A comprehensive decoy-state quantum key distribution model for practical single-photon sources

Roberto G. Pousa

supervised by Daniel K. L. Oi and John Jeffers

Computational Nonlinear and Quantum Optics Group

Department of Physics

University of Strathclyde, Glasgow

September 2024

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Abstract

The most widely used quantum key distribution (QKD) protocol has been the Bennett-Brassard 1984 (BB84). Practical quantum sources that reach ideal single-photon emission behaviour do not presently exist, making them vulnerable to photon number splitting (PNS) attacks. Weak coherent pulses (WCPs) are favoured in QKD for their feasibility and cost-effectiveness. The exploitable multiphoton emissions of WCPs have rendered the decoy method, which is essential to prevent PNS attacks while offering key rate enhancement. Seeking potential key-rate and finite-block scaling advantages in BB84, we evaluate high brightness, low-$g^{(2)}(0)$ single-photon sources (SPSs) as alternative QKD sources, given their low multiphoton contributions. The challenge lies in their diverse quantum-mechanical systems, lacking a generic statistical distribution for their photon emissions. Researchers often assume distributions that do not accurately represent the SPS statistics, hence we propose a partial characterisation of the SPS using the time-zero second-order correlation function and the mean photon number to estimate secure keys for our non-decoy SPS protocol, where we introduce tight finite-key bounds based on decoy WCP techniques. This approach drastically reduces the required block sizes to approach the asymptotic key rates and shows SPSs' potential for key enhancement in short-range QKD networks. We also present two decoy SPS methods, deriving novel security bounds of the yields and relaxing previous assumptions on arbitrary distributions. These methods highlight the necessary SPS characteristics to surpass decoy WCP. Finally, we implement our non-decoy SPS protocol in our satellite-to-ground QKD model, identifying the optimal wavelength and estimating the annual key volume for our non-decoy SPS, based on a 2D material defect, and for a 2-decoy WCP protocol.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Dr. Daniel Oi, for providing me with the opportunity to pursue my academic career. I am particularly thankful for his support from the very beginning of my PhD journey, particularly for all the invaluable discussions and advice at both personal and academic levels. His passion for scientific inquiry and his commitment to rigorous discussions have been a constant source of inspiration, motivating me to persevere through the toughest and most challenging moments. His influence will remain with me in my future research journey. I also wish to extend my sincere thanks to my second supervisor, Professor John Jeffers, whose profound insights and thoughtful discussions have always been enriching, to Luca Mazzarella, Jasminder Sidhu, Duncan McArthur and Tomas Brougham.

I am also deeply appreciative of my collaborators, particularly the researchers of Professor Tobias Vogl's group, although I owe special thanks to Mostafa Abasifard and Tobias Vogl himself, as well as Chris Morrison, Frederik Barnes and Professor Alessandro Fredizzi, with whom I look forward to continuing our collaborations in the future. I would also like to acknowledge the researchers who have inspired me through their brilliant scientific conversations, with a special mention to Adomas Baliuka.

Last but not least, I am profoundly grateful to my parents, Maria Luz and Roberto, whose unwavering support has made it possible for me to embark on and, hopefully, complete this PhD journey. Finally, I want to acknowledge the unconditional support of Elena Bueno Benito, the light that guides me and the person who always understands me completely.

Statement of contributions

This thesis is based on the two published articles, in which I developed my quantum key distribution (QKD) theoretical analysis with single-photon sources (SPS) in collaboration with experimentalists and a preprint paper:

- Morrison, C. L., **Pousa, R. G.**, Graffitti, F., Koong, Z. X., Barrow, P., Stoltz, N. G., ... and Fedrizzi, A. (2023). Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates. Nature Communications, 14(1), 3573.

- Abasifard, M., Cholsuk, C., **Pousa, R. G.**, Kumar, A., Zand, A., Riel, T., ... and Vogl, T. (2024). The ideal wavelength for daylight free-space quantum key distribution. APL Quantum, 1(1).

- **Pousa, R. G.**, Jeffers, J. and Oi, D. K. (2024). Comparison of non-decoy single-photon source and decoy weak coherent pulse in quantum key distribution. arXiv preprint arXiv:2405.19963.

In the first paper, my contribution was the entire theoretical QKD analysis of the non-decoy SPS protocol using a quantum dot source. The model of the paper is described in Chapter 4 and its results for the experimental quantum dot are specifically shown in Section 4.5.1. The analysis of the non-decoy SPS is expanded on the preprint paper, some of its detailed theoretical aspects are also described in Chapter 4 and its main outcomes are depicted in Section 4.5.2. My contribution to the second paper was the finite-key analysis of an SPS based on the layered material hexagonal boron nitride in a satellite-to-ground QKD model. In particular, I derived the geometric considerations of the channel model and the remaining aspects of the QKD system were developed in

collaboration with the other co-authors, shown in Section 6.1. My experimental collaborators identified the proposed wavelength candidates. To evaluate their experimental SPS in space, I adapted the simulation toolkit of SatQuMa [1] for my non-decoy SPS protocol. SatQuMa was originally created for a 2-decoy weak coherent pulse protocol, whose analysis was published in

- Sidhu, J. S., Brougham, T., McArthur, D., **Pousa, R. G.**, and Oi, D. K. (2022). Finite key effects in satellite quantum key distribution. npj Quantum Information, 8(1), 18.

I contributed to the editing of that paper. Finally, the decoy SPS methods presented in Chapter 5 are entirely my contribution and are aimed to be published soon as a theoretical study and part of it has been published in the following collaborative paper with experimentalists

- Barnes, F. B., **Pousa, R. G.**, Morrison, C. L., Koong, Z. X., Ho, J., Graffitti, F., ... and Fedrizzi, A. (2026). Decoy-state quantum key distribution over 227 km with a frequency-converted telecom single-photon source. Phys. Rev. Lett. 137, 060801.

Further details about the materials of these papers presented in this thesis are described in Section 1.2.

List of Abbreviations

QKD quantum key distribution

SPS single-photon source

QD quantum dot

hBN hexagonal boron nitride

HBT Hanbury-Brown-Twiss

WCP weak coherent pulse

RSA Rivest-Shamir-Adleman

PQC post-quantum cryptography

BB84 Bennett-Brassard 1984

CPTP completely positive trace-preserving

PNS photon number splitting

i.i.d. independent and identically distributed

POVM positive operator-valued measure

AKR asymptotic key rate

SKL secure key length

SKR secure key rate

OGS optical ground station

Contents

Contents

Chapter 1

Introduction

Throughout history, the desire to exchange secret messages has been ever-present. The earliest secret codes from the Persians and Greeks date back to the fifth century BC. Over time, encryption codes and ciphers have evolved significantly, profoundly impacting society. A notable example is Alan Turing's success in cracking the Enigma code during World War II. This ongoing battle between code breakers and code designers has persisted for centuries, leading to substantial efforts in developing classical cryptographic schemes to protect private and confidential data.

The security of classical public key cryptosystems is built upon the hardness of certain mathematical problems, assuming no computational algorithm can efficiently solve them in a reasonable timeframe [2]. One of the most commonly employed public key encryption protocols is the Rivest-Shamir-Adleman (RSA) algorithm [3, 4], which is fundamentally predicated on the mathematical problem of prime factorization. The core concept relies on the asymmetry of computational difficulty between two operations: the multiplication of two large prime numbers, which is trivial, and the inverse process of factorising their product, which is computationally infeasible for current classical computers to perform in a reasonable time.

The future advent of quantum computers, first envisioned by Feynman [5], threatens classical cryptographic systems. Classical encryption schemes based on prime factorisation and discrete logarithm will become insecure when a practical quantum computer is able to implement Shor's factoring algorithm [6, 7]. However, quantum computers

are also expected to solve problems that are currently intractable for classical computers [8]. This context underscores the need for quantum-safe cryptography. The two current solutions are post-quantum cryptography (PQC) [9] and quantum cryptography [10]. PQC involves developing new cryptographic algorithms that are secure against the threats posed by quantum computers (see a review of PQC in [11]). In contrast, quantum cryptography leverages the principles of quantum mechanics to achieve secure communication. Specifically, PQC is a software solution, whose security relies on the computational complexity of solving a mathematical problem. This might potentially lead to endless generations of increasingly more robust algorithms. On the other hand, quantum cryptography is a physically-based solution, as its security relies on the correctness of quantum theory principles and the equipment's behaviour aligning with the theoretical model [12].

Stepping back in time, the concept of exploiting quantum properties for secure interactions has been around since the 1970s, beginning with the idea of unfalsifiable quantum banknotes by Wiesner [13]. Although impractical due to its complex requirements for single-photon storage, Wiesner paved the way for quantum key distribution. The development of the Bennett and Brassard 1984 (BB84) QKD protocol [14] demonstrated that photons were more useful for transmitting information rather than storing it. Over the past few decades, numerous other protocols have been introduced, including entanglement-based [15,16] and device-independent protocols [17,18], some of which have been experimentally implemented [19–21]. QKD protocols serve as cryptographic systems that securely distribute secret keys between distant parties. The key, a string of classical bits, enables the encryption and decryption of messages for private communication. Unlike other cryptographic protocols, the security of QKD does not rely on assumptions about an adversary's computational limitations. Instead, QKD provides unconditional security [22, 23], also known as information-theoretic security [24], by exploiting the intrinsic quantum properties of photons, even if the eavesdropper has unlimited computational power. Thus, it provides a way of detecting an eavesdropper when all the required steps of the QKD protocol succeed, such as quantification of the information leaked to the adversary or classical post-processing. However, experimen-

tal challenges must be addressed to align the QKD implementation with the theoretical model and prevent security threats.

In prepare-and-measure QKD protocols, such as the BB84, entangled states are not a requirement, although if they are used, it helps to ensure a secure preparation of the transmitted states [25]. The sender (Alice) encodes the key, a string of random bits, into polarized quantum states. She transmits these states through a quantum channel to a receiver (Bob), who measures them to obtain the encoded bits of the key. The security of this protocol is based on the no-cloning theorem [26], which forbids the perfect cloning of an unknown quantum state, and the Heisenberg uncertainty principle, which sets a fundamental limit on the accuracy with which two complementary variables can be measured, such as the mutually unbiased orthogonal bases used for the BB84 polarized states. The no-cloning theorem prevents an eavesdropper from making a copy of the transmitted quantum state to gain information about the key while re-sending the original state to Bob. Hence, to acquire knowledge about the encoded bit, an eavesdropper (Eve) must measure the sent state. If Eve measures using the complementary basis to the one used by Alice and Bob, she inevitably disturbs the polarised state. This disturbance does not go unnoticed by the parties, allowing them to detect Eve's presence and abort the protocol.

Early security proofs for QKD protocols assumed ideal device behaviour to demonstrate that QKD is information-theoretically secure [27], meaning it is unbreakable under the proposed theoretical model. However, practical challenges in QKD implementations threaten protocol security because the behaviour of real devices often deviates from these theoretical assumptions. Security proofs have been revised continually to address these deviations and maintain protocol security [28, 29]. Additionally, researchers in quantum hacking have explored these deviations, identifying security loopholes that can be exploited by Eve's attacks [30, 31].

One of the most commonly discussed attacks is the photon number splitting (PNS) attack [32, 33], where Eve exploits the multiphoton emission from Alice's source to extract the key while remaining undetectable. An ideal QKD system would employ a quantum source that consistently sends single-photons. Although ongoing research

aims to approach this ideal behaviour [34], it is strictly unachievable in practice. In real-life scenarios, this inherent nonideality of practical sources is exploited by the PNS attack. This attack is particularly effective in noisy channels, where low detection rates at Bob's apparatus allow Eve to gain knowledge of the entire key. To counteract Eve's strategy, the decoy-state method was introduced for the BB84 protocol [35], wherein Alice uses multiple intensities to prepare her states. The principle behind the decoy technique is that the yield, i.e. detection rate for a particular n-photon state, must be the same for different intensity levels. Thus, the parties can estimate the yields of secure events (non-multiphotons) using the statistics generated by all intensities while upper bounding the multiphoton contribution, representing insecure events.

Another practical challenge is estimating the secret key for finite statistics. Initially, QKD security proofs estimated the key rate for the asymptotic limit, where Alice and Bob shared an arbitrarily large block of correlated events, also interpreted as the running time of the QKD experiment tending to infinity. However, in a real experiment, the gathered statistical blocks are finite and subject to fluctuations from their expected outcomes. Consequently, studies were proposed to account for these finite-key effects [36,37]. Ignoring these deviations from the estimated values threatens protocol security, as it can lead to an overestimation of the secure events forming the final key.

1.1 Motivations and Contributions

Overall, the main current challenges in QKD are to distribute higher amounts of secret bits and extend the tolerable range of loss (distance) between the parties. The QKD community is exploring ways to address these challenges, such as proposing novel or updated protocols, employing alternative quantum sources, using free space as the quantum channel, and discovering more optimal transmission wavelengths. In this work, we explore these ideas to improve the BB84 QKD protocol performance.

Weak coherent pulse (WCP) sources are strongly attenuated lasers that approach the single-photon regime and have been the most commonly employed sources in the

BB84 protocol due to their feasibility [38]. WCP sources have offered adequate QKD performance due to their high brightness despite their considerable multiphoton emission. However, recent advancements in practical single-photon sources (SPSs), based on defects in 2D materials or quantum dots, exhibit significantly lower multiphoton emission than WCPs [39–41]. Efforts are being made to achieve more optimal SPSs due to their various important applications beyond QKD, making them promising sources for QKD implementations.

In particular, recent advancements in SPSs show that they can potentially improve the ratio between single-photon and multiphoton emissions, which is crucial for QKD transmission, whereas WCPs lack this capacity for improvement. Thus, it arises the motivation for building a theoretical formalism for the BB84 protocol adapted to the nature of SPSs to provide a model to experimentalists that aim to evaluate their particular SPS in QKD. Consequently, the inability to further suppress multiphoton emissions in WCPs led to their shift away from non-decoy BB84, driven by the need for enhanced security against PNS attacks and higher key generation in practical QKD systems. However, SPSs emerge as suitable candidates for a non-decoy BB84 protocol, where only one intensity is used, due to their extremely low multiphoton emission. Therefore, we develop an updated non-decoy method for an SPS and we show the key rate performance of an experimental quantum dot in [42]. We compare our non-decoy SPS with a decoy WCP protocol. Although the non-decoy SPS protocol avoids the complexity of adding a decoy state, decoy WCP protocols are mature and cost-effective, being an optimal choice for QKD implementations. However, here we propose specific scenarios where an SPS with certain characteristics in a non-decoy method may be preferable based on key rate performance or maximum tolerable loss of the system.

Clearly, we do not limit the study of SPSs in QKD to non-decoy protocols. We extend this analysis to the decoy method, which not only prevents PNS attacks but also enhances the key generation. We develop a novel theoretical decoy BB84 protocol adapted to any practical SPS. Thus, we examine if these alternative quantum sources can outperform the widely used WCP within the decoy method and identify the required SPS characteristics to achieve it.

Finally, utilizing a free-space channel drastically reduces transmission loss compared to optical fibre [43]. Therefore, we introduce our non-decoy SPS protocol in a satellite-to-ground QKD model and compare it with a decoy WCP. We develop this analysis for a specific SPS based on the layered material hexagonal boron nitride (hBN). We analyze different wavelengths suitable for this SPS, as well as the C-band, commonly employed for WCPs, for both non-decoy SPS and decoy WCP protocols during daylight and night operations.

To recap, our goals in this thesis align with the previous ideas and were conceived as follows. First, we identified alternative quantum sources that have not been analyzed in-depth in the QKD field but possess the potential to enhance the key performance. Practical SPSs emerged as promising candidates. Second, we selected the protocol that best suits the nature of SPSs. We chose the BB84 protocol and derived novel security bounds adapted to any type of SPS for both non-decoy and decoy methods. The development of the latter was inspired by techniques used in up-to-date decoy WCP protocols. Third, we analysed the SPS performance in free-space QKD for a satellite-to-ground model, evaluating different wavelengths to identify the optimal one for each scenario. In conclusion, testing novel quantum light sources to determine if they can potentially outperform the commonly employed WCPs in various QKD scenarios, and identifying the required characteristics of the proposed source and protocol, is a valuable aim that contributes to the progress of the QKD field.

1.2 Thesis Structure

The thesis is organised as follows. In Chapter 2, we review the fundamental elements of quantum systems and information theory that underpin both classical and quantum cryptography. These concepts are essential for understanding the security of quantum key distribution, presented in Chapter 3. This chapter covers the main theoretical aspects of the secure key derivations, from the asymptotic limit using efficient BB84 to the finite-key analysis incorporating the decoy method with weak coherent pulses.

Chapters 4 to 6 contain the primary contributions of our research. In Chapter 4, we present our non-decoy SPS protocol, showing a key enhancement and significantly

reducing the required block sizes to reach the asymptotic key rate compared to previous non-decoy analysis in the literature. Furthermore, we demonstrate how non-decoy SPS can improve the key performance and maximum tolerable loss of the 2-decoy WCP in a considerably constrained region of short acquisition times (block sizes) and low losses, provided the mean photon number is sufficiently high. While this serves as an initial comparison between SPS and WCP in QKD, acknowledged that the comparison is not entirely fair due to the use of different QKD protocols for each source. To address this, in Chapter 5, we provide a comparative analysis of SPS and WCP within the framework of the decoy method. We present novel decoy models adapted to any conceivable SPS with a measurable time-zero second-order correlation function and mean photon number. We examine which SPS characteristics are needed to surpass WCP in decoy methods and aim to relax the assumptions on the photon emission statistics in previous studies using arbitrary distributions. Given SPSs are not tied to a generic statistical distribution, due to the diversity of quantum-mechanical systems used to construct them, our protocols' applicability to any practical SPS is of significant relevance.

In Chapter 6, we evaluate the key performance of our non-decoy protocol in our satellite-to-ground QKD simulation model. We compare it with the commonly employed 2-decoy WCP over three wavelength candidates, two of which are selected for their potential in daylight communication. We identify which wavelength, combined with the protocol and source, is the most optimal for distributing secure key bits under our particular free-space channel model. Finally, we draw the conclusions of the thesis in Chapter 7.

1.3 Conventions

To ensure clarity and consistency throughout the thesis, here, we state our adopted conventions:

- ρ denotes a density operator (matrix), representing the state of a quantum system and it is the only operator without a hat.

- Creation and annihilation operators are denoted by $\hat{a}$ and $\hat{a}^\dagger$, respectively.
- General operators, including observables, are marked with a hat ($\hat{A}$) to distinguish them from scalar quantities and states.
- Scalar quantities and state vectors do not carry hats.
- We define the set of natural numbers $\mathbb{N}$ as the non-negative integers, hence including 0.
- Te logarithm symbol is always intended in base 2 and it holds $0 \log 0 = 0$.

This notation is chosen to align with common practices in quantum cryptography and quantum information, where it is common to see ρ without a hat, and it prevents the notation from appearing heavier in complex derivations.

Chapter 2

Elements of Classical and Quantum Cryptography

In this chapter, we review the required formalism of quantum mechanics to describe quantum systems used in quantum information theory and later applied to quantum cryptography (Section 2.1). We introduce the mathematical tools to characterise the quantum states of a system (Section 2.1.1-2.1.4), their transmission (Section 2.1.6) and measurement (Section 2.1.5). We present the fundamental concepts related to information theory starting from the classical theory to their analogues in the quantum world (Section 2.2). To characterise information processing tasks, we introduce the entropies that constrain how much classical information can be reliably transmitted between two parties. In particular, the Shannon and von Neumann entropies (Sections 2.2.1 and 2.2.2) for a classical and quantum channel, respectively, which operate in the asymptotic limit, i.e. for arbitrarily large data blocks. Then we introduce the smooth entropies (Section 2.2.3) that are applied to finite blocks of statistics in quantum cryptography. In the QKD context, these entropies are crucial, for instance, to calculate how much information an eavesdropper can extract about the key shared by the legitimate parties communicating through a quantum channel. These results will be crucial to estimate the asymptotic secret key rate for the BB84 protocol. We show how to characterise the capacity of either a classical or quantum channel (Section 2.2.6). Prior we elaborate on quantities and concepts relevant to these channel capacities (Sections

2.2.4 and 2.2.5).

2.1 Description of Quantum Systems

Here, we introduce the foundational mathematical formalism to describe quantum mechanical systems. We review fundamental concepts of quantum mechanics using linear algebra, including tensors, Hilbert spaces, Dirac notation, and the density operator formalism. The presented quantum systems and operators are crucial for the main components of a generic quantum mechanical experiment—preparation, transmission, and measurement—especially in a QKD system. First, in the study of QKD protocols, the density operators of composite systems are examined to determine the secret key, specifically the composite system of Alice and Bob and the one composed of Alice's and Eve's systems. Therefore, we present a mathematical description of these quantum composite systems. Bob needs to measure the received quantum states to decode them and access the key formed by the classical bits encoded by Alice. Thus, we provide the formalism for this quantum measurement, known as the positive-operator-valued measure (POVM). We also introduce the quantum bits, or qubits, and the Pauli operator, which describe the quantum states used by the parties in QKD to share an identical secure key. Finally, since Alice uses a quantum channel to transmit the states to Bob, we analyse the evolution of the state caused by the quantum channel and its properties. Most of the elements defined in this section can be found in [44–47].

2.1.1 Hilbert Spaces and Dirac Notation

The state space of a quantum system is described by a Hilbert space $\mathcal{H}$. In particular, a Hilbert space is a vector space over the complex numbers $\mathbb{C}$. We use the Dirac notation to denote vectors in a Hilbert space. If the quantum system has d degrees of freedom, the state of the system is represented by a vector $|\psi\rangle$ in a finite Hilbert space $\mathcal{H}$ of dimension d. For a quantum system with infinite degrees of freedom, it is represented in the infinite Hilbert space. The dual vector corresponding to the *ket* $|\psi\rangle$ is called *bra* and is denoted as $\langle\psi| \in \mathcal{H}^*$, where $\mathcal{H}^*$ is the dual Hilbert space of $\mathcal{H}$.

The inner product between two vectors $|\psi\rangle$ and $|\varphi\rangle$ in the same Hilbert space $\mathcal{H}$ is defined by the following map

$$\langle\psi|\varphi\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C} \tag{2.1}$$

where $\langle\psi|\varphi\rangle$ is called *braket*, and it satisfies the following properties:

1. Linearity in the second argument. $\langle\psi| (\alpha |\varphi\rangle + \beta |\phi\rangle) = \alpha \langle\psi|\varphi\rangle + \beta \langle\psi|\phi\rangle$ where $|\psi\rangle, |\varphi\rangle, |\phi\rangle \in \mathcal{H}$ and $\alpha, \beta \in \mathbb{C}$.

2. Conjugate linearity in the first argument. $(\alpha \langle\varphi| + \beta \langle\phi|) |\psi\rangle = \alpha^* \langle\varphi|\psi\rangle + \beta^* \langle\phi|\psi\rangle$ where α^* and β^* represent the complex conjugates of α and β, respectively.

3. Conjugate symmetry. $\langle\psi|\varphi\rangle = \overline{\langle\varphi|\psi\rangle}$.

4. Positive-definiteness. $\langle\psi|\psi\rangle \geq 0$ and $\langle\psi|\psi\rangle = 0$ if and only if $|\psi\rangle = 0$

In particular, if the vectors $|\psi\rangle$ and $|\varphi\rangle$ in a Hilbert space are represented by some orthonormal basis $\{|e_i\rangle\}$,

$$|\psi\rangle = \sum_i \alpha_i |e_i\rangle \quad \text{and} \quad |\varphi\rangle = \sum_i \beta_i |e_i\rangle , \tag{2.2}$$

their inner product $\langle\psi|\varphi\rangle$ can be specifically expressed as

$$\langle\psi|\varphi\rangle = \left(\sum_i a_i^* \langle e_i|\right) \left(\sum_j b_j |e_j\rangle\right) = \sum_{i,j} a_i^* b_j \langle e_i|e_j\rangle , \tag{2.3}$$

where the inner product of the orthonormal basis equals the Kronecker delta $\langle e_i|e_j\rangle = \delta_{ij}$. Hence, any orthonormal basis $\{|e_i\rangle\}_{i=1}^d$ of an d-dimensional Hilbert space $\mathcal{H}$ satisfies the completeness relation $\sum_{i=1}^d |e_i\rangle \langle e_i| = \mathbb{1}$, where $\mathbb{1}$ is the identity operator.

These vectors have additional properties defined as follows. Two vectors $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal if their inner product is zero, $\langle\psi|\varphi\rangle = 0$. A vector is normalised if $\langle\psi|\psi\rangle = 1$. Moreover, the norm induced by the inner product is given by $|| |\psi\rangle || = \sqrt{\langle\psi|\psi\rangle}$.

Besides the inner product, we define the outer product of two states $|\psi\rangle \in \mathcal{H}$ and $\langle\varphi| \in \mathcal{H}^*$ as $|\psi\rangle\langle\varphi|$, which acts on another state $|\phi\rangle \in \mathcal{H}$ as $|\psi\rangle\langle\varphi|\phi\rangle = \langle\varphi|\phi\rangle|\psi\rangle$. Moreover, the outer product of a vector $|\psi\rangle$ by itself is represented by a projection of another vector $|\varphi\rangle$ onto the one-dimensional subspace spanned by $|\psi\rangle\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle|\psi\rangle$.

2.1.2 Linear and Density Operators

Using the completeness relation of an orthonormal basis $\{e_i\}$, any linear operator $\hat{A}$ can be represented using the outer product as follows

$$\hat{A} = \mathbb{1}\hat{A}\mathbb{1} = \sum_{i,j}^{d} \langle e_i|\hat{A}|e_j\rangle |e_i\rangle\langle e_j|, \tag{2.4}$$

where $\langle e_i|\hat{A}|e_j\rangle$ are the elements of the matrix representation of $\hat{A}$ for each i-th row and j-th column in the d-dimensional Hilbert space. If the operator $\hat{A} \in \mathcal{D}(\hat{A})$, where $\mathcal{D}(\hat{A})$ is its domain, the adjoint operator $\hat{A}^\dagger$ is defined as an operator with domain $\mathcal{D}(\hat{A}^\dagger)$ such that $(\langle\psi|\hat{A}^\dagger|\varphi\rangle)^* = \langle\psi|\hat{A}|\varphi\rangle$ for all $|\psi\rangle \in \mathcal{D}(\hat{A})$ and $|\varphi\rangle \in \mathcal{D}(\hat{A}^\dagger)$. Hence, it follows that $(|\psi\rangle\langle\varphi|)^\dagger = |\varphi\rangle\langle\psi|$ and that the dual operator of $\hat{A}|\psi\rangle$ is $\langle\psi|\hat{A}^\dagger$.

An operator $\hat{A}$ is defined as symmetric if $(\langle\psi|\hat{A}|\varphi\rangle)^* = \langle\psi|\hat{A}|\varphi\rangle$. Furthermore, the observables in quantum mechanics are self-adjoint operators. A linear operator $\hat{A}$ is called self-adjoint if $\hat{A}$ and its adjoint $\hat{A}^\dagger$ are identical $\hat{A} = \hat{A}^\dagger$, i.e. $\hat{A}$ is symmetric and their domains coincide $\mathcal{D}(\hat{A}) = \mathcal{D}(\hat{A}^\dagger)$.

A linear operator $\hat{A}$ is Hermitian if it is self-adjoint and bounded. This last condition occurs if there is a positive number $M \geq 0$ such that $||\hat{A}|\psi\rangle|| \leq M||\,|\psi\rangle\,||$ for any state $|\psi\rangle \in \mathcal{H}$, which holds $\mathcal{D}(\hat{A}) = \mathcal{H}$.

