (LDPC) codes due to their performance approaching the Shannon limit [69]. However, practical codes cannot fully retrieve the entirety of the available mutual information $I(X;Y)$, as they do not operate at perfect channel capacity. To account for this thermodynamic cost, a *reconciliation efficiency* parameter $\beta \in [0, 1]$ is introduced into the secret key rate equation. This factor quantifies the efficiency of the information reconciliation process, indicating how closely the implemented codes perform relative to the theoretical capacity limit.

Furthermore, the reliability of the post-processing stage is not absolute: a certain percentage of data blocks may fail to converge during error correction or fail the subsequent verification hash check. These failures necessitate the discarding of the affected blocks, thereby reducing the effective key generation rate. This loss is modeled by the *Frame Error Rate* (FER), which represents the fraction of rejected frames.

The secret key rate is then modified as follows:

$$K = (1 - \mathrm{FER}) \left[\beta \cdot I(X;Y) - \sup_{\mathcal{N}_{A' \to B}} S(E;Y) \right] \tag{3.14}$$

The computation of the maximum Holevo information, $\sup_{\mathcal{N}_{A' \to B}} S(E;Y)$, relies on the proven extremal properties of Gaussian states [70], [71]. Specifically, for any arbitrary state ρ_{AYE}, the Holevo quantity is upper-bounded by that of a Gaussian state ρ^G_{AYE} sharing the exact same first and second moments. A lower bound for the secret key fraction K is established as:

$$K \geq (1 - \mathrm{FER})[\beta \cdot I(X;Y) - S(E;Y)_{\rho^G}] \tag{3.15}$$

where $S(E;Y)_{\rho^G}$ denotes the *Holevo bound* calculated for the equivalent Gaussian state. It is important to note that while Gaussian attacks are optimal against Gaussian modulation, this assumption may not yield tight bounds for protocols employing discrete modulation or operating in the finite-size regime.
The Holevo bound can also be expressed as:

$$\chi(E;Y) = S(E) - S(E|Y) \tag{3.16}$$

where $S(E)$ is the entropy of Eve's subsystem and $S(E|Y)$ represents the conditional entropy of Eve's state given Bob's measurement outcome Y. In the context of this thesis, Bob will perform *heterodyne* measurements, whose implications will be analyzed shortly. In the framework of Gaussian quantum information, the properties of bosonic modes are fully described by the first and second moments of the quadrature operators. Consequently, the von Neumann entropy of a Gaussian state can be directly calculated from the symplectic eigenvalues ν_i of the associated covariance matrix Σ. Mathematically, symplectic transformations in phase space correspond to unitary operations in the Hilbert space. A real $2N \times 2N$ matrix S is defined as symplectic if it preserves the symplectic form Ω, satisfying the condition:

$$S\Omega S^T = \Omega \tag{3.17}$$

where Ω is the commutation matrix. When such an operator is applied to a Gaussian state, it induces a linear transformation on the vector of quadrature operators $\mathbf{x}$ and a congruence transformation on the covariance matrix Σ:

$$\mathbf{x} \to S\mathbf{x} \tag{3.18}$$

$$\Sigma \to S\Sigma S^T \tag{3.19}$$

The symplectic eigenvalues ν_i are the absolute values of the eigenvalues of the matrix $i\Omega\Sigma$. Leveraging this formalism, the von Neumann entropy can be expressed as a function of these eigenvalues using the auxiliary *entropy function* $g(x)$, which describes the entropy of a thermal state with a mean photon number x:

$$g(x) = (x+1)\log_2(x+1) - x\log_2(x) \tag{3.20}$$

Consequently, the Holevo information is computed as:

$$\chi_{EB} = \sum_{i=1}^{2} g\left(\frac{\nu_i - 1}{2}\right) - \sum_{j=3}^{4} g\left(\frac{\nu_j - 1}{2}\right) \tag{3.21}$$

The behavior of the bipartite bosonic state shared by Alice and Bob is encapsulated in the *covariance matrix* Γ_{AB}. This matrix contains the variances of the local quadrature operators (q_A, p_A, q_B, p_B) on the diagonal and the mutual covariances on the off-diagonal blocks (correlation parameter Z). Since the parameters of Alice's prepared state and Bob's measured statistics are known from the parameter estimation phase, the symplectic eigenvalues required for the Holevo bound can be derived analytically from the invariants of Γ_{AB}. The symplectic eigenvalues $\nu_{1,2}$ characterizing the state ρ_{AB} are given by [72] as:

$$\nu_{1,2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)} \tag{3.22}$$

Similarly, the conditional symplectic eigenvalues $\nu_{3,4}$, which describe the state remaining after Bob's measurement, are derived from [72] as:

$$\nu_{3,4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)} \tag{3.23}$$

The coefficients A and B are defined as:

$$A = V^2 + T^2(V + \chi_{line})^2 - 2Z^2 \tag{3.24}$$

$$B = (TV^2 + TV\chi_{line} - Z^2)^2 \tag{3.25}$$

where $V = V_{mod} + 1$. The coefficients C and D depend specifically on the detection scheme employed by Bob. In the case of heterodyne detection, where there is additional vacuum noise introduced by splitting the signal, compared to the homodyne technique, they are

given by:

$$C_{het} = \frac{A\chi_{het}^2 + B + 1 + 2\chi_{het}(V\sqrt{B} + T(V + \chi_{line})) + 2Z^2}{[T(V + \chi_{tot})]^2} \tag{3.26}$$

$$D_{het} = \left(\frac{V + \sqrt{B}\chi_{het}}{T(V + \chi_{tot})}\right)^2 \tag{3.27}$$

The channel-added noise, denoted as χ_{line}, quantifies the degradation introduced during propagation. Expressed in Shot Noise Units (SNU)-which is the basic unit for calibrating the CV-QKD system-and referred to the input, it aggregates the vacuum noise introduced by the optical loss (where T is the transmittance) and the excess noise generated at the transmitter side (ξ_{Alice}):

$$\chi_{line} = \frac{1}{T} - 1 + \xi_{Alice} \tag{3.28}$$

Subsequently, the noise contribution arising from the realistic detection apparatus must be quantified. For a heterodyne receiver, the detector-added noise χ_{het} incorporates the intrinsic penalty of simultaneous quadrature measurement (the 3 dB limit), the electronic noise V_{el}, and the finite detection efficiency η. This term is expressed as:

$$\chi_{het} = \frac{2 + 2V_{el} - \eta}{\eta} \tag{3.29}$$

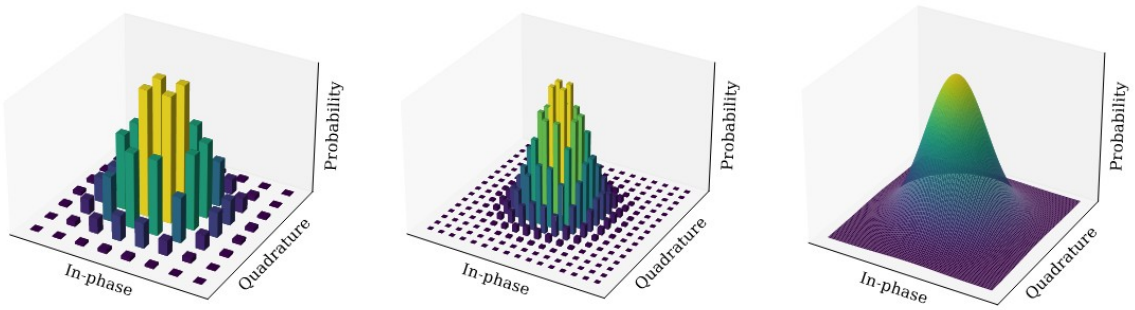
Finally, the total equivalent noise χ_{tot} referred to the channel input is obtained by combining the channel noise with the detector noise. The latter must be scaled by the inverse of the transmittance T, reflecting the fact that detection noise occurs after the signal has been attenuated:

$$\chi_{tot} = \chi_{line} + \frac{\chi_{het}}{T} \tag{3.30}$$

A fundamental distinction must be made regarding the computation of the correlation parameter Z within the covariance matrix construction. Its analytical derivation is strictly dependent on the statistical properties of the modulation scheme adopted by the transmitter. In the case of ideal Gaussian Modulation, where the input quadratures follow a continuous normal distribution, the parameter Z is derived directly from the statistical moments of the measured signal, reflecting the continuous nature of the source:

$$Z = \sqrt{T(V_{mod}^2 + 2V_{mod})} \tag{3.31}$$

Conversely, when employing Discrete Modulation formats, such as Quadrature Amplitude Modulation (QAM) with finite-size constellations, the input distribution is no longer Gaussian. Consequently, the calculation of Z requires a modified approach to correctly



(a) 64 QAM (b) 256 QAM (c) Gaussian modulation

Figure 3.3: The symbol probability and placing in the IQ-plane for PS 64 and 256 QAM and Gaussian modulation [27].

bound the properties of the equivalent Gaussian state used for the security analysis. Recent work [67] has obtained a practical bound $Z > Z^*$ for any finite-size modulation. The lower bound is given by:

$$Z^* = 2\sqrt{T}\mathrm{Tr}\left(\tau^{1/2}\hat{a}\tau^{1/2}\hat{a}^\dagger\right) - \sqrt{2T\xi_{Alice}w} \tag{3.32}$$

Having derived the bound Z^* for a generic discrete modulation, it is necessary to specify the input distribution $p_{k,j}$ adopted in this simulation to evaluate the specific performance. To maximize the SKR, the discrete constellation should approximate the optimal Gaussian distribution as closely as possible. To achieve this, Alice employs a Probabilistically Shaped QAM (PS-QAM) scheme following a normalized random walk distribution. This constellation consists of $M = m^2$ coherent states $|\alpha_{k,j}\rangle$, where the grid points for each quadrature are equally spaced between $-\sqrt{m-1}$ and $\sqrt{m-1}$. The specific amplitude of each symbol is defined as:

$$\alpha_{k,j} = \alpha\frac{\sqrt{2}}{\sqrt{m-1}}\left(k - \frac{m-1}{2}\right) + i\alpha\frac{\sqrt{2}}{\sqrt{m-1}}\left(j - \frac{m-1}{2}\right) \tag{3.33}$$

where $k, j \in \{0, \ldots, m-1\}$. To approximate the Gaussian statistics required for high mutual information, each symbol is associated with a probability derived from the binomial distribution:

$$p_{k,j} = \frac{1}{2^{2(m-1)}}\binom{m-1}{k}\binom{m-1}{j} \tag{3.34}$$

As illustrated in Figure 3.3, this distribution (Figures 3.3a, 3.3b) rapidly converges to the ideal Gaussian profile (Figure 3.3c) as m increases, allowing the protocol to approach the theoretical capacity limits while maintaining a discrete alphabet.

Conclusively, the practical Secret-Key Rate (SKR), expressed in bits per second, is governed by the following analytical expression, which incorporates both the asymptotic limits and the necessary finite-size corrections:

$$SKR = \frac{n}{N} \cdot (1 - \text{FER}) \cdot [\beta I_{AB} - \chi_{BE} - \Delta(n)] \tag{3.35}$$

where N is the total number of transmitted symbols and n represents the effective block length utilized for key generation, which indicates how many of the total number of symbols sent is intended to be used to form the secret key. The factor $(1-\text{FER})$ accounts for the Frame Error Rate, discarding blocks that fail the error correction or verification steps, while β is the reconciliation efficiency. Regarding the information-theoretic terms, I_{AB} represents the Shannon mutual information between Alice's transmitted variable and Bob's measured data, while χ_{BE} is the Holevo bound limiting the maximum information accessible to Eve under collective attacks. Crucially, the term $\Delta(n)$ represents the security penalty imposed by finite-size effects during the privacy amplification stage. This penalty is explicitly defined as [73]:

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} + \frac{2}{n}\log_2\left(\frac{1}{\varepsilon_{PA}}\right) \tag{3.36}$$

where $\bar{\varepsilon}$ is a smoothing parameter and ε_{PA} is a failure probability associated with the privacy amplification step, arising from the application of the Leftover Hash Lemma [74]. To guarantee universally composable security, the total security parameter ε is defined as the sum of the individual failure probabilities of the protocol sub-routines:

$$\varepsilon = \varepsilon_{PE} + \varepsilon_{EC} + \bar{\varepsilon} + \varepsilon_{PA} \tag{3.37}$$

In alignment with standard safety criteria found in the literature [73], this thesis adopts a conservative approach by setting all constituent parameters to a uniform threshold of:

$$\varepsilon = \varepsilon_{PE} = \varepsilon_{EC} = \bar{\varepsilon} = \varepsilon_{PA} = 10^{-10} \tag{3.38}$$

ensuring a high level of security for the generated key.

As established earlier on, the finite-size analysis is performed by employing statistical worst-case estimators for the critical channel parameters—specifically excess noise (ξ) and transmittance (T). Alice and Bob model the physical link as a normal linear channel relating the input symbols x and output measurements y. For heterodyne detection, this

relationship is given by:

$$y = tx + z \tag{3.39}$$

where $t = \sqrt{T\eta}$ represents the effective transmission coefficient, and z is a centered normal random variable characterizing the total noise with variance $\sigma_z^2 = 2+2V_{el}+\xi_{Bob}$. Since the accuracy of these estimates is constrained by the finite number of symbols $N_{PE} = N - n$ reserved for this phase, statistical fluctuations must be bounded to guarantee security. To ensure the SKR is valid with a probability of at least $1 - \varepsilon_{PE}$, we derive a lower bound t_{min} and an upper bound $\sigma^2_{z,max}$, assuming individual failure probabilities of $\varepsilon_{PE}/2$. These worst-case estimators are computed as:

$$t_{min} \approx \sqrt{T\eta} - z_{\varepsilon_{PE}/2}\sqrt{\frac{\sigma_z^2}{N_{PE}V_A}} \tag{3.40}$$

$$\sigma^2_{z,max} \approx 2 + 2V_{el} + \xi_{Bob} + z_{\varepsilon_{PE}/2}\left(\frac{\sigma_z^2\sqrt{2}}{\sqrt{N_{PE}}}\right) \tag{3.41}$$

where the factor $z_{\varepsilon_{PE}/2}$ is determined by the inverse error function such that $1 - \mathrm{erf}(z_{\varepsilon_{PE}/2}/\sqrt{2}) = \varepsilon_{PE}$. Finally, the conservative values for the channel transmittance and excess noise, which are substituted into the final key rate equation, are derived as:

$$T_{min} = \frac{t^2_{min}}{\eta}, \qquad \xi_{Alice,max} = \frac{\sigma^2_{z,max} - 2 - 2V_{el}}{\eta T_{min}} \tag{3.42}$$

3.2.2. Implementation and Analysis of CV-SKR

In order to provide a quantitative assessment of the CV-QKD protocol's performance and to validate the theoretical model described in the previous paragraph, the analytical expressions for the SKR were implemented in a numerical simulation environment based on MATLAB. This computational approach enables the exploration of system behavior under varying operational conditions and the identification of the physical limits of secure transmission. The performance assessment starts by conducting a comprehensive sensitivity analysis to characterize the system's robustness under fixed operating conditions. The investigation focuses on the behavior of the SKR across three critical domains: the transmission distance, the modulation variance (V_{mod}) and the channel excess noise at Bob's side (ξ_{Bob}). To conduct these simulations, a set of realistic experimental parameters was selected based on current state-of-the-art technology. These values are maintained constant throughout this static analysis and are summarized in Table 3.2. It should be noted that the reported SKR values are not derived from a composable finite-size security

V_{mod} [SNU]	$\alpha[dB/km]$	η_{Bob}	ξ [SNU]	V_{el} [SNU]	β	FER	N	ε	n/N
5.3	0.2	0.45	0.005	0.12	0.96	0.3	10^8	10^{-10}	0.5

Table 3.2: CV-QKD parameter values used for numerical simulation.

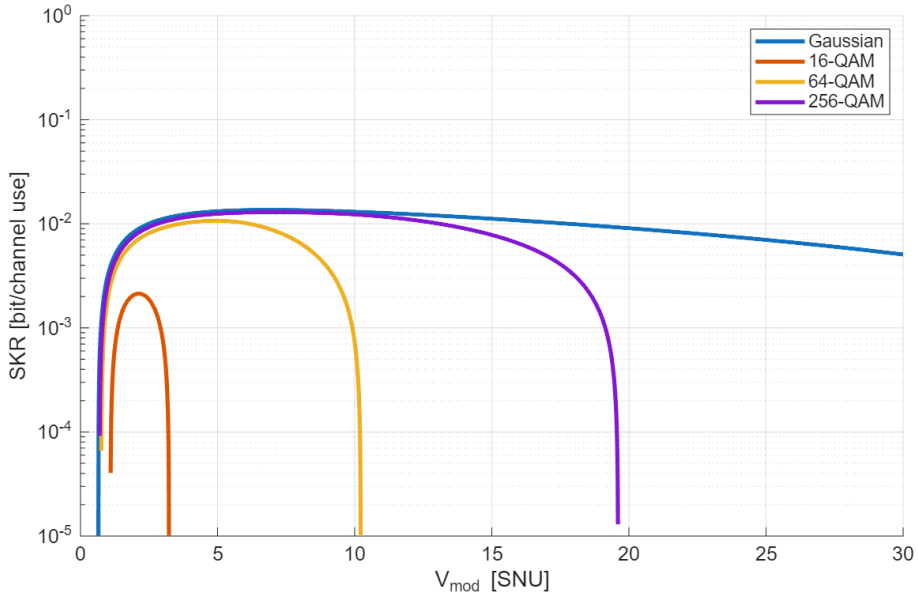
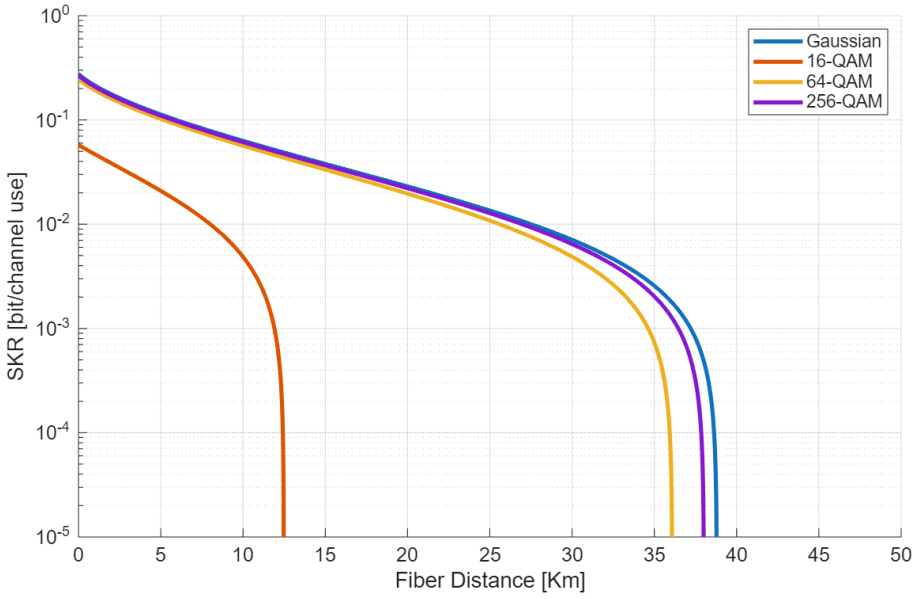


Figure 3.4: Comparison of the SKR as a function of V_{mod} for different modulation formats, at a fixed transmission distance of 25 km and with $N = 10^8$.

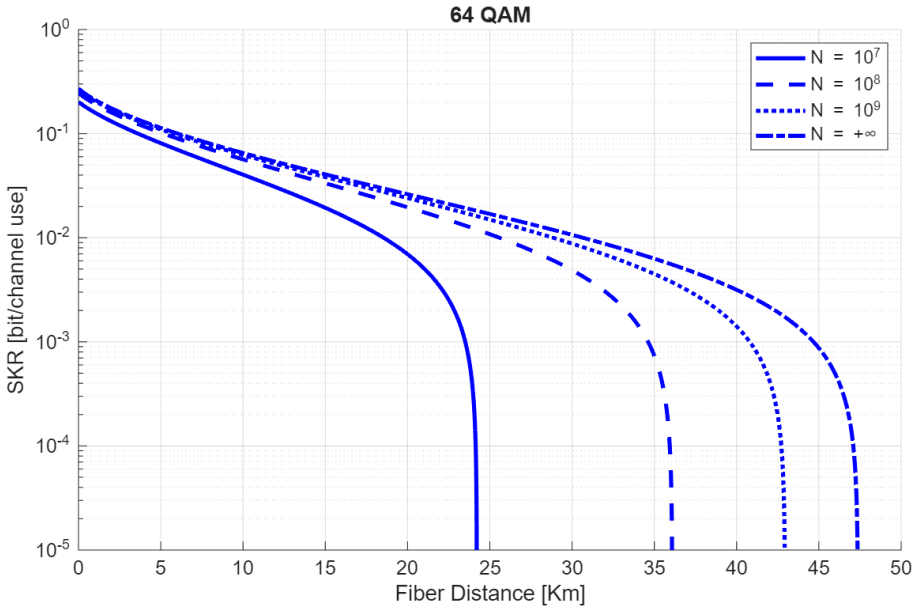
proof for 16-QAM, 64-QAM and 256-QAM, as this remains an open and ongoing area of research.

The initial parametric analysis focuses on the modulation variance (V_{mod}), a parameter directly proportional to the optical signal power emitted from Alice's transmitter. As illustrated in Figure 3.4, the SKR exhibits a distinct convex behavior with respect to V_{mod}, indicating an optimal operational range that maximizes the key generation depending on the chosen modulation format.

Next, a transmission distance sweep is conducted to evaluate the comparative performance of the discrete modulation formats under identical system parameters. As depicted in Figure 3.5a, there is a clear convergence behavior: as the modulation order increases, the performance of the discrete constellations progressively approaches the theoretical upper bound set by the ideal Gaussian modulation. A critical parameter governing practical CV-QKD implementations is the total block length N. Larger values of N are strictly required to mitigate the statistical fluctuations inherent in the finite-size regime. Because the simulations conducted in this thesis try to emulate a practical implementation, the

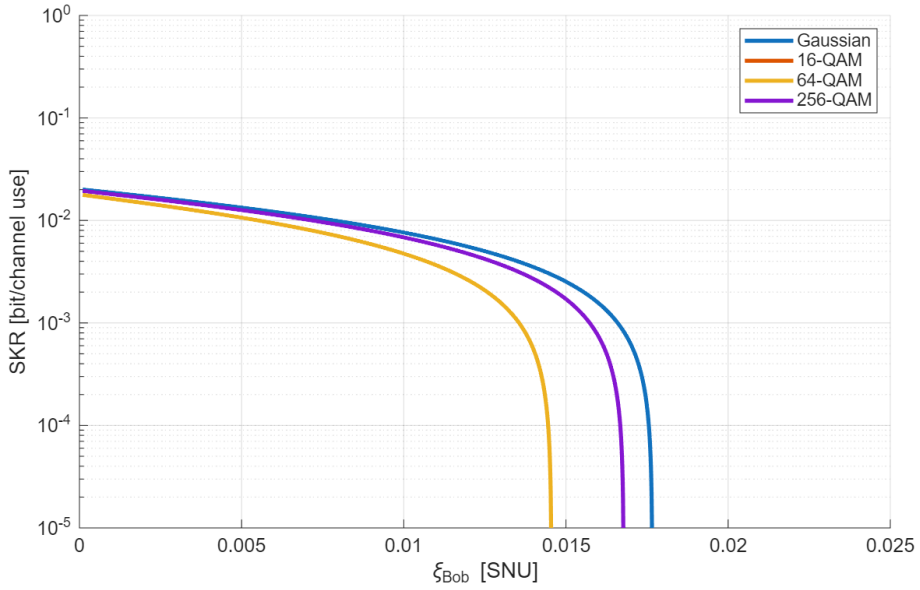


(a)

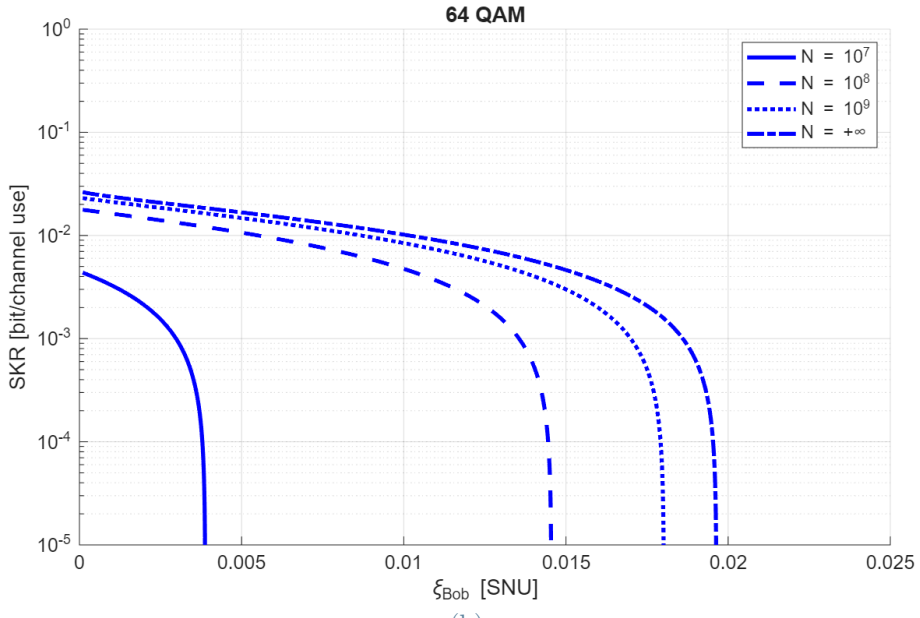


(b)

Figure 3.5: (a) SKR performance over transmission distance for different modulation schemes with fixed $N = 10^8$. (b) Impact of block length N on the SKR with probabilistically shaped 64-QAM across different distances.



(a)



(b)

Figure 3.6: (a) Comparison of the SKR as a function of excess noise measured at Bob's side for different modulation formats, at a fixed transmission distance of 25 km. (b) SKR performance for probabilistically shaped 64-QAM as a function of ξ_{Bob} for different values of N, at a fixed distance of 25 km.

asymptotic limit of an infinite key is taken only as a comparison reference. Target block lengths of $N = 10^7$, $N = 10^8$, $N = 10^9$ were selected for the simulations to ensure stable and secure key generation.
Finally, the system's robustness is quantified by analyzing the maximum amount of excess noise (ξ_{Bob}) that the protocol can tolerate while maintaining a strictly positive SKR. Figure 3.6a illustrates this maximum tolerable excess noise, evaluated at Bob's receiver, across the various modulation formats. For the 16-QAM constellation operating at a block length of $N = 10^8$, the intrinsic statistical penalty combined with the channel attenuation at 25 km is sufficient to drive the SKR to zero, even in an ideal scenario with no external excess noise ($\xi_{Bob} = 0$). A fundamental factor limiting this tolerance is the worst-case parameter estimation framework, which is heavily dependent on the chosen block length N. As demonstrated in Figure 3.6b, increasing N yields tighter statistical confidence intervals during the parameter estimation phase. This enhanced precision directly translates into a higher resilience to excess noise, enabling the system to remain secure even under degraded channel conditions.

Subsequent to the static characterization, the CV-QKD system is subjected to a rigorous multi-variable optimization process, to ensure a fair and consistent benchmarking with the DV technology. A direct comparison would be inherently biased if the CV system parameters were merely fixed at arbitrary values while the DV system utilized optimized settings, as described in Section 3.1. Therefore, the final part of this section introduces a routine designed to maximize the achievable key rate at each transmission distance by dynamically tuning two critical degrees of freedom: the *modulation variance* (V_{mod}), which corresponds to the signal power injected by Alice and the *ratio of block usage* ($\alpha = n/N$), which defines the fraction of the total transmitted symbols (N) allocated for secret key generation (n) versus those sacrificed for parameter estimation ($N_{PE} = N - n$). The numerical results of this optimization are presented to determine the theoretical upper bound of the system's performance. These optimized results will serve as the reference baseline for the comparative study in the next chapter. All other physical system parameters remain fixed at the reference values detailed in Table 3.2.

As evidenced by the graphical results in Figure 3.7, implementing the multi-variable optimization routine yields a substantial improvement in the overall system performance compared to the static parameter scenario. Notably, the maximum secure transmission reach is extended by 10 km or more across all analyzed modulation formats. This enhancement underscores the absolute necessity of dynamically adapting the control variables in response to channel attenuation to maximize the SKR. To fully comprehend this improvement, it is crucial to analyze the evolution of the optimal parameters as a function

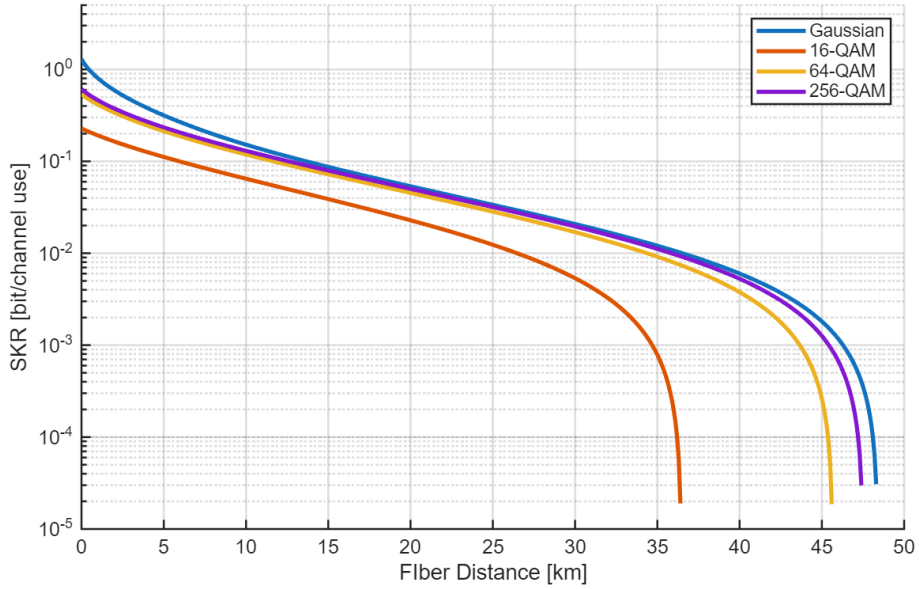


Figure 3.7: CV SKR performance as a function of transmission distance for different modulation schemes with optimized parameters V_{mod} and $\alpha = n/N$ (dedicated fiber).

of distance (Figure 3.8):

- The trend of the optimal modulation variance reveals distinct behaviors between the continuous and discrete modulations at short distances, which eventually converge at longer reaches. In the high-SNR regime (short distances), the ideal Gaussian modulation saturates at the maximum upper bound set by the algorithm (fixed at 30 SNU), before progressively decreasing to almost align with the 256-QAM curve. Conversely, the discrete modulations (16-QAM, 64-QAM, and 256-QAM) exhibit a more conservative behavior from the start, maintaining stable optimal values around 5 SNU. Despite these initial differences, a clear downward trend in V_{mod} is observed for all formats as the fiber length increases. This dynamic is driven by a fundamental cryptographic requirement: when channel conditions deteriorate due to high attenuation, transmitting signals with high power (high variance) would provide a disproportionate information advantage to a potential eavesdropper (Eve). Reducing the signal variance limits the information accessible to Eve in noisy channels and simultaneously optimizes the SNR at the receiver. This careful tuning is required to maximize the efficiency of the error correction algorithms (reconciliation phase), which would otherwise fail or operate inefficiently at low SNR levels.
- An equally critical trend is observed for the parameter $\alpha = n/N$, which defines the fraction of the data block allocated for actual key generation. At short distances, the curves for all modulation formats start at the imposed maximum limit of 0.95.

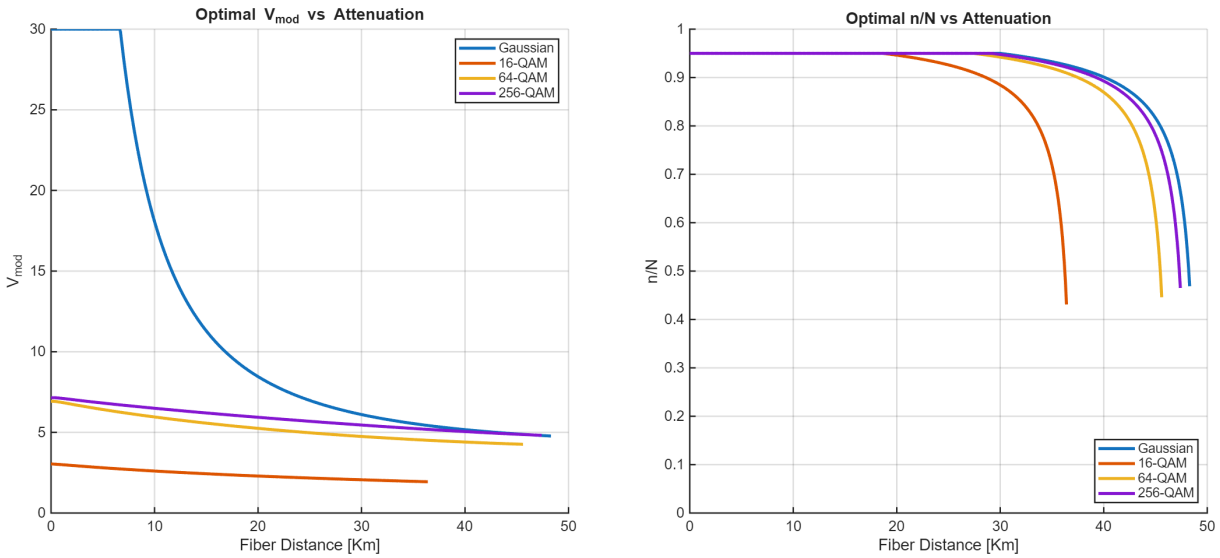


Figure 3.8: Evolution of the optimal CV parameters as a function of the transmission distance.

In this favorable regime, noise and attenuation are minimal, making the channel parameter estimation intrinsically highly accurate. This allows Alice and Bob to allocate almost the entire transmitted block to extract the final SKR. However, the value of n/N experiences a drastic and progressive decline beyond a certain distance threshold. The reason behind this behavior lies entirely in the management of finite-size effects. As attenuation increases, the statistical uncertainty in estimating the channel transmittance (T) and the excess noise (ξ_{Bob}) amplifies significantly. To prevent these statistical fluctuations from resulting in a worst-case estimation that would completely nullify the SKR, the protocol is forced to expand the data set used for the security analysis. Consequently, the system must sacrifice an increasingly larger fraction of the transmitted symbols for parameter estimation, inevitably reducing the portion n available for key generation to guarantee the unconditional security of the link.

3.2.3. Impact of Modulation Cardinality in CV-QKD

Following the comparative analysis of the system performance under optimized conditions, it is necessary to formally establish a reference modulation format for the remainder of this thesis. As previously discussed, CV-QKD encodes information in the continuous quadrature values (x and p) of coherent states, meaning the achievable SKR is directly limited by the entropy of the chosen modulation constellation. To maximize the mutual information and approach the channel capacity, theoretical frameworks inherently assume

an ideal Gaussian modulation. However, in practical implementations, generating a true continuous Gaussian distribution is physically unrealizable due to the finite resolution of Digital-to-Analog Converters (DACs). Consequently, state-of-the-art practical systems employ Probabilistically Shaped (PS) discrete constellations, such as 256-QAM, to closely approximate the optimal Gaussian profile. As demonstrated in the optimized performance evaluation (Figure 3.7), the high-density 256-QAM constellation exhibits a performance that is incredibly close the ideal Gaussian limit across the operational ranges relevant to this network study. Despite the practical reality of discrete formats, the Gaussian modulation will be adopted as the definitive reference benchmark for the network-level comparative analysis in Chapter 5. In this context, the Gaussian model is not intended to represent a directly deployable hardware configuration, but rather serves as a robust, analytically tractable mathematical proxy for a highly optimized, high-order PS-QAM system. This strategic methodological choice is driven by three fundamental justifications:

- *Computational efficiency*: from a simulation perspective, evaluating the SKR for ultra-dense constellations like 256-QAM imposes a severe computational bottleneck in the MATLAB environment. The numerical computation of probabilities and phase-space distances for 256 individual states critically slows down the multi-variable optimization routines required for the coexistence analysis. The analytical equations of the Gaussian model, conversely, ensure rapid convergence and numerical stability during the optimization loops.
- *Tractability of security proofs*: security proofs for high-order discrete constellations against collective attacks often rely on numerical, pessimistic lower bounds (such as the evaluation of Z^*). The Gaussian modulation allows for exact and analytical security derivations using the covariance matrix formalism. This decouples the system's performance evaluation from the mathematical penalties and discretization artifacts introduced by numerical approximation methods.
- *Theoretical upper bound*: by maximizing the entropy for a given signal variance, the Gaussian distribution represents the absolute information-theoretic capacity limit for CV protocols.