Similarly to Eq. (2.4), an Hermitian operator $\hat{A} = \hat{A}^\dagger$ can be expressed in its spectral decomposition as

$$\hat{A} = \sum_{i=1}^{d} a_i |a_i\rangle\langle a_i|, \tag{2.5}$$

where a_i and $\{|a_i\rangle\}_{i=1}^d$ are the eigenvalues the eigenbasis of $\hat{A}$ on the d-dimensional Hilbert space $\mathcal{H}$, respectively. $|a_i\rangle\langle a_i|$ are rank-one orthogonal projectors on their

eigenvectors $|a_i\rangle$. Its trace can be expressed as

$$\mathrm{Tr}\left[\hat{A}\right] = \sum_{i=1}^{d} \langle e_i|\hat{A}|e_i\rangle \,. \tag{2.6}$$

which can be interpreted as the sum of the eigenvalues of $\hat{A}$, counting each one by its algebraic multiplicity. These eigenvalues do not depend on the chosen basis to represent the operator. When applying a transformation that changes the basis, the diagonal elements of the matrix representation change, however, the eigenvalues remain the same. Thus, the trace of the linear operator, being the sum of the eigenvalues, also remains unchanged, hence it is independent of the chosen basis. Another important norm is the trace norm given by $||O||_1 \equiv \mathrm{Tr}\left[\sqrt{O^\dagger O}\right]$, which will be used in future sections.

The evolution of a closed quantum system is determined by a unitary operator $\hat{U}$, meaning its adjoint operator equals its inverse $\hat{U}^\dagger = \hat{U}^{-1}$. This unitary operator can also link two bases $\{e_i\}_{i=1}^d$ and $\{e'_i\}_{i=1}^d$ of dimension d such that $|e'_i\rangle = \hat{U}\,|e_i\rangle$. These bases are mutually unbiased if their inner product for each i and j equals the inverse of the basis dimension $|\,\langle e'_i|e_i\rangle\,| = 1/d$.

In quantum mechanics, density operators are used to describe the state of a quantum system, particularly when dealing with mixed states. A pure state of a quantum system is described by a single *ket* vector $|\psi\rangle$ in a Hilbert space, i.e. what we called before just state. However, in practice, a quantum system may not be in a single-state vector. In this case, we can define it as a mixed state, i.e. a statistical ensemble of pure states, each with a certain probability. Formally, a quantum system described by the statistical mixture of pure states $\{|\psi\rangle\}_{i=1}^d \in \mathcal{H}$, with probabilities p_i, satisfying $\sum_{i=1}^d p_i = \mathbb{1}$, is a mixed state and it can be described by the following density operator with spectral decomposition

$$\rho = \sum_{i=1}^{d} p_i \,|\psi_i\rangle\,\langle\psi_i|\,. \tag{2.7}$$

Note the state of the system is then characterised by the ensemble $\{p_i, \psi_i\}$. The matrix representation of ρ is known as the density matrix and it is commonly employed to

also indicate the quantum operator itself. If the quantum system is in a pure state, then the density operator (matrix) can be reduced to simply $\rho = |\psi\rangle\langle\psi|$. Note a pure state must fulfil $\mathrm{Tr}\left[\rho^2\right] = 1$, whereas for a mixed state $\mathrm{Tr}\left[\rho^2\right] < 1$. Furthermore, the density operator satisfies the following properties: if it is normalised, $\mathrm{Tr}\left[\rho\right] = 1$; if it is Hermitian, $\rho^\dagger = \rho$; and if it is positive semi-definite $\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle$. For convenience, we usually express it as $\rho \geq 0$. Thus, for a pure state $\rho = |\psi\rangle\langle\psi|$, the expectation value of the observable $\hat{A}$ is given by

$$\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle = \mathrm{Tr}\left[\rho\hat{A}\right]. \tag{2.8}$$

In many realistic situations, a quantum system may not be in a single pure state but rather in an incoherent superposition of several states. Thus, we do not have complete knowledge of the exact state of the system. The density operator is essential to deal with systems described by mixed states since it contains complete probabilistic information about the possible states of the system. In particular, in quantum information, density operators are indispensable for accurately modelling real quantum systems, which usually exhibit noise or decoherence due to the quantum channel used to transmit the state or the interaction with the environment. Specifically in quantum cryptography, where part of the security proofs of the protocols relies on the characterization of the density matrices between the quantum systems involved.

Finally, let us define some set of density operators that will be useful in Sections 2.1.6 and 2.2.3. Let $\mathcal{H}$ be a finite-dimensional Hilbert space. The collection of the entire bounded linear operators acting on $\mathcal{H}$ is denoted by $\mathcal{B}(\mathcal{H})$, e.g. the density operators $\rho \in \mathcal{B}(\mathcal{H})$. We denote the collection of positive semi-definite operators on $\mathcal{H}$ by $\mathcal{P}(\mathcal{H})$. We define the set of normalised quantum states as [48]

$$\mathcal{S}_=(\mathcal{H}) = \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{Tr}\left[\rho\right] = 1\} \tag{2.9}$$

and the subnormalised states as

$$\mathcal{S}_\leq(\mathcal{H}) = \{\rho \in \mathcal{P}(\mathcal{H}) : 0 < \mathrm{Tr}\left[\rho\right] \leq 1\}. \tag{2.10}$$

2.1.3 Composite Systems

The composite system of two quantum states is defined in the tensor product of their corresponding Hilbert spaces $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with states $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$. Hence, states of this tensor product Hilbert space are linear combinations of tensor products $|\psi_A\rangle \otimes |\psi_B\rangle$. Similarly, the dimension of the composite space is a product of the subsystem dimensions $\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = \dim(\mathcal{H}_A)\dim(\mathcal{H}_B) = d_A d_B$. Selecting orthonormal bases for each system, i.e. $\{|a_j\rangle\}_{j=1}^{d_A}$ and $\{|b_k\rangle\}_{k=1}^{d_B}$, the composite system has the basis $\{|a_j\rangle \otimes |b_k\rangle\} \equiv \{|a_j b_k\rangle\}$, an arbitrary bipartite pure state can be expressed as

$$|\psi_{AB}\rangle = \sum_{j,k}^{d_A,d_B} \sqrt{c_{j,k}}\,|a_j b_k\rangle \tag{2.11}$$

where the coefficients $\sqrt{c_{jk}}$ form a matrix $C = (\sqrt{c_{jk}}) \in \mathbb{C}^{d_A \times d_B}$. This admits a singular value decomposition $C = UDV$ where $U = (\sqrt{u_{ji}}) \in \mathbb{C}^{d_A \times d_A}$ and $V = (\sqrt{v_{ik}}) \in \mathbb{C}^{d_B \times d_B}$ are unitary matrices and $D = (\sqrt{\lambda_i}) \in \mathbb{R}^{d_A \times d_B}$ is a diagonal matrix of positive values. Therefore, the coefficients of the C matrix can be expressed as $\sqrt{c_{jk}} = \sum_i^{\min(d_A,d_B)} \sqrt{u_{ji}\lambda_i v_{ik}}$. Introducing this decomposition in Eq. (2.11), we obtain

$$|\psi_{AB}\rangle = \sum_{j,k}^{d_A,d_B} \sum_{i}^{\min(d_A,d_B)} \sqrt{u_{ji}\lambda_i v_{ik}}\,|a_j b_k\rangle\,. \tag{2.12}$$

Defining the new bases as $|a_i\rangle = \sum_{j=1}^{d_A} u_{ji}\,|a_j\rangle$ and $|b_i\rangle = \sum_{k=1}^{d_A} u_{ik}\,|b_k\rangle$ abusing the notation, an arbitrary pure state can be written by Schmidt decomposition as

$$|\psi_{AB}\rangle = \sum_{i}^{\min(d_A,d_B)} \sqrt{\lambda_i}\,|a_i b_i\rangle\,, \tag{2.13}$$

where $\lambda_i > 0$ are the positive real quantum coefficients, known as Schmidt coefficients, and $\sum_i \lambda_i = 1$. The Schmidt rank is equal to the number of coefficients $\sqrt{\lambda_i}$ and must be less or equal to $\min(d_A, d_B)$.

Suppose the quantum systems A and B both hold pure states, $|\psi_A\rangle$ and $|\psi_B\rangle$, respectively. Generally, the states of each quantum system, $|a_i\rangle$ and $|b_i\rangle$, can be locally prepared according to the value of λ_i. The density operator of the composite system

AB is a Hermitian matrix given by

$$\rho_{AB} = |\psi_{AB}\rangle \langle \psi_{AB}| = \sum_{i}^{\min(d_A, d_B)} \lambda_i |a_i b_i\rangle \langle a_i b_i| . \tag{2.14}$$

This represents a separable state if it admits a combination of pure product states $|a_i\rangle \otimes |b_i\rangle$. Otherwise, the quantum state ρ_{AB} is called entangled.

An ability of the density operator formalism is to describe quantum subsystems of the entire composite system through the reduced density operator. Thus, if we are interested in the subsystem A, we sum over the subsystem B, i.e. take its partial trace, denoted by Tr_B, which operates as the regular trace of Eq. (2.6) but only acts on the corresponding subsystem as follows

$$\rho_A \equiv \mathrm{Tr}_B [\rho_{AB}] = \sum_i (\mathbb{1}_A \otimes \langle b_i|_B) \rho_{AB} (\mathbb{1}_A \otimes |b_i\rangle_B) \tag{2.15}$$

where $\{|b_i\rangle_B\}$ is any orthonormal basis of the Hilbert space $\mathcal{H}_B$ and $\mathbb{1}$ is the identity operator. Similarly, the partial trace over subsystem X is defined as

$$\rho_B \equiv \mathrm{Tr}_B [\rho_{AB}] = \sum_i (\langle a_i|_A \otimes \mathbb{1}_B) \rho_{AB} (|a_i\rangle_A \otimes \mathbb{1}_B) \tag{2.16}$$

where $\{|a_i\rangle_A\}$ is any orthonormal basis of the Hilbert space $\mathcal{H}_A$. Note this partial trace can be generalised to composite systems of more than two subsystems.

In quantum cryptography, if the legitimate parties hold a quantum system A and there is an eavesdropper, Eve, holding the system E, one must assume the worst-case scenario where Eve's system has all possible quantum correlations with A. This is represented by Eve holding a purifying system, which is defined as follows.

Definition 1 *(Purification). Let ρ_A be a state of the quantum system A. Suppose the auxiliary system E holds a pure state with the system A, $|\psi_{AE}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E \equiv \mathcal{H}_{AE}$. If this pure state can be reduced to ρ_A, such that*

$$\mathrm{Tr}_E [|\psi_{AE}\rangle \langle \psi_{AE}|] = \rho_A, \tag{2.17}$$

then $|\psi_{AE}\rangle$ *is a purification of* ρ_A.

The density operator formalism can also be used to represent classical states. Suppose X is a set of classical variables whose values, also called realisations, are $x \in X$, which are distributed with probability $p(x)$. The classical values can be represented by orthonormal states $|x\rangle$, which are always perfectly distinguishable in this classical case, in a Hilbert space $\mathcal{H}_X$. The density operator is now represented by the classical ensemble $\{p(x), |x\rangle \langle x|\}$ and is given by

$$\rho_X = \sum_{x \in X} p(x) |x\rangle \langle x| . \tag{2.18}$$

This can be extended to a *classical-quantum* (cq) state in the tensor product Hilbert space $\mathcal{H}_X \otimes \mathcal{H}_E$, where $\mathcal{H}_E$ represents Eve's quantum system, and it is given by

$$\rho_{XE} = \sum_{x \in X} p(x) |x\rangle \langle x|_X \otimes \rho_E^x, \tag{2.19}$$

where Eve's states ρ_E^x depend on the classical values x.

2.1.4 Qubits and Pauli Operators

A quantum bit or qubit is the fundamental unit of quantum information, analogous to the classical bit but with inherently quantum properties. Unlike a classical bit, which can be in a state of either 0 or 1, a qubit can exist in a superposition of both states and is represented in a two-dimensional Hilbert space $\mathcal{H}_2$, where one commonly used basis is the rectilinear basis $\{|0\rangle, |1\rangle\}$. Thus, a pure qubit state is described by the general form $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

The Bloch sphere is defined as a unit sphere in $\mathbb{R}^3$ and provides a geometric representation of qubit states. Any pure qubit state can be mapped onto a point on the surface of the Bloch sphere, which is represented in spherical coordinates as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle , \tag{2.20}$$

where $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$ are the polar and azimuthal angles, respectively. The

north and south poles of the Bloch sphere correspond to the rectilinear basis states $|0\rangle$ and $|1\rangle$, respectively, while points on the equator represent equal superpositions of these states, see Figure 2.1.

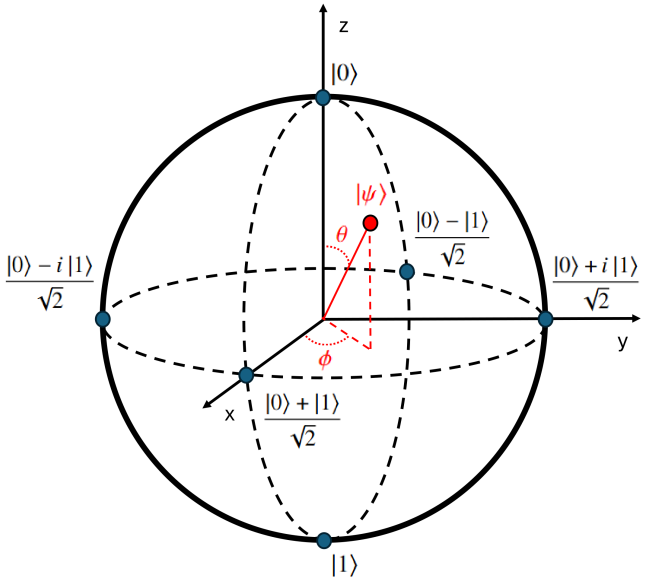

Figure 2.1: Graphic representation of the Bloch sphere. The superposition states of the sphere are commonly denoted as $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, $|+i\rangle = (|0\rangle + i\,|1\rangle)/\sqrt{2}$ and $|-i\rangle = (|0\rangle - i\,|1\rangle)/\sqrt{2}$.

The matrix representations of the Pauli operators with respect to the rectilinear basis are given by

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.21}$$

These operators correspond to rotations about the x-, y- and z-axes of the Bloch sphere by π radians, respectively. Each operator is traceless and has eigenstates associated with the eigenvalues ± 1, known as the following states:

1. Z states (rectilinear basis), which are the eigenstates of $\hat{\sigma}_z$, $|0\rangle$ and $|1\rangle$.

2. X states (diagonal basis), which are the eigenstates of $\hat{\sigma}_x$, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$

and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, located on the equator of the Bloch sphere at $\phi = 0$ and $\phi + \pi$.

3. Y states, which are the eigenstates of $\hat{\sigma}_y$, $(|0\rangle \pm i\,|1\rangle)/\sqrt{2}$, another superposition of states located on the equator at $\phi = \pi/2$ and $\phi = 3\pi/2$.

The Pauli operators form a complete basis for the space of two-dimensional Hermitian matrices, enabling any single-qubit operation to be expressed as a combination of these fundamental rotations.

Generally, the density matrix of a qubit, which can represent either a pure or a mixed state, can be expressed as a combination of the Pauli operators $\hat{\boldsymbol{\sigma}} = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)^T$ [49]

$$\rho = \frac{\mathbb{1} + \mathbf{r} \cdot \hat{\boldsymbol{\sigma}}}{2} \tag{2.22}$$

where $\mathbf{r} = (r_x, r_y, r_z) \in \mathbb{R}^3$ is the Bloch vector with $||r|| \leq 1$.

2.1.5 Projective Measurement and Positive-Operator-Valued Measure

In quantum theory, measurement is defined by a set of operators $\{\hat{M}_x\}$, where the index x represents the possible outcome of the measurement within a finite outcome set X. The measurement operators satisfy the completeness relation $\sum_{x \in X} \hat{M}_x \hat{M}_x^\dagger = \mathbb{1}$. Considering the system in a given pure state $|\psi\rangle$, the probability of obtaining an outcome x after measurement is given by

$$p(x|\psi) = \langle \psi | \hat{M}_x \hat{M}_x^\dagger | \psi \rangle \,, \tag{2.23}$$

where x represents a classical variable. Using the expectation value of the density operator formalism for a state $\rho = |\psi\rangle \langle\psi|$ shown in eq. (2.8), the previous probability can be expressed as

$$p(x|\psi) = \mathrm{Tr}\left[\hat{M}_x \hat{M}_x^\dagger \rho\right]. \tag{2.24}$$

In the case of projective measurements, the operators $\{\hat{M}_x\}$ are orthogonal projectors (or projection operators) denoted by $\{\hat{P}_x\}$, where each projector is a linear operator satisfying $\hat{P}_x^2 = \hat{P}_x$ and $\hat{P}_x^\dagger = \hat{P}_x$ (Hermitian) on a Hilbert space $\mathcal{H}$, hence $\hat{P}_x = \hat{M}_x \hat{M}_x^\dagger$

and the completeness relation for projective measurements is $\sum_{x\in X}\hat{P}_x = \mathbb{1}$. Thus, the probability of obtaining an outcome x for the given state ρ when a projective measurement is performed is given by

$$p(x|\rho) = \mathrm{Tr}\left[\hat{P}_x\rho\right], \tag{2.25}$$

Note that the action of a projector on a state $|\psi\rangle \in \mathcal{H}$ is to project $|\psi\rangle$ itself, which can be written in an orthonormal basis $\{e_i\}$ as $\hat{P} = \sum_i |e_i\rangle\langle e_i|$ onto a subspace of $\mathcal{H}$.

In prepare-and-measure QKD, the aim is to generate measurement statistics at Bob's apparatus from Alice's states and build a correlation between their prepared and measured instances. There is no interest in knowing the post-measurement state of the system, what matters is Bob's outcomes. In practice, not all measurements correspond to orthogonal projectors, thus the formalism of Bob's quantum measurement is described by a positive-operator-valued measure (POVM), which provides a more general framework.

A positive operator-valued measure (POVM) is a measure whose values are positive semi-definite operators $\{\hat{E}_x\}$ on a Hilbert space. This collection of measurement operators are Hermitian, positive semi-definite $\hat{E}_x \geq 0$, and also satisfy the completeness relation $\sum_{x\in X}\hat{E}_x = \mathbb{1}$. Unlike projective measurements, POVMs allow for a broader range of measurements, including those that can be implemented through indirect measurements or those that are inherently probabilistic and cannot be described by a simple projection onto an orthogonal subspace. This generalisation is crucial to cover the full range of quantum measurement processes in quantum information theory. The probability of obtaining a certain outcome for a POVM is also described by Eq. (2.25).

Consider a quantum system S, *Naimark's theorem* provides a connection between POVMs and projective measurements by stating that any POVM on a Hilbert space $\mathcal{H}_S$ can be realised as a projective measurement on an extended Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_E$. Formally, given a set of POVMs $\{\hat{E}_k\}$ on $\mathcal{H}_S$, there exists a projective measurement

$\{P_x\}$ on $\mathcal{H}_S \otimes \mathcal{H}_E$ and an isometry $\hat{V} : \mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_E$ such that

$$\hat{E}_x = \hat{V}^\dagger (\mathbb{1}_{\mathcal{H}_S} \otimes \hat{P}_x) \hat{V}. \tag{2.26}$$

This result demonstrates that any POVM can be interpreted as a measure arising from a projective measurement on a larger system, with the ancillary system on $\mathcal{H}_E$ representing additional degrees of freedom that are not directly observed.

2.1.6 Quantum Channels

A quantum channel is a communication channel able to transmit quantum information from a sender to a receiver. For a given input the channel maps it probabilistically to an output, i.e. it is a stochastic mapping, contrary to a deterministic transformation. Therefore, a quantum channel describes of the physical evolution of an open quantum system interacting with an ancillary system, often interpreted as the environment or a measurement process. When the outcomes of a POVM are discarded, we describe this as unconditional evolution.

Formally, a quantum channel is a linear and completely positive trace-preserving (CPTP) map $\mathcal{E}$, which can be generally defined as follows.

Definition 2 *(Quantum channel map). Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be the Hilbert spaces of Alice and Bob, respectively. The map of the quantum channel is defined as $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$, where Alice's $\rho_A \in \mathcal{B}(\mathcal{H}_A)$ and Bob's $\rho_B \in \mathcal{B}(\mathcal{H}_B)$ density operators satisfy $\rho_B = \mathcal{E}(\rho_A)$.*

Note the ball $\mathcal{B}(\mathcal{H})$ represents the set of density operators, which is convex, meaning any convex combination of density operators is also a valid density operator. Consequently, let us introduce the definitions of the properties that a quantum channel or CPTP map must fulfill.

Definition 3 *(Linearity). The quantum channel map $\mathcal{E}$ is linear if*

$$\mathcal{E}(\alpha\hat{\rho}_A + \beta\hat{\sigma}_A) = \alpha\mathcal{E}(\hat{\rho}_A) + \beta\mathcal{E}(\hat{\sigma}_A) = \alpha\hat{\rho}_B + \beta\hat{\sigma}_B \tag{2.27}$$

for $\alpha, \beta \in \mathbb{C}$.

A quantum channel must preserve positive semi-definite operators to ensure it maps density operators to density operators, meaning it must be a positive map.

Definition 4 *(Positivity). Let* $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *be the Hilbert spaces of the parties. The quantum channel map* $\mathcal{E}$ *is positive if* $\rho_B = \mathcal{E}(\rho_A)$ *is positive semi-definite* $\forall \rho_A \in \mathcal{B}(\mathcal{H}_A)$*, which are positive semi-definite operators.*

In general, a map is positive if it maps positive elements to positive elements. In this case, these positive elements can be interpreted as the density operators described in Definition 4. However, this is not sufficient, we require the quantum channel map $\mathcal{E}$ to be completely positive, to guarantee the consistency of quantum state evolution and to ensure that operations are well-defined irrespective of how the composite system is partitioned. This prevents inconsistencies or non-physical states on subsystems, which are not positive semi-definite. Hence, the required complete positivity is stated as follows.

Definition 5 *(Complete positivity). The quantum channel map* $\mathcal{E}$ *is completely positive if the map*

$$\mathbb{1}_n \otimes \mathcal{E} : \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{B}(\mathcal{H}_B) \tag{2.28}$$

is positive $\forall n \in \mathbb{N}$*, where* $\mathbb{1}_n$ *denotes the identity map in* $\mathbb{C}^n$.

Finally, trace preservation is also needed to ensure the quantum channel maps density operators to density operators.

Definition 6 *(Trace preservation). The map* $\mathcal{E}$ *is trace preserving if* $\mathrm{Tr}\left[\rho_A\right] = \mathrm{Tr}\left[\mathcal{E}\left(\rho_A\right)\right] = \mathrm{Tr}\left[\rho_B\right]$ *for* $\rho_A \in \mathcal{B}(\mathcal{H}_A)$.

To sum up, the completely positive property of the quantum channel is an important requirement because certain quantum states can generate negative eigenvalues of the matrix after applying a positive operator, e.g. applying the transpose operation to a Bell state constructing its density operator (see Section 2.2.2. of [ramona qkd]). However, if the operation applied by the quantum channel map is completely positive, it ensures

that the transformation generates valid matrices with positive eigenvalues, satisfying the properties of a density operator. Therefore, the quantum channel preserves positive eigenvalues, taking density matrices to density matrices. Additionally, the noise of the quantum channel must be trace-preserving. This ensures the preservation of the total probability of the quantum system, hence having a quantum analogue to a stochastic map. The stochastic effect of this map can be interpreted as the intrinsic quantum noise of the channel.

To represent the effects of a quantum channel $\mathcal{E}$, the Kraus operators $\{K_m\}$ are used. Thus, the action of $\mathcal{E}$ on a density matrix ρ can be expressed using a set of Kraus operators as

$$\mathcal{E}(\rho) = \sum_m \hat{K}_m \rho \hat{K}_m^\dagger \tag{2.29}$$

which satisfy the completeness relation $\sum_m \hat{K}_m \hat{K}_m^\dagger = 1$. In particular, these operators capture the influence of the interaction with the ancillary system, e.g. embedding the effects of decoherence and dissipation inherent in the system-environment coupling.

Furthermore, *Stinespring dilation theorem* describes how any CPTP map can be represented as a unitary evolution on an extended Hilbert space, followed by a partial trace over an ancillary system. Suppose the joint system SE interaction is described as a unitary operator $\hat{U} : \mathcal{H}_S \otimes \mathcal{H}_E \to \mathcal{H}_S \otimes \mathcal{H}_E$. Let the initial state of the ancillary system be $|e_0\rangle$ and $\rho = |\psi\rangle\langle\psi|$ the initial state of S. The combined state of the joint system is $\rho \otimes |e_0\rangle\langle e_0|$ and its evolution is defined as $\hat{U}(\rho \otimes |e_0\rangle\langle e_0|)\hat{U}^\dagger$. The reduced state of system S is obtained by tracing out the ancillary system as

$$\mathcal{E}(\rho) = \mathrm{Tr}_E \left[\hat{U}(\rho \otimes |e_0\rangle\langle e_0|)\hat{U}^\dagger \right]. \tag{2.30}$$

Expanding the initial ancillary state $|e_0\rangle$ in terms of an orthonormal basis $\{e_m\}$ of the space $\mathcal{H}_E$ on a decomposition of $\hat{U}(|\psi\rangle \otimes |e_0\rangle) = \sum_m (\hat{K}_m |\psi\rangle) \otimes |e_m\rangle$, we find the Kraus operators $\hat{K}_m$ as the relative states in this decomposition. Therefore, we can express Eq. (2.30) similarly to Eq. (2.29). Formally, this theorem is defined as follows.

Definition 7 *(Stinespring dilation theorem). Suppose the CPTP map* $\mathcal{E} : \mathcal{B}(\mathcal{H}_S) \to$

$\mathcal{B}(\mathcal{H}_S)$, where $\mathcal{B}(\mathcal{H}_S)$ denotes the space of the bounded linear operator on $\mathcal{H}_S$. There exists an auxiliary Hilbert space $\mathcal{H}_E$, a linear operator $\hat{V} : \mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_E$ and a unitary operator $\hat{U} : \mathcal{H}_S \otimes \mathcal{H}_E \to \mathcal{H}_S \otimes \mathcal{H}_E$, such that

$$\mathcal{E}(\rho) = \mathrm{Tr}_E \left(\hat{V} \rho \hat{V}^\dagger \right) \tag{2.31}$$

for all $\rho \in \mathcal{B}(\mathcal{H}_S)$, where $\hat{V} = \left(\mathbb{1}_{\mathcal{H}_S} \otimes \hat{W} \right) U$, being $\hat{W} : \mathcal{H}_S \to \mathcal{H}_E$ an isometry, hence they both fulfil the isometric condition $\hat{V}\hat{V}^\dagger = \mathbb{1}_{\mathcal{H}_S}$ and $\hat{W}\hat{W}^\dagger = \mathbb{1}_{\mathcal{H}_S}$, where $\mathbb{1}_{\mathcal{H}_S}$ is the identity operator on $\mathcal{H}_S$.

According to this theorem, any CPTP map on a density matrix ρ can be realised as in Eq. (2.30). Embedding the original system into this extended space, the quantum operations we perform in the extended space can be related to those in the original space. Therefore, a POVM on the original Hilbert space can be realised as a projective measurement on the extended Hilbert space, whose outcomes correspond to a POVM on the original system after tracing out the ancillary degrees of freedom.