In this chapter, we have established the theoretical foundations and derived the analytical expressions for the SKR of both Discrete-Variable and Continuous-Variable QKD protocols. By incorporating finite-size analysis and evaluating protocol-specific configurations, we provided a rigorous assessment of the achievable key rates over a dedicated fiber link. The numerical results presented in the previous sections highlighted the sensitivity of

both technologies to the finite data length and channel attenuation, defining the baseline performance limits in an idealized point-to-point scenario.
However, theoretical equations alone are insufficient for a flexible and comprehensive analysis of complex network scenarios. To bridge the gap between these mathematical models and their practical application in varying network architectures, a dedicated simulation tool is required. The next chapter will therefore present the MATLAB-based software tool developed specifically for this thesis: an application that integrates the derived SKR models into a user-friendly Graphical User Interface (GUI), allowing for the dynamic simulation of PON topologies.

4 | Development of a QKD Analysis Tool for PON Architectures

Following the theoretical derivation of the security bounds for Discrete-Variable and Continuous-Variable QKD, the practical evaluation of these protocols in realistic scenarios requires a robust computational framework. To address this challenge, a dedicated software tool has been developed within the MATLAB environment. The primary objective of this application is to provide a flexible and interactive Graphical User Interface (GUI) that allows network designers to simulate the performance of QKD systems seamlessly and to easily tune their network parameters and conditions. The tool enables the user to define critical PON and protocol-specific QKD parameters and to perform automated parameter sweeps. This chapter details the software architecture, the design of the user interface and the computational logic implemented to convert the mathematical models of Chapter 3 into a dynamic simulation environment. Furthermore, this tool serves as the enabling technology for the comparative analysis performed in Chapter 5, providing the robust numerical data necessary to benchmark DV- and CV-QKD under identical and realistic network conditions.

4.1. Software Architecture

The simulation tool was developed within the MATLAB environment (version R2025b), utilizing the App Designer framework to ensure a robust and responsive user experience. The architectural design follows a modular paradigm, strictly separating the Graphical User Interface (GUI) layer from the computational core (Backend). This separation of concerns ensures that the mathematical models derived in Chapter 3 can be updated or refined without altering the visualization logic, and vice-versa.

The architecture is composed of three main functional blocks:

- *The input aggregation layer* (Frontend): this layer is responsible for user interaction. It collects the heterogeneous input parameters—ranging from topological constraints to device specifications—and validates them to prevent physical inconsistencies.
- *The interaction and control layer* (App designer code): acting as the bridge between the user and the computational engine, this layer manages the application's logic flow. It operates on an event-driven basis: a physical action performed by the user (such as clicking the "Run Simulation" button or changing a dropdown menu) triggers a specific callback function. This layer is responsible for collecting the current state of the inputs from the GUI, packaging them into a structured format, and invoking the appropriate backend functions.
- *The integrated computational and visualization engine* (Backend): this backend layer constitutes the core of the software. Unlike traditional architectures where calculation and plotting are separate, this engine integrates both tasks to maximize efficiency. Upon being called by the control layer, the dedicated MATLAB functions execute the algorithms to compute the Secret-Key Rate. Simultaneously, these functions handle the data visualization: they directly access the GUI's axes handles to render the resulting SKR curves in real-time. This approach ensures that the visual output is strictly coupled with the generated numerical data, providing immediate feedback on the simulation performance.

Furthermore, the system block diagram in Figure 4.1 shows how the software operations follow a hierarchical, multi-stage workflow. This structure ensures that the common network infrastructure is defined independently from the specific quantum protocol employed. The workflow is segmented as follows:

1. Upon initializing the application (MATLAB App Start), the user is first required to define the PON parameters. These inputs—representing the shared physical layer constraints such as feeder and distribution fiber length, number of users, PON standard and fiber topology—are protocol-agnostic. This design choice allows the user to simulate different quantum technologies over the exact same network topology without re-entering the infrastructure data. After the PON parameters have been configured, the "Visualize PON Scheme" button allows the user to display a simplified representation of the network in a dedicated section.
2. Once the environment is set, the workflow bifurcates at the Select Protocol stage. Choosing between the DV-QKD or CV-QKD modes activates the corresponding configuration panel. In this dedicated stage, the user populates the protocol-specific variables. This separation ensures that the interface remains clean, presenting only

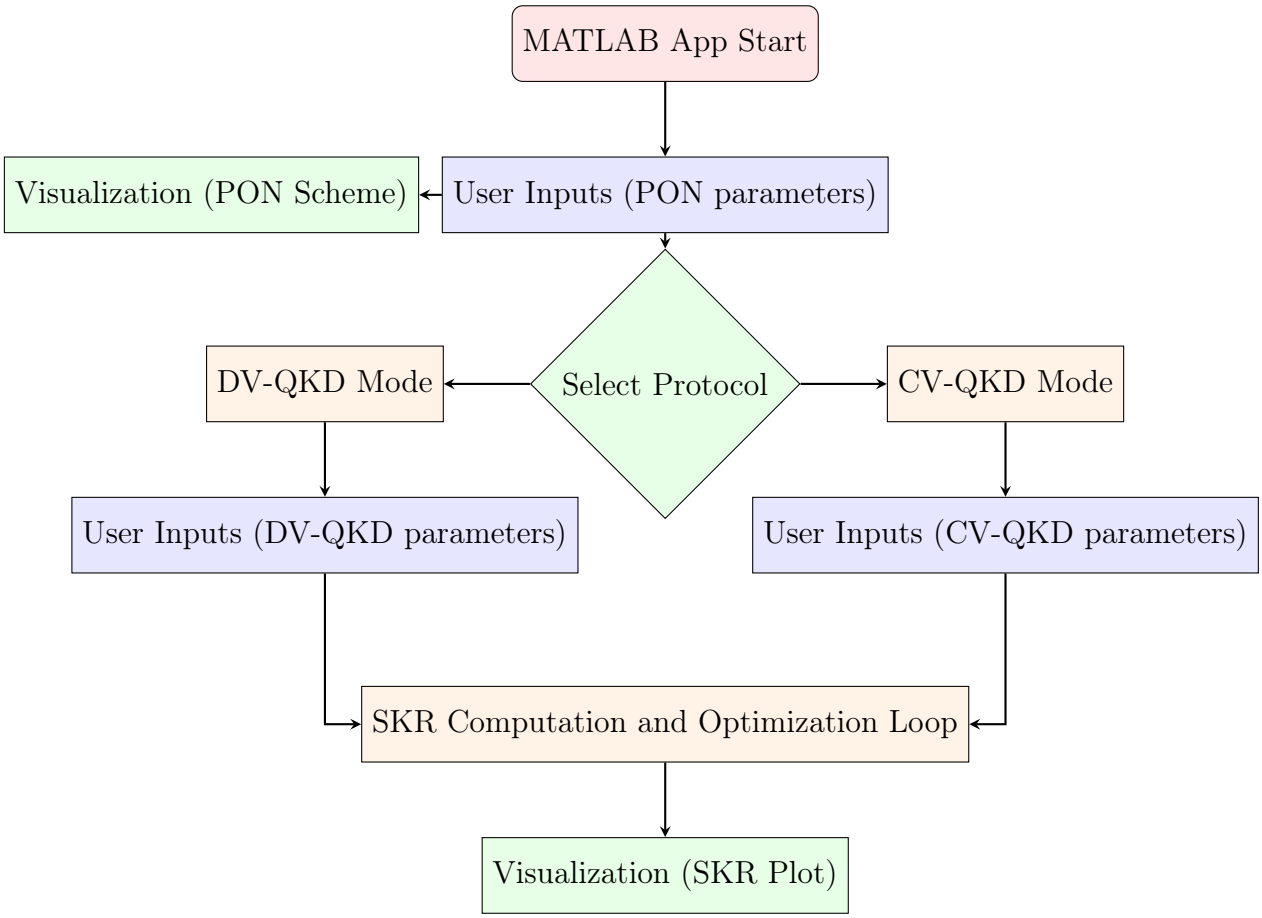


Figure 4.1: Operational flowchart of the developed software tool. The diagram illustrates the data flow from the User Interface inputs to the computational backend engines and the final visualization.

the parameters relevant to the selected technology.

3. After all parameters are aggregated, the SKR Computation engine is triggered. This block merges the global topological constraints with the specific protocol settings. The backend then executes the computation routine, obtaining key rate values for each simulated distance or for each of the other sweeping parameters (like modulation variance or excess noise for the CV-QKD mode).

4. Finally, the computed data is passed to the Visualization module, which plots the SKR curves in real-time, allowing for immediate assessment of the system's performance.

A core principle guiding the development of the software was modularity. To avoid a monolithic code structure, which is often prone to errors and difficult to debug, the computational backend was divided into independent functional blocks. This design choice

ensures that the distinct quantum protocols are handled by separate dedicated calculation engines. The calculation routines for the Decoy-state DV protocol and the Gaussian-modulated or Discrete-modulations CV protocols are encapsulated in distinct MATLAB functions. The *interaction layer* (App designer code) acts as a switch, invoking the specific engine required by the user's selection without any cross-interference. This ensures that updates or debugging performed on one protocol module do not inadvertently affect the stability of the other. Common physical models shared by both architectures, such as the fiber attenuation profile or the splitter insertion loss calculations (dependent on the number of users), are implemented as shared utility functions. This reduces code redundancy and guarantees that the channel model remains consistent across all simulations. The architecture is designed to be future-proof. New functionalities, such as alternative channel noise models or additional QKD protocols, can be integrated simply by adding the corresponding backend function and linking it to a new GUI callback, without requiring a restructuring of the existing codebase.

4.2. Graphical User Interface (GUI) Design

While the software architecture defines the robustness and logical flow of the simulation, the Graphical User Interface (GUI) determines its usability and practical effectiveness. Developed using the MATLAB App Designer framework, the interface was designed with a user-centric philosophy, aimed at closing the gap between the complex mathematical formalism of QKD security bounds and the intuitive requirements of network engineering. The primary objective of the GUI is to abstract the underlying computational complexity. It allows the user to define sophisticated PON and quantum protocol parameters without requiring direct interaction with the source code or the mathematical scripts. The layout is structured to mirror the logical workflow described in the previous section, guiding the user sequentially through network definition, protocol configuration and simulation control. Furthermore, the interface acts as a first line of defense against configuration errors. Through integrated input validation routines, the GUI ensures that all physical parameters remain within feasible physical bounds before any computation is triggered. The following parts detail the organization of the interface, the specific input panels, and the data visualization capabilities.

As shown in Figure 4.2, the Graphical User Interface is not designed as a monolithic block of inputs but is organized into distinct functional modules. This modular segmentation allows the user to focus on one aspect of the system design at a time.
In the following subsections, the specific functionalities and input parameters of each

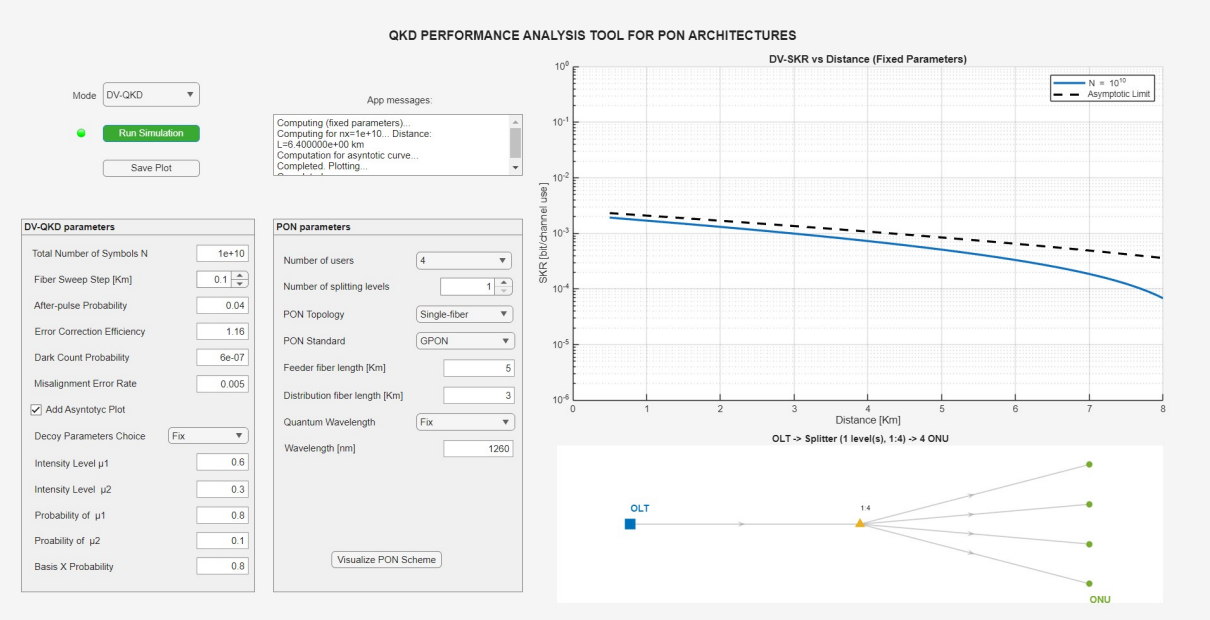


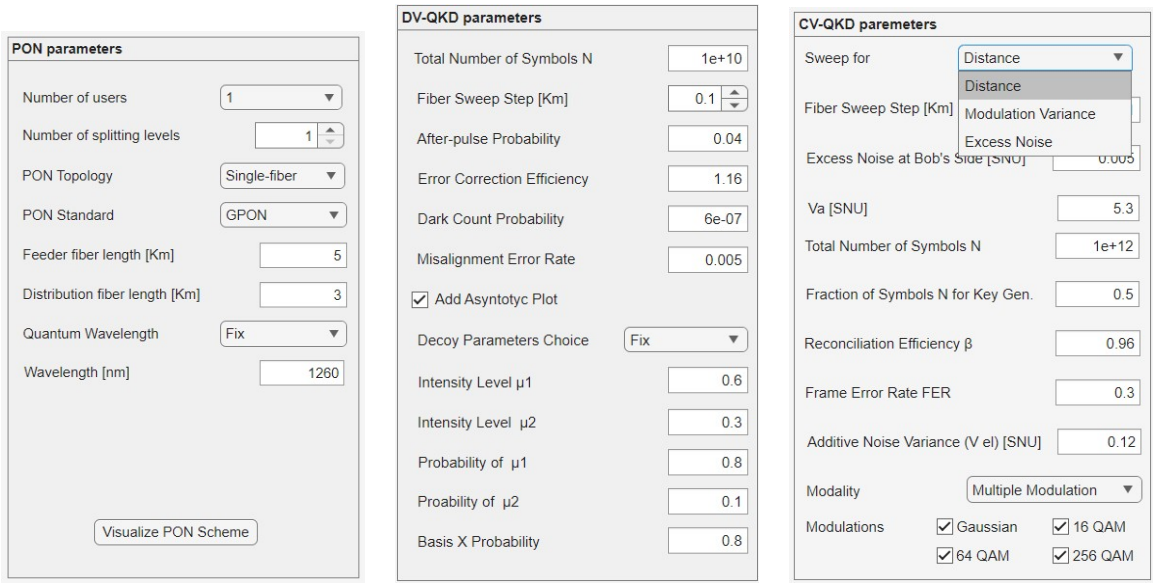
Figure 4.2: Overview of the Graphical User Interface (GUI). The window is divided into three functional areas: network topology configuration, protocol-specific parameters configuration and visualization panels.

module are analyzed in detail.

4.2.1. Network Topology Configuration

This panel serves as the digital interface for defining the structural and physical constraints of the Passive Optical Network. As shown in Figure 4.3a, the user configures the simulation environment through several critical parameters that directly influence the channel model:

- Fiber lengths (L_f and L_d): the user defines the lengths of the *Feeder fiber* and *Distribution fiber*, respectively. Beyond determining the total propagation distance ($L = L_f + L_d$), these values are fundamental for the noise model. The simulation uses these lengths to integrate the Raman scattering equations along the fiber, thereby calculating the accumulated noise power and deriving the effective quantum channel attenuation coefficient α_q, which accounts for the specific spectral interplay between quantum and classical signals.
- Number of users: this dropdown menu selects the cardinality of the PON (1, 4, 8, 16, 32, 64 users). This parameter introduces the characteristic lumped losses of the access network. Consequently, the total channel attenuation is computed as a function of the total distance L, the effective coefficient α_q and the splitting losses



(a) (b) (c)

Figure 4.3: Overview of: (a) the network topology panel, (b) the DV parameters panel and (c) the CV parameters panel.

dictated by the number of users, as shown in Eq. 2.2.