2.2 Classical and Quantum Information Theory

Entropies are a relevant mathematical tool to characterise the uncertainty and information that an observer has about a physical system. In other words, the entropy can be interpreted as the amount of *randomness* quantifying the system from the observer's perspective. In this section, we first introduce the classical Shannon entropy, describing its purpose in classical information theory. This helps build an intuition of the entropy's role in the quantum world and points out the differences and similarities between the quantum von Neumann entropy and its classical counterpart. From the von Neumann entropy, we elaborate on the smooth entropies, which are crucial to derive the secure key length (SKL) in the finite-key analysis of BB84. Here, we also introduce the quantum mutual information and coherent information, which are essential for the channel capacities characterisation. We present the data *compression rate*, which estimates the minimum amount of bits required to reliably transmit a message in a single realisation for classical communication. This rate is related to the Shannon entropy in the *Shan-*

non's noiseless channel coding theorem. Additionally, we discuss the rate considering a noisy channel in Shannon's theorem. Finally, we review the channel capacities over noisy classical and quantum channels [50]. For the quantum channel, we also address its private capacity, which estimates how much classical information a sender can reliably and, more importantly, privately, transmit to a receiver. This is extremely relevant since it is the prior step to accurately estimate how many correlated classical key bits can be generated between Alice's and Bob's systems in the BB84 protocol.

2.2.1 Shannon Entropy

In classical information theory, Shannon introduced a method for quantifying the *redundancy* required to reliably communicate a message while preventing errors. Shannon's entropy quantifies the *randomness* or uncertainty of the states of a system, and it is also used to evaluate the *redundancy* in a message [51].

Consider a random variable X defined by an ensemble $X = \{x, p(x)\}$ where the outcomes x are the values of an alphabet A_X, which contains all possible outcomes. Concretely, $x = \{x_1, x_2, \ldots, x_N\}$ and their associated probabilities $p(x) = \{p(x_1), p(x_2), \ldots, p(x_N)\}$ satisfy $\Pr(X = x) = p(x) \geq 0$ and $\sum_{x \in X} p(x) = 1$. The Shannon entropy is defined as follows

$$H(X) = -\sum_{x \in X} p(x) \log p(x). \tag{2.32}$$

The Shannon entropy must satisfy the following properties [52]:

1. $H(X)$ must be continuous in $p(x)$.

2. Given N the number of possible values, if all the $p(x)$ are equal, $p(x) = 1/N$, then $H(X)$ must monotonically increase as a function of N.

3. Considering a system which some of its outcomes further evolves giving other final outcomes, hence making two successive choices, its entropy must be a weighted sum of the individual values. For instance, having a system with three different final outcomes $\{x_0, x_{1a}, x_{1b}\}$, if the system first generates two outcomes $\{x_0, x_1\}$ according to the distribution $\{1/3, 2/3\}$ and the outcome x_2 immediately evolves

to outcomes x_{1a} or x_{1b} according to $\{1/2, 1/2\}$. This property tell us that the weighted entropy must be given by

$$H(\{1/3, 1/3, 1/3\}) = H(\{1/3, 2/3\}) + \frac{2}{3}H(\{1/2, 1/2\}).$$

The *redundancy* is estimated as one minus the relative entropy, given by $1 - H(X)/H_{\max}(X)$, which represents the ratio between the actual Shannon entropy $H(X)$ of an ensemble X and its maximum possible entropy $H_{\max}(X) = \log |A_X|$, assuming a binary outcome possibility for each event [53]. This maximum is achieved by a source when the successive outcomes comprising a message can be chosen freely and occur with equal probability on average, i.e. $p(x_1) = p(x_2) = \cdots = p(x_N)$. Therefore, the entropy of a uniform random variable equals $\log |A_X|$, where $|A_X|$ is the size of the set of all possible outcomes. Thus, the entropy measures the information content of a random variable, represented by $-\log p(x)$.

Suppose there are two systems modelled by two random variables X and Y, the joint entropy is defined by

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y). \tag{2.33}$$

The conditional entropy measures the entropy of a system given the state of another system and is defined as

$$H(Y|X) = -\sum_{x,y} p(x, y) \log p(y|x). \tag{2.34}$$

Given a particular $X = x$, the conditional entropy becomes

$$H(Y|X = x) = -\sum_{y} p(y|x) \log p(y|x). \tag{2.35}$$

Thus, the conditional entropy in Eq. (2.34) can be expressed using Eq. (2.35) as

$$\begin{aligned} H(Y|X) &= -\sum_x p(x)p(y|x)\log p(y|x) \\ &= -\sum_x p(x)H(Y|X=x). \end{aligned} \tag{2.36}$$

Additionally, the conditional entropy can be written in terms of the joint entropy as

$$\begin{aligned} H(Y|X) &= -\sum_{x,y} p(x,y)\log\frac{p(x,y)}{p(x)} \\ &= -\sum_{x,y} p(x,y)\left[\log p(x,y) - \log p(x)\right] \\ &= H(X,Y) + \sum_x p(x)\log p(x) \\ &= H(X,Y) - H(X). \end{aligned} \tag{2.37}$$

Another fundamental measure in classical information theory, calculated using Shannon entropy, is the mutual information for the random variable X and Y

$$I(X;Y) = H(X) + H(Y) - H(X,Y), \tag{2.38}$$

which can also be expressed in terms of probabilities as

$$I(X;Y) = \sum_{x,y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}. \tag{2.39}$$

2.2.2 von Neumann Entropy

The von Neumann entropy $S(A)$, also denoted by $S(\rho)$, can be interpreted as the quantum generalisation of the Shannon entropy $H(A)$. It inherits its fundamental properties, thus characterising the uncertainty an observer has about the outcomes of a quantum system. The von Neumann entropy of a source represents the minimum number of qubits, i.e. at least $S(A)$ qubits, required for reliable communication in the encoding and decoding of each quantum state. In other words, the size of the code must be at least as great as the von Neumann entropy of the source.

Describing the state of a quantum system A by a density matrix ρ, the von Neumann entropy is defined as [54]

$$S(A) = S(\rho) = -\mathrm{Tr}\left[\rho \log \rho\right] \tag{2.40}$$

where ρ is a Hermitian matrix, which can be expressed by spectral decomposition as in Eq. (2.7), substituting this equation of the density matrix ρ into Eq. (2.40), we obtain

$$S(\rho) = -\mathrm{Tr}\left[\sum_i \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \log \left(\sum_j \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right|\right)\right] \tag{2.41}$$

$$= -\mathrm{Tr}\left[\sum_{i,j} \lambda_i \log(\lambda_j) \left|\psi_i\right\rangle \left\langle\psi_i|\psi_j\right\rangle \left\langle\psi_j\right|\right] \tag{2.42}$$

$$= -\sum_i \lambda_i \log(\lambda_i) \mathrm{Tr}\left[\left|\psi_i\right\rangle \left\langle\psi_i\right|\right] \tag{2.43}$$

$$= -\sum_i \lambda_i \log(\lambda_i) \tag{2.44}$$

$$= H(\{\lambda_i\}), \tag{2.45}$$

where the coefficients λ_i are the eigenvalues of ρ and $|\psi_i\rangle$ are the eigenvectors. Suppose the same system as in Shannon entropy of Section 2.2.1, described by a random variable X with probability $p(x)$ when $X = x$, then the entropy of the system using Eq. (2.44) is equivalent to the Shannon entropy in Eq. (2.32).

Suppose ρ_{AB} is the state describing the composite system AB, then the conditional von Neumann entropy is defined as [55]

$$S(B|A) = S(AB) - S(A) \tag{2.46}$$

similarly to the conditional Shannon entropy of Eq. (2.37). Moreover, the quantum mutual information between the quantum subsystems A and B is defined as

$$I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}), \tag{2.47}$$

If one considers classical random variables X and Y instead of the quantum subsystems A and B, the quantum mutual information has a one-to-one correspondence to Eq. (2.38).

2.2.3 Smooth Min- and Max-Entropy

The von Neumann entropy has been extremely successful in characterising a wide range of quantum information theory tasks. For instance, it will be highly useful to estimate the key rate of the BB84 protocol in the asymptotic limit in Section 3.6.1. However, in finite-key analysis, when the parties deal with a finite block of statistics, the use of the von Neumann entropy is no longer justified. A new entropy was required to deal with finite statistics in QKD, which was also driven by other applications in alternative areas of physics. Consequently, the formalism of the smooth min- and max-entropies, denoted by $H_{\min}^{\varepsilon}$ and $H_{\max}^{\varepsilon}$, were introduced in [56,57] and further developed in [58,59]. The positive value ε determines the desired accuracy when these entropies are used to characterise an operational task. Here, we present the smooth entropy definitions following [48].

In QKD, Alice and Bob aim to bound the smooth min-entropy of Alice's subsystem A conditioned on Eve's system E. This quantity, denoted by $H_{\min}^{\varepsilon}(A|E)_{\rho}$, characterises the number of fully mixed qubits that can be extracted from Alice's quantum source in A and are independent of side information E. Furthermore, in QKD, one must assume the worst-case scenario, where the composite system between Alice and Eve AE is in a pure state. Thus, Eve's system E holds all possible correlations with A, commonly called a *purifying system*. This purification is applied as described in Definition 1.

Let us first introduce the definitions of min- and max-entropies [duality]. For the complete definition of the sets of normalised quantum states $\mathcal{S}_{=}(\mathcal{H})$ and subnormalised states $\mathcal{S}_{\leq}(\mathcal{H})$, see Eqs. (2.9) and (2.10), respectively.

Definition 8 *(Min-entropy). Let $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ be the state of the composite system between Alice and Bob, the min-entropy of A conditioned on B is defined as*

$$H_{\min}(A|B)_{\rho} = \max_{\sigma_B \in \mathcal{S}_{\leq}(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} : 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \geq \rho_{AB}\} \tag{2.48}$$

Definition 9 *(Max-entropy). Let the state $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ and $\rho_{ABC} \in \mathcal{S}_{\leq}(\mathcal{H}_{ABC})$ an arbitrary purification (see Definition 1) of ρ_{AB}, i.e. ρ_{ABC} is pure, the max-entropy of A conditioned on B of ρ_{AB} is defined as*

$$H_{\max}(A|B)_{\rho} = -H_{\min}(A|C)_{\rho}. \tag{2.49}$$

Using the min- and max-entropies we can define the ε-smooth entropies, which depend on the *smoothing parameter* ε that determines the desired accuracy. These can be interpreted as a generalisation of the von Neumann entropy. To obtain these smooth entropies, an optimisation is applied to the non-smooth entropies over a ball which is ε-close to the states ρ using the purified distance. This ball of states is defined as follows.

Definition 10 *(Ball of states). Let $\varepsilon \geq 0$ and a state $\rho \in \mathcal{S}_{\leq}(\mathcal{H})$ with $\mathrm{Tr}\,[\rho] > \varepsilon^2$. We define an ε-ball of operators on the Hilbert space $\mathcal{H}$ around a state ρ as follows,*

$$\mathcal{B}^{\varepsilon}(\rho) = \{\tau \in \mathcal{S}_{\leq}(\mathcal{H}) : P(\rho, \tau) \leq \varepsilon\} \tag{2.50}$$

where $P(\rho,\tau) = \sqrt{1 - \bar{F}(\rho,\tau)}$ is the purified distance and the generalised fidelity is given by $\bar{F}(\rho,\tau) = ||\sqrt{\tau}\sqrt{\rho}|| + \sqrt{(1 - \mathrm{Tr}\,[\rho])\,(1 - \mathrm{Tr}\,[\tau])}$.

Definition 11 *(Smooth min-entropy). Let $\varepsilon \geq 0$ and the state $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$, the ε-smooth min-entropy of A conditioned on B of ρ_{AB} is defined as*

$$H^{\varepsilon}_{\min}(A|B)_{\rho} = \max_{\sigma_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\sigma} \tag{2.51}$$

This entropy is monotonically increasing in ε and the non-smooth entropy can be recovered simply by $H^{\varepsilon=0}_{\min}(A|B)_{\rho} = H_{\min}(A|B)_{\rho}$.

Definition 12 *(Smooth max-entropy). Let $\varepsilon \geq 0$ and the state $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$, and $\rho_{ABC} \in \mathcal{S}_{\leq}(\mathcal{H}_{ABC})$ an arbitrary purification of ρ_{AB}, the ε-smooth max-entropy of X conditioned on Y of ρ_{AB} is defined as*

$$H^{\varepsilon}_{\max}(A|B)_{\rho} = -H^{\varepsilon}_{\min}(X|C)_{\rho} \tag{2.52}$$

The non-smooth entropy can be recovered by $H_{\max}^{\varepsilon=0}(A|B)_\rho = H_{\max}(A|B)_\rho$.

The smooth min-entropy and max-entropy are completely independent of the Hilbert spaces where their density operators are represented locally. Finally, considering an independent and identically distributed (i.i.d.) state $\rho^{\otimes N}$, which is not a required condition for the states of the smooth entropies, one can recover the von Neumann entropies from the smooth entropies using the asymptotic equipartition property (AEP) as follows [60]

$$S(A|B) = \lim_{\varepsilon\to 0}\lim_{N\to\infty}\frac{1}{N}H_{\min}^{\varepsilon}(A^N|B^N)_{\rho^{\otimes N}} \tag{2.53}$$

$$S(A|B) = \lim_{\varepsilon\to 0}\lim_{N\to\infty}\frac{1}{N}H_{\max}^{\varepsilon}(A^N|B^N)_{\rho^{\otimes N}}. \tag{2.54}$$

2.2.4 Coherent Information

The coherent information measures the entropy difference between the initial and output quantum states after passing through a quantum channel [61]. Its interpretation parallels that of mutual information in classical information theory.

Before defining the quantum coherent information, we first introduce the concept of *entropy exchange* between Alice's system A and Bob's output system B, through the quantum channel $\mathcal{E}$. To do this, we introduce a reference system R to purify the initial state. Suppose the initial quantum system RA, i.e. the joint system of Alice's and the reference systems, is in a pure entangled state $|\psi_{RA}\rangle$. The density matrix of Alice's system is obtained by taking the partial trace over the reference system

$$\rho_A = \mathrm{Tr}_R\left[|\psi_{RA}\rangle\langle\psi_{RA}|\right]. \tag{2.55}$$

We also introduce an environment system E, initially in a pure state $|0\rangle_E$, though other choices are possible. The role of E is primarily as a mathematical artifice, while the focus remains on the dynamics of A. It is important to note that the reference system R is completely isolated from the environment E.

The initial pure state of the joint system RAE is $|\psi_{RAE}\rangle = |\psi_{RA}\rangle \otimes |0\rangle_E$. After

transmission through the quantum channel, Bob receives the mixed output state

$$\rho_{RAE} = (\mathbb{1}_R \otimes \mathcal{E}_A \otimes U_E) \left(|\psi_{RAE}\rangle \langle \psi_{RAE}| \right), \tag{2.56}$$

where A, $\mathcal{E}(A) = B$ is the quantum channel unitary transformation and also $U_E \left(|0\rangle_E \right) = |0\rangle_E$. The entropy acquired by the joint system RA after the evolution of the initial states ρ_A under the channel's action is known as the *exchange entropy*, and it is given by

$$S_{\mathrm{e}} = S_{\mathrm{e}} \left(\rho_A : \mathcal{E}(\rho_A) \right) = S \left(\rho_{RB} \right), \tag{2.57}$$

which can be interpreted as the von Neumann entropy of the output system RB. This entropy of the bipartite state ρ_{RB} can also be expressed in terms of the initially pure environment after transformations $S \left(\rho_{RB} \right) = S \left(\rho_E \right)$. It is worth noting that this entropy exchange is analogous to the classical conditional entropy, although here we keep the quantum interpretation.

Using Eq. (2.57), the quantum coherent information of a quantum channel $\mathcal{E}$ is defined as [50]

$$\begin{aligned} I_{\mathrm{c}} \left(\rho_A : \mathcal{E}(\rho_A) \right) &= S(\mathcal{E}(\rho_A)) - S_{\mathrm{e}}(\rho_A : \mathcal{E}(\rho_A)) \\ &= S \left(\rho_B \right) - S(\rho_{RB}) \\ &= S \left(\rho_B \right) - S \left(\rho_E \right) \end{aligned} \tag{2.58}$$

We employ the *Stinespring dilation theorem*, as defined in Theorem 7, which facilitates the understanding of coherent information by providing the structural framework to model the quantum channel as a unitary interaction with the ancillary system, here the environment. This is essential for analysing how much information is distributed between the system and the environment. Applying the theorem, the action of the quantum channel $\mathcal{E}$ on ρ_A can be represented as

$$\mathcal{E}(\rho_A) = \mathrm{Tr}_E \left[U(\rho_A \otimes |0\rangle_E \, {}_E\langle 0|) U^\dagger \right] \tag{2.59}$$

which describes how the state ρ_A interacts with the environment E and serves as the

input of the first von Neumann entropy in Eq. (2.58), reflecting how much information is contained in the output state.

We use ρ_A as we consider a purification $|\psi_{RA}\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A$ of the state $\rho_X \in \mathcal{B}(\mathcal{H}_A)$, such that $\rho_A = \mathrm{Tr}_R(|\psi_{RA}\rangle \langle\psi_{RA}|)$. The complete initial system evolves as

$$(\mathcal{I} \otimes \mathcal{E})(|\psi_{RA}\rangle \langle\psi_{RA}|) = \mathrm{Tr}_E \left[(\mathbb{1}_R \otimes U)(|\psi_{RA}\rangle \langle\psi_{RA}| \otimes |0\rangle_{E\,E}\langle 0|)(U \otimes \mathbb{1}_R)\right] = \rho_{RB} \tag{2.60}$$

where $\mathcal{I}$ is the identity superoperator on the reference system R and $\mathbb{1}_R$ is the identity operator on $\mathcal{H}_R$. This state, identified as ρ_{RB}, serves as the input of the second von Neumann entropy in Eq. (2.58), which reflects how much information is lost to the environment E.

The coherent information can also be expressed as $I_{\mathrm{c}}(\rho_A : \mathcal{E}(\rho_A)) = I_{\mathrm{c}}(\rho_{AB}) = I_{\mathrm{c}}(A : B)$. If the state $|\psi_{RA}\rangle$ is maximally entangled and the quantum channel $\mathcal{E}$ is noiseless, i.e. it operates as the identity $\mathcal{E} = \mathcal{I}$, the quantum coherent information reaches its maximum value, $I_{\mathrm{c}}(\rho_{AB}) = H(\rho_B)$, since the following conditions are fulfilled $H(\rho_A) = H(\rho_B)$ and $H(\rho_{AB}) = 0$.

2.2.5 Data Compression

Data compression was introduced to eliminate unwanted *redundancy*, thereby reducing the number of bits required to encode a given amount of Shannon information [62]. Consider a source that emits a set of independent and identically distributed (i.i.d.) random variables X with a probability distribution that satisfies $\Pr(X = x) = p(x)$. With i representing the i-th outcome, the i.i.d. assumption implies that each random variable $X_i = \{x_i, p(x_i)\}$ follows the same distribution as X.

Shannon's noiseless channel coding theorem asserts that in the asymptotic limit, when the number of source outcomes $N \to \infty$, the source distributing X must be encoded with a *compression rate* greater than or equal to $H(X)$. In other words, a lossless data compression scheme cannot, on average, compress messages to fewer than one bit of Shannon information per bit of encoded message. Formally, $\ell^{\varepsilon}(X)$ represents the minimum number of required bits to compress X with no information loss, with

failure probability ε, i.e. the number of noiseless channel bits. Thus, the *compression rate* is given by

$$r_{\text{compr}}(X) := \lim_{\varepsilon \to 0} \lim_{N \to \infty} \frac{\ell^{\varepsilon}(X)}{N} = \lim_{\varepsilon \to 0} \lim_{N \to \infty} \frac{NH(X)}{N} = H(X). \tag{2.61}$$

This result demonstrates that there exists a compression scheme for a noiseless channel such that the information prepared by the source can be encoded by $H(X)$ bits per source outcome. This rate is proven to be optimal, hence compressing beyond this point will lead to a high probability of errors when recovering the original message. This result provides an operational interpretation of Shannon entropy and the proof of optimality can be found in Chapter 18 of [63].

Thus, Shannon entropy is instrumental in characterizing the *randomness* in data compression tasks, which is related to information reconciliation tasks. Reconciliation aims to transform correlated classical values x and y, belonging to different parties, into pairs of fully correlated strings, while minimizing the amount of leaked information to an eavesdropper. This aligns with the objective of QKD, which seeks to establish correlations between Alice's and Bob's instances. Specifically, this is accomplished during the basis reconciliation step in the BB84 protocol, where the parties share their basis choices to discard events with unmatched bases and construct their sifted key, which contains identical outcomes for both parties. [1]

2.2.6 Channel Capacity

The capacity of a channel describes the capability of a sender, Alice, to transmit information to a receiver, Bob, over a noisy channel in a reliable manner, meaning the receiver can accurately recover the original message. An ideal channel is a lossless channel that acts as an identity map, perfectly preserving the transmitted information. However, such an ideal channel is not realistic in practice. This section discusses how a noisy channel affects the amount of information that can be reliably transferred.

First, we introduce *Shannon's noisy channel coding theorem*, which defines the chan-

[1] Further classical post-processing steps are necessary to achieve an identical string of key bits shared by the parties in a QKD protocol. For more details, see Section 3.6.

nel capacity of a noisy classical discrete memoryless channel (DMC), as detailed in Section 2.2.6.1. The *channel coding theorem* exploits *redundancy* to ensure reliable communication. Alice sends repeated information bits through the classical channel so that Bob can mitigate errors by comparing the received bits and selecting the redundant ones. This theorem defines the classical capacity of a classical channel, providing an upper bound on the number of classical bits that can be reliably transmitted per channel use with an arbitrarily small error probability at Bob's end. This capacity can be expressed by the mutual information between the parties over the possible distributions chosen by Alice.

Next, we discuss the classical capacity of a quantum channel, which was elucidated by Schumacher and Westmoreland, and later by Holevo. Their work, known as the *Holevo-Schumacher-Westmoreland (HSW) theorem* [64, 65], is a generalization of *Shannon's noisy channel coding theorem*, extending it from classical to quantum noisy channels. The *HSW theorem* demonstrates that is possible to transmit classical information reliably through a noisy quantum channel. Schumacher and Westmoreland showed the maximum amount of classical information that Alice can securely transmit to Bob through a quantum channel is quantified by the quantum mutual information in a one-time pad cryptographic scheme, as derived in Section 2.2.6.2. These results are relevant in QKD since its protocols aim to securely send classical bits encoded in quantum states. However, to ensure that an adversary cannot reliably access the encoded information transmitted through the quantum channel without revealing their presence, the additional requirement of *secretly* transmitting the classical information is needed. Therefore, the rate at which Alice can *privately* send classical information to Bob's quantum systems is quantified by the private classical capacity in Section 2.2.6.3. Note the concepts of *secretly* and *privately* can be used interchangeably.

2.2.6.1 Classical Capacity of a Noisy Classical Channel

Here, we evaluate the impact on the capacity of a noisy classical channel. Shannon entropy quantifies the required memory to store the compressed data of a source or the capacity of a channel, characterising the amount of information contained in the

system. Shannon demonstrated that even a given noisy classical channel can be utilized for reliable communication at a non-zero rate in the asymptotic limit when the channel is used an infinite number of times. This is encapsulated in *Shannon's noisy channel coding theorem*, which provides the optimal attainable rate for a discrete memoryless channel (DMC) [66].

First, we define the properties of a DMC as follows. Let $x = \{x_0, x_1, \ldots, x_k, \ldots, x_K\} \in X$ be Alice's inputs with the a priori probabilities $\{p(x_0), p(x_1), \ldots, p(x_k), \ldots, p(x_K)\}$ and $y = \{y_m\}_{m=1,2,\ldots,M} \in Y$ represent Bob's outputs with probabilities $\{p(y_m)\}$, received after transmission through the channel. The transition probabilities are given by $0 \leq p(y_m|x_k) \leq 1$. Therefore, the DMC is described by the *channel matrix*, also called the *transition matrix*, of size $K \times M$, which contains all the possible transition probabilities. The rows of the matrix correspond to the inputs and the columns to the outputs of the classical channel. The sum of the elements in each row of the *channel matrix* satisfies $\sum_{k=0}^{K} p(y_m|x_k) = 1$.

Definition 13 *(Discrete memoryless channel). The channel $\mathcal{N}$ is a DMC if it is discrete, i.e. X and Y are finite sets, and if it is memoryless, i.e. it satisfies the following conditions:*

1. The joint probability of transmitting x_k and receiving the output y_m, belonging to their respective random variables X and Y, can be defined as

$$p(x_k, y_m) = p(y_m|x_k)p(x_k). \tag{2.62}$$

2. The marginal probability distribution $p(y_m)$ of any output $y_m \in Y$ can be calculated by averaging the dependence of the known elements of the channel matrix $p(y_m|x_k)$ on x_k given the input a priori probabilities $p(x_k)$ as follows

$$p(y_m) = \sum_{k=0}^{K} p(y_m|x_k)p(x_k). \tag{2.63}$$

This definition ensures the noise introduced by the channel has no memory and acts independently across time. In other words, any particular output y_k depends only on

its corresponding kth-input x_k and is completely independent of any previous inputs.

Once the properties of a discrete memoryless channel are established, we address Shannon's theorem [67].

Theorem 1 *(Shannon's noisy channel coding theorem). Consider a discrete memoryless channel with input X sent by Alice and output Y received by Bob with channel capacity*

$$C(\mathcal{N}) := \max_{p(x)} I(X:Y), \tag{2.64}$$

where $I(X:Y)$ is the mutual information shared by Alice and Bob, maximised over the possible input distributions $p(x)$ of the random variable X.

For any $\varepsilon > 0$ and rate $R < C$, there exists a code of length N, assuming a sufficiently large N, with a rate $r \geq R$ and a decoding algorithm such that the maximum error probability is $\varepsilon_{\max} < \varepsilon$. Conversely, if $R > C$, it is not achievable, as the probability of successfully decoding approaches zero exponentially as the number of channel uses increases.

It is important to note that the classical channel capacity $C(\mathcal{N})$ of the classical channel $\mathcal{N}$ depends solely on the conditional probabilities $p(y_m|x_k)$, which represents the probability of Bob receiving y_m given that x_k was sent by Alice. The mutual information depends not only on $p(y_m|x_k)$ but also on the prior probabilities $p(x)$. Shannon showed that the rate cannot exceed the channel capacity, and the error probability approaches zero as the length of the message $N \to \infty$.

2.2.6.2 Classical Capacity of a Noisy Quantum Channel

We have analysed the information transfer through noisy classical channels. Here, we explore the limitations of the classical channel capacity when sending classical information via quantum channels. This is particularly relevant to the BB84 protocol, where Alice encodes her string of classical bits by exploiting physical quantum properties and transfers her generated qubits through a quantum channel.

Here, we present the HSW (Holevo-Schumacher-Westmoreland) capacity $C(\mathcal{E})$, also called the *product-state* classical capacity, determined by the *HSW theorem* [64,68]. We

also point out its similarities with the capacity $C(\mathcal{N})$ of a noisy classical channel $\mathcal{N}$. The HSW capacity $C(\mathcal{E})$ represents the maximum transmittable classical information through a noisy quantum channel $\mathcal{E}$, thoroughly defined in Section 2.1.6, and is a natural extension of the capacity of a classical channel to the quantum world. Notably, the HSW capacity discussed here refers to the *unentangled* version, where no entangled states are used.

In a *one-time pad* cryptographic scheme, the key has a single use, hence its value lies in the amount of information it can encrypt. This scheme will be addressed in detail in Section 3.3. To derive the bound for the amount of classical information Alice can send to Bob, we examine a quantum system analogue to a *one-time pad* scheme, as proposed in [69].

Suppose Alice and Bob shared the average initial state ρ^{AB} of their correlated composite quantum system AB. Alice encodes a string of classical bits, i.e. the key, by performing operations denoted by ξ^A with probability p_ξ. Consequently, Alice generates the new state $\sigma_\xi^A = \xi^A(\rho^A)$ and transfers it to Bob. The eavesdropper, Eve, can only access Alice's system A, hence to be secure, Alice must ensure her subsystem does not provide information to Eve. The parties aim to upper bound the classical information contained in their final state $\sigma^{AB} = \sigma^A \otimes \rho^B$. This quantity is known as the Holevo information χ^{AB} [70], and Alice and Bob aim to ensure $\chi^{AB} > 0$. The correlations within ρ^A enable the parties to communicate.

From the initial state shared by the parties ρ^{AB}, Alice generates the following new state performing the operation ξ

$$\sigma_i^{AB} = \left(\xi_i^A \otimes \mathbb{1}^B\right) \rho^{AB}, \tag{2.65}$$

which on average over the possible Alice's operations is $\sigma^{AB} = \sum_\xi p_\xi \sigma_\xi^{AB}$ defined by the ensemble $\{p_\xi, \sigma_\xi^{AB}\}$. For simplicity, we exclude the existence of an eavesdropper, assuming Eve cannot extract any classical information encoded by Alice, which means $\chi^A = 0$. Therefore, the information Alice can transmit to Bob is defined as the von Neumann entropy of the average quantum system minus the entropy of each operation

times its associated probability

$$\chi^{AB} = S\left(\sigma^{AB}\right) - \sum_{\xi} p_{\xi} S\left(\sigma_{\xi}^{AB}\right). \tag{2.66}$$

The ordinary subadditive property can be applied to the first entropy as follows

$$\chi^{AB} \leq S\left(\sigma^{A}\right) + S\left(\sigma^{B}\right) - \sum_{\xi} p_{\xi} S\left(\sigma_{\xi}^{AB}\right). \tag{2.67}$$

Alice's operation does not affect Bob's system, hence his state $\sigma^B = \rho^B$ remains unchanged and assuming there is no eavesdropper $\sigma_{\xi}^{A} = \sigma^{A}$ for all ξ,

$$\chi^{AB} \leq S\left(\rho^{B}\right) + \sum_{\xi} p_{\xi} \left[S\left(\sigma_{\xi}^{A}\right) - S\left(\sigma_{\xi}^{AB}\right)\right]. \tag{2.68}$$

The terms of the summation can be identified with the quantum coherent information. Using the definition in Eq. (2.58), consider the following coherent information $I_{\mathrm{c}}((\xi^A \otimes \mathbb{1}^B)\rho^{AB} : \xi^A(\rho^A)) = S(\xi^A(\rho^A)) - S((\xi^A \otimes \mathbb{1}^B)\rho^{AB} : \xi^A(\rho^A))$. Simplifying the notation of this equation, we obtain $I_{\mathrm{c}}(\sigma_{\xi}^{AB} : \sigma_{\xi}^{A}) = I_{\mathrm{c}}(AB : A) = S(\sigma_{\xi}^{A}) - S(\sigma_{\xi}^{AB})$. This entropy difference between Alice's state σ_{ξ}^{A} and the state shared by the parties σ_{ξ}^{AB}, both after Alice's operation, cannot be greater than the following initial entropy difference

$$I_{\mathrm{c}}(AB : A) \leq S(\rho^{A}) - S(\rho^{AB}), \tag{2.69}$$

otherwise, there would be an increment of the coherent information, which is not possible. Introducing this inequality in Eq. (2.68)

$$\chi^{AB} \leq S\left(\rho^{B}\right) + S\left(\rho^{A}\right) - S\left(\rho^{AB}\right) = I(A : B). \tag{2.70}$$

The classical information of a quantum system in a measurement is upper bounded by the quantum mutual information between Alice's and Bob's quantum systems $I(A : B)$, defined in eq. (2.47). This mutual information can also be interpreted as a measurement of the correlation degree in the initial state ρ_{AB} used to transmit information to Bob.

In other words, the maximum information Alice can reliably send to Bob is bounded by the quantum mutual information of their shared system. It is important to notice that this result, derived from the particular quantum-mechanical system proposed, can be directly extrapolated to a *one-time pad* scheme. To ensure the parties share an identical secret key, some additional classical information about Alice's preparation and Bob's measurement needs to be shared between them. Once they share the key, they can use it to send perfectly encrypted messages over a public channel.

For the *one-time pad* scheme, consider N qubits are needed to encode the classical bit string (key), which is equivalent to consecutively transmitting quantum states N-times through the quantum channel $\mathcal{E}$, denoted by $\mathcal{E}^{\otimes N}$. Supposing $N \to \infty$, *product input states*, and a single measurement setting on the receiver's side, the asymptotic classical capacity of the quantum channel $\mathcal{E}$ can be written as the maximum of the quantum mutual information

$$C(\mathcal{E}) = \max_{\{p_i,\rho_i\}} I(A:B), \tag{2.71}$$

over the ensembles of all possible input states $\{p_i, \rho_i\}$. Without loss of generality is the same as its single-use version ($N = 1$), hence $C(\mathcal{E}) = C^{(1)}(\mathcal{E})$. The classical capacity of a noisy quantum channel can also be expressed in terms of the Holevo information using Eq. (2.66)

$$\begin{aligned} C(\mathcal{E}) &= \max_{\{p_i,\rho_i\}} \chi^{AB} = \max_{\{p_i,\rho_i\}} \left[S(\rho^{AB}) - \sum_i p_i S(\rho_i^{AB}) \right] \\ &= \max_{\{p_i,\rho_i\}} \left[S\left(\sum_i p_i \rho_i^{AB} \right) - \sum_i p_i S\left(\rho_i^{AB} \right) \right]. \end{aligned} \tag{2.72}$$

If Alice transmits a classical bit string, representing the key that is encoded in the quantum states, through a noisy quantum channel at a rate of $R < C(\mathcal{E})$, there exists a quantum code with an arbitrarily small error probability that can transmit at that rate R, similar to the statement of *Shannon's noisy channel coding theorem* for a classical channel.

Additionally, the maximum attainable communication rate from Alice to Bob was

also analysed for a mixture of product states, different from the input states considered in the quantum-mechanical system presented here, where $\chi^{AB} \to I(A:B)$ is reached asymptotically considering a particular ensemble of Alice's operations in [69]. Proving the mutual information describes the secure communication rate without involving an eavesdropper in both classical and quantum channels.

2.2.6.3 Private Capacity of a Noisy Quantum Channel

The private classical capacity $C_P(\mathcal{E})$ of a noisy quantum channel $\mathcal{E}$ is essential in QKD to ensure that the parties share a secret key. This concept was first introduced by [71] and later by [72]. It describes the rate at which Alice can reliably and privately transmit classical information through the quantum channel. Here, *privately* means that no information about the message can be leaked to an eavesdropper, i.e. Eve's presence, aiming to access the encoded bit string, is reliably detected by the legitimate parties.

To estimate the private capacity, it is crucial to characterise and then discard the information that can be gained by Eve, assuming she fully controls the quantum channel $\mathcal{E}$ and has access to Alice's input states $\rho_A = \sum_i p_i \rho_i$. As shown in Section 2.2.6.2, the maximum classical information that can be extracted by Eve, or any other receiver, through a noisy quantum channel is quantified by the quantum mutual information $I(A:E)$. Eve's quantum system is denoted by E, with state ρ_E, and the output of the quantum channel received by Bob is $\mathcal{E}(\rho_A) = \rho_B$. Therefore, the single-use private classical capacity of the quantum channel can be expressed as the difference between the following quantum mutual information quantities

$$C_P^{(1)}(\mathcal{E}) = \max_{\{p_i,\rho_i\}} \left[I(A:B) - I(A:E) \right], \tag{2.73}$$

and in the asymptotic limit, it is given by

$$C_P(\mathcal{E}) = \lim_{N\to\infty} \frac{C_P^{(1)}(\mathcal{E}^{\otimes N})}{N} \tag{2.74}$$

$$= \lim_{N\to\infty} \frac{1}{N} \max_{\{p_i,\rho_i\}} \left[I(A:B) - I(A:E) \right]. \tag{2.75}$$

This result is used to calculate the asymptotic rate in the BB84 protocol (see Section 3.6.1), and it can also be written in terms of the Holevo information as

$$C_P(\mathcal{E}) = \lim_{N\to\infty} \frac{1}{N} \max_{\{p_i,\rho_i\}} \left[\chi^{AE} - \chi^{AB}\right], \tag{2.76}$$

where χ^{AB} is shown in Eq. (2.72) and

$$\chi^{AE} = S\left(\sigma^{AE}\right) - \sum_{\xi} p_\xi S\left(\sigma_\xi^{AE}\right). \tag{2.77}$$

Finally, while the maximised quantum mutual information is always additive for a quantum channel, the difference between two mutual information is not, nor is the Holevo information. Therefore, to compute the true private capacity, it has to be regularised in the asymptotic limit, i.e. $C_P(\mathcal{E}) \neq C_P^{(1)}(\mathcal{E})$, thus a regularisation is needed to calculate the asymptotic capacity from the single-use one, as shown in Eq. (2.74). In contrast to the capacities for noisy classical and quantum channels, where no regularisation is required, i.e. $C^{(1)}(\mathcal{N}) = C(\mathcal{N})$ and $C^{(1)}(\mathcal{E}) = C(\mathcal{N})$.

Chapter 3

Security of Quantum Key Distribution

Quantum key distribution has experienced substantial advancement over recent decades in both experimental and theoretical domains. To understand the reasons for this progress, we must address the foundational concepts underlying QKD protocols. Generally, QKD facilitates securely distributing an identical and secret key, formed by a classical bit string, between two distant parties over a public communication channel, see the illustration of Figure 3.1. This shared key by the parties can be used for secure encryption and decryption of messages. Unlike traditional cryptographic systems, the security of QKD does not rely on computational assumptions; instead, it is based on the strategy of the protocol, which fundamentally exploits principles of quantum mechanics. However, practical and technological challenges arise in real-world implementations, which means that the correctness and completeness of quantum physics alone are insufficient to guarantee the security of QKD. Sophisticated theoretical techniques, such as the decoy-state method or the finite-key analysis, have been proposed to address security loopholes arising from non-idealities, such as multiphoton contributions and finite block statistics.

We first examine the origins of QKD within the context of classical cryptography and the specific quantum principles that motivated the development of QKD as a method for secure key distribution. Second, we discuss a provably secure cryptographic

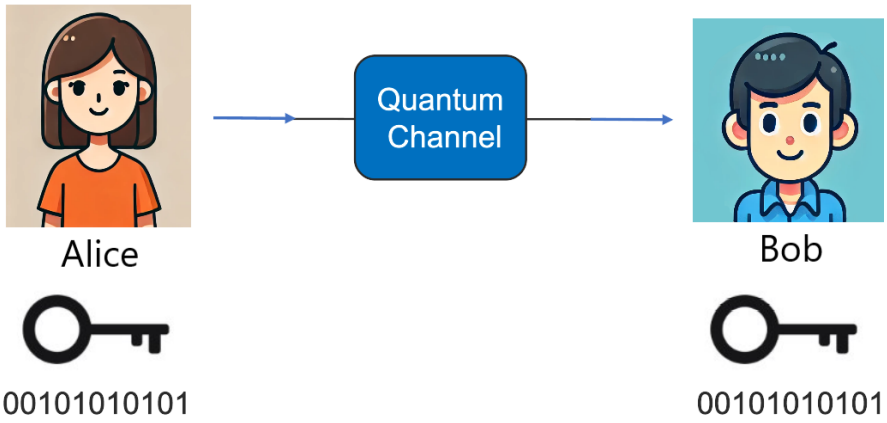

Figure 3.1: Aim of quantum key distribution. Alice and Bob share a secret and identical key after performing the protocol by transmitting the encoded key bits through a quantum channel.

scheme against general eavesdropper attacks, known as the *one-time pad* scheme, elaborating on the concept of the key in QKD and its crucial single-use property for achieving ever-lasting secure communication. Third, we outline the foundational assumptions required for QKD before introducing the security definition in QKD and the composable security framework in Section 3.5. We provide an overview of the Bennett-Brassard 1984 (BB84) QKD protocol. Lastly, we derive the asymptotic key rate of BB84 and highlight the importance of the decoy-state method to prevent photon number splitting (PNS) attacks before presenting the 2-decoy BB84 protocol with weak coherent pulses (WCPs).

3.1 Origins: Classical Cryptography

The concept of two distant parties exchanging secret messages by using a private key is ancient. For example, codes and ciphers have been historically utilised for centuries as classical encryption schemes [73]. A simple example is the *Caesar cipher*, where each letter of the original message is encrypted by shifting it to a certain number of positions in the alphabet. Thus, one constructs a cipher alphabet to create any cipher (encrypted) message. Secure communication relies on the parties knowing the strategy for constructing the cipher alphabet from the original alphabet. However, even if an

attacker does not know the relation between the original and cipher alphabets, they can computationally analyse the frequency use of the letters in the language of the original message, and deduce the correspondence between the original and cipher alphabets. More sophisticated encryption schemes than the *Caeser cipher*, such as the *Vigenere cipher*, which took centuries to crack, offered greater security. Despite this, classical schemes rely on the assumption that there is no effective algorithm or method to break them, thus the great desire for a cryptographic scheme that is provably unbreakable, commonly called in technical terms *information-theoretically secure*, without relying on computational assumptions or constraints about the attacker's capabilities.

The key is defined as the tool used to encrypt or decrypt the message. For instance, in the *Caeser cipher*, the key is the fixed number of positions by which the letters are shifted. Advanced classical public key cryptosystems have long proposed "secure" communication schemes between parties using two keys, one for encryption, randomly applying an operation whose mutually inverse is used for decryption. Although the encryption method can be publicly disclosed, the decryption instructions must remain confidential. This allows anyone to encrypt a message, then the parties can swap roles and converse secretly. In these classical public key systems, the private key cannot be guaranteed to be impervious to derivation from the encrypted message by computational methods. Thus, the security of classical cryptographic schemes relies on the computational difficulty of solving a "complicated" mathematical problem. This does not ensure ever-lasting secure communication, as the attacker can store the encrypted data and may eventually decrypt the message with improved algorithms or greater computational power. Furthermore, with the rapid progress in quantum computers, the security of currently deployed public key cryptosystems is in jeopardy [74–76], highlighting the desire to move towards quantum-secure communication methods that do not rely on the computational complexity assumptions. Consequently, QKD has emerged as a viable solution for distributing symmetric key pairs between distant parties, leveraging quantum physics.

Classical symmetric key ciphers, such as AES-256 [77] and the *one-time pad scheme*, explained in detail in Section 3.3, are foundational to cryptographic security. AES-256,

with its 256-bit key, is widely adopted for its robustness and efficiency, while *one-time pad* offers theoretical unbreakability when used correctly but faces significant practical challenges due to key management. In the context of QKD, AES-256 proves more practical as it leverages QKD for secure key distribution, ensuring strong security even under quantum attack. In contrast, *one-time pad*, despite its theoretical superiority, remains less feasible for widespread use due to the complexities of key generation and distribution [78].

3.2 Motivation

For the most widely deployed class of QKD methods, so-called prepare-and-measure protocols, Alice prepares specific quantum signal states and transmits them to Bob through the quantum channel. This channel is assumed to be under the control of an eavesdropper (Eve). In the original BB84 protocol, the polarisation degree of freedom of photons encodes the quantum signals used to generate the key, which must hold secret correlations between the parties. The motivation for employing QKD, particularly prepare-and-measure protocols, is based on two fundamental principles: *no-cloning theorem* and the *Heisenberg uncertainty principle*. These principles prevent Eve from extracting information about the encoded quantum state without being detected by Alice and Bob. To illustrate this, let us first demonstrate how quantum mechanics prohibits perfectly cloning an unknown quantum state.

Here, we present the general proof where an ancillary system is introduced. By contradiction, suppose Eve has access to a machine that perfectly clones quantum states, i.e. it copies an arbitrary quantum state $|\psi\rangle \in \mathcal{H}$ onto a fixed reference state that represents a fiducial state $|0\rangle \in \mathcal{H}$. Let $|C\rangle \in \mathcal{H}_C$ be the state of the ancillary system (the cloner). The following unitary operation represents the cloning action

$$\hat{U}_{\text{clone}} \left(|\psi\rangle \otimes |0\rangle \otimes |C\rangle \right) = |\psi\rangle \otimes |\psi\rangle \otimes |C'\rangle \,, \tag{3.1}$$

where $|C'\rangle$ is some possibly different state of the ancilla after the operation.

Consider two arbitrary quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$, any superposition of them is

given by $|\psi\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle$, where $\alpha, \beta \in \mathbb{C}$. Applying the linearity of the unitary $\hat{U}_{\text{clone}}$ and then Eq. (3.1) to the superposition state, we obtain

$$\begin{aligned}\hat{U}_{\text{clone}}(|\psi\rangle \otimes |0\rangle \otimes |C\rangle) &= \alpha\hat{U}_{\text{clone}}(|\psi_1\rangle \otimes |0\rangle \otimes |C\rangle) + \beta\hat{U}_{\text{clone}}(|\psi_2\rangle \otimes |0\rangle \otimes |C\rangle) \\ &= \alpha(|\psi_1\rangle \otimes |\psi_1\rangle \otimes |C_1\rangle) + \beta(|\psi_2\rangle \otimes |\psi_2\rangle \otimes |C_2\rangle).\end{aligned} \tag{3.2}$$

However, if $\hat{U}_{\text{clone}}$ were the operation of a perfect cloning machine, defined in Eq. (3.1), the result would be

$$\begin{aligned}\hat{U}_{\text{clone}}(|\psi\rangle \otimes |0\rangle \otimes |C\rangle) =&(\alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle) \otimes (\alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle) \otimes |C'\rangle \\ =&\big[\alpha^2\,|\psi_1\rangle \otimes |\psi_1\rangle + \alpha\beta(|\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\psi_2\rangle) \\ &+ \beta^2\,|\psi_2\rangle \otimes |\psi_2\rangle\big] \otimes |C'\rangle\,.\end{aligned} \tag{3.3}$$

For these two previous expressions, Eqs. (3.2) and (3.3), to be equal, we must have $|C_1\rangle = |C_2\rangle = |C'\rangle$, $\alpha\beta = 0$, $\alpha^2 = \alpha$ and $\beta^2 = \beta$. Thus, to simultaneously hold all these conditions either $\alpha = 1$ and $\beta = 0$, which corresponds to the state $|\psi\rangle = |\psi_1\rangle$, or $\alpha = 0$ and $\beta = 1$, which corresponds to the state $|\psi\rangle = |\psi_2\rangle$. However, these conditions contradict the assumptions that $|\psi\rangle$ is an arbitrary superposition as they cannot hold if α and β are arbitrary non-zero coefficients. Therefore, no unitary operator $\hat{U}_{\text{clone}}$ can clone an arbitrary quantum state, proving the *no-cloning theorem*. Hence, Eve cannot clone the unknown states transmitted by Alice and forward a perfect copy to Bob while gaining information about the key from the other copy.

Consequently, if Eve wishes to extract information, she must measure Alice's states and relay the measurement outcomes to Bob. However, due to the principles of quantum mechanics, this strategy is disadvantageous for Eve. Here comes the other motivation for QKD, the *Heisenberg uncertainty principle*, which asserts that any attempt by Eve to gain information about the key will inevitably disturb Alice's signal with some probability, introducing errors when Bob measures, thereby revealing Eve's presence. The uncertainty principle states that increasing the precision of measuring one observable (such as the position of a particle) increases the uncertainty in determining its conjugate observable (such as the momentum of a particle), and vice versa. This principle

applies to pairs of complementary variables, which cannot be simultaneously measured with perfect accuracy.

In the quantum realm of qubits, the uncertainty principle manifests in the rectilinear basis (Z basis) with qubits $|0\rangle$ and $|1\rangle$, and the diagonal basis (X basis) with qubits $|+\rangle$ and $|-\rangle$, which are introduced in Section 2.1.4. These two mutually unbiased (MU) bases are commonly employed in QKD protocols. Measurements corresponding to these conjugate bases do not commute, one cannot measure both observables simultaneously without disturbing the state, as stated by the *Heisenberg uncertainty principle*. The qubits in the rectilinear (diagonal) basis possess uncertainty in the diagonal (rectilinear) basis. Eve aims to determine the state Alice sends and because she cannot perfectly copy it, must measure it on a certain basis and forward the result to Bob. If Eve guesses the basis used by Alice to prepare the state incorrectly, she inevitably disturbs the state. For example, measuring a photon state diagonally polarized, either $|+\rangle$ or $|-\rangle$, using the rectilinear basis, the outcome is random, providing no information about the input state. We can illustrate this with cases where Eve chooses the opposite basis from Alice.

Consider the case where Alice sends the state $|0\rangle$ and Eve measures it on the X basis. The initial state is disturbed either obtaining $|+\rangle$ or $|-\rangle$. The probabilities for each outcome are calculated using the Born rule, which states that the probability of obtaining a state after measuring is the square of the amplitude of the initial system at that state, hence $p(\langle +|0\rangle) = |\langle +|0\rangle|^2 = 1/2$. Similarly, the probability of getting $|-\rangle$ as the outcome for a given $|0\rangle$ is also $p(\langle -|0\rangle) = 1/2$. For the other case where Alice transmits the state $|1\rangle$ and Eve measure in the X basis, the probabilities are the same, $p(\langle +|1\rangle) = p(\langle -|1\rangle) = 1/2$. Conversely, if Alice prepares either $|+\rangle$ or $|-\rangle$ and Eve measures in the Z basis, the probabilities of obtaining either $|0\rangle$ or $|1\rangle$ are also a half, i.e. $p(\langle 0|+\rangle) = p(\langle 0|-\rangle) = p(\langle 1|+\rangle) = p(\langle 1|-\rangle) = 1/2$.

When Eve intervenes and measures on the wrong basis, i.e. on the opposite basis of Alice's state, she always obtains a state that belongs to this opposite basis. Bob, expecting to share the same outcome as Alice if he uses the same basis, will find discrepancies if Eve has disturbed the state. This method to detect Eve's presence is

fundamental in QKD protocols, such as BB84, as detailed in Section 3.6. However, note that if Eve guesses the basis correctly, then both she and Bob obtain the same state, introducing no errors.

3.3 One-Time Pad Encryption Scheme

The *one-time pad* encryption scheme, also called the *Vernam cipher*, was introduced as a provably secure scheme by [79]. Before describing this cryptographic protocol, some useful technical aspects are necessary. In general, Alice and Bob aim to perfectly encrypt and decrypt classical messages, ensuring that a potential eavesdropper is unable to read them. They need a key to achieve this. Conceptually, the term *key* represents any strategy, set of rules, or device that provides a method to encrypt the message. Here, we consider a *key* in the form of a string of classical bits.

The steps of the *one-time pad* encryption protocol work as follows. First, suppose Alice an Bob share a key. Alice can encrypt the message M using her key K_A, e.g. performing a binary addition to obtain a ciphertext $C = M \oplus K_A$, which is the encrypted message. Bob receives this ciphertext through a public channel, which can be accessed by an eavesdropper. To obtain the message, Bob decrypts the ciphertext by performing the same operation as Alice, i.e. the following binary addition $M = C \oplus K_B$. In this ideal scenario, not considering any practical constraint, Bob obtains the exact same message as Alice if their keys are identical $K = K_A = K_B$, see proof in Section 1.2 of [46]. Note that the message, ciphertext and key are classical bit strings, $M, C, K \in \{0,1\}^n$, where n represents their length.

This encryption method was demonstrated information-theoretically secure by Shannon [80], meaning the ciphertext does not contain any information about the message M, when the key satisfies the following properties: it is actually random, with no correlations between the bits that formed the key; it has the same length as the message M; and it must be used only one time. If the latter is not fulfilled, an eavesdropper can gain some information about the messages that have used the same key. This can be shown as follows.

Suppose the parties use the same key K to encrypt two different messages M and

N. If the two generated ciphertext C_M and C_N can be accessed through the public channel, an eavesdropper can perform the operation $C_M \oplus C_N = M \oplus K \oplus N \oplus K$. Knowing the keys are equal it follows $K \oplus K = \{0\}^n$, hence $C_M \oplus C_N = M \oplus N$, which contains information about the original messages, contradicting the premise of an information-theoretically secure scheme.

3.4 Assumptions

To validate the aforementioned motivations, or in other words, to prove the security of a QKD protocol even in an idealised scenario where all experimental difficulties are neglected, some assumptions must be made regarding quantum theory and authentication between the communication parties. It is important to highlight that although these assumptions are not sufficient to ensure the security of QKD in practice, they are inevitably necessary. These foundational assumptions are:

1. Quantum theory is correct. If this theory is false, it is not possible to create a secure communication scheme as QKD, nor to estimate measurement outcomes accurately using quantum mechanics.

2. Free randomness is required to exist. This means that the encoding of classical bits into quantum states by Alice is independent of the quantum measurement performed by Bob. Furthermore, in prepare-and-measure protocols, it is required that the preparation of Alice's state is completely random, assuming the devices are trusted. This is not needed in device-independent QKD protocols.

3. Quantum theory is complete. If this theory is missing some phenomena, it can potentially be a security loophole that can be exploited to gain information about the key.

4. Authentication between Alice and Bob is possible. Otherwise, Eve could impersonate one of the parties without being detected.

Note that the free randomness requirement together with the correctness of quantum mechanics implies quantum theory is also complete. Apart from these assumptions,

there are multiple other considerations to be made to prove the security of an actual QKD experiment. Clearly, it is insufficient to prove security for an idealized scenario. In the last decade, security QKD proofs have become mature, bringing the theoretical model closer to the actual experiment. However, one must be cautious since any deviation of the QKD protocol implementation from the theory may cause a security loophole. A comprehensive examination of the assumptions made in quantum cryptography was conducted by [14, 81]. The most relevant assumptions are related to the isolation of Alice's and Bob's devices in their respective laboratories, Alice's preparation of her quantum states, Bob's measurement devices, classical post-processing, and timing. As mentioned before, device-independent QKD encompasses protocols that avoid dealing with the assumptions related to the laboratories and devices employed by the parties.

3.5 Definition of Security

Here, we introduce the concept of *security* in QKD. It is necessary to clarify the technological power of Eve to understand which types of eavesdropping attacks she is allowed to perform. For generic security proofs, Eve should be considered fully powerful, both computationally and technologically, and exclusively constrained by the laws of physics. In any case, it is always assumed that she is entitled to fully control the quantum communication channel used by Alice and Bob.

To prove the security of a QKD protocol, one might think it is sufficient to ensure that the information gathered by Eve about the key from Alice's system is insignificant. However, having a maximum value of the mutual information between Alice's and Eve's systems that is less than an arbitrarily small failure probability of the protocol, $\max I(A:E) \leq \varepsilon$, is not enough to ensure security.

Therefore, stronger criteria are needed to state that the key is safe for any arbitrary context and applications, which is technically called *universal security* [82]. The main idea behind this concept is to prove that there is almost no difference between an ideal protocol and the real one, i.e. they are indistinguishable except for an arbitrarily small probability $\varepsilon_{\mathrm{QKD}}$. Note that by definition the ideal protocol is perfectly secure.