- Number of splitting levels: this parameter specifies the hierarchical structure of the distribution network, indicating whether the total splitting ratio is achieved through a single stage (one splitter) or distributed across two cascaded levels (a primary splitter followed by secondary splitters closer to the user premises).
- PON topology: this selection defines the physical architecture of the network, offering three distinct configurations:
  - *Single-fiber:* models the standard bidirectional architecture where all signals share the same medium, representing the worst-case scenario for Raman noise.
  - *Dual-fiber:* simulates a scenario with physically separated fibers for upstream and downstream (or quantum and classical) traffic, significantly mitigating backscattering noise.
  - *Dual-feeder fiber:* represents a protected architecture or a hybrid topology where the feeder segment is duplicated, altering the noise accumulation profile compared to the distribution segment.
- PON standard: the user selects the specific ITU-T standard (between GPON, XG-PON, NG-PON2, HS-PON). This choice automatically populates the simulation

with the standardized classical wavelengths and launch powers, establishing the interference environment.

- Wavelength allocation mode: the panel allows for the spectral definition of the quantum channel. The user can either fix a specific quantum wavelength (λ_q) for a targeted analysis or enable the *Sweep mode*. In the latter case, the user defines a spectral range $[\lambda_{min}, \lambda_{max}]$, instructing the tool to iteratively evaluate the SKR across the entire band to identify the optimal spectral allocation.

4.2.2. Protocol-specific Parameters Configuration

This section of the interface (Figures 4.3b, 4.3c) is designed to be fully dynamic: it automatically updates its input fields based on the selected quantum technology (CV-QKD or DV-QKD), ensuring that the simulation utilizes only the variables strictly relevant to the chosen protocol. In CV-QKD Mode, the panel allows the user to define the primary independent variable for the performance analysis. Through a specific dropdown menu, the user can select the sweep type for the final plot, choosing between Distance, Modulation Variance or Excess Noise. Regardless of the chosen sweep, a set of common physical parameters must be configured to define the baseline system performance: the total number of transmitted symbols (N), the reconciliation efficiency (β), the Frame Error Rate (FER), the fraction of symbols allocated for key generation and the electronic noise variance (V_{el}). Furthermore, the interface provides control over the modulation strategy: the user can opt to simulate a specific Single Modulation format (Gaussian or discrete) alongside the asymptotic limit for benchmarking purposes, or select Multiple Modulations to visualize and compare several schemes simultaneously on the same graph. Conversely, when DV-QKD Mode is selected, the inputs shift to the specific constraints of discrete-variable technology. The critical parameters available for configuration include the dark count probability (p_{dark}), the after-pulse probability (p_{ap}), the total number of transmitted symbols (N), the error correction efficiency (f_{ec}) and the misalignment error rate (e_{mis}). Additionally, the panel addresses the decoy-state method configuration: the user can either manually set the intensity and probability parameters for the signal and decoy states or enable an automatic optimization routine, allowing the software to determine the optimal values that maximize the SKR.

4.2.3. Visualization and Results Module

The final component of the GUI is the Visualization Module, designed to provide an immediate and intuitive interpretation of the simulation outcomes. This module, pre-

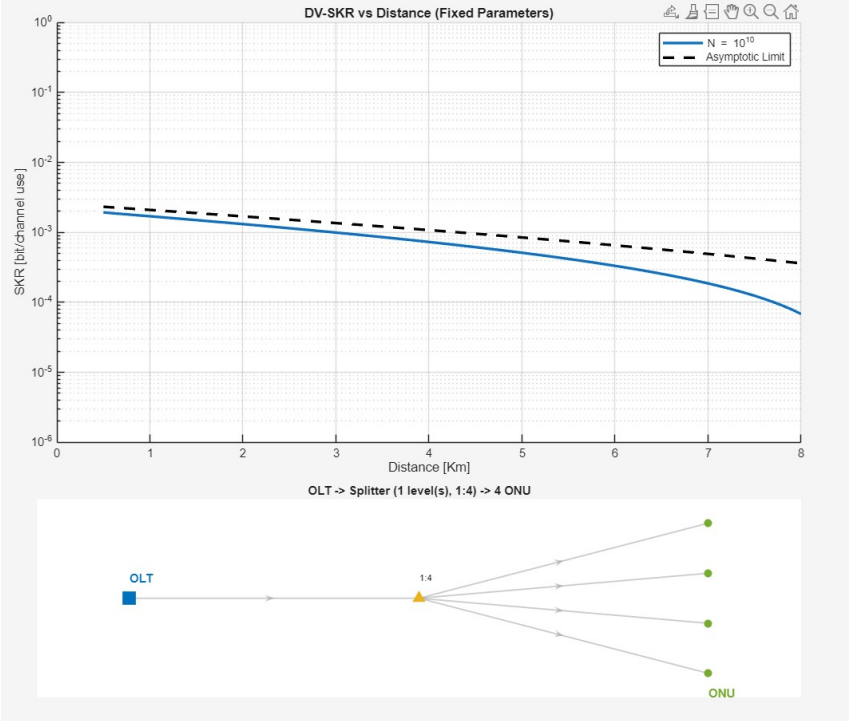


Figure 4.4: Overview of the visualization module interface.

sented in Figure 4.4, is divided into two panels: the *dynamic plotting interface* and the *network topology schematic*. The plotting interface is the core analytical tool, dedicated to the graphical representation of the SKR. A key feature of this panel is its context-aware adaptability: the axes and scales automatically reconfigure based on the selected simulation mode. For instance, when analyzing the attenuation limit, the abscissa represents the fiber distance, while in spectral coexistence analysis, it shifts to the wavelength domain. The ordinate (SKR) typically employs a logarithmic scale to properly visualize the transition from the asymptotic regime to the finite-size cut-off. Complementing the numerical data, the network schematic panel offers a synthesized visual representation of the simulated physical layer. This panel dynamically plots the topological structure of the Passive Optical Network, illustrating the hierarchy from the Optical Line Terminal (OLT) through the splitting stages down to the Optical Network Units (ONUs). The schematic updates upon pressing the "Visualize PON Scheme" button to reflect the parameters set in the configuration panel. Specifically, the graphical representation of the splitting levels and the density of the ONU endpoints adjust to match the selected *number of users* and *number of splitting levels*, providing the user with an immediate visual confirmation of the network complexity and the branching factor being simulated.

With the architecture and the functional modules of the simulation framework fully defined, the following chapter focuses on the practical application of the developed tool. The developed software is effectively employed to conduct a rigorous comparative analysis between Continuous-Variable and Discrete-Variable QKD protocols, evaluating their respective performance, coexistence capabilities, and implementation challenges within the realistic infrastructure of Passive Optical Networks.

5 | Performance Analysis and Comparisons

Having established the theoretical security bounds in Chapter 3 and developed the dedicated computational framework in Chapter 4, this chapter focuses on the comprehensive performance analysis of Quantum Key Distribution within Passive Optical Networks (PONs) in the finite-key condition. The transition from idealized point-to-point links to complex access architectures introduces severe impairments that critically limit the operational range of quantum protocols. The primary objective of this chapter is to perform a systematic simulative analysis between Discrete-Variable (DV) and Continuous-Variable (CV) QKD protocols. Using the MATLAB simulation tool presented in the previous chapter, we tested the two technologies under identical network conditions, taking into account different PON standards.

5.1. Simulated Network Architecture

The simulation framework developed in this thesis is built upon a reference topology that reflects the most prevalent infrastructure in current access networks. Driven by the significant costs associated with laying new optical cables and the scarcity of available dark fibers, the majority of deployed PONs rely on a single-fiber bidirectional configuration, where both upstream (US) and downstream (DS) traffic share the same Optical Distribution Network (ODN) [63]. This architecture, which represents the primary focus of this analysis, poses the most significant challenges for quantum coexistence due to the high density of optical signals propagating within a single waveguide. The investigated topology is schematically illustrated in Figure 5.1. In this configuration, the quantum signal is assumed to propagate in the upstream direction (from the ONU to the OLT). This directional choice is strategic for practical deployment, as it allows the sensitive and costly quantum receiver (Bob) to be housed at the secure central office (OLT), while keeping the user equipment (Alice at the ONU) as compact and cost-effective as possible. Simultaneously, the fiber carries two distinct high-power classical data streams that act

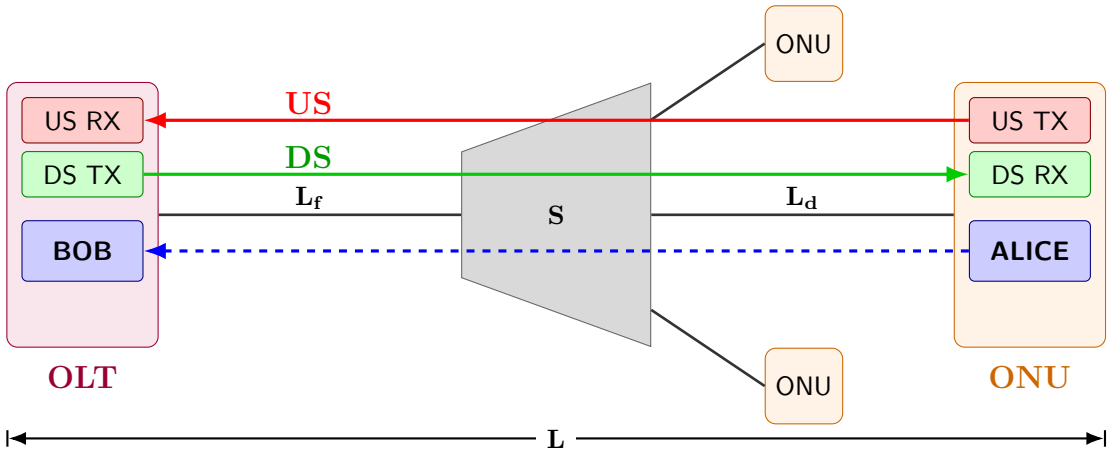


Figure 5.1: Simulated single-fiber PON architecture, where the US (red) and DS (green) classical signals and the QKD one (dashed blue) can be identified.

as noise sources:

- A co-propagating classical upstream channel.
- A counter-propagating classical downstream channel.

To evaluate the system under the most stringent conditions, a *worst-case scenario* strategy was adopted for the spectral allocation. The classical carrier frequencies were selected based on the PON standards discussed in Chapter 2, specifically choosing the channels spectrally closest to the candidate quantum allocation. This approach intentionally maximizes the efficiency of Raman cross-talk, as the scattering probability increases as the wavelength detuning between the pump (classical data) and the signal (quantum) decreases. Consequently, if the system can guarantee a positive SKR under these aggressive noise conditions, its security in less congested spectral configurations is implicitly assured. The specific wavelength values adopted for this worst-case analysis are summarized in Table 5.1. As detailed in Section 2.3, the intensity of the generated noise is governed by the Raman efficiency coefficient β, which is strictly dependent on the frequency shift between the interacting signals. Although Raman scattering is isotropic in principle, the impact on the system is determined solely by the photons that impinge upon Bob's receiver. Consequently, the noise sources are modeled as follows:

- The downstream (DS) classical signal, propagating opposite to the quantum channel, acts as the source for Backward Raman Scattering.
- The upstream (US) classical signal, sharing the same propagation direction as the quantum channel, generates Forward Raman Scattering.

PON Standard	λ_c^{US} [nm]	λ_c^{DS} [nm]
GPON	1290	1480
XG-PON	1280	1575
NG-PON2	1524	1596
HS-PON	1310	1344

Table 5.1: Worst case classical carrier wavelengths in both directions, for each PON standard.

The total noise affecting the receiver is computed as the superposition of these bidirectional contributions. It is important to note that the simulation relies on realistic physical parameters; specifically, the Raman efficiency coefficients ($\beta_{US,DS}$) and the fiber attenuation profiles ($\alpha_{c,q}$) used in the following computations are derived from experimental characterizations [63].

Beyond the generic PON architectural constraints, the numerical simulations rely on a specific set of typical hardware and protocol parameters to accurately model the performance of the quantum transceivers. For the DV-QKD implementation, the receiver is characterized by an optical filter bandwidth of $\Delta\nu = 12.5$ GHz and a detector gate interval of $\Delta t = 1$ ns. The protocol dynamics are governed by an intrinsic optical misalignment error of $e_{mis} = 3.2 \cdot 10^{-3}$, corresponding to an equivalent extinction ratio of 25 dB. Furthermore, the Single-Photon Avalanche Diode (SPAD) is modeled with a quantum efficiency of $\eta_{DV} = 0.16$, an intrinsic dark count probability of $p_{dc} = 10^{-6}$ and an error correction inefficiency factor set to $f_e = 1.15$. Conversely, the CV-QKD configuration assumes a standard heterodyne detection scheme, with an optical filter bandwidth of $\Delta\nu = 1$ GHz and a detector gate interval of $\Delta t = 1$ ns. The physical receiver is defined by a overall quantum efficiency of $\eta_{CV} = 0.44$, an electronic noise variance of $V_{el} = 0.063$ in Shot Noise Units (SNU) and a specific detection excess noise of $\xi_{Bob} = 2 \cdot 10^{-4}$ SNU. On the protocol side, the information reconciliation phase operates with an efficiency of $\beta = 0.95$, while the Frame Error Rate (FER) is set to a value of 0.3.

In the simulations presented in this work, the SKR is systematically evaluated and normalized in terms of *bits/channel use*. This metric quantifies the fundamental cryptographic efficiency of the protocol, indicating the exact fraction that can be securely extracted for each single quantum state transmitted through the optical channel. The choice of this unit decouples the intrinsic performance of the protocol from the specific clock speed of the underlying hardware, allowing for a strictly theoretical comparison between CV and

DV technologies. However, to translate this efficiency metric into a practical key generation rate, measured in bits per second (bps), the SKR value must be multiplied by the repetition rate (ρ) of the system, which is the operational frequency of the transmitter. In a real-world implementation, it is precisely on this parameter that critical architectural differences emerge between the two paradigms. In DV-QKD systems, the maximum repetition rate is physically constrained by the characteristics of the optical receivers. The use of Single-Photon Avalanche Diodes (SPADs) imposes an intrinsic *dead time*, a mandatory recovery period to quench the electronic avalanche following a detection event. This hardware constraint typically limits the practical transmission frequency of commercial DV systems between 100 MHz and 1.25 GHz. While recent laboratory demonstrations have pushed DV-QKD clock rates up to the 5-10 GHz regime [75], achieving such speeds strictly requires the deployment of Superconducting Nanowire Single-Photon Detectors (SNSPDs) operating at cryogenic temperatures, which poses significant integration challenges for standard access networks. Conversely, CV-QKD systems employ standard coherent components derived from classical telecommunications (such as PIN photodiodes), which measure macroscopic electromagnetic fields and do not suffer from the physical limitations of dead time. This allows the optical counterpart of CV-QKD to easily operate at frequencies of tens of GHz [76]. However, the true bottleneck of CV-QKD shifts from the optical domain to the computational one: processing continuous, ultra-high-speed data streams requires extremely demanding Digital Signal Processing (DSP) and complex error correction algorithms. This massive optical bandwidth confirms the potential of CV-QKD to natively support the high-speed demands of next-generation optical infrastructures, provided that the computational bottlenecks of classical post-processing are adequately addressed.

Finally, it is important to recall that throughout the simulation campaign, the performance of both the CV and DV protocols will be strictly evaluated using the optimization procedures introduced in Chapter 3. This methodological approach ensures that the final comparative analysis is performed by assessing each technology under its respective optimal operating conditions, thereby maximizing the extractable SKR and guaranteeing a fair, rigorous and potential-to-potential evaluation.

5.2. Impact of Finite Block Length on Secret Key Rate Generation

Prior to addressing the spectral optimization of the quantum channel, it is mandatory to evaluate the influence of the finite block size, denoted as N, on the system's performance both in the DV- and CV-QKD scenarios. As the investigation of finite-size effects in PON architectures represents a novel contribution of this thesis, establishing the impact of the transmitted sequence length is a prerequisite for any further analysis. In practical CV-QKD implementations, the secret key rate is strictly dependent on the length of the transmitted symbol sequence utilized for parameter estimation. Unlike the asymptotic regime, where the statistical uncertainty vanishes, the finite-size regime introduces a penalty due to the worst-case estimation of channel parameters (transmittance T and excess noise ξ) required to guarantee security against coherent attacks. Similarly, in practical DV-QKD implementations employing the decoy-state method, the achievable SKR is fundamentally constrained by the total number of transmitted pulses N. The finite-size regime imposes a rigorous penalty to guarantee unconditional security against coherent and Photon-Number-Splitting (PNS) attacks. This penalty arises from the necessity to compute worst-case statistical limits; to manage these statistical uncertainties and properly characterize the channel, the protocol must carefully partition the finite block of signals: a dominant fraction is measured in the primary basis (the X basis) for raw key extraction, while the remaining signals, measured in the conjugate basis across varying decoy intensities, are sacrificed to estimate the channel parameters and tightly bound the phase error rate.

In this preliminary analysis, the total propagation distance L, defined as the sum of the feeder and distribution fiber lengths ($L = L_f + L_d$), is held constant to a value of $L = 5$ km ($L_f = 3$ km and $L_d = 2$ km). To ensure a rigorous evaluation under optimal operating conditions, the analysis was performed by first identifying the optimal quantum carrier wavelength that maximizes the SKR for each considered PON standard (GPON, XG-PON, NG-PON2, HS-PON) and for each user configuration (number of users), as reported in Table 5.2. This step ensures that the assessment of the block length impact is decoupled from spectral penalties associated with sub-optimal wavelength allocations. The system performance is subsequently plotted as a function of the number of transmitted symbols N, effectively illustrating the transition from the finite-size regime to the asymptotic saturation (Figures 5.2, 5.3, 5.4, 5.5).

	GPON		XG-PON		NG-PON2		HS-PON	
N_{users}	λ_{DV}^{opt}	λ_{CV}^{opt}	λ_{DV}^{opt}	λ_{CV}^{opt}	λ_{DV}^{opt}	λ_{CV}^{opt}	λ_{DV}^{opt}	λ_{CV}^{opt}
1	1260	1621	1464	1570	1322	1523	1672	1570
4	1260	1460	1458	1511	1321	1455	1681	1635
8	1260	1289	1456	1506	1321	1452	1686	1658
16	1260	1289	-	1505	1319	1444	1689	1664
32	1260	1289	-	-	1298	1323	1691	1669
64	1260	1289	-	-	1260	1322	1693	-

Table 5.2: DV and CV quantum wavelengths (in nm) corresponding to the maximum SKR for each PON standard, evaluated when the feeder segment is equal to 3 km, as a function of the number of users served.

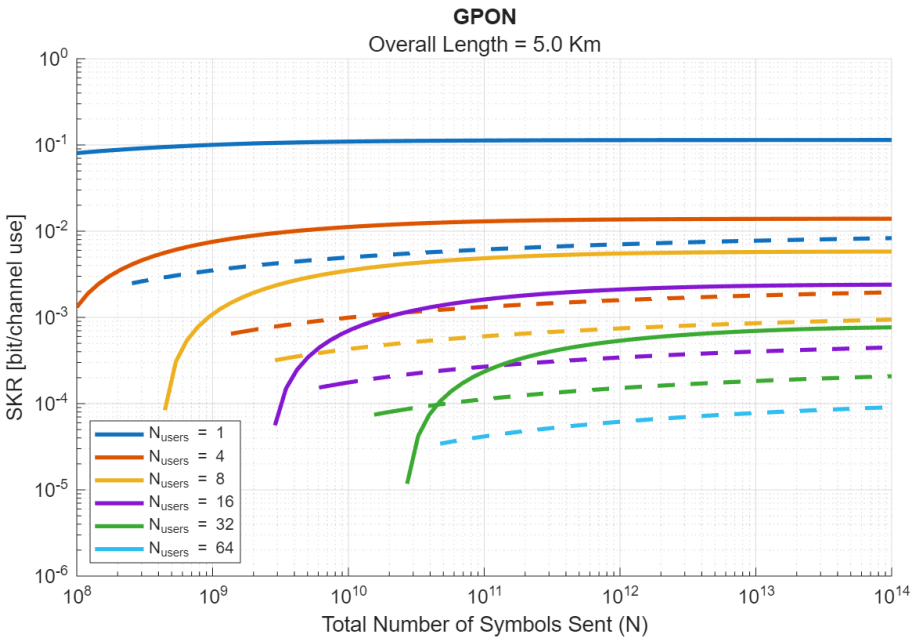


Figure 5.2: GPON DV (dashed lines) and CV (continuous lines) SKR as a function of the total number of transmitted symbols (N) and number of users, when the overall fiber length is fixed at 5 km.

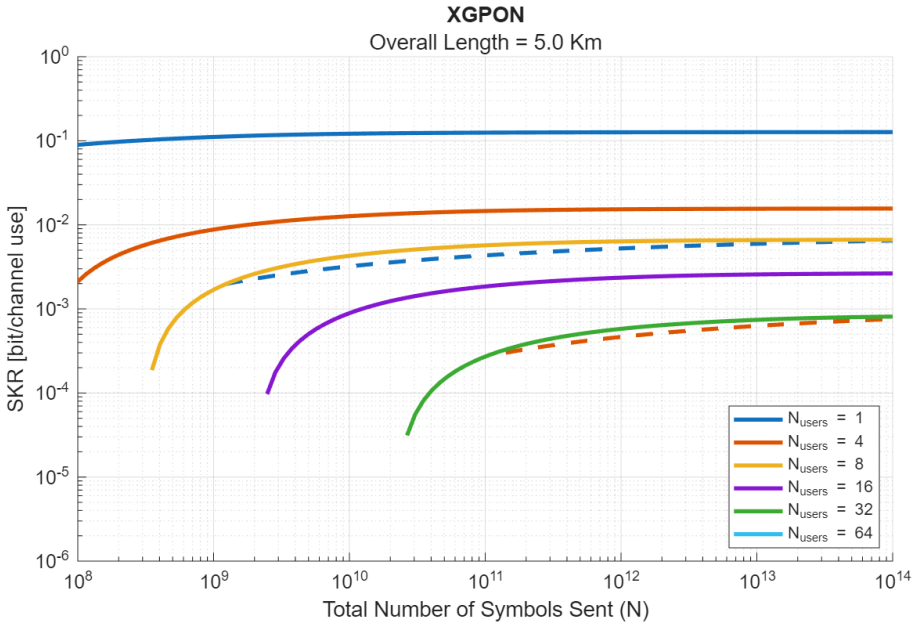


Figure 5.3: XG-PON DV (dashed lines) and CV (continuous lines) SKR as a function of the total number of transmitted symbols (N) and number of users, when the overall fiber length is fixed at 5 km.

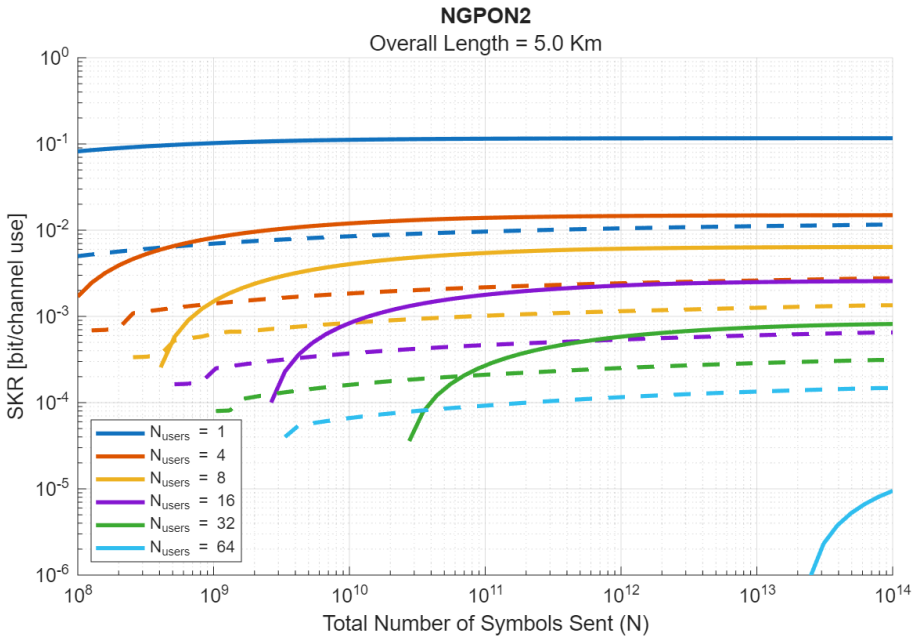


Figure 5.4: NG-PON2 DV (dashed lines) and CV (continuous lines) SKR as a function of the total number of transmitted symbols (N) and number of users, when the overall fiber length is fixed at 5 km.

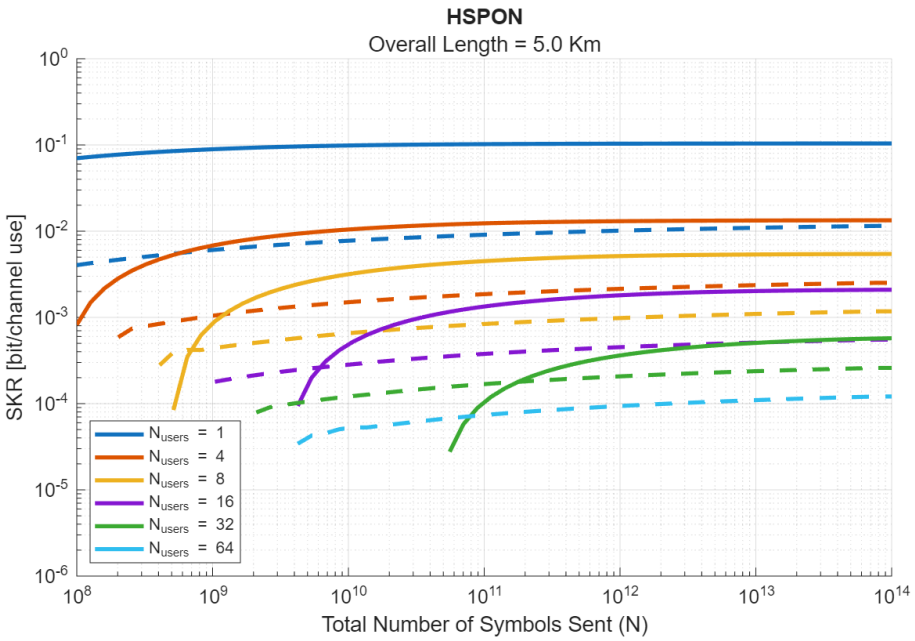


Figure 5.5: HS-PON DV (dashed lines) and CV (continuous lines) SKR as a function of the total number of transmitted symbols (N) and number of users, when the overall fiber length is fixed at 5 km.

Across all evaluated architectures and for both DV and CV protocols, a fundamental physical constraint consistently emerges: below a specific block size threshold, the parameter estimation uncertainties become too severe, forcing the extractable key rate to abruptly drop to zero. Furthermore, it is strictly observable that as the topological splitting ratio increases to serve a larger number of users (N_{users}), this critical "knee" progressively shifts towards higher values of N. This dynamic clearly demonstrates that the severe localized attenuation introduced by the passive optical splitters dramatically degrades the SNR, thereby requiring the accumulation of significantly larger data blocks to successfully distill a secure cryptographic key. Comparing the two QKD paradigms within this finite-key regime reveals distinct technological behaviors. With an equal number of transmitted symbols N, the CV-QKD protocol generally delivers superior performance, yielding higher maximum asymptotic key rates compared to its discrete counterpart, as long as the number of users in the network remains under 32. This advantage is primarily attributed to the inherent resilience of coherent detection against the broadband Spontaneous Raman Scattering (SpRS) noise generated by the coexisting classical channels. Conversely, while DV-QKD guarantees secure key exchanges, it suffers from strictly lower SKR upper bounds due to its heightened sensitivity to the Raman noise floor.

Despite these general trends, the finite-size analysis highlights varying degrees of infras-

tructural hostility among the different standards. While GPON, HS-PON and NG-PON2 architectures enable both protocols to sustain secure communications even in highly branched topologies, provided the block size N is sufficiently large, XG-PON stands out as an exceptionally challenging environment. Within the XG-PON coexistence scenario, the specific spectral allocation of the high-power classical bands introduces severe noise penalties that disproportionately impact the DV protocol. Consequently, the performance degradation in this standard is highly asymmetric. The sensitive DV-QKD approach experiences a premature collapse, as the finite-key constraints become a severe bottleneck, failing entirely to support optical distribution networks with more than 4 users. In stark contrast, these critical issues do not affect the continuous-variable approach. Thanks to its inherent resilience, CV-QKD avoids this drastic degradation, maintaining a level of performance and network scalability fully in line with its operation in the other evaluated PON standards. The drastic performance collapse of DV-QKD in the XG-PON scenario can be directly attributed to the fundamental vulnerability of its detection architecture when exposed to severe background noise. DV-QKD relies on direct detection via Single-Photon Detectors (SPDs). Because Spontaneous Raman Scattering (SpRS) generates a broadband noise spectrum, a significant number of Raman photons inevitably pass through the optical filters and reach the detectors. This high influx of noise photons generates false detection events, drastically elevating the Quantum Bit Error Rate (QBER) beyond the secure threshold and saturating the detectors due to their inherent dead time. Conversely, CV-QKD bypasses this vulnerability by employing coherent detection coupled with a Local Oscillator (LO). This detection scheme acts as a natural, ultra-narrowband temporal and spatial filter, which inherently rejects the vast majority of the broadband Raman noise, allowing the protocol to seamlessly sustain its optimal performance levels regardless of the harsh XG-PON spectral environment.

Analyzing the minimum block length N required to generate a positive SKR reveals a distinct trade-off across the standard PON architectures (excluding the pathological case of XG-PON). A clear regime shift is observed depending on the splitting ratio. In scenarios with a low number of users, CV-QKD demonstrates superior efficiency, exhibiting a lower *activation threshold* that allows it to extract secure keys with smaller data blocks compared to DV-QKD. However, as the network scales to 16 users and beyond, DV-QKD proves to be more robust against severe attenuation. Consequently, the discrete protocol maintains a manageable minimum N requirement, whereas CV-QKD demands significantly larger block sizes to overcome the statistical uncertainties associated with the degraded SNR, eventually failing to generate a key before DV does.

5.3. Quantum Channel Spectral Coexistence and Allocation

Having assessed the impact of the finite block length, the simulative analysis has focused on the spectral allocation of the quantum channel, to identify its optimal wavelengths to maximize the coexistence performance with respect to intense classical traffic presence. To determine the optimal placement, the quantum channel wavelength is swept across a broad spectral range, spanning from 1260 to 1700 nm. Based on the previously presented finite-size analysis, the total number of transmitted symbols is fixed at $N = 10^{10}$. This specific value is selected to represent a highly realistic and optimal operational trade-off. Considering a system repetition rate of 1 GHz—a clock speed that, as previously discussed, is nowadays technologically feasible for both CV and advanced DV architectures—this block size corresponds to an acquisition time of exactly 10 seconds. On one hand, gathering 10^{10} symbols provides a sufficiently large statistical sample to effectively mitigate the parameter estimation uncertainties intrinsic to the finite-key regime, thereby enabling a stable and improved SKR. On the other hand, a 10-second transmission window ensures that the protocol remains highly practical for real-world deployment, avoiding excessive latency and waiting times that would otherwise hinder the responsiveness of the cryptographic network. Moreover, the optical launch powers for both the upstream (US) and downstream (DS) data channels across all evaluated PON standards have been set to an intermediate value between their respective minimum and maximum limits dictated by the standard recommendations.

5.3.1. GPON Scenario

In the specific analysis of the GPON standard, the simulation exploits the physical layer parameters previously summarized in Table 5.1. The classical carrier wavelengths are centered at $\lambda_{c,US} = 1290$ nm and $\lambda_{c,DS} = 1480$ nm, with associated optical launch powers of $P_{in,US} = 5.18$ dBm and $P_{in,DS} = 5.45$ dBm, respectively. A critical constraint for the coexistence feasibility is the strict avoidance of the standardized classical bandwidths. Specifically, the quantum channel cannot be allocated within the upstream spectral window, which extends from 1290 nm to 1330 nm, nor within the downstream band, spanning from 1480 nm to 1500 nm, as reported in Table 2.2. These exclusion regions are enforced to prevent direct interference and ensure compliance with the ITU-T G.984 recommendations.

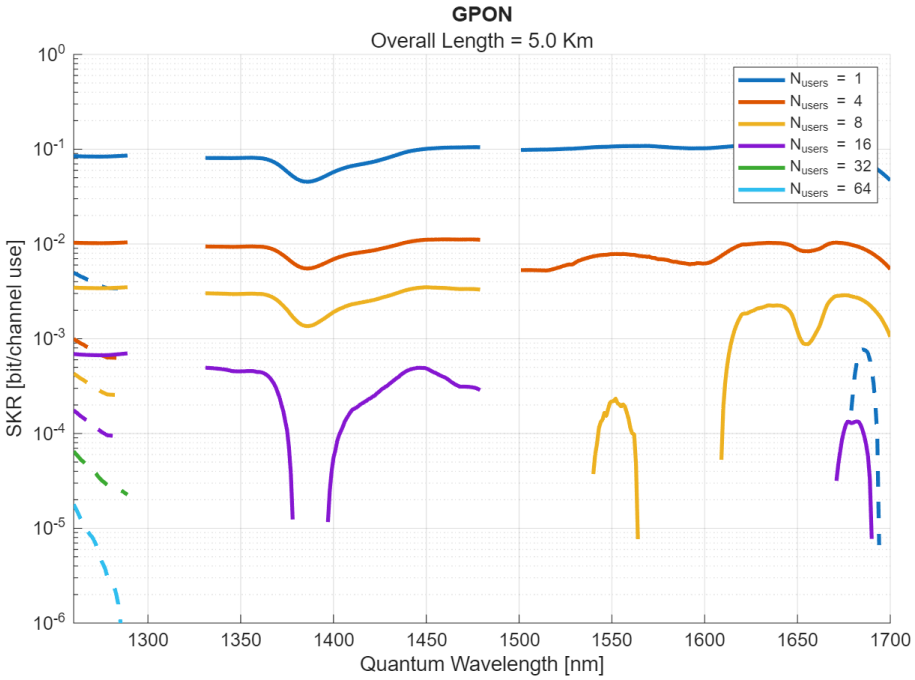


Figure 5.6: GPON DV (dashed lines) and CV (continuous lines) quantum bands allocation as a function of the number of users, when the overall fiber length is fixed at 5 km and $N = 10^{10}$.

Figure 5.6 presents the SKR in function of the optical wavelength of the quantum channel, expressed in nanometers (nm), for several splitting ratio conditions. The curves are obtained by fixing the operation conditions, i.e. maintaining constant the overall fiber length to a value of 5 km and the initial input non-optimized parameters, while systematically varying the number of connected users (the PON splitting ratio). DV-QKD exhibits remarkable resilience to passive splitting losses within the GPON standard. The discrete protocol successfully maintains a strictly positive SKR even when scaling up to fully loaded optical distribution networks with 64 users. To achieve this extensive coverage, its feasible spectral allocation is strictly confined to the shorter wavelength region (below 1290 nm), strategically avoiding the classical data bands and mitigating the impact of Spontaneous Raman Scattering. Instead, CV-QKD consistently delivers significantly higher peak SKR values in low-splitting regimes, outperforming the discrete alternative for up to 16 users across a broad spectral range. However, it fails entirely to generate a key for 32 and 64 users due to the severe insertion losses. This confirms that while CV-QKD is optimal for maximizing throughput in lightly shared links, DV-QKD remains the essential technology for guaranteeing extensive coverage in densely populated GPON deployments.

The two QKD solutions can be compared also in terms of maximum achievable SKR. As shown in Figure 5.7, while DV-QKD demonstrates superior scalability by supporting a higher user count, CV-QKD delivers significantly higher peak SKR values within the regime where splitter attenuation is not prohibitive.