This security criterion is defined by satisfying the following two requirements. First, Alice and Bob must possess an identical key, defined as a classical bit string, to say the protocol is *correct*, which formally obeys the following definition.

Definition 14 *(Protocol correctness). Let K_A and K_B be the keys held by Alice and Bob, respectively, formed by random bits strings $K_A, K_B \in \{0,1\}^N$. The QKD protocol is ε_{cor}-correct if*

$$\Pr(K_A \neq K_B) \leq \varepsilon_{\text{cor}}. \tag{3.4}$$

Second, the key shared by the parties should not be distributed to any other adversary (Eve) to say the protocol is *secret*. Suppose the secret key is correlated to Eve's quantum system E represented by the state ρ_E. The joint state between the legitimate parties and Eve is a *classical-classical-quantum* (ccq) state given by

$$\rho_{ABE} = \sum_{K_A,K_B} \Pr(K_A, K_B) \left|K_A\right\rangle \left\langle K_A\right| \otimes \left|K_B\right\rangle \left\langle K_B\right| \otimes \rho_E^{(K_A,K_B)}. \tag{3.5}$$

An ideal state held by Alice and Bob is expressed by

$$\rho_{ABE}^{\text{ideal}} = 2^{-N} \sum_K \left|K\right\rangle_A {}_A\langle K| \otimes \left|K\right\rangle_B {}_B\langle K| \otimes \rho_E \tag{3.6}$$

which is assumed to be private by definition, and Alice and Bob share an identical key $K = K_A = K_B$. Note that ρ_E is completely independent of the secret key K since Eve has no information about K for this ideal protocol. Using these elements, we can define the second requirement.

Definition 15 *(Protocol secrecy). Consider the protocol does not abort, which occurs with probability $1 - p_{\text{abort}}$. The QKD protocol is ε_{sec}-secret, if the state of the composite system of Alice and Eve ρ_{AE} is close in trace distance to the private state of the ideal protocol ρ_{AE}^{ideal}*

$$\min_{\rho_E} \frac{1}{2}(1 - p_{\text{abort}}) ||\rho_{AE} - \rho_{AE}^{\text{ideal}}||_1 \leq \varepsilon_{\text{sec}} \tag{3.7}$$

where $\rho_{AE} = \sum_{K_A} p(K_A) \left|K_A\right\rangle \left\langle K_A\right| \otimes \rho_E^{(K_A)}$ and $\rho_{AE}^{\text{ideal}} = 2^{-N} \sum_{k \in \mathcal{K}} \left|K\right\rangle_A {}_A\langle K| \otimes \rho_E$ formed by a mixed state in the key space $\mathcal{K}$, which contains all possible key bit strings,

and Eve's state.

This *secrecy* definition of a QKD protocol holds a composable security property from its trace-distance measure. The composable security concept means that the protocol can preserve its security when is composed with another protocol. There are two cases: first, when an output of one run of the protocol is used as an input for the next run, then the security of the following run depends on the security of the prior run, known as sequential composition. For example, this occurs in the authentication step, where Alice must make sure she is communicating with Bob and not an adversary. For the first run of the QKD protocol, suppose Alice can authenticate Bob with a probability $1-\varepsilon_{\text{non-auth}}$. After the first run, Alice and Bob share a secure key. Suppose Alice uses a small part of the generated key to authenticate Bob for the second time the protocol is run. In this scenario, the authentication process of the first run compromises the security of the rest. Generally, the QKD protocol must ensure is secure not only for the first run but for all the subsequent runs. In particular, this case of sequential composition was proved using the triangle inequality of the trace distance. The second case is called parallel composition and occurs when two protocols are run at the same time and are finally treated as one, combining both protocols. Without going into further details, which can be found in [83, 84], the security of a QKD protocol must be proved under the composable security framework [85]. To conclude, using the Definitions 14 and 15, we can state that a QKD protocol is ε_{QKD}-secure with $\varepsilon_{\text{qkd}} = \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$, if it is ε_{cor}-correct and ε_{sec}-secret.

3.6 Efficient BB84 Protocol

The Benett-Brassard 1984 (BB84) protocol is the most commonly employed prepare-and-measure protocol. It uses four polarised states, two for each mutually unbiased basis: the horizontal $|0\rangle$ and vertical $|1\rangle$ for the rectilinear basis (X basis) and the diagonal $|+\rangle$ and antidiagonal state $|-\rangle$ for the diagonal basis (Z basis). The states $|0\rangle$ and $|+\rangle$ are associated with the classical bit 0, while the states $|1\rangle$ and $|-\rangle$ correspond to the bit 1. Here, we present the efficient BB84 protocol, where one basis is used for key

generation (in our case, the X basis), and the other basis is for parameter estimation (the Z basis). This is different from standard BB84, see Chapter 4 for further details on the selection of efficient BB84 instead of standard BB84.

1. State preparation and transmission. Alice generates two random strings of classical bits, $K_A = \{0,1\}^N$ and $a = \{0,1\}^N$ each of length N, to encode the classical information into polarised states. The first string corresponds to the key bit strings she aims to distribute to Bob. In particular, the bit value 0 represents the vertical and diagonal polarisations (X basis), while 1 represents the horizontal and antidiagonal states (Z basis). The second string determines the basis used to encode the bit value. Specifically, the X basis is associated with the bit value 0 and the Z basis with 1, and these bits are randomly selected with probability p_X^A and $p_Z^A = 1 - p_X^A$, respectively, by Alice. To prepare the quantum states, Alice takes a bit of the second string a to choose the basis and a bit of the key string K_A to select a polarisation of the chosen basis. Then, Alice transmits these randomly generated quantum states to Bob through the quantum channel.

2. Receiver's measurements. Bob receives Alice's signals and randomly selects a basis to measure them with probability p_X^B for the X basis and p_Z^B for the Z basis. Thus, he also has a bit string $b = \{0,1\}^N$ to choose the basis. Then Bob observes a click on one of his detectors corresponding to a certain polarisation state. These states are associated with a classical bit value that forms his final key bit string K_B. Thus, Alice and Bob share a key bit string associated with their quantum states, known as the *raw key*.

3. Basis reconciliation. Alice and Bob publicly announce their basis choice, i.e. a and b, through the classic authenticated channel and proceed to discard the pair events $\{K_{Ai}, K_{Bi}\}$ in which their bases do not match $a_i \neq b_i$, where i represents the position in their strings. This step is called *sifting* and results in the *sifted key*. Assuming both parties use the same basis bias, i.e. $p_X \equiv p_X^A = p_X^B$ and $p_Z \equiv p_Z^A = p_Z^B$, has found to be the optimal strategy. Therefore, the *sifting ratio* that forms the *sifted key* is defined as $p_{\text{sift}} = p_X^2 + p_Z^2$. In standard BB84 this

is fixed to $p_{\text{sift}} = 1/2$, however, in efficient BB84, it can be optimised for any channel loss (distance) enhancing the key generation. Note that the *sifted key* is not the final secure key as in efficient BB84 we only use the events in the X basis. The remaining steps are commonly known as *classical post-processing* steps, as the quantum communication is over.

4. Parameter estimation. The parties publicly reveal the Z events of their shared *sifted key*, whose instances do not contribute to the key, and compare them to estimate the phase errors of the X basis, as they are interested in bounding the errors in the key generation basis. They cannot directly use the X basis events to estimate the phase error rate since they would be revealing their key bit values. By setting an error threshold, Alice and Bob have a criterion to abort the protocol if the phase error rate exceeds a certain level, in which case they assume Eve's presence. Otherwise, they continue. Additionally, the observed disturbance quantified by this phase error rate is used to bound the amount of leaked information to Eve can.

5. *Error correction* and *privacy amplification*. The parties perform *error correction*, where a code is implemented to correct errors, e.g. the widely employed low-density parity-check code (LDPC) [86] in which Alice applies LDPC transmits the syndrome to Bob, who applies bit flips to correct the identified errors. Alice and Bob also perform *privacy amplification*, where hash functions are used by both parties to minimise the information leaked to Eve [87]. Finally, an identical secret key, $K = K_A = K_B$, shared by Alice and Bob is distilled.

After introducing a description of the protocol steps, we expand on the motivations for QKD presented in Section 3.2 through a transmission example in BB84 assuming the presence of Eve. As in Figure 3.2, suppose Alice randomly obtains the key bit value 0 and randomly chooses to encode it in the Z basis, hence she sends the vertically polarized state to Bob. If Eve does not correctly guess the basis chosen by Alice, she certainly disturbs the state, generating half of the times a diagonal state and the other half an antidiagonal state. Suppose Bob measures either of these received states

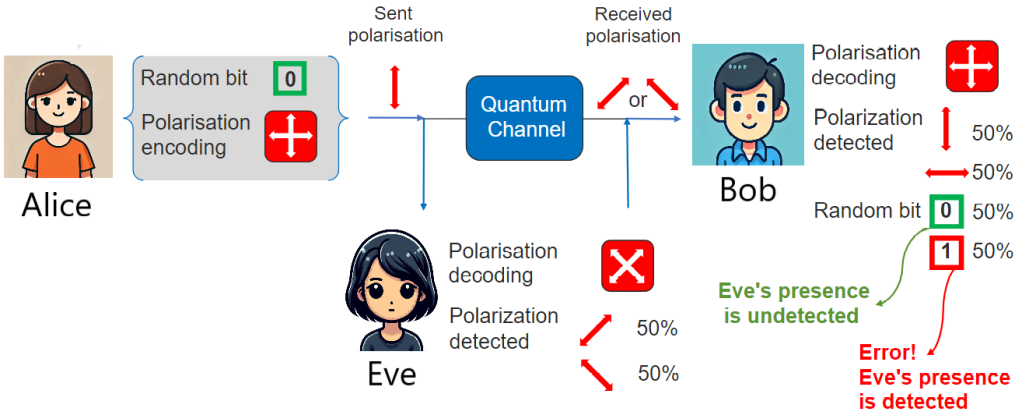

Figure 3.2: Eve causing errors in the BB84 protocol. This represents when Alice and Bob use the Z (parameter estimation) basis and Eve measures in the X (key generation) basis. Note Eve knows the key bits are encoded on the X basis, hence she consistently measures on this basis. However, for this particular case, as the parties are using the parameter estimation basis, Eve's basis selection corresponds to the complementary basis compared to the parties' basis, hence generating an error on Bob's side with probability a half.

on the same basis used by Alice (Z basis). There is also a 50% chance of obtaining either a horizontal or vertical state. If Bob observes vertical, associated with the bit 0, he shares the same bit with Alice, hence there is no error, and Eve is lucky since it is undetected by the parties. However, half of the time Bob observes the vertical polarisation, corresponding to the bit 1, which inevitably results in an error caused by an eavesdropper that can detected by the parties. When Alice and Bob use the same basis, they know they must obtain the same outcome. Overall, it is important to notice that measuring in the Z (parameter estimation) basis is detrimental for Eve since it reveals nothing about the key bits, which are encoded in the X basis. Therefore, Eve should only measure in the X (key generation) basis, although she causes errors when the parties choose the parameter estimation basis as shown in Figure 3.2. Note that Eve cannot determine on which basis the bit is encoded.

Thus, this example highlights how the BB84 protocol allows Alice and Bob to detect an eavesdropper by exploiting principles of quantum mechanics. It provides a strategy between them to share an identical secret key that can be used to encrypt messages via a public channel without relying its security on computational power or complex

algorithms. Evidently, practical challenges are bringing further difficulties for real-life implementations. However, here we aim to stress the theoretical motivations for pursuing the study of QKD, while in the following sections, we will address some of the experimental challenges.

3.6.1 Asymptotic Secure Key

The derivation of the private capacity in Section 2.2.6.3 was the prior work which led to estimating the secret rate that can be generated through the quantum channel. To understand the relation between these two quantities, we formally introduce the *private channel code*, which is defined by the used N rounds, the failure probability ε, and its rate R. The *direct coding theorem* proved that the right-hand side of Eq. (2.74) is achievable without using the classical public channel of the parties. This is heavily supported in Winter's POVM compression paper [88]. While the *converse theorem* showed it is an upper bound. Formally expressed it says that the rate R is achievable, if for every positive $\delta, \varepsilon > 0$, and a sufficiently large number of rounds N, it exists a (N, ε) code with a secret key rate $R - \delta$ such that [89]

$$R - \delta \leq \frac{1}{N} \max_{\{p_i, \rho_i\}} \left[I(A:B) - I(A:E) \right]. \tag{3.8}$$

Thus, the private channel capacity is a supremum of the achievable rates $R \leq C_P(\mathcal{E})$.

However, Alice's goal is to send one classical bit string, which represents the key, out of the 2^{NR} possible bit strings to Bob such that he can identify the string with high probability. Given the bit string K_A uniformly distributed on the set $\{1, 2, \ldots, 2^{NR}\}$, Alice transmits the random variable $X^N = X^N(K_A, M)$, which is generated by encoding her key K_A using a classical random variable M. The (N, ε) *private channel code*, also so-called (N, ε) *protocol*, must have a probability of the parties sharing a different key less than the protocol failure probability $\Pr(K_A \neq K_B) \leq \varepsilon$, plus other two conditions: one, the public information is practically uncorrelated with K_A; and second, by the use of the Holevo bound in Eq. (2.70), ensuring there is no possible strategy for Eve to extract more than ε bits of K_A exploiting the information of the public channel.

In the context of prepare-and-measure QKD protocols, Alice's aim is to set classical correlations with Bob, not sending a specific message, ensuring Eve has arbitrarily small information about Alice's transmission. Therefore, (N, ε) *key generation code* is almost the same as a *private channel code*, the difference is that K_A depends on the random variable M. The *secret key capacity* $C_K(\mathcal{E})$ equals the supremum of the achievable rates, hence $C_K(\mathcal{E}) = C_P(\mathcal{E})$ and can be expressed as

$$C_K(\mathcal{E}) \geq I(A:B) - I(A:E). \tag{3.9}$$

In the QKD field, this was later called the *asymptotic secure key rate*. We use the term *secure* to emphasise the composable security criterion of the QKD protocol, introduced in Section 3.5. Thus, as well as the protocol, the key rate is secure, if it is secret and correct. Then, the *asymptotic secure key rate* of the BB84 protocol is given by $R_{\text{BB84}}^{(\text{asym})} \equiv C_K(\mathcal{E})$. The conceptual explanation of this key rate expression is that it is formed by the amount of information shared by Alice and Bob $I(A:B)$ minus the information of Alice's key gained by Eve $I(A:E)$.

To compute the secure key rate, it is required to express it in terms of the conditional Shannon and von Neumann entropies, hence introducing the definition of the quantum mutual information in Eq. (2.74), we obtain

$$\begin{aligned} R_{\text{BB84}}^{(\text{asym})} &\geq S(A) + S(B) - S(AB) - S(A) - S(E) + S(AE) \\ &= S(AE) - S(E) - S(AB) + S(B). \end{aligned} \tag{3.10}$$

Introducing the conditional von Neumann entropies using Eq. (2.46), the asymptotic key rate of the BB84 protocol, known as the Devetak-Winter bound [49], reads as

$$R_{\text{BB84}}^{(\text{asym})} \geq S(A|E) - S(A|B). \tag{3.11}$$

To calculate the von Neumann entropies of the key rate in Eq. (3.11), we employ an entangled version of the preparation of the polarised states. Therefore, we assume

that Charlie, a third party, prepares the following four basic two-qubit Bell states

$$|\Psi_{ij}\rangle = \frac{|0,j\rangle + (-1)^i |1,1-j\rangle}{\sqrt{2}} \tag{3.12}$$

where $i,j \in \{0,1\}$. Charlie distributes the two qubits to Alice and Bob through the quantum channel. The received qubits can be either in the Z basis, i.e. $\{|\Psi_{00}\rangle, |\Psi_{10}\rangle\}$, or in the X basis, i.e. $\{|\Psi_{01}\rangle, |\Psi_{11}\rangle\}$. This scenario is correlated to the prepare-and-measure BB84 since Alice's measurement of her qubit conditions Bob's outcome, hence it is analogous to Alice preparing a state and then Bob measuring it.

Consider before Charlie distributes the state ρ_{AB} to the parties, the eavesdropper, Eve, applies a measurement aiming to extract information about the state, thus Eve prepares the state $\tilde{\rho}_{AB}$ and distributes it instead of ρ_{AB}. One can show that Eve does not increase her uncertainty on Alice's system, i.e. $S(A|E)_\rho \geq S(A|E)_{\tilde{\rho}}$, see the proof in Section 3.5 of [47]. Here we assume the worst-case scenario where first Eve holds a composite system shared with Alice AE that contains all the possible correlations with Alice's subsystem A. Second, Eve can perform a partial trace on her subsystem to obtain a *purification* of Alice's state. This assumption is commonly employed in quantum cryptography and is described in Definition 1.

In particular, Eve measures the state prepared by Charlie ρ_{AB} either in one basis $\hat{D}_X = X \otimes X$ or the other $\hat{D}_Z = Z \otimes Z$ before it reaches the parties. Eve's operation can be expressed with generality as the following map

$$\mathcal{D}_{X(Z)} = \frac{1}{2}\rho_{AB} + \frac{1}{2}\hat{D}_{X(Z)}\rho_{AB}\hat{D}^\dagger_{X(Z)}. \tag{3.13}$$

Then the state after Eve's measurement received by the parties is $\tilde{\rho}_{AB} = (\mathcal{D}_X \circ \mathcal{D}_Z)\rho_{AB}$, which has the same diagonal coefficients than the original ρ_{AB}, hence it is diagonal in the Bell basis $\{|\Psi_{ij}\rangle\}^1_{i,j=0}$ of two qubits, see Eq. (3.13) of [47], and it can be expressed using the density operator formalism for composite systems of Eq. (2.14) as

$$\tilde{\rho}_{AB} = \sum_{i,j=0}^{1} \lambda_{ij} |\Psi_{ij}\rangle \langle\Psi_{ij}| \tag{3.14}$$

where the sum of the eigenvalues $0 \leq \lambda_{ij} \leq 1$ equals the unity $\sum_{i,j} \lambda_{ij} = 1$.

As expected, the state prepared by Eve $\tilde{\rho}_{AB}$ contains the same eigenvalues as the initial state ρ_{AB}. From the parties' perspective, Eve's action causes a flip of both bits of Alice and Bob with probability 1/2, hence it does not impact the observed quantum bit error rate (QBER) by the parties, nor their shared correlated bits since it simultaneously does affects both parties or does not. This situation is equivalent to the parties flipping their observed values with probability 1/2 without an eavesdropper's presence. The consequence of Eve's measurements is the symmetrisation of the marginal distributions (see Eq. (2.63)) of Alice's and Bob's outcomes (raw key bits), denoted by $p(a|x)$ and $p(b|y)$ for all $x, y \in \{0, 1\}$, where a and b are the outcomes of Alice and Bob, respectively. This process requires classical communication between the parties through the public channel.

Assuming Eve holds the purifying system of the state $\tilde{\rho}_{AB}$, the global state shared with the parties is also a pure state. Using the formalism of Eq. (2.13) it is given by

$$|\Psi_{ABE}\rangle = \sum_{i,j=0}^{1} \sqrt{\lambda_{ij}}\, |\Psi_{ij}\rangle_{AB} \otimes |e_{ij}\rangle_{E} \tag{3.15}$$

where $\{|e_{ij}\rangle\}_{i,j=0,1}$ is the orthonormal basis of Eve's Hilbert space $\mathcal{H}_E$. In this scenario, assuming Eve performs *collective attacks* to the state ρ_{AB} for every round of the protocol, and there is no correlation between past and future rounds, the parties may detect Eve's presence from the observed errors in each basis after measuring their shared state $\tilde{\rho}_{AB}$ prepared by Eve.

These errors occur when the two-qubit state yields different outcomes, i.e. the parties do not share the same bit. In the Z basis, which consists of the states $|0\rangle$ and $|1\rangle$, the errors correspond to obtaining either $|01\rangle$ or $|10\rangle$ outcome. Hence, errors only occur for the prepared Bell states $|\Psi_{01}\rangle$ and $|\Psi_{11}\rangle$. In the X basis, which consists of the states $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, the errors occur when the outcome is either $|+-\rangle$ or $|-+\rangle$. This is the case for the Bell states $|\Psi_{10}\rangle$ and $|\Psi_{00}\rangle$,

which expressed in terms of the X basis are

$$|\Psi_{10}\rangle = \frac{|+-\rangle + |-+\rangle}{\sqrt{2}} \tag{3.16}$$

$$|\Psi_{00}\rangle = \frac{|+-\rangle - |-+\rangle}{\sqrt{2}}. \tag{3.17}$$

Measuring either in the Z basis for the Bell states $|\Psi_{01}\rangle$ and $|\Psi_{11}\rangle$, or in the X basis for $|\Psi_{10}\rangle$ and $|\Psi_{00}\rangle$, guarantees the same value for both qubits.

Thus, the errors in each basis are calculated as follows

$$\begin{aligned} E_Z &= \mathrm{Tr}\left[\left(|+\rangle\langle+| \otimes |-\rangle\langle-| + |-\rangle\langle-| \otimes |+\rangle\langle+|\right)\tilde{\rho}_{AB}\right] \\ &= \mathrm{Tr}\left[\left(|+\rangle\langle+| \otimes |-\rangle\langle-| + |-\rangle\langle-| \otimes |+\rangle\langle+|\right)\left(\lambda_{01}|\Psi_{01}\rangle\langle\Psi_{01}| + \lambda_{11}|\Psi_{11}\rangle\langle\Psi_{11}|\right)\right] \\ &= \lambda_{01} + \lambda_{11}, \end{aligned} \tag{3.18}$$

$$\begin{aligned} E_X &= \mathrm{Tr}\left[\left(|0\rangle\langle0| \otimes |1\rangle\langle1| + |1\rangle\langle1| \otimes |0\rangle\langle0|\right)\tilde{\rho}_{AB}\right] \\ &= \mathrm{Tr}\left[\left(|0\rangle\langle0| \otimes |1\rangle\langle1| + |1\rangle\langle1| \otimes |0\rangle\langle0|\right)\left(\lambda_{00}|\Psi_{00}\rangle\langle\Psi_{00}| + \lambda_{10}|\Psi_{10}\rangle\langle\Psi_{10}|\right)\right] \\ &= \lambda_{00} + \lambda_{10}. \end{aligned} \tag{3.19}$$

Tracing out Bob's subsystem of the global state $|\Psi_{ABE}\rangle$, we obtain the following *classical-quantum* (cq) state

$$\tilde{\rho}_{AE} = \sum_{a=0}^{1} p(a)\,|a\rangle\langle a|_A \otimes \tilde{\rho}_E^a, \tag{3.20}$$

similarly to Eq. (2.19), where Eve's quantum state conditioned on Alice's classical bit value a, which is distributed with probability $p(a)$, reads as

$$\tilde{\rho}_E^a = \sum_{i,j,k=0}^{1} \sqrt{\lambda_{ij}\lambda_{kj}}(-1)^{(i+k)a}\,|e_{ij}\rangle\langle e_{ij}|\,. \tag{3.21}$$

The positive eigenvalues, which are independent of the outcome x, are determined by either the errors in the X basis, Eq. (3.19), or Z basis, Eq. (3.18). Here, since the X basis is used for the key generation, the conditional von Neumann entropy of E

conditioned on A is expressed as

$$S(E|A) = \sum_{a=0}^{1} p(a) S(\tilde{\rho}_E^a) = H\left(\lambda_{00} + \lambda_{10}\right) = h_2\left(E_Z\right) \tag{3.22}$$

where the binary entropy $h_2(E_Z) = -E_Z \log E_Z - (1 - E_Z)\log(1 - E_Z)$ is employed because there are only two possible outcomes $\{0, 1\}$. The symmetrised marginal distributions of the parties, with probabilities as in Eq. (2.63), imply $S(A) = 1$ plus the entropies of the system E and AB are identical and depend on the eigenvalues, $S(E) = S(AB) = H\left(\{\lambda_{ij}\}\right)$, since $|\Psi_{ABE}\rangle$ is a pure state. It is important to note that to introduce the eigenvalues in the latter entropy and in Eq. (3.22) the derivation from Eq. (2.41) to (2.45) is applied.

To estimate the Devetak-Winter rate of Eq. (3.11), we need to compute its first conditional von Neumann entropy using Eq. (3.22) along with other mentioned entropies

$$S(A|E) = S(E|A) + S(A) - S(E) = h_2(E_X) + 1 - H\left(\{\lambda_{ij}\}\right). \tag{3.23}$$

Here, we must minimise the private rate by minimising the entropy over the eigenvalues $\{\lambda_{ij}\}$, which are not completely fixed but are constrained by the observed errors in Eqs. (3.18) and (3.19). Implementing this minimisation [28], the entropy reads as

$$S(A|E) = 1 + h_2(E_X) - h_2(E_X) - h_2(E_Z) = 1 - h_2(E_Z). \tag{3.24}$$

Regarding the entropy between Alice's and Bob's systems, due to the symmetrisation of their marginal distribution in the asymptotic limit, it can be expressed solely by the errors in the X basis as $S(A|B) = h_2(E_X)$. Replacing this and Eq. (3.24) into Eq. (3.11), we obtain the final expression for the asymptotic key rate of the BB84 protocol [90]

$$R_{\mathrm{BB84}}^{(\mathrm{asym})} = 1 - h_2(E_Z) - h_2(E_X), \tag{3.25}$$

where $h_2(E_Z)$ represents the fraction of the sifted key bits that are used to perform privacy amplification and reduce the information leaked to Eve, and $h_2(E_X)$ is the fraction of sifted key bits sacrificed to perform the error correction code assuming

perfect efficiency.

3.6.2 Decoy-State Method and Finite-Key Analysis

Here, we review the importance and original motivation of the decoy-state method. In a BB84 protocol employing exclusively one source intensity, known as non-decoy, Eve, who fully controls the channel, can perform PNS attacks to effectively intercept the key whilst remaining undetectable by exploiting the multiphotons. By employing quantum nondemolition measurements [91], Eve identifies the number of photons contained in each pulse. She then blocks the single-photon pulses and splits the multiphoton pulses into single-photons, which are forwarded to Bob, while the remaining photons are stored and measured by Eve after basis reconciliation. Therefore, to ensure the security of the BB84 protocol, the click probability of Bob's detectors has to be greater than the multiphoton emission of Alice, $p_{\text{click}} > p_{\text{mp}}$. Otherwise, assuming all multiphoton emissions cause a detection event on Bob's apparatus through Eve's lossless channel, the expected detection rate by Bob can be reproduced by Eve exclusively using the sent multiphotons in a lossy channel, compromising the secrecy of the entire shared key bit string. Consequently, only non-multiphoton detections can be considered secure events.