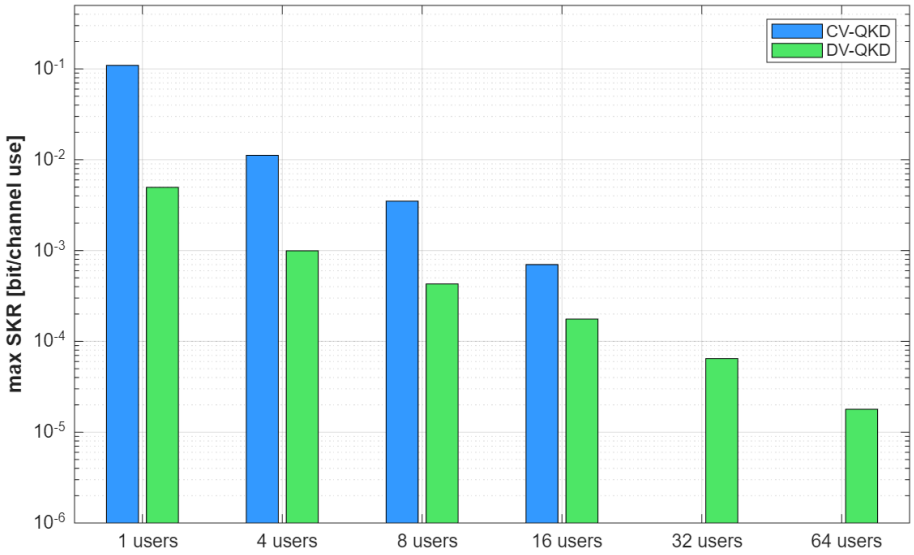


Figure 5.7: GPON DV and CV maximum SKR comparison, as function of the number of users, when the overall fiber length is equal to 5 km.

5.3.2. XG-PON Scenario

The same analysis can be performed for the XG-PON standard. Following the specifications outlined in Table 5.1, the simulation adopts reference classical carrier wavelengths of $\lambda_{c,US} = 1280$ nm for the upstream link and $\lambda_{c,DS} = 1575$ nm for the downstream link. The corresponding optical launch powers are set to $P_{in,US} = 5.18$ dBm and $P_{in,DS} = 4.45$ dBm, respectively. regarding spectral allocation, strict exclusion zones are enforced to avoid interference with the standardized data channels. As anticipated in Table 2.3, the reserved upstream bandwidth spans from 1260 nm to 1280 nm, while the downstream allocation occupies the spectral region between 1575 nm and 1580 nm.

The spectral performance analysis of the XG-PON architecture reveals a particularly hostile environment for quantum coexistence, markedly inferior to the legacy GPON standard. The results highlight a severe bifurcation in protocol performance driven by the intense broadband Raman noise characteristic of this standard. As illustrated in Figure 5.8, DV-QKD exhibits a drastic performance collapse, resulting fragile in this scenario, failing to establish a secure link for network splits exceeding 4 users. The feasible spectral windows for DV-QKD are extremely fragmented and narrow, vanishing entirely under

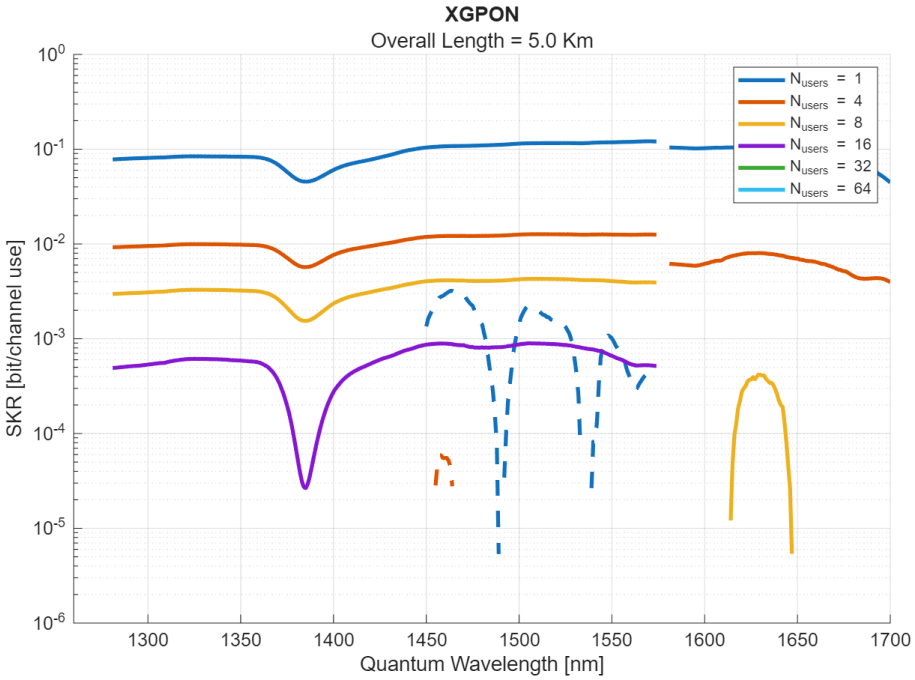


Figure 5.8: XG-PON DV (dashed lines) and CV (continuous lines) quantum bands allocation as a function of the number of users, when the overall fiber length is fixed at 5 km and $N = 10^{10}$.

higher splitting losses due to the saturation of single-photon detectors by the XG-PON background noise. Conversely, CV-QKD maintains acceptable Secret Key Rates and supports a splitting ratio of up to 16, significantly outperforming its discrete counterpart. However, the overall performance in the XG-PON architecture is notably degraded compared to the GPON scenario. The combination of higher insertion losses and the specific spectral placement of XG-PON channels imposes a tighter operational limit, preventing the CV protocol from reaching the high-capacity targets (32 or 64 users) achievable in other PON standards.

Interestingly, literature works such as [77] show that in a purely asymptotic regime, DV-QKD can tolerate the XG-PON noise floor up to approximately 5.5 km. The premature failure observed in this finite-size analysis highlights that the true limiting factor is the parameter estimation process. The high influx of Raman noise photons dramatically amplifies the statistical uncertainties inherent to finite blocks, imposing a rigorous penalty that drives the secure key generation to zero well before the physical reach limit is met.

The evaluation of the maximum achievable SKR confirms the overwhelming dominance of CV-QKD in this high-noise environment. As depicted in Figure 5.9, the CV protocol consistently yields key rates orders of magnitude higher than DV-QKD, effectively sup-

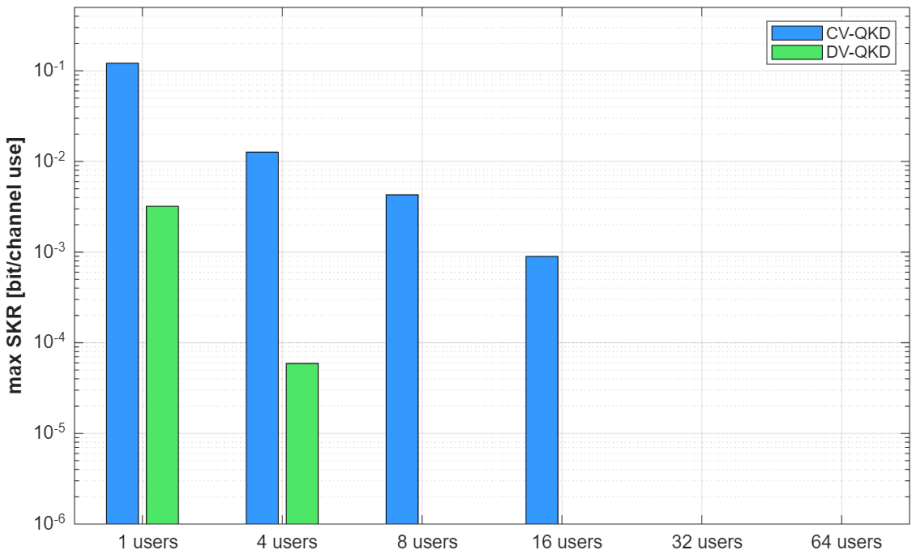


Figure 5.9: XG-PON DV and CV maximum SKR comparison, as function of the number of users, when the overall fiber length is equal to 5 km.

porting up to 16 users. It is important to underline that the analyzed US and DS launch powers don't permit any quantum exchange in case of 32 and 64 users.

5.3.3. NG-PON2 Scenario

The Next-Generation Passive Optical Network 2 (NG-PON2) represents a multi-wavelength standard leveraging Time and Wavelength Division Multiplexing (TWDM). As detailed in Table 2.4, the classical spectral bands are allocated from 1524 nm to 1544 nm for the upstream and from 1596 nm to 1603 nm for the downstream. For the purpose of Raman noise computation, the reference wavelengths are fixed at the lower edges of these bands, specifically $\lambda_{c,US} = 1524$ nm and $\lambda_{c,DS} = 1596$ nm (see Table 5.1). The associated optical input powers are $P_{in,US} = 7.18$ dBm and $P_{in,DS} = 5.45$ dBm per channel. It is important to note that this specific analysis assumes a configuration comprising a single active channel in the upstream direction and four active channels in the downstream direction.

The spectral performance analysis of the NG-PON2 architecture reveals a highly favorable environment for the discrete-variable approach. The results, illustrated in Figure 5.10, highlight a remarkable robustness of DV-QKD when coexisting with the high-power TWDM classical channels characteristic of this standard. DV-QKD exhibits exceptional scalability and resilience in this scenario, maintaining a strictly positive SKR across a broad operational spectral window at shorter wavelengths. Notably, it is capable of establishing a secure link even under severe passive splitting losses, effectively supporting fully loaded optical distribution networks with up to 64 users. Conversely, while CV-QKD

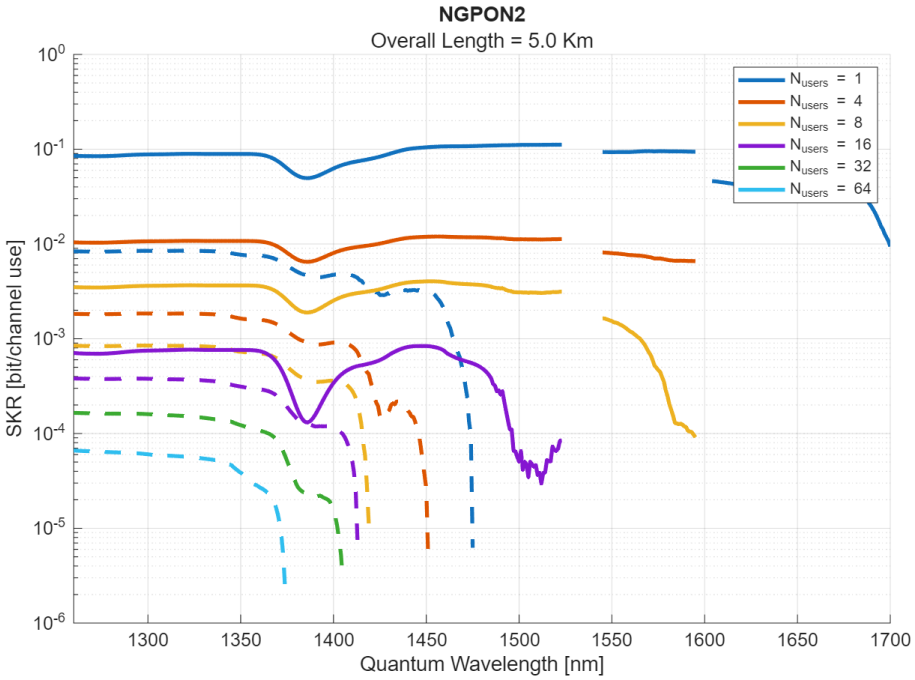


Figure 5.10: NG-PON2 DV (dashed lines) and CV (continuous lines) quantum bands allocation as a function of the number of users, when the overall fiber length is fixed at 5 km and $N = 10^{10}$.

consistently delivers significantly higher peak SKR in low-splitting regimes, it suffers from a steeper performance decay as the network branches out. The continuous protocol fails to sustain secure communications for 32 and 64 users at this 5 km distance, capping its viability at a 16-user split.

Mirroring the trends observed in the GPON architecture, the evaluation of the maximum achievable SKR in NG-PON2 (Figure 5.11) confirms that while CV-QKD delivers superior peak rates at lower splitting ratios (up to 16 users), DV-QKD exhibits unparalleled scalability, emerging as the sole protocol capable of sustaining a secure key exchange for 32 and 64 users.

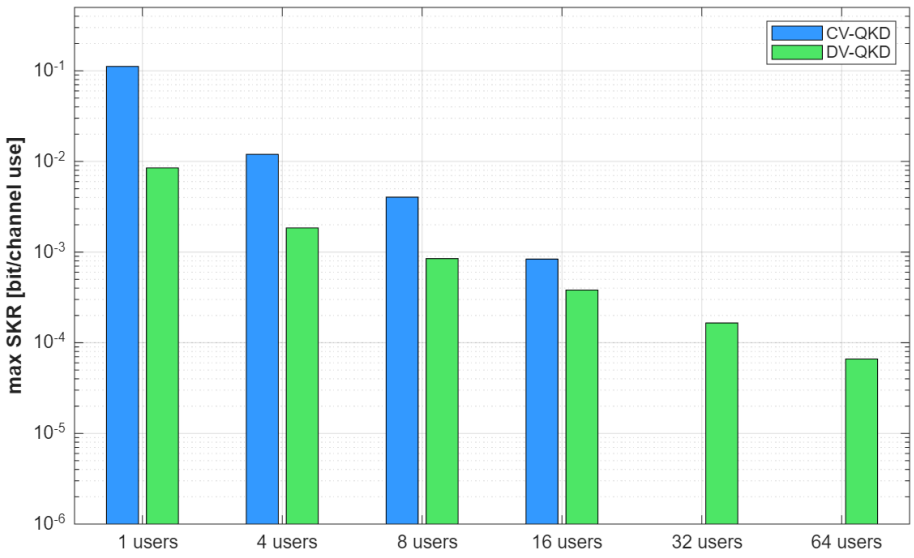


Figure 5.11: NG-PON2 DV and CV maximum SKR comparison, as function of the number of users, when the overall fiber length is equal to 5 km.

5.3.4. HS-PON Scenario

Finally, the study addresses the High-Speed Passive Optical Network (HS-PON) standard. As summarized in Table 5.1, the operational wavelengths are centered at $\lambda_{c,US} = 1310$ nm for the upstream and $\lambda_{c,DS} = 1344$ nm for the downstream. This standard is characterized by higher optical power levels, with input powers defined as $P_{in,US} = 7.18$ dBm and $P_{in,DS} = 9.07$ dBm, respectively. Regarding the spectral occupation, Table 2.5 indicates that the upstream band definition varies depending on coexistence requirements with legacy systems. The simulation considers a standalone scenario where the upstream band ranges from 1290 nm to 1310 nm, while the downstream band is defined between 1340 nm and 1344 nm.

Observing Figure 5.12, it is evident that the behavior of this standard aligns consistently with the previously analyzed PON architectures. Specifically, the CV-QKD protocol maintains a secure operational regime up to a split ratio of 16 users ($N_{users} \leq 16$), consistently guaranteeing a broader available quantum bandwidth compared to its discrete counterpart. However, for higher split ratios where the localized attenuation becomes too severe, the DV-QKD approach emerges as the only viable technological solution capable of sustaining a positive key rate. Furthermore, regarding the spectral allocation, the dedicated DV quantum band is strictly confined to the Stokes region of both the US and DS classical channels. This positioning is fundamentally dictated by the lack of available, unallocated spectral windows on the anti-Stokes side. Consequently, to effectively mitigate

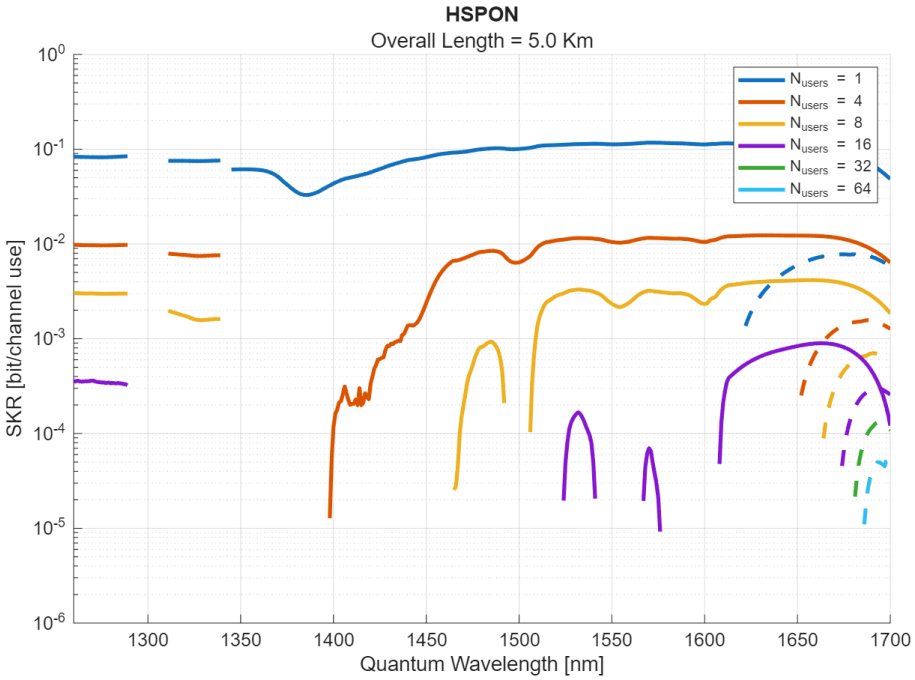


Figure 5.12: HS-PON DV (dashed lines) and CV (continuous lines) quantum bands allocation as a function of the number of users, when the overall fiber length is fixed at 5 km and $N = 10^{10}$.

the severe physical impairments induced by Spontaneous Raman Scattering (SpRS), the quantum channel is deliberately allocated at the maximum possible spectral distance from the high-power classical bands.

Finally, the maximum achievable SKR for both technologies for the HS-PON is reported in Figure 5.13. As in all previous cases, when CV is able to work, its maximum SKR is higher than DV.

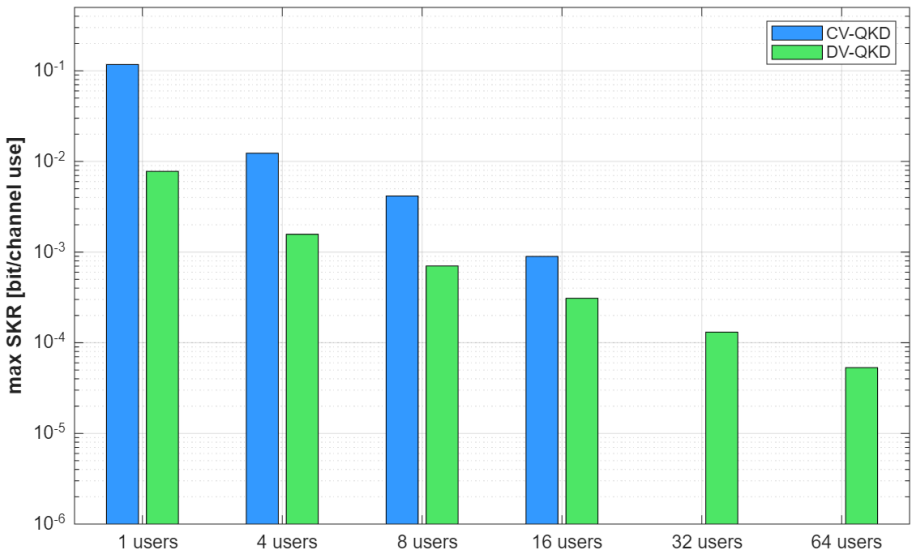
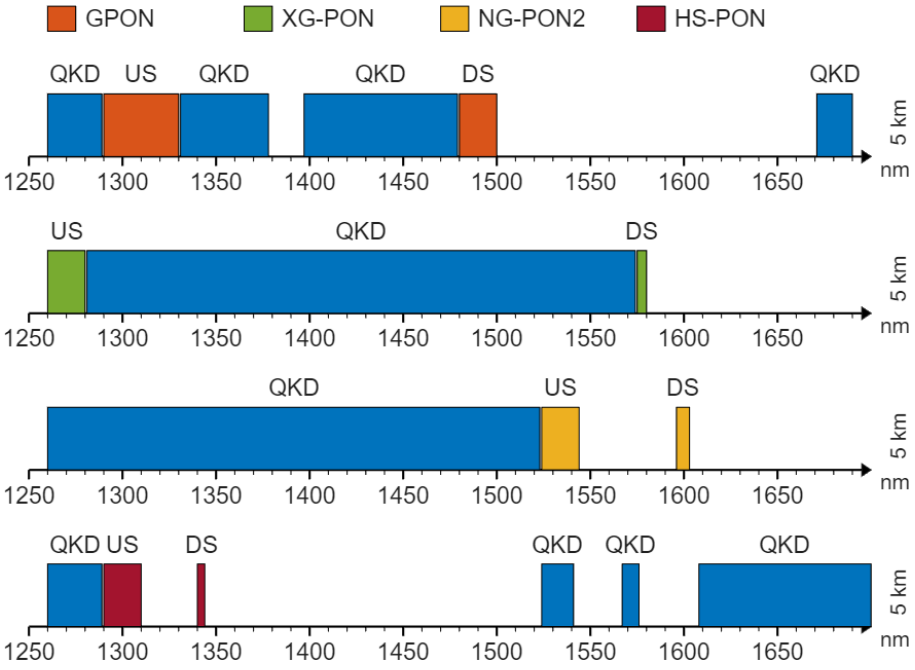
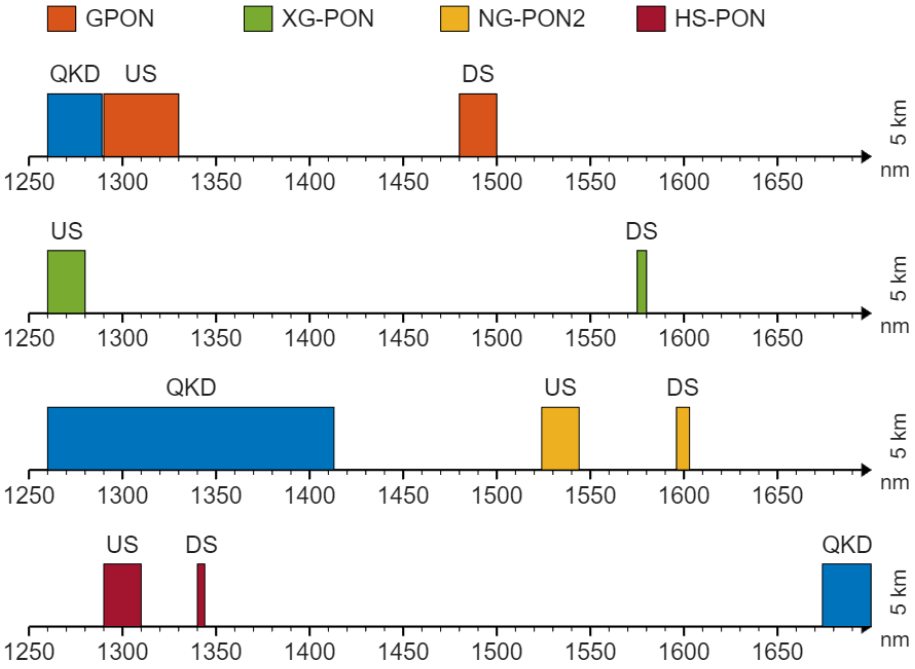


Figure 5.13: HS-PON DV and CV maximum SKR comparison, as function of the number of users, when the overall fiber length is equal to 5 km.

To synthesize the spectral coexistence findings and provide a comprehensive overview, Figure 5.14 illustrates a direct comparison of the available quantum bandwidths across all four evaluated PON standards, specifically focusing on a representative network split of 16 users ($N_{users} = 16$). These visual summaries clearly highlight the fundamental disparities in spectral resilience and flexibility between the two protocols. As depicted in Figure 5.14a, CV-QKD demonstrates remarkable spectral adaptability, maintaining broad and often contiguous operational windows across XG-PON and NG-PON2, with only minor fragmentation in HS-PON and GPON architectures. In stark contrast, the DV-QKD comparison (Figure 5.14b) provides clear visual confirmation of the severe constraints imposed on the discrete protocol. Its feasible quantum bands are strictly confined to much narrower spectral regions. Most notably, this comparison perfectly captures the complete performance collapse of DV-QKD in the XG-PON architecture, where the intense background noise completely annihilates the available quantum bandwidth for a 16-user split, rendering the technology unfeasible in that specific standard.
Furthermore, it is crucial to emphasize that this 16-user scenario represents the ultimate threshold for a direct protocol comparison. Expanding the network split to 32 users causes the CV-QKD operational windows to vanish entirely across all evaluated standards due to the prohibitive insertion losses. Consequently, a side-by-side spectral comparison would be impractical, as DV-QKD emerges as the sole viable technology capable of sustaining a secure link at a 5 km transmission distance under such highly branched topologies.



(a) CV-QKD



(b) DV-QKD

Figure 5.14: A comprehensive comparison of the feasible quantum spectral allocation for (a) CV-QKD and (b) DV-QKD across the four evaluated PON standards for a fixed splitting ratio of 16 users and a transmission distance of 5 km. The classical US and DS bands are reported for context.

5.4. Impact of Distance on Secret Key Rate Generation

Having established the optimal spectral allocation that minimizes the Raman noise impact for each PON standard, the analysis now proceeds to evaluate the system's performance in terms of achievable reach. The transmission distance L represents a very critical constraint in optical access networks, as it directly dictates the channel transmittance T and consequently the SNR available at the receiver. In this section, the SKR is evaluated against the total fiber length, sweeping the distance from 2 to 20 km to determine the maximum secure reach. Specifically, this total distance extension is achieved by incrementally varying the feeder fiber length (L_f), while maintaining a fixed 2 km drop fiber (L_d) to simulate a realistic distribution network. To ensure a consistent *best-case* evaluation, the quantum and classical carrier wavelengths are fixed to the optimal values (λ_{opt}) identified in Table 5.2.

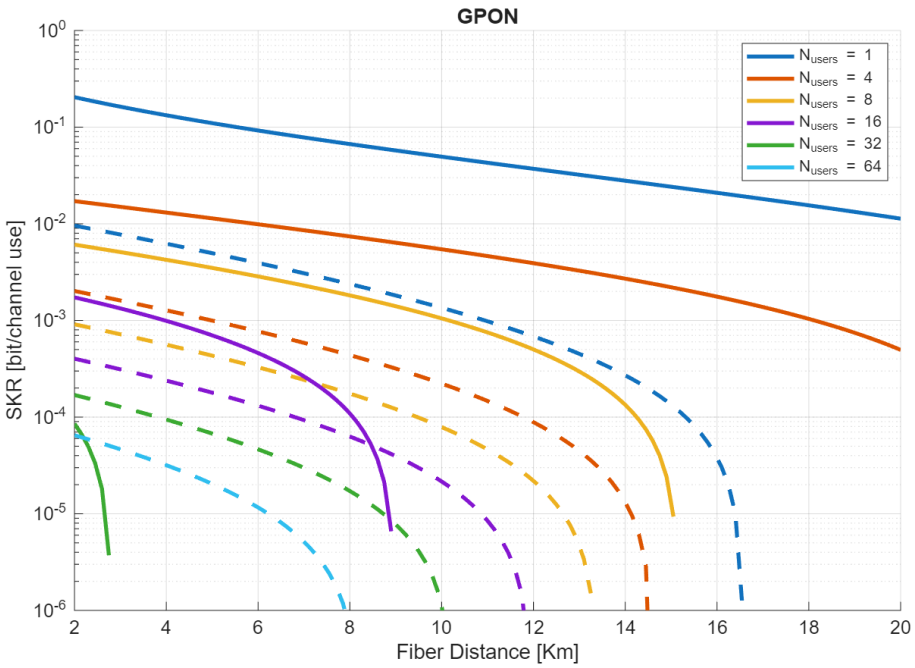


Figure 5.15: GPON DV (dashed line) and CV (continuous line) SKR versus distance, as a function of the number of users served.

The evaluation of the GPON architecture (Figure 5.15) reveals a performance strictly dependent on the network split ratio. In the low-splitting regime, the CV protocol demonstrates superior reach capabilities, successfully exceeding a transmission distance of 20 km. In this specific configuration, the DV alternative is outperformed, reaching a saturation

point where the secure link is physically limited to approximately 17 km. However, as the number of users increases, the scenario changes drastically due to the dominant impact of passive splitting losses. CV-QKD, being highly sensitive to channel attenuation, suffers a rapid degradation in performance: while it maintains a viable link up to roughly 15 km with 8 users, its reach collapses to just 3 km when the network is loaded with 32 users, as the signal-to-noise ratio drops below the coherent reconciliation threshold. Conversely, DV-QKD proves to be the far more resilient solution for high-capacity networks. Thanks to its robustness against attenuation, it successfully maintains a secure key exchange up to 10 km with 32 connected users and sustains operations up to approximately 8 km even in a fully loaded scenario with 64 users. Consequently, while CV-QKD is optimal for dedicated or lightly shared GPON links, DV-QKD is the requisite choice for ensuring coverage in densely populated optical distribution networks.

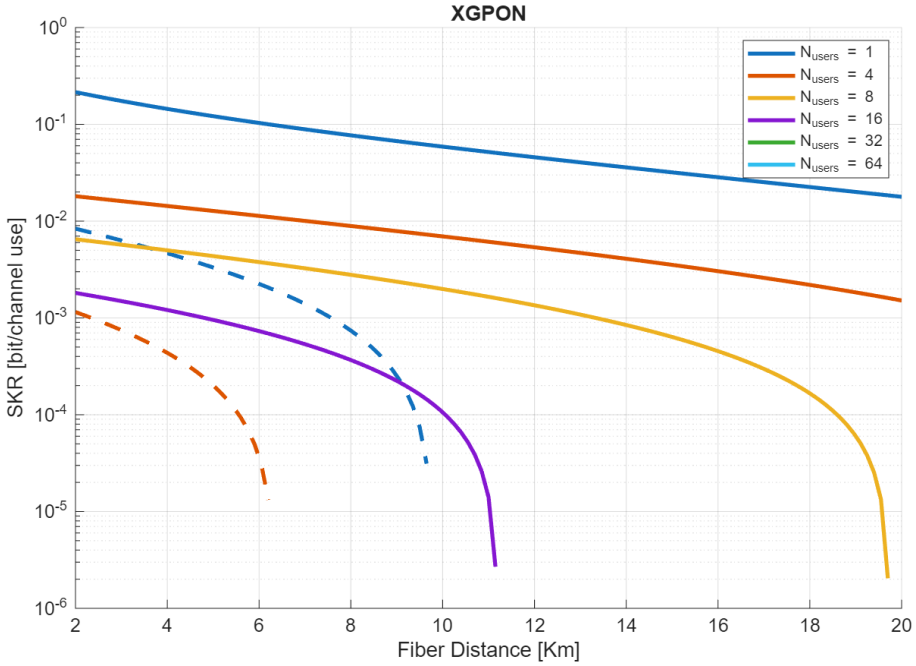


Figure 5.16: XG-PON DV (dashed line) and CV (continuous line) SKR versus distance, as a function of the number of users served.

The XG-PON architecture (Figure 5.16) represents a unique anomaly in the proposed analysis, specifically inverting the performance trends observed in the other standards. Due to the exceptionally high intensity of Spontaneous Raman Scattering (SpRS) generated by the classical channels, the Discrete-Variable protocol suffers a catastrophic performance degradation. Contrary to its behavior in other setups, DV-QKD fails to guarantee long-reach connectivity: even with low split ratios, the pervasive broadband noise saturates the single-photon detectors, preventing the establishment of a secure link beyond

short metro ranges. Conversely, the CV protocol demonstrates remarkable resilience in this hostile environment, outperforming its discrete counterpart. Thanks to the coherent detection scheme, which effectively filters out the incoherent Raman noise, CV-QKD achieves unexpected coverage. The simulation results indicate that with 8 users, the system maintains a secure key exchange up to nearly 19.5 km. Furthermore, even with a 1:16 splitting ratio, CV-QKD remains operational up to 11 km, proving to be the more robust solution for the specific noise regime of XG-PON.

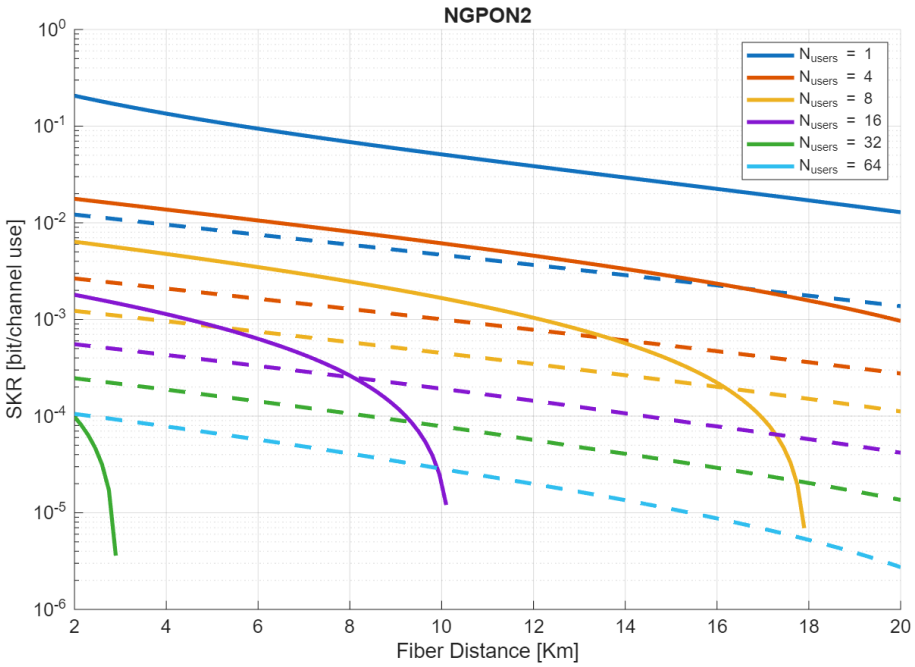


Figure 5.17: NG-PON2 DV (dashed line) and CV (continuous line) SKR versus distance, as a function of the number of users served.

The NG-PON2 standard highlights the most promising performance for the discrete approach, as reported in Figure 5.17. In this configuration, DV-QKD is remarkably robust, being able to serve up to 64 users for the entire 20 km span. This makes it a highly suitable candidate for extended optical distribution networks. In contrast, the CV-QKD performance exhibits a steeper decay. With 8 users, the maximum achieved distance is 18 km, but as the split ratio increases to 16 users, the reach decreases to 10 km and with 32 users it is strictly limited to roughly 3 km. Consequently, while CV offers high rates for short, point-to-point-like links, it cannot support the extensive branching typical of NG-PON2 without intermediate amplification.

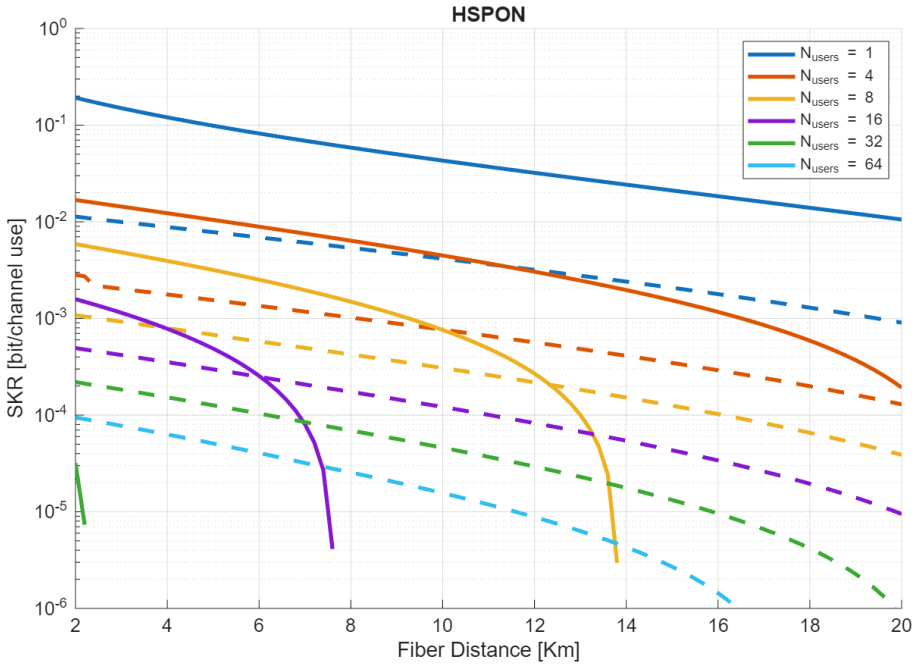


Figure 5.18: HS-PON DV (dashed line) and CV (continuous line) SKR versus distance, as a function of the number of users served.