Let us illustrate through an example why this condition $p_{\text{click}} > p_{\text{mp}}$ must be fulfilled to achieve secure communication. See the schemes showing Eve's strategy in Figures 3.3 and 3.4. Suppose Alice has a source distribution that emits single-photon 90% of the time and multiphotons the remaining 10%. Consider that Alice and Bob are considerably distant from each other, hence having access to a quantum channel of 90% of loss, which they have characterised. For this particular lossy channel, Bob expects a detection rate of 10%. Here comes Eve's strategy to gain information about the entire key. When Alice sends a multiphoton, Eve performs a PNS attack as explained above. Therefore, since the 10% of Alice's signals are multiphotons, Eve can split them and re-send single-photons to Bob for every one of them, matching the expected detection rate by Bob (10%). This is illustrated in Figure 3.3. When Alice sends a single-photon, Eve just has to block it and not let it reach Bob, see Figure 3.4. Note that she recognises the

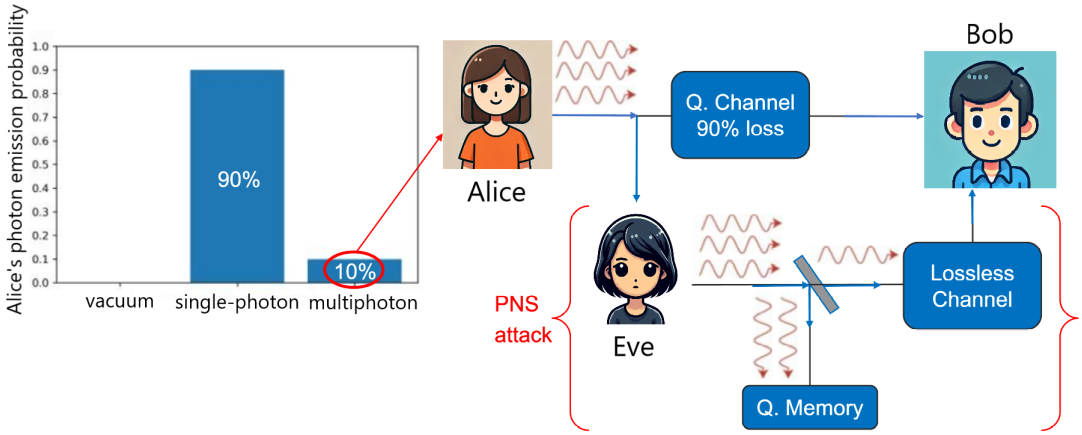

Figure 3.3: Photon number splitting (PNS) attack. This diagram illustrates Eve's strategy when she performs a PNS attack in a lossy quantum channel for certain chosen probabilities. In particular, we assume that Alice emits 90% of the time single-photon and the remaining 10% multiphotons and a quantum channel with 90% loss, hence Bob expects a detection rate of 10% of the total states sent by Alice. Here Eve splits the multiphoton states and re-sends single-photons to Bob. With this strategy, Eve can figure out all the bit values encoded in the transmitted states, assuming she measures when the parties reveal their basis choices.

single-photons by performing nondemolition measurements for every sent state. The legitimate parties cannot detect Eve's presence and after basis reconciliation, when the parties publicly announce their selected bases, Eve can measure her stored photons and know the entire key. To conclude, in this example, Bob's detection rate is equal to Alice's multiphoton emissions, i.e. $p_{\text{click}} = p_{\text{mp}}$, hence any $p_{\text{click}} < p_{\text{mp}}$ is also insecure, and Eve can perform the same strategy exploiting multiphotons trough PNS attacks. Thus, we illustrate with a simple case, that $p_{\text{click}} > p_{\text{mp}}$ must be satisfied to have the possibility of generating a secure key between two parties.

Weak coherent pulse (WCP) sources have been the most commonly employed sources in BB84. They have a sufficiently high multiphoton emission to be vulnerable to PNS attacks in lossy channels. The reduction of their multiphoton statistics was substantially restricted. Therefore, to mitigate the PNS attacks and ensure the $p_{\text{click}} > p_{\text{mp}}$ is met, the decoy-state method was proposed [35], which underwent significant refinement [92–95]. This technique involves using multiple intensity levels for

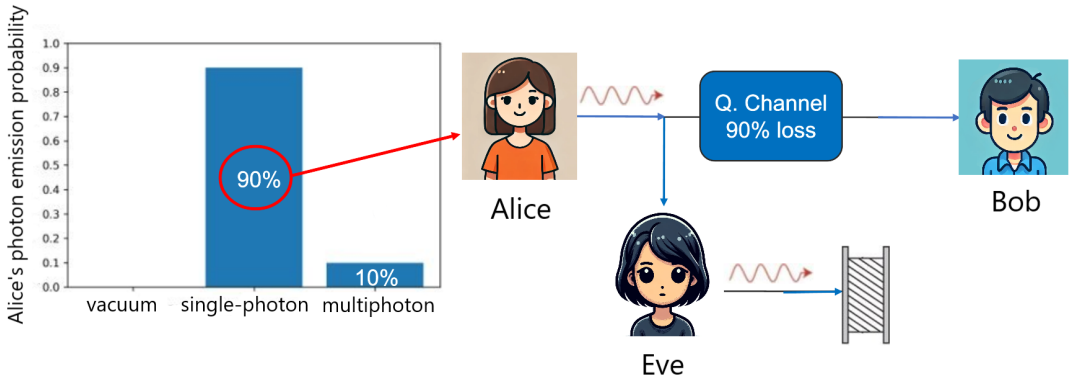

Figure 3.4: Eve's strategy for Alice's single-photons. Here we consider the same Alice's emission probabilities and channel loss as in Figure 3.3. When Alice sends a single-photon through this lossy quantum channel to Bob, Eve must block it, preventing it from reaching Bob, since Eve requires more than one photon to extract information about the key bits while forwarding these encoded values to Bob.

WCPs with identical characteristics to bound the multiphoton events, i.e. Bob's detections caused by multiphotons, while ensuring both parties agree on their single-photon and vacuum events estimate, i.e. Bob's detections caused by sent single-photons and vacuum states, commonly known as yields. This accurate estimation is possible since the used WCPs produce equal counting rates for any sent k-photon state, despite their distinct photon emission probabilities. In other words, even if each WCP with a different intensity generates different photon detection statistics on Bob's apparatus, the detection rate for a particular photon state transmitted by Alice must be identical amongst all intensity levels. In fact, deviations in the yields between different WCP intensities indicate the presence of an eavesdropper, who lacks knowledge regarding the transmitted distribution. As described above, we assume Eve is capable of knowing how many photons are contained in a sent signal. However, Eve does not have access to which intensity, which is also referred to as the mean photon number, Alice uses for each transmitted state. Hence, Alice's prepared state appears the same regardless of the chosen intensity from Eve's perspective.

3.6.2.1 2-Decoy with Weak Coherent Pulses

In this section, we highlight the main aspects of the 2-decoy weak coherent pulse (WCP) protocol utilizing the yield bounds of [96], while introducing tighter bounds on the finite-key analysis and error correction estimation, as in our work in [97] [1]. We consider an asymmetric efficient BB84 protocol, which means the basis selection is biased. This protocol is based on the transmission of phase-randomised laser pulses, employing one signal state and two decoy states with different intensity levels for each of them. The intensity for each state sent by Alice is randomly selected amongst the three optimised intensities μ_0, μ_1 and μ_2, which satisfy $\mu_1 > \mu_2 + \mu_0$. This intensity choice is denoted by $k \in \mathcal{K} = \{\mu_0, \mu_1, \mu_2\}$, with probabilities p_{μ_0}, p_{μ_1} and p_{μ_2}. Traditionally, in the QKD literature, the higher intensity, being here μ_1, is commonly called the *signal* state, while the remaining intensities are the *decoy* states. The name *decoy* emerged because it was originally used exclusively to estimate errors and spot Eve's PNS attacks, whereas the *signal* was the intensity used to generate the key. However, notice that this is not the case here, since we implement efficient BB84 where all the intensities are employed to estimate the secure key. Next, we introduce the security bounds to estimate the yields, i.e. the vacuum and single-photons detection events.

The analytical bounds of the yields are established by exploiting the nature of the conditional probabilities, which follow a Poissonian distribution as

$$p_{k|n} = \frac{p_k}{\tau_n} p_{n|k} = \frac{p_k}{\tau_n} \frac{e^{-k} k^n}{n!} \tag{3.26}$$

where $\tau_n = \sum_{k \in \mathcal{K}} p_k e^{-k} k^n / n!$ is the probability that Alice prepares an n-photon state.

The lower bound of the vacuum $s_{X,0}$ and single-photon events $s_{X,1}$ are derived in the X basis because we consider it the key generation basis, while the single-photon errors $e_{Z,1}$ are estimated in the Z (parameter estimation) basis. As previously explained in Section 3.6.2, they are identical for both parties and they are used to estimate the final secure key. Hence, the detection or error rate for a particular n-photon state is equal amongst the intensity levels, i.e. $s_{X,n} \equiv s^{\mu_2}_{X,n} = s^{\mu_1}_{X,n} = s^{\mu_0}_{X,n}$ and $e_{X,n} \equiv e^{\mu_2}_{X,n} = e^{\mu_1}_{X,n} =$

[1] Although this decoy analysis is implemented for a free-space channel, its tight bounds are applicable in general to any other channel.

$e_{X,n}^{\mu_0}$. Note we have to take the worst-case QKD scenario, hence, we aim to derive a lower bound for the secure key length formula and consequently, for the vacuum and single-photon events.

The symbol * represents expected values, thus the expected number of detection events for each intensity is denoted as $\{N_{X,k}^*\}_{k\in\mathcal{K}}$ and the expected number of errors for each intensity is expressed as $\{m_{X,k}^*\}_{k\in\mathcal{K}}$. Explicitly, they are written as

$$N_{X,k}^* = \sum_{n=0}^{\infty} p_{k|n} s_{X,n} \tag{3.27}$$

$$m_{X,k}^* = \sum_{n=0}^{\infty} p_{k|n} v_{X,n}. \tag{3.28}$$

Therefore, the exact expression of the vacuum events can be derived by solving for $s_{X,0}$ using Eq. (3.27) for the expected values of intensity μ_2 and μ_0,

$$s_{X,0} = \frac{\tau_0}{\mu_2 - \mu_0}\left(\frac{\mu_2 e^{\mu_0} N_{X,\mu_0}^*}{p_{\mu_0}} - \frac{\mu_0 e^{\mu_2} N_{X,\mu_2}^*}{p_{\mu_2}} + \mu_2\mu_0 \sum_{n=2}^{\infty} \frac{(\mu_2^{n-1} - \mu_0^{n-1}) s_{X,n}}{n!\tau_n}\right) \tag{3.29}$$

We particularly involve these intensities since they are the more attenuated ones, hence they emit more vacuum states than μ_1. We can get rid of the summation term by applying the intensity condition of $\mu_2 > \mu_0$, which also ensures the positivity of the denominator and avoids the problematic case where $\mu_2 = \mu_0$ and $\underline{s}_{X,0}$ goes to infinity. Thus, we reach the following lower bound,

$$s_{X,0} > \underline{s}_{X,0} = \frac{\tau_0}{\mu_2 - \mu_0}\left(\frac{\mu_2 e^{\mu_0} N_{X,\mu_0}^*}{p_{\mu_0}} - \frac{\mu_0 e^{\mu_2} N_{X,\mu_2}^*}{p_{\mu_2}}\right). \tag{3.30}$$

For the number of single-photon events, we solve for $s_{X,1}$ using Eq. (3.27) again for the intensities mu_2 and μ_0 and we obtain

$$s_{X,1} = \frac{\tau_1}{\mu_2 - \mu_0}\left[\frac{e^{\mu_2} N_{X,\mu_2}^*}{p_{\mu_2}} - \frac{e^{\mu_0} N_{X,\mu_0}^*}{p_{\mu_0}} + \sum_{n=2}^{\infty} \frac{(\mu_0^n - \mu_2^n) s_{X,n}}{n!\tau_n}\right]. \tag{3.31}$$

One can ensure $(\mu_2^2 - \mu_0^2)(\mu_2 + \mu_0)^{n-2} > \mu_2^n - \mu_0^n$ for $n \geq 2$, see details on the Appendix

of [96]. Using the intensity condition $\mu_1 > \mu_2 + \mu_0$, it is straightforward to see

$$(\mu_2^2 - \mu_0^2)\mu_1^{n-2} > (\mu_2^2 - \mu_0^2)(\mu_2 + \mu_0)^{n-2} \tag{3.32}$$

for $n \geq 2$. Introducing this inequality in the summation term of Eq. (3.31), we derive its lower bound,

$$\begin{aligned} s_{X,1} > \underline{s}_{X,1} = & \frac{\mu_1 \tau_1}{\mu_1(\mu_2 - \mu_0) - (\mu_2^2 - \mu_0^2)} \left[\frac{e^{\mu_2} N^*_{X,\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_0} N^*_{X,\mu_0}}{p_{\mu_0}} \right. \\ & \left. + \frac{\mu_2^2 - \mu_0^2}{\mu_1^2} \left(\frac{s_{X,0}}{\tau_0} - \frac{e^{\mu_1} N^*_{X,\mu_1}}{p_{\mu_1}} \right) \right]. \end{aligned} \tag{3.33}$$

Note that the intensity condition is strictly greater and not greater or equal, to again prevent the case where $\mu_1 = \mu_2 + \mu_0$ and $\underline{s}_{X,1} \to \infty$.

Finally, similarly to the $\underline{s}_{X,0}$ derivation, the upper bound on the number of single-photon errors is given by

$$v_{X,1} < \overline{v}_{X,1} = \frac{\tau_1}{\mu_2 - \mu_0} \left(\frac{e^{\mu_2} m^*_{X,\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_0} m^*_{X,\mu_0}}{p_{\mu_0}} \right). \tag{3.34}$$

These expected values are involved in the yields, Eqs. (3.30), (3.33) and (3.34), are only reached in the asymptotic limit. Therefore, the bounds of the yields are not directly applicable to the observed statistics in a BB84 decoy experiment. We must introduce bounds for the observed values. If an expected value of the security bounds of the yields contributes positively to the key length, then we must lower bound it, and vice-versa, if it has a negative contribution, we must upper bound it.

When the parties publicly announce their selected basis and intensity choices in the basis reconciliation process, they must check that the actual observed number of events on each basis and for each intensity, i.e. $N_{X,k}$ and $N_{Z,k}$, is not greater than the number of times the corresponding bases and intensities were chosen, $|\mathcal{X}_k|$ and $|\mathcal{Z}_k|$. If these conditions, i.e. $N_{X,k} \leq |\mathcal{X}_k|$ and $N_{Z,k} \leq |\mathcal{Z}_k|$, are not satisfied, Alice and Bob must start the protocol again. However, this condition about the observed number of events on Bob's side is not sufficient to directly apply them to the yields.

For every finite block of data generated by the parties in each run of the decoy

protocol, they collect different statistical outcomes, and these deviations pose a security threat. Suppose we directly compute the observed values in the equations of the yields, assuming they are equal to their true expected values, we can clearly see that a decrease or increase in the observed outcomes for each intensity modifies the final secure key, see Eq. (3.50). These statistical fluctuations occur because the observed values of each intensity deviate from their underlying expected values in a finite block.

Hence, assume a fixed finite block for every time Alice and Bob run the protocol. In one run, they can be unlucky and have, for example, a greater deviation for the number of events in intensity μ_2, N_{X,μ_2}, compared to the deviation of the events in other intensities. Assuming this deviation is an increase, and knowing these events contribute positively to the number of secure key bits, the parties would be overestimating the number of shared secure bits. This would not be an issue if the reason is an increase in the probability of selecting intensity μ_2, because this would also increase the expected N^*_{X,μ_2}. However, this is not the case, since the deviation of N_{X,μ_2} from N^*_{X,μ_2} is caused by the size of the collected statistics being finite. Therefore, the parties must take into account these fluctuations and derive bounds of the expected values from the observed values, whose tail probability is bounded with an arbitrarily small error. In other words, the parties must ensure the true underlying expected value of an observed outcome cannot be greater (lower) than this upper-bounded (lower-bounded) expected value. This can only fail with a considered small error probability $\varepsilon_{\mathrm{PE}}$. Hence, Alice and Bob prevent themselves from incurring in any insecure overestimation of a protocol quantity.

To model the statistical uncertainties of the expected parameters, we introduce correction terms that depend on the size of the collected finite statistic. Several methods were proposed to account for these statistical fluctuations in finite blocks for decoy WCP methods, such as the Gaussian analysis method [98], the Hoeffding inequality [96] and the multiplicative Chernoff bound [99]. However, an improved analytical Chernoff bound has reported tighter finite-key bounds, enhancing the key generation [100]. Thus, we bound the observed number of events in either basis or intensity $N_{\mathrm{X(Z)},k}$, and similarly, the number of observed errors $m_{\mathrm{X(Z)},k}$, using this updated Chernoff bound as

follows

$$N^{\pm *}_{\mathrm{X(Z)},k} = e^k \left[N_{\mathrm{X(Z)},k} \pm \Delta^{\pm} \right] / p_k \tag{3.35}$$

$$m^{\pm *}_{\mathrm{X(Z)},k} = e^k \left[m_{\mathrm{X(Z)},k} \pm \Delta^{\pm} \right] / p_k \tag{3.36}$$

where the deviation $\Delta^{\pm}$ depends on the number of events $N_{\mathrm{X(Z)},k}$ or errors $m_{\mathrm{X(Z)},k}$, denoted by x with generality, and the secrecy parameter $\varepsilon_{\mathrm{sec}}$,

$$\Delta^{+} = \beta + \sqrt{2\beta x + \beta^2}, \quad \Delta^{-} = \frac{\beta}{2} + \sqrt{2\beta x + \frac{\beta^2}{4}}, \tag{3.37}$$

where $\beta = -\log_{\mathrm{e}}(\varepsilon_{\mathrm{PE}})$ with parameter estimation $\varepsilon_{\mathrm{PE}} = \varepsilon_{\mathrm{sec}}/21$. Notice that the upper and lower bounds of these quantities are chosen to maintain the lower bound of the vacuum $\underline{s}_{\mathrm{X},0}$ and single-photon $\underline{s}_{\mathrm{X},1}$ events, and the upper bound of the single-photon error $\overline{v}_{X,1}$. For clarification, we specifically write the introduced finite-size bounds in Eq. (3.30),

$$N^{*}_{\mathrm{X},\mu_0} \geq N^{-*}_{\mathrm{X},\mu_0} = e^{\mu_0} \left[N_{\mathrm{X},\mu_0} - \Delta^{-} \right] / p_{\mu_0} \tag{3.38}$$

$$N^{*}_{\mathrm{X},\mu_2} \leq N^{+*}_{\mathrm{X},\mu_2} = e^{\mu_2} \left[N_{\mathrm{X},\mu_2} + \Delta^{+} \right] / p_{\mu_2} \tag{3.39}$$

in Eq. (3.33),

$$N^{*}_{\mathrm{X},\mu_2} \geq N^{-*}_{\mathrm{X},\mu_2} = e^{\mu_2} \left[N_{\mathrm{X},\mu_2} - \Delta^{-} \right] / p_{\mu_2} \tag{3.40}$$

$$N^{*}_{\mathrm{X},\mu_0} \leq N^{+*}_{\mathrm{X},\mu_0} = e^{\mu_0} \left[N_{\mathrm{X},\mu_0} + \Delta^{+} \right] / p_{\mu_0} \tag{3.41}$$

$$N^{*}_{\mathrm{X},\mu_1} \leq N^{+*}_{\mathrm{X},\mu_1} = e^{\mu_1} \left[N_{\mathrm{X},\mu_1} + \Delta^{+} \right] / p_{\mu_1} \tag{3.42}$$

and in Eq. (3.34),

$$m^{*}_{\mathrm{X},\mu_2} \geq m^{-*}_{\mathrm{X},\mu_2} = e^{\mu_2} \left[m_{\mathrm{X},\mu_2} - \Delta^{-} \right] / p_{\mu_2} \tag{3.43}$$

$$m^{*}_{\mathrm{X},\mu_0} \leq m^{+*}_{\mathrm{X},\mu_0} = e^{\mu_0} \left[m_{\mathrm{X},\mu_0} + \Delta^{+} \right] / p_{\mu_0}. \tag{3.44}$$

In the phase error rate estimation, Bob selects a subset of the *sifted key*, which

are the events in the Z basis, to estimate the phase errors in the X (key generation) basis. This subset may not be fully representative of the entire transmission for the X basis. Here is where the random sampling without replacement problem arises and a correction term γ is introduced to compensate for any potential statistical deviation due to the subset selection. Thus, we estimate the upper bound of the phase error rate in the X basis using the Z basis as follows

$$\phi^X \leq \overline{\phi}^{\mathrm{X}} = \frac{\overline{v}_{\mathrm{Z},1}}{\underline{s}_{\mathrm{Z},1}} + \gamma\left(\underline{s}_{\mathrm{X},1}, \underline{s}_{\mathrm{Z},1}, \frac{\overline{v}_{\mathrm{Z},1}}{\underline{s}_{\mathrm{Z},1}}, \frac{\varepsilon_{sec}}{21}\right). \tag{3.45}$$

Also, various γ functions have been derived to estimate the upper bound of the phase error rate. However, the following γ function of [100] has been proven tighter than others. We further discuss this in Section 4.4.2.1.

For a tail bound error ε', the upper bound of the unobserved value χ can be estimated from the observed value λ by

$$\chi = \lambda + \gamma\left(n, k, \lambda, \varepsilon'\right), \tag{3.46}$$

where

$$\begin{aligned}
\gamma\left(n, k, \lambda, \varepsilon'\right) &= \frac{1}{2 + 2\frac{A^2 G}{(n+k)^2}} \left\{ \frac{(1-2\lambda)AG}{n+k} \right. \\
&\quad \left. + \sqrt{\frac{A^2G^2}{(n+k)^2} + 4\lambda(1-\lambda)G} \right\}, \qquad (3.47) \\
A &= \max\{n, k\}, \qquad (3.48) \\
G &= \frac{n+k}{nk} \log_e \frac{n+k}{2\pi nk\lambda(1-\lambda)\varepsilon'^2}, \qquad (3.49)
\end{aligned}$$

under the assumption that $0 < \lambda < \chi < 0.5$ which is true for typical QKD scenarios. This now allows us to calculate the upper bound of Eq. (3.45).

The secrecy analysis of [96, 101], using a family of entropic relations of the smooth entropies shown in Section 2.2.3, reach the following finite secure key length formula

for the 2-decoy state WCP BB84 protocol

$$\ell_{2\mathrm{D}}^{(\mathrm{WCP})} > \underline{s}_{\mathrm{X},0} + \underline{s}_{\mathrm{X},1}\left[1 - h_2\left(\overline{\phi}_{\mathrm{X}}\right)\right] - \lambda_{\mathrm{EC}} - 6\log_2\frac{21}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} \tag{3.50}$$

where the leakage in one-way protocols is bounded as [102],

$$\begin{aligned}\lambda_{\mathrm{EC}} &= N_X h_2(e_X) \\ &\quad + \left[N_X\left(1-e_X\right) - F^{-1}\left(\varepsilon_{\mathrm{cor}};\, N_X,\, 1-e_X\right)\right]\log\frac{1-e_X}{e_X} \\ &\quad - \frac{1}{2}\log N_X - \log\frac{1}{\varepsilon_{\mathrm{cor}}},\end{aligned} \tag{3.51}$$

where $h_2(e_X) = -e_X \log e_X - (1-e_X)\log(1-e_X)$ is the binary entropy of the quantum bit error rate (QBER) $e_X = m_X/N_X = \sum_{k\in\mathcal{K}} m_{\mathrm{X},k}/N_{\mathrm{X},k}$ and $F^{-1}\left(\varepsilon_{\mathrm{cor}};\, N_X,\, 1-e_X\right)$ is the inverse of the cumulative distribution of the binomial distribution. Achievable rates by practical codes may not achieve this bound for large blocks. In fact, no practical code has reached a value below the Shannon limit of $\lambda_{\mathrm{EC}} = 1.16 N_X h_2\left(e_X\right)$. If $\lambda_{\mathrm{EC}}/N_{\mathrm{R}}H(e_X) < 1.16$, we recover the Shannon limit to estimate the number of bits sacrificed in error correction, hence we consider the efficiency factor cannot reach a value below $f_{\mathrm{EC}} < 1.16$ for practical reasons [103]. The remaining terms of the secure key length formula represent the bits used to verify the correctness and secrecy of the protocol, ensuring that the protocol is $\varepsilon_{\mathrm{qkd}}$-secure, where $\varepsilon_{\mathrm{qkd}} = \varepsilon_{\mathrm{sec}} + \varepsilon_{cor}$, if it is $\varepsilon_{\mathrm{sec}}$-secret and $\varepsilon_{\mathrm{cor}}$-correct within the universally composable security framework.

Chapter 4

Non-Decoy Efficient-BB84 with Single-Photon Sources

Future quantum networks will require bright, low-noise sources of single photons to enable applications including secure communication and distributed quantum computing [104]. There is a range of promising platforms for such a source, including quantum dots, molecules, quantum emitters in two-dimensional materials such as WSe_2 and hBN, and colour centres in wide band-gap materials such as diamond and SiC. Thus, practical single-photon sources (SPSs) emerge as an increasing alternative source for QKD experiments [105, 106]. In general, their extremely low time-zero second-order correlation function $g^{(2)}(0)$, hence their low multiphoton emission, positions them as potential good candidates for QKD against photon number splitting (PNS) attacks in lossy channels, even without implementing decoy states.

Among these platforms for single-photon emitters, quantum dots (QDs) have demonstrated the highest count rates with the lowest multiphoton emission probability [107–109]. Therefore, we present the first key generation results of the non-decoy single-photon source (SPS) efficient BB84 protocol over optical fibre for a bright frequency-converted quantum dot (QD) source, consisting of an InGaAs/GaAs quantum dot inside an oxide-apertured micropillar [110] emitting photons at 940 nm. For further technical aspects see [42].

Quantum frequency-conversion is a viable route to realise a bright, coherent tele-

com QD source with low multiphoton noise, leveraging the performance of shorter wavelength QDs [111–113]. Further experimental technicalities about the setup with a passive BB84 receiver for the particular QD are addressed in [42].

The presented model here, a non-decoy SPS efficient BB84 protocol, introduces several novel aspects and updates to the literature in QKD for practical SPSs. First, the use of efficient BB84 (Section 3.6) over standard BB84, where a signal state is used for key generation and a decoy state for parameter estimation. It has been shown efficient BB84 doubles the protocol efficiency compared to standard BB84 in the asymptotic limit [114]. Second, a single-photon source characterisation to upper bound Alice's multiphoton emission (Section 4.1), the simulation of Bob's count (Section 4.2)and an optimisation of the free protocol parameters (Section 4.3) are presented. Third, we implemented improved analytical bounds for the random sampling without replacement problem related to the phase error rate and the multiplicative Chernoff bound that has been proven to be a tighter finite key bound in other contexts [100]. These bounds are used to calculate the fluctuations between expected and observed values in the finite-key analysis and were already presented for the 2-decoy WCP model in Section 3.6.2.1. We provide a derivation of the asymptotic key (Section 4.4.1) and the secure finite key length formula employing the smooth min- and max-entropy of Section 2.2.3, some of its chain rules and the *leftover hashing lemma* [115] within the composable security framework (Section 4.4.2.1).

Multiphoton states sent by Alice are insecure due to being vulnerable against PNS attacks in lossy channels, hence $p_{\text{click}} > p_{\text{mp}}$ is needed to ensure protocol security, as addressed in previous Section 3.6.2. Considering no decoy states, low-$g^{(2)}(0)$ SPSs hold this security condition at higher channel losses than one WCP, making them good candidates for non-decoy protocols. However, to evaluate the QKD performance of practical SPSs, it is necessary to compare it with a state-of-the-art decoy WCP protocol. Thus, we expand the analysis of the quantum dot in [42], where we present the theoretical non-decoy SPS model, to other SPSs with different characteristics, and we compare it with a 2-decoy WCP protocol of Section 3.6.2.1. This comparison is shown in our preprint paper [116].