Finally, in the HS-PON infrastructure (Figure 5.18) the scenario is very similar to the NG-PON2 one, with a little degradation in performance for both protocols. DV-QKD again demonstrates superior coverage, effectively serving 32 users up to 20 km and maintaining a secure key exchange for 64 users up to 16 km. CV-QKD is once more constrained by the passive splitting ratios. Specifically, with 8 users the maximum reachable distance is approximately 14 km, which reduces to 8 km when 16 users are connected. For a fully loaded network of 32 users, the coherent protocol drops abruptly at just 2 km.

In summary, the analysis demonstrates that neither protocol is universally superior: the optimal technological choice is strictly dictated by the network's topological and spectral characteristics. CV-QKD emerges as the best option in scenarios with a low user count and in environments dominated by extreme background noise (such as the XG-PON standard). In these hostile conditions, its coherent detection acts as a natural filter against Raman scattering, allowing the system to maintain secure operations where single-photon detectors would saturate, while also delivering higher peak SKRs with smaller initial data blocks. In contrast, DV-QKD proves to be the ideal and most scalable solution for highly branched optical networks (16 users and beyond) within standards featuring a more manageable spectral noise floor (such as GPON, NG-PON2 and HS-PON). In these scenarios, its exceptional resilience to the severe localized attenuation introduced

by optical splitters enables it to maintain secure communications and serve a significantly larger number of users compared to its continuous counterpart.

6 | Conclusions and Future Developments

This thesis has presented a comprehensive theoretical and simulative investigation on the feasibility of integrating Quantum Key Distribution within Passive Optical Networks. The primary objective was to evaluate the coexistence of quantum channels alongside classical data streams, going beyond idealized asymptotic assumptions to rigorously account for finite-size statistical effects and the severe physical impairments introduced by Spontaneous Raman Scattering and passive optical splitters. The comparative analysis between DV- and CV-QKD protocols revealed a distinct technological dichotomy, demonstrating that there is no universal solution for quantum access networks. Instead, protocol performance is fundamentally dictated by the specific spectral wavelength plan and topological splitting ratio of the underlying standard.

A primary finding of this work is the critical bottleneck imposed by the finite block size N. The analysis confirmed that below a specific threshold of transmitted symbols, the parameter estimation uncertainties become too severe, forcing the SKR to drop abruptly to zero. As the splitting ratio increases to serve more users, this critical threshold shifts to significantly higher values of N, emphasizing the impact of localized attenuation on the quantum SNR. Furthermore, the comparative finite-size analysis revealed that in scenarios with a limited number of users, CV-QKD requires a smaller minimum block size N_{min} to initiate secure key generation. While this offers a distinct advantage in accumulation time for small-scale topologies, this benefit is quickly neutralized as the splitting ratio increases, heavily penalizing the continuous-variable approach.

The spectral allocation analysis, conducted at a fixed transmission distance of 5 km, reveals a clear technological dichotomy driven by the interplay between network splitting ratios and standard-specific Raman noise profiles. Across environments with manageable noise floors, specifically GPON, NG-PON2 and HS-PON, a consistent performance trade-off emerges. In lightly branched networks, CV-QKD maximizes the SKR and provides a broader available quantum bandwidth, effectively supporting up to 16 users before completely failing under the severe insertion losses of highly split topologies. Conversely,

DV-QKD demonstrates unparalleled scalability, emerging as the sole viable technology capable of supporting densely populated distribution networks with up to 64 users. To ensure this survival, the discrete protocol requires rigorous spectral engineering, strategically allocating the quantum channel at the maximum possible spectral distance from the high-power classical bands. This translates to exploiting the shorter wavelength anti-Stokes region in GPON and NG-PON2, while strictly utilizing the longer wavelength Stokes region in HS-PON due to the lack of available unallocated spectrum. A critical exception to this trend is observed in the XG-PON architecture, which provides an exceptionally hostile environment due to its intense broadband Raman noise. In this challenging scenario, the typical protocol scalability is entirely inverted. DV-QKD suffers a premature performance collapse, with its feasible spectral windows vanishing beyond a mere 4-user split due to severe single-photon detector saturation. In stark contrast, CV-QKD leverages its coherent detection scheme to effectively filter the overwhelming background noise, significantly outperforming its discrete counterpart and successfully maintaining a secure quantum link for up to 16 users.

When evaluating the maximum achievable reach and user capacity, the two protocols exhibited complementary strengths: DV-QKD proved to be exceptionally robust against high insertion losses, making it the optimal candidate for densely branched architectures. In standards with manageable noise floors (GPON, NG-PON2 and HS-PON) the discrete approach successfully sustained secure key exchanges for 32 users, reaching distances around 20 km. To survive, its spectral allocation must be strictly positioned at the maximum possible spectral distance from the high-power classical bands, exploiting either the Stokes or anti-Stokes regions depending on the specific standard. CV-QKD showcased remarkable resilience against background noise, primarily due to the intrinsic filtering capabilities of its coherent detection scheme. This advantage became distinctly apparent in the XG-PON standard, an exceptionally hostile environment characterized by a problematic spectral allocation that completely saturates DV-QKD single-photon detectors beyond a 4-user configuration. In this challenging scenario, CV-QKD maintained similar key rates to the ones achieved in other standards and supported up to 16 users, reaching over 20 km in less congested architectures. However, in low-noise and high-loss scenarios (like fully loaded NG-PON2 or HS-PON), the CV protocol's reach decays rapidly, limiting its applicability in highly branched topologies without intermediate amplification.

Ultimately, this work demonstrates that *quantum-to-the-home* connectivity is physically achievable. However, realizing its full potential requires rigorous spectral engineering and standard-specific protocol selection. As the quantum computing era introduces new vulnerabilities, optical networks must be proactively designed to accommodate these quantum channels, cementing QKD as an indispensable pillar of future telecommunications

and guaranteeing absolute security against tomorrow's computational threats.

Building upon the findings of this work, several scenarios for future research emerge, particularly regarding the methodology of the finite-key analysis. In this thesis, the comparative performance between DV- and CV-QKD protocols was evaluated under the assumption of an equal number of transmitted quantum states, fixing the block length N at the transmitter side. While this approach provides a fair baseline for evaluating the hardware generation rate at the source, it does not fully capture the asymmetric impact of severe channel losses on the two different technologies. A further step would be to reformulate the finite-size comparison by normalizing the block size based on the number of successfully received states. Conducting the finite-key analysis with an equal number of received states could unveil entirely new operational trade-offs, providing a more comprehensive perspective on which protocol is truly optimal for highly branched access networks from a latency and data-processing standpoint.

Bibliography

[1] Dennis Luciano and Gordon Prichett. Cryptology: From caesar ciphers to public-key cryptosystems. *The College Mathematics Journal*, 18(1):2–17, 1987.

[2] Giacomo Verticale. Security and cryptography. Lecture slides, Politecnico di Milano, 2025.

[3] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[4] John D. Dixon. Factorization and primality tests. *The American Mathematical Monthly*, 91(6):333–352, 1984.

[5] 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.

[6] Sina Jafarpour. Introduction to the world of quantum computers. In *2006 5th IEEE International Conference on Cognitive Informatics*, volume 2, pages 760–764, 2006.

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

[8] Daniel J Bernstein. Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1846–1847. Springer, 2025.

[9] Xuyang Wang, Siyou Guo, Pu Wang, Wenyuan Liu, and Yongmin Li. Realistic rate-distance limit of continuous-variable quantum key distribution. *Opt. Express*, 27(9):13372–13386, Apr 2019.

[10] Alexander Grebenchukov, Hui Lui, Gleb Nazarikov, Bruno Cimoli, Simon Rommel, and Idelfonso Tafur Monroy. Prospects of chip-based multi-protocol quantum key distribution transceivers. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, pages 1–4. IEEE, 2023.

[11] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[12] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[13] Yang Liu, Wei-Jun Zhang, Cong Jiang, Jiu-Peng Chen, Chi Zhang, Wen-Xin Pan, Di Ma, Hao Dong, Jia-Min Xiong, Cheng-Jun Zhang, Hao Li, Rui-Chun Wang, Jun Wu, Teng-Yun Chen, Lixing You, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.*, 130:210801, May 2023.

[14] M. Pittaluga, Y. S. Lo, A. Brzosko, et al. Long-distance coherent quantum communications in deployed telecom networks. *Nature*, 640:911–917, apr 2025.

[15] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014.

[16] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, July 2000.

[17] Matthias Christandl, Renato Renner, and Artur Ekert. A generic security proof for quantum key distribution, 2004.

[18] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5), April 2000.

[19] Xiang-Bin Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A*, 72:012322, Jul 2005.

[20] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5), August 2003.

[21] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[22] H.-K. Lo. Quantum key distribution with decoy states. In *Proceedings. International Symposium on Information Theory, 2004. ISIT 2004*, page 17. IEEE, June 2004.

[23] Heng Wang, Yang Li, Ting Ye, Li Ma, Yan Pan, Mingze Wu, Junhui Li, Yiming Bian, Yaodi Pi, Yun Shao, Jie Yang, Jinlu Liu, Ao Sun, Wei Huang, Stefano Pirandola, Yichen Zhang, and Bingjie Xu. High-rate continuous-variable quantum key distribution over 100 km fiber with composable security, 2025.

[24] Adnan Hajomer, Ivan Derkach, Vladyslav Usenko, Ulrik Andersen, and Tobias Gehring. Coexistence of continuous-variable quantum key distribution and classical data over 120-km fiber, 02 2025.

[25] Yoann Piétri, Luis Vidarte, Matteo Schiavon, Philippe Grangier, Amine Rhouni, and Eleni Diamanti. Cv-qkd receiver platform based on a silicon photonic integrated circuit. pages 1–3, 03 2023.

[26] 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).

[27] João C. dos Reis Frazão. *Practical Implementation of Continuous Variable Quantum Key Distribution in Coexistence with Classical Signals*. PhD thesis, Eindhoven University of Technology, 2025.

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

[29] Xiangyu Wang, Yichen Zhang, Song Yu, and Hong Guo. High speed error correction for continuous-variable quantum key distribution with multi-edge type ldpc code. *Scientific Reports*, 8(1), July 2018.

[30] Renato Renner. Security of quantum key distribution, 2006.

[31] M. Ben-Or, Michal Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution, 2004.

[32] Renato Renner and Robert Koenig. Universally composable privacy amplification against quantum adversaries, 2004.

[33] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[34] Alexander S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. 1973.

[35] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, January 2005.

[36] Josep Segarra, Vicent Sales, and Josep Prat. Olt design approach for resilient extended pon with obs dynamic bandwidth allocation sharing the olt optical resources.

In *2008 10th Anniversary International Conference on Transparent Optical Networks*, volume 4, pages 139–144, 2008.

[37] Yundi Huang, Tao Shen, Xiangyu Wang, Ziyang Chen, Bingjie Xu, Song Yu, and Hong Guo. Realizing a downstream-access network using continuous-variable quantum key distribution. *Phys. Rev. Appl.*, 16:064051, Dec 2021.

[38] Nokia. Q2 optical access networks - work program review. Contribution Q2/15, ITU-T, 2020.

[39] ITU-T. Gigabit-capable passive optical networks (GPON): General characteristics. Recommendation ITU-T G.984.1, March 2008. Geneva.

[40] ITU-T. Gigabit-capable passive optical networks (GPON): Physical media dependent (PMD) layer specification. Recommendation ITU-T G.984.2, 2019.

[41] ITU-T. Gigabit-capable passive optical networks (GPON): Enhancement band. Recommendation ITU-T G.984.5, 2014.

[42] ITU-T. Gigabit-capable passive optical networks (GPON): Reach extension. Recommendation ITU-T G.984.6, 2008.

[43] ITU-T. 10-gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations and acronyms. Recommendation ITU-T G.987, 2012.

[44] ITU-T. 10-gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification. Recommendation ITU-T G.987.2, 2020. Amendment 2.

[45] ITU-T. 10-gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification. Recommendation ITU-T G.987.3, 2014.

[46] Bostjan Batagelj, Vesna Eržen, Vitaly Bagan, and Y. Ignatov. Optical access network migration from gpon to xg-pon. *ACCESS 2012: The Third International Conference on Access Networks*, pages 62–67, 01 2012.

[47] ITU-T. 40-gigabit-capable passive optical networks (NG-PON2): General requirements. Recommendation ITU-T G.989.1, 2013.

[48] ITU-T. 40-gigabit-capable passive optical networks 2 (NG-PON2): Physical media dependent (PMD) layer specification. Recommendation ITU-T G.989.2, 2019.

[49] Derek Nesset. Ng-pon2 technology and standards. *Journal of Lightwave Technology*, 33:1–1, 03 2015.

[50] Jun Shan Wey, Derek Nesset, Maurizio Valvo, Klaus Grobe, Hal Roberts, Yuanqiu Luo, and Joe Smith. Physical layer aspects of ng-pon2 standards—part 1: Optical link design. *J. Opt. Commun. Netw.*, 8(1):33–42, Jan 2016.

[51] Yuanqiu Luo, Hal Roberts, Klaus Grobe, Maurizio Valvo, Derek Nesset, Kota Asaka, Harald Rohde, Joe Smith, Jun Shan Wey, and Frank Effenberger. Physical layer aspects of ng-pon2 standards—part 2: System design and technology feasibility. *J. Opt. Commun. Netw.*, 8(1):43–52, Jan 2016.

[52] ITU-T. Higher speed passive optical networks – requirements. Recommendation ITU-T G.9804.1, 2019.

[53] ITU-T. 50-gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification. Recommendation ITU-T G.9804.3, 2021.

[54] Dezhi Zhang, Dekun Liu, Xuming Wu, and Derek Nesset. Progress of itu-t higher speed passive optical network (50g-pon) standardization. *Journal of Optical Communications and Networking*, 12(10):D99–D108, 2020.

[55] R. Ramaswami, K. Sivarajan, and G. Sasaki. *Optical Networks: A Practical Perspective*. Morgan Kaufmann series in networking. Morgan Kaufmann, 2009.

[56] T. Schneider. *Nonlinear Optics in Telecommunications*. Advanced Texts in Physics. Springer, 2004.

[57] Norbert Hanik. Optical communication systems. Lecture slides, Technical University of Munich, 2025.

[58] Chintha Handapangoda, Saeid Nahavandi, and Malin Premaratne. *Review of Nanoscale Spectroscopy in Medicine*, pages 439–472. 11 2013.

[59] Gábor Keresztury, JM Chalmers, and PR Griffith. Raman spectroscopy: theory. *Handbook of vibrational spectroscopy*, 1:71–87, 2002.

[60] M.N. Islam. Raman amplifiers for telecommunications. *Selected Topics in Quantum Electronics, IEEE Journal of*, 8:548 – 559, 06 2002.

[61] Aleksei Gennad'evich Kuznetsov, Sergei A Babin, and Ivan S Shelemba. Fibreoptic distributed temperature sensor with spectral filtration by directional fibre couplers. *Quantum Electronics*, 39(11):1078, 2009.

[62] Hiroki Kawahara, A. Medhipour, and Kyo Inoue. Effect of spontaneous raman scattering on quantum channel wavelength-multiplexed with classical channel. *Optics Communications*, 284:691–696, 01 2011.

[63] Alessandro Gagliano, Alberto Gatto, Pierpaolo Boffi, Paolo Martelli, and Paola Parolari. Quantum key distribution spectral allocation and performance in coexistence with passive optical network standards. *IEEE Transactions on Communications*, 2024.

[64] Alessandro Gagliano, Alberto Gatto, Paolo Martelli, Pierpaolo Boffi, and Paola Parolari. Is the access network ready for quantum key distribution? In *2024 24th International Conference on Transparent Optical Networks (ICTON)*, pages 1–4, 2024.

[65] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89:022307, Feb 2014.

[66] Hua-Lei Yin, Min-Gang Zhou, Jie Gu, Yuan-Mei Xie, Yu-Shuo Lu, and Zeng-Bing Chen. Tight security bounds for decoy-state quantum key distribution. *Scientific Reports*, 10(1), August 2020.

[67] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540, September 2021.

[68] Georg Böcherer, Patrick Schulte, and Fabian Steiner. Probabilistic shaping and forward error correction for fiber-optic communication systems. *Journal of Lightwave Technology*, 37(2):230–244, 2019.

[69] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962.

[70] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006.

[71] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[72] S Fossier, E Diamanti, T Debuisschert, R Tualle-Brouri, and P Grangier. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 42(11):114014, May 2009.

[73] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis

of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010.

[74] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, August 2011.

[75] Zhiliang Yuan, Akira Murakami, Mamko Kujiraoka, Marco Lucamarini, Yoshimichi Tanizawa, Hideaki Sato, Andrew J. Shields, Alan Plews, Ririka Takahashi, Kazuaki Doi, Winci Tam, Andrew W. Sharpe, Alexander R. Dixon, Evan Lavelle, and James F. Dynes. 10-mb/s quantum key distribution. *Journal of Lightwave Technology*, 36(16):3427–3433, August 2018.

[76] Adnan A. E. Hajomer, Cédric Bruynsteen, Ivan Derkach, Nitin Jain, Axl Bomhals, Sarah Bastiaens, Ulrik L. Andersen, Xin Yin, and Tobias Gehring. Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver. *Optica*, 11(9).

[77] Alessandro Gagliano, Alberto Gatto, Pierpaolo Boffi, Paolo Martelli, and Paola Parolari. Discrete-variable quantum key distribution services hosted in legacy passive optical networks. *Journal of Optical Communications and Networking*, 17(1):A96–A102, 2024.

List of Figures

List of Tables