In the decoy method, the single-photon and vacuum events are lower-bounded by analysing the statistics from the implemented multiple source intensities. In contrast, the non-decoy protocol estimates secure non-multiphoton events, lumping together the single-photon and vacuum events, excluding the insecure multiphoton events from the total sifted events, i.e. instances shared by both parties when they chose the same basis. It is essential to upper bound the sent multiphotons and also the multiphoton events received at Bob's side.

Our finite key treatment implemented significantly reduces the number of signals Bob must receive to approach the asymptotic case compared with widely used previous single-photon source QKD analyses. The most commonly employed non-decoy finite-key analysis for an SPS in the literature is based on [37] and presented in Section 4.4.2.2. In the comparison of our non-decoy SPS with the 2-decoy WCP protocol of Section 3.6.2.1, our results indicate regions of acquisition times where an SPS with moderate performance can outperform the 2-decoy state WCP source, particularly as the block sizes and losses decrease. These results suggest that near-term SPSs may provide key rate enhancement for short-range, short-duration QKD links. It is worth highlighting this chapter is mainly based on the contributions of our published paper [42] and the preprint [116].

4.1 Sender Model: Single-Photon Source Characterization

In contrast to other quantum sources such as WCP sources, whose photon emission follows a Poissonian distribution, the diversity of quantum mechanisms to build a practical SPS, each with its own set of unique properties, precludes the formulation of a general statistical distribution that fully captures all the infinite photon emission probabilities for any conceivable SPS. In practice, although experimental models exist for characterising the photon emission statistics, they are also inherently tied to a specific type of SPS [117].

Assuming this generalised theoretical distribution is highly unattainable, our initial

approach to characterise a practical SPS involved examining how to extract $g^{(2)}(0)$ for a general photon distribution with threshold detectors and limited initial information in a high-loss regime. The goal was to establish a fundamental limit for $g^{(2)}(0)$. However, this turned out to be challenging and required assumptions regarding photon number emissions not helpful for the QKD analysis. Therefore, acknowledging a prepare-and-measure protocol must avoid underestimating the multiphoton contribution on the receiver side, since these represent insecure events, we explore the idea of constructing a photon number distribution constrained by easily measurable SPS characteristics, such as the time-zero second-order correlation function $g^{(2)}(0)$ and the mean photon number $\langle n \rangle$. We then upper bound the multiphoton emissions using the $g^{(2)}(0)$ definition and mathematically prove that it represents a supremum of the set of all possible photon number distributions for an SPS.

First, let us introduce the second-order correlation function $g^{(2)}(\tau)$, which is a quantum optical property of interest and can be interpreted as the conditional probability that if a photon is measured a second photon will also be present. It can be expressed as

$$g^{(2)}(\tau) = \frac{\langle \hat{a}^\dagger(0)\hat{a}^\dagger(\tau)\hat{a}(\tau)\hat{a}(0)\rangle}{\langle \hat{a}^\dagger(0)\hat{a}(0)\rangle \langle \hat{a}^\dagger(\tau)\hat{a}(\tau)\rangle}, \tag{4.1}$$

where the creation and annihilation operators are denoted by $\hat{a}$ and $\hat{a}^\dagger$, respectively. It can also be simplified for time zero $\tau = 0$,

$$g^{(2)}(0) = \frac{\langle \hat{a}^\dagger(0)^2\hat{a}(0)^2\rangle}{\langle \hat{a}^\dagger(0)\hat{a}(0)\rangle^2}. \tag{4.2}$$

This time-zero second-order correlation function can also be written as follows

$$g^{(2)}(0) = \frac{\sum_{n=2}^{\infty} n(n-1)p_n}{\langle n \rangle^2} \tag{4.3}$$

$$g^{(2)}(0) = \frac{\overline{n^2} - \langle n \rangle}{\langle n \rangle^2}, \tag{4.4}$$

where p_n is the probability of emitting an n-photon state, $\langle n \rangle$ is the average photon number and $\overline{n^2}$ is its variance.

The second-order correlation function is measured in a Hanbury-Brown-Twiss con-

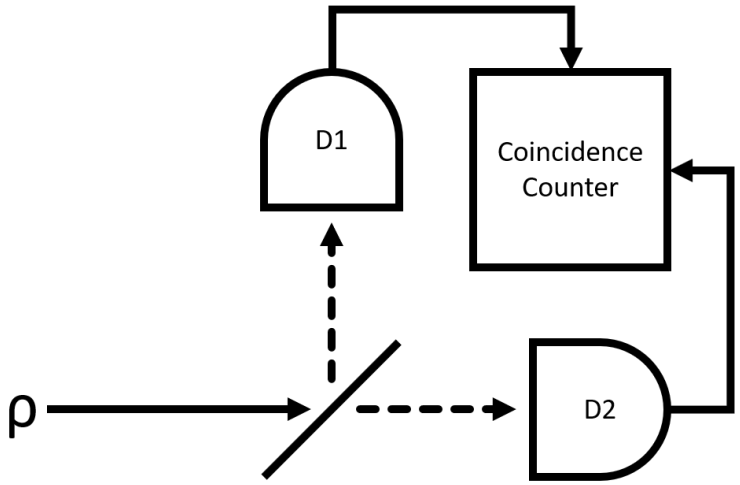

Figure 4.1: Hanbury-Brown-Twiss Measurement. An incident signal arrives at a 50:50 beamsplitter whose outputs are monitored by single photon detectors of equal detection efficiency. The detector clicks are correlated at a coincidence counter that also records the individual count rates of each detector.

figuration, see Figure 4.1. Let $C_{1,2}$ be the number of single counts in each detector, $D_{1,2}$, CC be the number of coincident counts and N_{inc} the total number of incident signals, then in the high loss limit (effective $\langle n \rangle \ll 1$),

$$g^{(2)}(0) \approx \frac{N_{\text{inc}} CC}{C_1 C_2}. \tag{4.5}$$

Thus, experimentally, implementing a Hanbury-Brown-Twiss (HBT) measurement one can observe the coincidence and individual counts of the detectors to estimate $g^{(2)}(0)$. For classical light, $g^{(2)}(0) \geq 1$, whereas for a perfect single-photon source $\{p_n = \delta_{1,n}\}$, $g^{(2)}(0) = 0$. For a Fock state $|n\rangle$, $g^{(2)}(0) = 1 - \frac{1}{n}$. We also note that for a single-photon source with non-unit efficiency, but otherwise zero multiphoton emission probability, $g^{(2)}(0) = 0$. However, even in extremely refined practical single-photon sources a small value of $g^{(2)}(0)$ is expected.

We seek a theoretical estimate of the source statistics that upper bounds the multiphoton emissions using the $g^{(2)}(0)$ definition. Assuming we have access to $g^{(2)}(0)$ by an HBT measurement and the mean photon number $\langle n \rangle$, which for example can be measured by using a power meter and knowledge of the source repetition rate, we derive the multiphoton upper bound of an SPS as follows.

First, we denote the true photon emission probabilities of the SPS in the Fock basis as $\{P_k^{(SPS)}\}_{k\in\mathbb{N}}$ for an infinite Hilbert space $\mathcal{H}$, where the multiphoton emission probability is $P_{\text{mp}}^{(SPS)} = \sum_{k\geq 2} P_k^{(SPS)}$. We assume these true probabilities are not directly accessible. However, knowing $g^{(2)}(0)$ and $\langle n\rangle$, the multiphoton probability can be upper-bounded as [118], [1]

$$P_{\text{mp}}^{(SPS)} \leq \overline{p}_{\text{mp}} = \frac{g^{(2)}(0)\,\langle n\rangle^2}{2}. \tag{4.6}$$

Here, uppercase P represents the true emission probabilities, while lowercase p denotes bounded estimates. This upper bound comes from the $g^{(2)}(0)$ definition, which using Eq. (4.3) can be expressed for the k-photon states as

$$g^{(2)}(0) = \frac{\sum_{k=2}^{\infty} k(k-1)P_k^{(SPS)}}{\langle n\rangle^2} \tag{4.7}$$

where $\langle n\rangle = \sum_{k=0}^{\infty} kP_k^{(SPS)}$ is the mean photon number and is lower-bounded as

$$g^{(2)}(0) = \frac{\sum_{k=2}^{\infty} k(k-1)P_k^{(SPS)}}{\langle n\rangle^2} \geq \frac{2\sum_{k=2}^{\infty} P_k^{(SPS)}}{\langle n\rangle^2} = \frac{2\,P_{\text{mp}}^{(SPS)}}{\langle n\rangle^2}, \tag{4.8}$$

which leads to the above mentioned $\overline{p}_{\text{mp}}$.

To later apply the exact formulas of the click probability (Section 4.2) and the pre-attenuated probabilities (Section 5.2), we aim to select the set of photon states emitted by Alice's source that precisely reaches $\overline{p}_{\text{mp}}$, ensuring no other combination of states exceeds this upper bound. We evaluate two types of distributions. First, we examine a pathological distribution, where all the emission probabilities are null except three: vacuum, single-photon and K-photon probabilities $\{p_0, p_1, p_K\}$, where $K \geq 3$ is a fixed value. In this case, all multiphotons are K-photon states, and any possible distribution yields a lower upper bound than $\overline{p}_{\text{mp}}$. As expected, when $K \to \infty$, the multiphoton probability approaches $\overline{p}_{\text{mp}}$. In Figure 4.2, we illustrate a finite set of pathological distributions that show this tendency when K increases. Thus, a

[1] Note the security QKD analysis of [118] is outdated because it is not valid against all general and collective eavesdropping attacks

pathological distribution with a sufficiently high K saturates the initial upper bound on the multiphoton probability of Eq. (4.6).

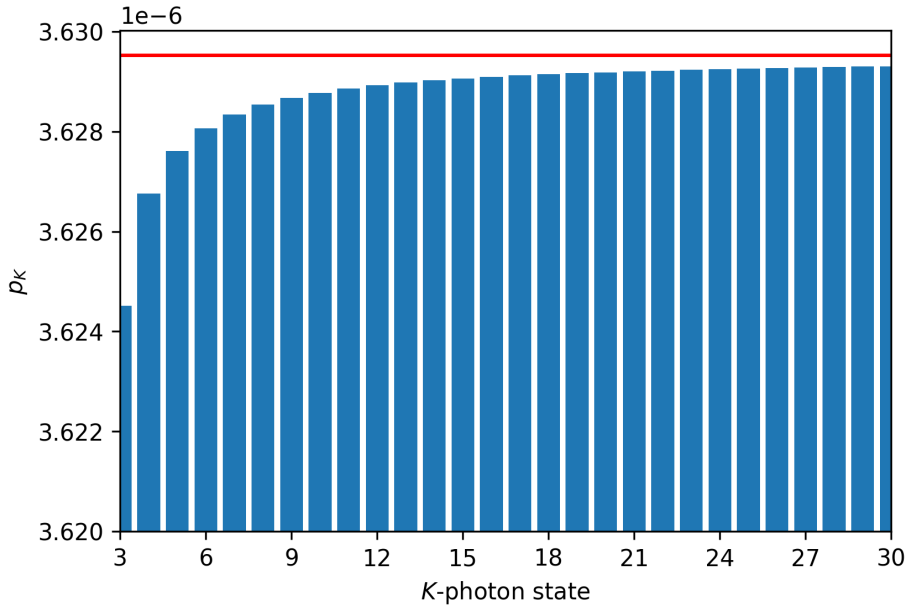

Figure 4.2: Multiphoton emission probability $p_{\text{mp}} = p_K$ of pathological distributions for different K-photon states. The solid red line represents the upper bound on the multiphoton probability $\overline{p}_{\text{mp}}$ of Eq. (4.6), considering $\langle n \rangle = 0.0142$ and $g^{(2)}(0) = 0.036$, which are the parameters of the quantum dot source of [42]. We take this particular SPS because it will be analysed in Section 4.5.1.

We consider an SPS that exhibits a monotonic decrease in its kth-order correlation functions $g^{(k+1)}(0) \leq g^{(k)}(0)$ for $k \geq 2$ when the order k increases, which is a reasonable assumption for realistic SPSs. Expressing each true emission probability of the SPS $P_k^{(SPS)}$ in terms of its associated $g^{(k)}(0)$, the upper bound of the true multiphoton probability is derived as follows

$$\begin{aligned} P_{\text{mp}}^{(SPS)} &= P_2^{(SPS)} + \sum_{k=3}^{\infty} P_k^{(SPS)} \\ &= \frac{g^{(2)}(0)\,\langle n \rangle^2}{2} + \sum_{k=3}^{\infty} \frac{k-1}{k} (-1)^k g^{(k)}(0)\,\langle n \rangle^k \\ &\leq \overline{P}_{\text{mp}}^{(SPS)} = \overline{p}_{\text{mp}} + g^{(2)}(0) \underbrace{\sum_{k=3}^{\infty} \frac{k-1}{k} (-1)^k\,\langle n \rangle^k}_{<0}, \end{aligned}$$

where we introduced Eq. (4.6), hence $\overline{P}_{\mathrm{mp}}^{(SPS)} \leq \overline{p}_{\mathrm{mp}}$. Note that this inequality holds for any truncated Hilbert space, making the summation finite. Though counterintuitive, we conclude that any distribution with states higher than two-photons decreases the overall multiphoton probability. Consequently, we find the truncated distribution $\{p_k\}_{k=0,1,2}$ with $p_{k>2} = 0$ reaches the maximum multiphoton upper bound $\overline{p}_{\mathrm{mp}}$, since it satisfies the equality $p_2 = \overline{p}_{\mathrm{mp}}$. Thus, Alice's emission probabilities read as

$$p_2 = \frac{g^{(2)}(0)\,\langle n\rangle^2}{2} \tag{4.9}$$

$$p_1 = \langle n\rangle - 2p_2 \tag{4.10}$$

$$p_0 = 1 - p_2 - p_1. \tag{4.11}$$

Waks [119] proposed the addition of linear attenuation of the signals prior to injection into the quantum channel, to heavily reduce the multiphoton emissions while leaving the $g^{(2)}(0)$ invariant. Thus, pre-attenuating Alice's source increases the maximum tolerable channel loss, defined as the highest loss that generates a positive key. In the high-loss regime, when the multiphoton contribution dominates, pre-attenuating the source provides a greater reduction in multiphoton emissions than in single-photon emissions, thereby enabling the generation of secure keys over a higher range of loss that was previously unattainable. The limit of the tolerable range is limited by the mentioned multiphoton contribution plus any background light and detector dark counts.

We define this pre-attenuation by a transmissivity value η_{tr}, representing the fraction of signal that passes through the attenuator to the quantum channel. This transmissivity reduces Alice's photon emission probabilities as follows

$$p_2^{(\mathrm{att})} = \frac{g^{(2)}(0)\eta_{\mathrm{tr}}^2\,\langle n\rangle^2}{2} \tag{4.12}$$

$$p_1^{(\mathrm{att})} = \eta_{\mathrm{tr}}\,\langle n\rangle - 2p_2^{(\mathrm{att})} \tag{4.13}$$

$$p_0^{(\mathrm{att})} = 1 - p_2^{(\mathrm{att})} - p_1^{(\mathrm{att})}. \tag{4.14}$$

where the new pre-attenuated mean photon number is $\langle n\rangle_{\mathrm{att}} = \eta_{\mathrm{tr}}\,\langle n\rangle$. The key enhancement can be mathematically shown by comparing the effect of the pre-attenuation

on the click probability of Bob's detectors and Alice's multiphoton emission probability. We discuss this in the following section, where the detection probability is introduced.

Furthermore, we consider a single mode of light emitted by an SPS with annihilation operator $\hat{a}$ and Fock states $\{|n\rangle\}$. A general density operator $\rho = \sum_{n,m=0}^{\infty} p_{nm}^{(\mathrm{att})} |n\rangle \langle m|$, $\rho \geq 0$ and $\mathrm{Tr}[\rho] = 1$. We assume there are no coherences (off-diagonal elements of the density matrix) between photon number states of Alice's SPS. In other words, we assume Alice's mixed state can be represented as a statistical mixture of pure states and lacks such coherences. Therefore, the density matrix is diagonal in the photon number basis,

$$\rho = \sum_{n=0}^{\infty} p_n^{(\mathrm{att})} |n\rangle \langle n| , \tag{4.15}$$

where $p_n^{(\mathrm{att})}$ represents the pre-attenuated probability of an n-photon emission. This density operator is described using Schmidt decomposition as introduced in Eq. (2.14).

4.2 Receiver Model: Detection Events Simulation

In this section, we present a theoretical model to simulate the counts of Bob's apparatus. In a real-life QKD implementation, experimentalists directly work with the observed count rates from their devices to estimate the generated secure key. Hence, this section does not concern them. However, since we are performing a theoretical analysis, it is necessary to simulate the number of counts on the receiver side. It is important to note that when we estimate the secure key in the finite-key analysis, we will blind ourselves from this simulation model and will treat the counts as if they were gathered from a real QKD experiment.

Considering the commonly employed single-photon avalanche diode (SPAD) detector in the Geiger mode, which only gives two outcomes, firing when a photon is detected and not firing when there is no photon. The operator that represents when a detection event occurs is defined as

$$\hat{\Pi}_{nc} = \sum_{n} (1 - p_{\mathrm{dc}}) (1 - \eta_{\mathrm{det}})^n |n\rangle \langle n| , \tag{4.16}$$

where η_{det} is the detector efficiency, i.e. the probability of the detector firing when a photon arrives, hence a perfect detector would be $\eta_{\text{det}} = 1$, and p_{dc} is the dark count probability. While the operator of getting a click in the detector is given by $\hat{\Pi}_c = 1 - \hat{\Pi}_{nc}$. Therefore, for the given diagonal density operator of Eq. (4.15), the probability of getting a detection event is $p_{\text{click}} = \text{Tr}\left[\rho\,\hat{\Pi}_c\right]$, which represents the probability of obtaining an outcome at Bob's apparatus when a POVM is performed, as described in Eq. (2.25). It can be calculated as

$$\begin{aligned} p_{\text{click}} = \text{Tr}\left[\rho\,\hat{\Pi}_{\text{c}}\right] &= \sum_n p_n^{(\text{att})}\left[1-(1-p_{\text{dc}})\,(1-\eta_{\text{ch}}\eta_{\text{det}})^n\,\text{Tr}\left[|n\rangle\,\langle n|n\rangle\,\langle n|\right]\right] \\ &= 1-(1-p_{\text{dc}})\sum_n p_n^{(\text{att})}\,(1-\eta_{\text{ch}}\eta_{\text{det}})^n\,, \end{aligned} \tag{4.17}$$

where p_{dc} is the dark count probability, η_{ch} is the channel efficiency, η_{det} is the efficiency of each detector and the summation of all photon emission probabilities $\sum_n p_n = 1$ is applied. If the efficiency and dark counts of the detectors for each basis are not the same, one can adapt the click probability to their different experimental detector characterisation between bases as follows

$$p_{\text{click}}^{X,Z} = 1-\left(1-p_{\text{dc}}^{X,Z}\right)\sum_n p_n^{(\text{att})}\left(1-\eta_{\text{ch}}\eta_{\text{det}}^{X,Z}\right)^n. \tag{4.18}$$

Note that $p_{\text{click}}^{X,Z}$ and $\eta_{\text{det}}^{X,Z}$ are the average of the two detectors associated with each polarisation of a basis.

For simplicity, let us assume the detectors of each basis behave identically, hence $p_{\text{click}}^{X} \equiv p_{\text{click}}^{Z} \equiv p_{\text{click}}$. Then, we lump together the channel and detector efficiencies into the system efficiency $\eta_{\text{sys}} \equiv \eta_{\text{ch}}\eta_{\text{det}}$. An approximation of this click probability can be derived considering a Taylor expansion of the function $f\,(\eta_{\text{sys}}) = p_n^{(\text{att})}\,(1-\eta_{\text{sys}})^n$ that is infinitely differentiable at zero. Thus, denoting the nth-derivative of the function

$f(\eta_{\text{sys}})$ as $f^{(n)}(\eta_{\text{sys}})$, the power series is a Maclaurin series that takes the form

$$\begin{aligned} f(\eta_{\text{sys}}) &= \sum_{n}^{\infty} f^{(n)}(0)\,\frac{\eta_{\text{sys}}^{n}}{n!} \\ &= f^{(0)} + f^{(1)}\eta_{\text{sys}} + f^{(2)}\frac{\eta_{\text{sys}}^{2}}{2} + f^{(3)}\frac{\eta_{\text{sys}}^{3}}{6} + \dots \\ &= p_{n}^{(\text{att})}\left(1 - n\eta_{\text{sys}} + \frac{n(n-1)}{2}\eta_{\text{sys}}^{2} + \frac{n(n-1)(n-2)}{6}\eta_{\text{sys}}^{3} + \dots\right). \end{aligned} \tag{4.19}$$

By considering the relevant terms in the series, making a first order approximation $f(\eta_{\text{sys}}) \approx p_n(1 - n\eta_{\text{sys}})$ and replacing it in Eq. (4.17), we can approximate the click probability under realistic system efficiency conditions as

$$p_{\text{click}} \approx p_{\text{dc}} + (1 - p_{\text{dc}})\,\eta_{\text{sys}} \sum_{n}^{\infty} n p_{n}^{(\text{att})} = p_{\text{dc}} + (1 - p_{\text{dc}})\,\eta_{\text{sys}}\,\langle n\rangle_{\text{att}}\,, \tag{4.20}$$

where $\langle n\rangle_{\text{att}} = \sum_n n p_n^{(\text{att})}$ is the mean photon number.

Increasing the loss between the source and measurement through introducing an attenuator after Alice's source results in key rate enhancement for lossy channels since linear loss leaves $g^{(2)}(\tau)$ invariant. This pre-attenuation is determined by the transmissivity value η_{tr}, which reduces the multiphoton probability of Eq. (4.6) quadratically $\overline{p}_m^{(\text{att})} = g^{(2)}(0)\eta_{\text{tr}}^2\langle n\rangle^2/2$, while decreasing the click probability at Bob's detectors linearly at a first-order Taylor approximation, $p_{\text{click}} \approx p_{\text{dc}} + (1 - p_{\text{dc}})\,\eta_{\text{tr}}\eta_{\text{sys}}\langle n\rangle$. Therefore, the multiphoton probability decreases more rapidly than the click probability on Bob's side. This enhances the key generation at the high-loss regime, where $\overline{p}_m^{(\text{att})}$ dominates, by reducing the multiphoton contribution more than the total detection rate, thereby increasing the ratio between non-multiphotons (secure events) and multiphotons (insecure events which are discarded). Consequently, it also widens the range of tolerable losses of the QKD system. Note that the pre-attenuation of the source impacts key generation in the range of losses where multiphoton states dominate Alice's emissions. The impact of Alice's pre-attenuation is shown in Figure 4.4.

Although we compute the exact expression in our model, the click probability approximation of Eq. (4.20) is valid for most practical SPS as multiphoton states do not

dominate its photon emission, which is mainly dictated by vacuum states and a smaller portion of single-photons. To avoid answering the question of how many photons one must assume are contained in the emitted multiphoton states to securely simulate Bob's count, previous studies used to employ even a further approximated detection probability than Eq. (4.20), $p_{\text{click}} \approx p_{\text{dc}} + \eta_{\text{sys}} \langle n \rangle$, which is valid if the dark counts of the detector are extremely low [118]. However, this question has already been answered in Section 4.1, stating that to reach the maximum upper bound of the multiphoton emission probability, which is one of the QKD security requirements, one must consider all multiphotons are two-photon states. Thus, the click probability approximation is not needed anymore and if one aims to compute an SPS distribution that does not operate dominated by vacuum and single-photon, it is now possible by using the emission probabilities of Eqs. (4.12), (4.13) and (4.14) in the exact click probability expression of Eq. (4.17) or (4.18). Avoiding concern about distancing from its first-order Taylor approximation. Thus, we provide a more general solution to the problem of partially characterising the SPS while upper-bounding the multiphoton emissions compared to previous studies.

It is worth noting that we do not state that practical SPS emits multiphotons that are exclusively two-photon states in real life. We do not assume anything about the true SPS emission probabilities $\{P_k^{(SPS)}\}_{k\in\mathbb{N}}$. We simply partially characterise these unknown true probabilities by upper bounding the multiphoton emissions, which prevents us from underestimating the multiphoton contribution and being vulnerable against PNS attacks.

To simulate Bob's counts, we estimate the detection events, where the parties select the same basis and the errors. Then, let us introduce the error probability on either basis

$$p_{\text{err}}^{X,Z} = \frac{p_0\, p_{dc}^{X,Z}}{2} + \sum_{n=1}^{\infty} p_n^{(att)} \left[1 - (1 - p_{dc}^{X,Z})(1 - \eta_{ch}\eta_{det}^{X,Z})^n p_{\text{mis}}\right], \tag{4.21}$$

where p_{mis} is the probability of error due to the misalignment of the set-up. Maintaining the general approach where the detectors of each basis may have different efficiency and

dark counts, the detection probability on Bob's side is estimated by introducing Alice's pre-attenuated emission probabilities of Eqs. (4.14), (4.13) and (4.12) in Eq. (4.18). Suppose Alice and Bob consider the same basis bias, i.e. they both have an identical probability of selecting the X basis or the Z basis, given by $p_X \equiv p_X^A = p_X^B$ and $p_Z = 1 - p_X \equiv p_Z^A = p_Z^B$, respectively. Considering N_{S} the number of sent signals by Alice, after sifting, when the parties discard the events with an unmatched basis, the number of detection events and errors, which are directly observed in a QKD experiment, are simulated as follows.

The number of received events by Bob when both parties chose either the Z or the X basis are $N_{\mathrm{R}}^X = N_{\mathrm{S}} p_X^2 p_{\mathrm{click}}^X$ and $N_{\mathrm{R}}^Z = N_{\mathrm{S}} p_Z^2 p_{\mathrm{click}}^Z$. We also determine the errors as $m_X = N_S p_X^2 p_{\mathrm{err}}^X$ and $m_Z = N_S p_Z^2 p_{\mathrm{err}}^Z$, which are the instances where the parties chose the same basis but the detector of the opposite basis fired. The legitimate parties publicly compare the Z basis results to determine the number of errors m_Z, while the X basis results are never directly revealed, since we adopt the efficient BB84 convention, where the Z basis is used for parameter estimation and the X basis for key generation (see further details in Section 3.6).

4.3 Optimisation of Protocol Parameters

To maximise the key rate and tolerable loss of the protocol whilst maintaining security, we optimise the basis bias p_X, i.e. the probability of choosing the X basis. It is important to optimise this unequal basis bias p_X in efficient BB84 since it balances the amount of raw key bits (proportional to p_X^2) and parameter estimation signals (proportional to $(1 - p_X)^2$). We also optimise Alice's source pre-attenuation by the transmissivity parameter η_{tr} for each channel loss. These optimisations provide some improvement over standard protocol values, such as equal basis choice and no attenuation.

Alice and Bob randomly and independently choose their basis for each signal with bias p_X and p_Z. Concretely, the legitimate parties form the following data block after Alice sends N_{S} states from her pre-attenuated SPS and Bob measures them, obtaining N_{R} detection events: the discarded events due to sifting $N_{\mathrm{R}} 2 p_X (1 - p_X)$, i.e. when the parties choose different bases, the events used for key generation $N_{\mathrm{R}} p_X^2$ and the

events used for parameter estimation $N_{\mathrm{R}}\,(1-p_X)^2$. The sifting ratio is $p_{\mathrm{sift}} = p_X^2 + (1-p_X)^2 = 1 - 2p_X(1-p_X) > \frac{1}{2}$ for unequal bias, higher than the sifting ratio $\frac{1}{2}$ for $p_X = \frac{1}{2}$ as in standard BB84. Additionally, this simplification also reduces the number of parameters to be estimated, hence improving finite-statistical bounds and the reduction in key length due to composable security parameters [97, 120–123].

At long channel distances (high losses), the key rate is limited by the multiphoton emission and dark count probabilities. When the upper bound on the number of multiphoton emissions exceeds the number of detections, then Eve can have full information about Alice's key bit string by exploiting these multiphotons performing PNS attacks, as explained in Section 3.6.2 in more detail. Consequently, since the multiphoton contribution is insecure and must be discarded, applying pre-attenuation reduces the multiphoton emissions by a factor of η_{tr}^2 whilst the mean photon number is only reduced by η_{tr}, which has a linear dependence with the first-order approximation of p_{click}. This optimises the distance range tolerable by the parties. At high losses and with sufficiently low dark count rates, the reduction in detection probability (and increase in QBER) may be offset by the greater fraction of Bob's received events being the result of non-multiphoton emissions by Alice, potentially leading to increased key rate and extending the non-zero key rate region to longer ranges.

4.4 Security Analysis

We distinguish two scenarios for the secure key length estimation: the asymptotic case and finite-key analysis. In the asymptotic limit, it is traditionally assumed that the experiment runs for an infinite duration, resulting in a large block of statistics that tends to infinity, in which case one obtains Eq. (3.25). However, taking the limit where the number of sent or received signals tends to infinity does not yield to a computable result in the entropy equations.

To solve this, we can reinterpret the conditions of the asymptotic limit. Given that the asymptotic data block is sufficiently large, it allows us to consider $p_X \to 1$ (key generation basis), which implies that the sifting ratio also approaches unity $p_{\mathrm{sift}} =$

$p_X^2 + (1 - p_X)^2 \to 1$. Additionally, the phase error rate becomes negligible, hence $p_Z \to 0$. Consequently, the count rates converge to their underlying true expectation values.

In a real experiment, the obtained statistics are finite and subject to fluctuations from their expected outcomes. Thus, when assessing the performance of a practical QKD system the finite key rate must be considered. Consequently, studies were proposed to account for the effect of finite statistics [36]. To date, experimental work with single-photon emitters [124,125] have used the method outlined in [126] to derive finite block size estimates of the secure key. Since the publication of [126], there have been considerable developments in tighter statistical estimation bounds, mainly in the context of weak coherent pulse decoy states and entangled protocols. Here, we adapt and employ recent results based on Chernoff bounds to produce significant improvements in the finite key rate. This reduces the block size required for a positive key rate or, conversely, results in a much greater key rate for a fixed block size.

4.4.1 Asymptotic Limit

Here, we estimate the asymptotic key rate (AKR) by introducing correction terms for Eq. (3.11), which will lead us to a different AKR from Eq. (3.25). This update ensures the exclusion of multiphoton events in the key generation basis X, which are insecure (vulnerable to PNS attacks). Therefore, a correction factor must be added to the first von Neumann entropy in Eq. (3.11), $S(A|E)$. This entropy characterises the correlation between Alice's A and Eve's system E. We also need to introduce a factor of the number of signals used in the error correction process for the second conditional entropy of Eq. (3.11), $S(A|B)$, which represents the correlation between Alice and Bob. Finally, it is required to divide by the total number of sent signals by Alice N_{S} for both entropy terms of Eq. (3.11), since it is a rate.

Let us introduce several quantities from the observed and expected statistics received by Bob after sifting before addressing the AKR for the non-decoy SPS protocol. The multiphoton events of the key generation basis are $N^X_{\mathrm{R,mp}} = N_{\mathrm{S}} p_X^2 \overline{p}^{(att)}_{\mathrm{mp}}$, where the click probability for a given multiphoton sent by Alice is considered to be unity.

Otherwise, we might be underestimating the multiphoton contribution on Bob's side. We can also interpret this as assuming Eve exploits every multiphoton emission and creates a detection on Bob's devices. Note that $N_{\mathrm{R,mp}}^{X*}$ is an expected value and cannot be directly observed by Bob, where * denotes any expected value. The observed quantities by Bob are exclusively the detection events in each basis, N_{R}^{X} and N_{R}^{Z}, and the errors, m_X and m_Z, as described in the receiver model of Section 4.2. In this non-decoy method, we lump together the vacuum and single-photon events into the non-multiphoton events, since the absence of additional decoy states prevents us from characterising them separately. Knowing this, we can estimate the non-multiphoton events on the X basis, which are the secure events that form the key,

$$N_{\mathrm{R,nmp}}^{X} = N_{\mathrm{R}}^{X} - N_{\mathrm{R,mp}}^{X} = N_{\mathrm{S}} p_X^2 \left(p_{\mathrm{click}}^{X} - \overline{p}_{\mathrm{mp}}^{(att)} \right). \tag{4.22}$$

Similarly, for the parameter estimation basis

$$N_{\mathrm{R,nmp}}^{Z} = N_{\mathrm{R}}^{Z} - N_{\mathrm{R,mp}}^{Z} = N_{\mathrm{S}} p_Z^2 \left(p_{\mathrm{click}}^{Z} - \overline{p}_{\mathrm{mp}}^{(att)} \right). \tag{4.23}$$

The ratio between these non-multiphotons in the X basis and N_{S} is the correction factor introduced in the first entropy of the asymptotic key rate in Eq. (3.11), thus

$$S(A|E) = \frac{N_{\mathrm{R,nmp}}^{X}}{N_{\mathrm{S}}} \left[1 - h_2\left(\phi^X \right) \right] = p_X^2 \left(p_{\mathrm{click}}^{X} - \overline{p}_{\mathrm{mp}}^{(att)} \right) \left[1 - h_2\left(\phi^X \right) \right], \tag{4.24}$$

where the phase error rate of the X basis is estimated using the parameter estimation basis Z

$$\phi^X = \frac{m_Z}{N_{\mathrm{R,nmp}}^{Z}} = \frac{p_{\mathrm{err}}^{Z}}{p_{\mathrm{click}}^{Z} - \overline{p}_{\mathrm{m}}^{(att)}}. \tag{4.25}$$

While the second entropy of Eq. (3.11) is modified as

$$S(A|B) = f_{\mathrm{EC}} \frac{N_{\mathrm{R}}^{X}}{N_{\mathrm{S}}} h_2(e_X) = f_{\mathrm{EC}} p_{\mathrm{click}}^{X} p_X^2 h_2(e_X) \tag{4.26}$$

where $f_{\mathrm{EC}} = 1$ is the error correction efficiency factor in the asymptotic limit and $e_X = m_X / N_{\mathrm{R}}^{X}$ is the quantum bit error rate (QBER) on the X basis.

Applying the asymptotic limit as described above, the key rate is given by

$$R^{(asym)}_{\mathrm{ND-SPS}} \geq \lim_{\substack{p_X \to 1 \\ p_Z \to 0}} \left(S(A|E) - S(A|B) \right). \tag{4.27}$$

Replacing Eqs. (4.24), (4.25) and (4.26) in the asymptotic limit of Eq. (4.27), the final asymptotic key rate in terms of the number of events for the non-decoy SPS is given by

$$R^{(asym)}_{\mathrm{ND-SPS}} \geq \lim_{\substack{p_X \to 1 \\ p_Z \to 0}} \frac{1}{N_{\mathrm{S}}} \left\{ N^X_{\mathrm{R,nmp}} \left[1 - h_2 \left(\frac{m_Z}{N^Z_{\mathrm{R,nmp}}} \right) \right] - N^X_{\mathrm{R}} h_2 \left(\frac{m_X}{N^X_{\mathrm{R}}} \right) \right\}, \tag{4.28}$$

and in terms of probabilities

$$\begin{aligned} R^{(asym)}_{\mathrm{ND-SPS}} &\geq \lim_{\substack{p_X \to 1 \\ p_Z \to 0}} p_X^2 p^X_{\mathrm{click}} \left\{ \left(1 - \frac{\overline{p}^{(att)}_{\mathrm{mp}}}{p^X_{\mathrm{click}}} \right) \left[1 - h_2 \left(\frac{p^Z_{\mathrm{err}}}{p^Z_{\mathrm{click}} - \overline{p}^{(att)}_{\mathrm{m}}} \right) \right] - h_2 \left(\frac{p^X_{\mathrm{err}}}{p^X_{\mathrm{click}}} \right) \right\} \\ &\geq p^X_{\mathrm{click}} \left\{ \left(1 - \frac{\overline{p}^{(att)}_{\mathrm{mp}}}{p^X_{\mathrm{click}}} \right) \left[1 - h_2 \left(\frac{p^Z_{\mathrm{err}}}{p^Z_{\mathrm{click}} - \overline{p}^{(att)}_{\mathrm{m}}} \right) \right] - h_2 \left(\frac{p^X_{\mathrm{err}}}{p^X_{\mathrm{click}}} \right) \right\}. \end{aligned} \tag{4.29}$$

Introducing the non-multiphoton fraction in either basis, i.e. the probability that a sent non-multiphoton state causes a click on Bob's detector, which reads as

$$\Delta^{X,Z}_{\mathrm{nmp}} = 1 - \frac{\overline{p}^{(att)}_{\mathrm{mp}}}{p^{X,Z}_{\mathrm{click}}}, \tag{4.30}$$

the asymptotic key rate can be also written as

$$R^{(asym)}_{\mathrm{ND-SPS}} \geq p^X_{\mathrm{click}} \left\{ \Delta^X_{\mathrm{nmp}} \left[1 - h_2 \left(\frac{p^Z_{\mathrm{err}}}{p^Z_{\mathrm{click}} \Delta^Z_{\mathrm{nmp}}} \right) \right] - h_2 \left(\frac{p^X_{\mathrm{err}}}{p^X_{\mathrm{click}}} \right) \right\}. \tag{4.31}$$

Note these three expressions represent the same asymptotic rate.

Assuming the same click and error probabilities for both basis, $p_{\mathrm{click}} \equiv p^X_{\mathrm{click}} = p^Z_{\mathrm{click}}$ and $p_{\mathrm{err}} \equiv p^X_{\mathrm{err}} = p^Z_{\mathrm{err}}$, i.e. assuming the four detectors on Bob's side, corresponding to the four polarisations, have the same detection efficiency and dark counts, the AKR of

the non-decoy SPS protocol can be simplified as

$$R_{\mathrm{ND-SPS}}^{(asym)} \geq p_{\mathrm{click}} \left\{ \Delta_{\mathrm{nmp}} \left[1 - h_2 \left(\frac{p_{\mathrm{err}}}{p_{\mathrm{click}} \Delta_{\mathrm{nmp}}} \right) \right] - h_2 \left(\frac{p_{\mathrm{err}}}{p_{\mathrm{click}}} \right) \right\}, \tag{4.32}$$

where $\Delta_{\mathrm{nmp}} = 1 - \overline{p}_{\mathrm{mp}}^{(att)} / p_{\mathrm{click}}$.

4.4.2 Finite-Key Analysis

In practical QKD implementation, generating large block sizes to produce secure key bits shared by the parties is typically costly and time-consuming. Therefore, it is necessary to treat smaller finite blocks that are not in the asymptotic regime. Here, we present the derivation of the secure key length formula for the finite-key analysis using the smooth min- and max-entropy of Section 2.2.3 and the failure probabilities related to the security parameters of the protocol. In the absence of the asymptotic limit, where the channel is only used a small number of times, the von Neumann entropy is no longer justified. However, the smooth entropies overcome this limitation, e.g. the min-entropy enables bounding the conditional entropy between Alice and Eve for finite blocks of data. Reaching a tight estimate of the min-entropy is a challenging task since the parties can only estimate it by using the observed statistics in the parameter estimation step. In other words, the min-entropy employed here cannot be directly computed since the parties are unaware of Eve's behaviour. Hence, the state that defines Alice's key and Eve's side information is not known. Here, we first introduce our novel finite-key analysis for the non-decoy SPS protocol inspired by up-to-date techniques commonly employed in decoy WCP protocols. Our analysis uses tighter bounds on the smooth entropies and the characterisation of the finite-key effects using the Chernoff bound compared to previous literature. Next, we introduce the finite-key analysis of [126], commonly extended as the model to estimate finite key rates for non-decoy SPS. In Section 4.5, we will compare the key rate performance of both methods.

4.4.2.1 Secure Key Length Estimation

To derive the finite key formula, we use uncertainty relations to bound Bob's raw key obtained from Alice's raw key and conditioned on Eve's information. First, consider Eve's information E and Alice's raw key K_A, which is generated by choosing a random sample from N_{R}^{X}, after the error correction and verification steps. In particular, K_A is a random classical bit string that can take any value $k \in \mathcal{K}_A$ with probability $p(k)$, where $\mathcal{K}_A$ is Alice's key space. Let $\rho_{E|k}$ be the state on the Hilbert space $\mathcal{H}_E$ conditioned on $K_A = k$. The question is how much information Eve can extract from K_A that is completely unknown to her. To do so, Eve possesses a *classical-quantum* (cq) state correlated with the bit values of Alice's key, similar to Eq. (3.20),

$$\rho_{K_A E} = \sum_{k \in \mathcal{K}_A} p(k) \left|k\right\rangle \left\langle k\right| \otimes \rho_E^k, \tag{4.33}$$

where $\{|k\rangle\}_{k \in \mathcal{K}_A}$ is an orthonormal basis representing Alice's possible keys. Eve aims to gain information about K_A by measuring her state ρ_E^k. The probability of Eve correctly guessing K_A applying an optimal extraction strategy is given by

$$p_{\mathrm{guess}}\left(K_A|E\right) = \max_k \sum_e p_E(e) p_{K_A|E=e}(k). \tag{4.34}$$

In the classical case, this optimal strategy means to guess the value k of K_A with the highest conditional probability $p_{K_A|E=e}(k)$ for each value e of E. The probability of guessing K_A given E is defined as the min-entropy (Definition 8) [101],

$$H_{\min}\left(K_A|E\right)_\rho = -\log p_{\mathrm{guess}}\left(K_A|E\right). \tag{4.35}$$

In other words, the operational interpretation of this quantity is the number of uniformly random classical bits that can be extracted from K_A, using the optimal guessing strategy with access to E.

Furthermore, assume that Bob can extract a part K_B of K_A with length ℓ, uniformly conditioned on the information E. Thus, there is a function f_s that maps K_A to Bob's raw key $K_B = f_s(K_A)$ considering the quantum state between Alice and Eve $\rho_{K_A E}$ is

fixed. The probability of guessing K_B is $p_{\text{guess}}(K_B|E) = 2^{-\ell}$ and analogously to Eq. (4.35), we obtain,

$$H_{\min}(K_B|E)_\rho = \ell, \tag{4.36}$$

where ℓ is the secure key length. Furthermore, because K_B is derived from K_A, the probability of correctly guessing K_B must be greater than the probability of guessing K_A. Therefore, the min-entropies of the parties' keys, K_A and K_B, conditioned on Eve's system E, can be expressed with the following inequality

$$H_{\min}(K_B|E)_\rho \leq H_{\min}(K_A|E)_\rho \Rightarrow \ell \leq H_{\min}(K_A|E)_\rho . \tag{4.37}$$

To extend this to the general case of almost uniform randomness, the smooth min-entropy $H^{\varepsilon}_{\min}(K_A|E)$ needs to be introduced. This is set as the maximum value of $H_{\min}(K_A|E)$ and it is defined in Definition 11. For privacy amplification, we consider that Alice and Bob apply a two-universal hash function. The *leftover hashing lemma* provides an exact equation for the inequality of Eq. (4.37) using the smooth min-entropy of Definition 11 to relate Eve's information E and Alice's raw key K_A

$$\ell = H^{\varepsilon}_{\min}(K_A|E)_\rho - 2\log\frac{1}{2\varepsilon_{\text{PA}}} \tag{4.38}$$

which gives the maximum number of extractable bits ℓ that are ε_{PA}-close to uniform, conditioned on E.

We consider leakage λ_{EC} during error correction and additional bits for verification. Thus, the information that remains in Eve's system E' after error correction is related to,

$$H^{\varepsilon}_{\min}(K_A|E)_\rho \geq H^{\varepsilon}_{\min}\left(K_A|E'\right)_\rho - \lambda_{\text{EC}} - \log\frac{2}{\varepsilon_{\text{cor}}} \tag{4.39}$$

where ε_{cor} is the error correction failure probability. The number of bits sacrificed in performing the error correction code is tightly determined by the bound of Eq. (3.51). As explained in Section 3.6.2.1, if the efficiency factor of error correction is below 1.16, which is the limit set by practical codes, we recover the Shannon limit for $\lambda_{\text{EC}} = 1.16 N^X_{\text{R}} h_2(e_X)$. In any case, to estimate this, the QBER of the X basis is used.

However, note that the errors m_X are not publicly revealed and are exclusively used to estimate the number of bits required to perform error correction. In a real experiment, one just runs the code and knows exactly how many bits are leaked.

We use an uncertainty relation for smooth min-entropy to establish a bound between the remaining information that Eve has, E', and Alice's raw key, K_A. This reflects the principle that the more accurately Bob can estimate Alice's raw key Z_A in the Z basis, the worse Eve can guess Alice's raw key K_A in the X basis, formally expressed as [127]

$$H_{\min}^{\varepsilon}\left(K_A|E'\right)_{\rho} \geq q\, N_{\mathrm{R,nmp}}^{X} - H_{\max}^{\varepsilon}\left(Z_A|Z_B\right)_{\rho}, \tag{4.40}$$

where Z_B is Bob's raw key on the Z basis. This smooth min-entropy is limited to the non-multiphoton events in the key generation basis X (Eq. 4.22) and the used smooth max-entropy is introduced in Definition 12. Here, q quantifies the efficiency of Bob's orthogonal qubit measurements and it is given by

$$q = \log \frac{1}{\max_{k,z} ||\sqrt{M_x}\sqrt{N_z}||_{\infty}^2} \tag{4.41}$$

where $k \in \mathcal{K}_A$ and $z \in \mathcal{Z}_A$ and $\{M_k\}$ and $\{N_z\}$ are two POVMs acting on $\mathcal{K}_A$ and $\mathcal{Z}_A$, respectively. The norm $||\cdot||_{\infty}$ evaluates the largest singular value. Considering projective and rank-one measurements, i.e. $M_k = |k\rangle\langle k|$ and $N_z = |z\rangle\langle z|$, Eq. (4.41) reduces to

$$q = \log \frac{1}{\max_{k,z} |\langle k|z\rangle|^2} \tag{4.42}$$

which represents the maximum overlap between the two bases used by Alice, since the key bit values k correspond to the X basis (key generation basis). In a BB84 protocol with ideal state preparation used by Alice $q = 1$, which is what we assume in this work. However, in practice, the sent states by Alice are not perfect qubits and when Alice's bases are not perfectly complementary to each other, q is reduced accordingly [128].

The smooth max-entropy $H_{\max}^{\varepsilon}\left(Z_A|Z_B\right)_{\rho}$ of Z_A conditioned on Z_B measures the remaining uncertainty in Z_A given knowledge of Z_B. When Z_B and Z_A are highly correlated, $H_{\max}^{\varepsilon}\left(Z_A|Z_B\right)_{\rho}$ is small, implying a small number of observed errors, as

shown by the following bound [127],

$$H_{\max}^{\varepsilon}\left(Z_A|Z_B\right)_{\rho} \leq N_{\mathrm{R,nmp}}^{X} h_2(\phi^X), \tag{4.43}$$

where ϕ^X is the phase error rate of non-multiphoton events on the X basis. Hence, introducing Eq. (4.43) in the bound of the min-entropy of Eq. (4.40), we obtain

$$H_{\min}^{\varepsilon}\left(K_A|E'\right)_{\rho} \geq N_{\mathrm{R,nmp}}^{X}\left[1-h_2(\phi^X)\right]. \tag{4.44}$$

Finally, replacing Eqs. (4.39) and (4.44) into Eq. (4.38), we derive the secure key length (SKL) formula

$$\ell_{\mathrm{ND}}^{(\mathrm{SPS})} \geq N_{\mathrm{R,nmp}}^{X}\left[1-h_2\left(\phi^X\right)\right] - \lambda_{\mathrm{EC}} - 2\log\frac{3}{\varepsilon_{\mathrm{sec}}} - \log\frac{2}{\varepsilon_{\mathrm{cor}}}. \tag{4.45}$$

The secrecy parameter of the protocol is $\varepsilon_{\mathrm{sec}} \geq \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}}$ where: $\varepsilon_{\mathrm{PA}} = \varepsilon'$ is the privacy amplification failure probability; $\varepsilon_{\mathrm{PE}} = 2n_{\mathrm{PE}}\varepsilon'$ is the parameter estimation failure probability where $n_{\mathrm{PE}} = 2$ is the number of constraints quantified in classical post-processing; $\varepsilon_{\mathrm{EC}} = \varepsilon'$ is the error correction failure probability. Thus, the secrecy comes from setting each failure probability to a common value ε', i.e. $\varepsilon_{\mathrm{sec}} = 6\varepsilon'$, hence $\varepsilon_{\mathrm{PA}} = \varepsilon_{\mathrm{sec}}/6$. Moreover, the QKD protocol is $\varepsilon_{\mathrm{qkd}}$-secure if it is $\varepsilon_{\mathrm{cor}}$-correct and $\varepsilon_{\mathrm{sec}}$-secret with $\varepsilon_{\mathrm{qkd}} \geq \varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}}$.

The secure key rate is calculate as $R_{\mathrm{ND}}^{(\mathrm{SPS})} = \ell_{\mathrm{ND}}^{(\mathrm{SPS})}/N_{\mathrm{S}}$. To estimate the secure key, we blind ourselves to the simulation model for Bob's counts in Section 4.2, and we directly work with the observed values as if gathered from a real QKD experiment. For this non-decoy protocol, Alice exclusively uses one source with one mean photon number (intensity). Hence, after sifting, Bob's observed detection events, N_{R}^{X} and N_{R}^{Z}, and errors, m_X and m_Z, in each basis are not subjected to any deviation, even though they are finite, since they are undoubtedly caused by Alice's unique source, hence no finite-key bound is applied to them. However, the multiphoton contribution on Bob's side, which is not accessible in a QKD experiment, is subjected to fluctuations from its expected outcomes. Consequently, the multiphoton events on Bob's side may

vary for every generated block. To estimate the secure key for the observed statistics taking into account the finite-key effects, one must apply a mathematical bound to the expected multiphoton events received by Bob in either basis, $\overline{N}^{X*}_{\mathrm{R,mp}}$ and $\overline{N}^{Z*}_{\mathrm{R,mp}}$, to obtain and upper bounds of their observed values. Note the overline symbol of these expected values represents an upper bound that comes from Alice's bound on her pre-attenuated multiphoton emission probability. Otherwise, assuming these expected values will always be the exact number of multiphotons in every run of the QKD protocol brings a security threat. Since for some protocol runs we would certainly have more multiphoton than $N^{X*}_{\mathrm{R,mp}}$ plus $N^{Z*}_{\mathrm{R,mp}}$. Hence, that assumption would cause an overestimation of the number of secure key bits. We apply the finite-key analysis for the non-decoy protocol as follows.

With generality, we define the number of multiphoton states received by Bob as a finite set of independent Bernoulli random variable $\{X^B_1, X^B_2, \cdots, X^B_{N_\mathrm{S}}\}$ with two possible outcomes $\{0, 1\}$. Its observed value is $X^B \equiv \sum_{i=1}^{N_\mathrm{S}} X^B_i$ that satisfy $\Pr\left(X^B_i = 1\right) = P_{i,\mathrm{click}|m}\, P^{(att)}_{i,m}$ for fixed $m \geq 2$, i.e. the product of the conditional probability of a click when a multiphoton is sent after Alice's pre-attenuation $P_{i,\mathrm{click}|m}$ and the probability of sending a multiphoton $P^{(att)}_{i,m}$. Note that each random variable denoted by the subscript i represents the position in the string of a multiphoton state with a fixed number of photons $m \geq 2$, which may change for each variable, hence its probabilities too. To prevent an overestimation of the secure events, we assume the worst-case scenario where each sent multiphoton, which is untrustworthy, causes a click on Bob's apparatus, i.e. $P_{i,\mathrm{click}|m} = 1$. Therefore, an expected value of X^B is expressed as $X^{B*} = \sum_{i=1}^{N_\mathrm{S}} P^{(att)}_{i,m}$, where $N_\mathrm{S} = R_{\mathrm{rate}} t$ is the number of sent signals by Alice that forms the finite block, defined by the acquisition time t, i.e. the time the experiment is run, and the source repetition rate R_{rate}. However, since we lack access to the true attenuated photon emission probabilities of the SPS $P^{(att)}_{i,m}$, we bound them as $X^{B*} = \sum_{i=1}^{N_\mathrm{S}} P^{(att)}_{i,m} \leq \sum_{i=1}^{N_\mathrm{S}} \overline{p}^{(att)}_{\mathrm{mp}} = N_\mathrm{S} \overline{p}^{(att)}_{\mathrm{mp}}$. Note that even if the legitimate parties had access to them from perfect SPS characterisation, they would not know how many photons Alice sends in each state. After sifting, the expected number of multiphoton events received by Bob in the key generation basis is

$N_{\mathrm{R,mp}}^{X\,*} = p_X^2 X^{B*} \leq N_{\mathrm{S}} p_X^2 \overline{p}_{\mathrm{mp}}^{(att)} = \overline{N}_{\mathrm{R,mp}}^{X\,*}$, which is upper bounded by the bound of Alice's pre-attenuated multiphoton emission probability $\overline{p}_{\mathrm{mp}}^{(att)}$.

In a real QKD experiment, Bob does not know how many photons were contained in the states which caused a click on his detectors. One may think if Bob uses a photon number resolving detector, he might solve his lack of knowledge about the detections caused by multiphotons. However, even doing that, his results cannot be trusted since Eve can potentially convert Alice's multiphotons into single-photon detections at Bob's apparatus by PNS attacks. Therefore, we need a consistent method that for a given expected value of multiphoton events at Bob's side $N_{\mathrm{R,mp}}^{X,Z\,*}$ in a data block, derives an upper bound of the observed value $\overline{N}_{\mathrm{R,mp}}^{X,Z}$, whose tail probability is bounded with a parameter estimation failure probability as $\Pr\left[N_{\mathrm{R,mp}}^{X,Z} \geq \left(1+\Delta^U\right) N_{\mathrm{R,mp}}^{X,Z\,*}\right] \leq \varepsilon_{\mathrm{PE}} = 2\varepsilon_{\mathrm{sec}}/3$.

As explained in Section 3.6.2.1, the Chernoff bound of [100] provides tighter results than other alternative bounds, and here we apply it one more time. However, in this case, we apply the reverse Chernoff bound as we estimate an observed value from a given expected value. Therefore, to estimate the upper bound of the observed multiphotons $\overline{N}_{\mathrm{R,mp}}^{X,Z} = \overline{N}_{\mathrm{R,mp}}^{X,Z\,*} + \Delta^U$ with $\Delta^U = \left(\beta + \sqrt{8\beta\overline{N}_{\mathrm{R,mp}}^{X,Z\,*} + \beta^2}\right)/2\overline{N}_{\mathrm{R,mp}}^{X,Z\,*}$ where $\beta = -\ln\varepsilon_{\mathrm{PE}}$. The lower bound of the observed non-multiphoton events on either basis is given by

$$\underline{N}_{\mathrm{R,nmp}}^{X,Z} = N_{\mathrm{R}}^{X,Z} - \overline{N}_{\mathrm{R,mp}}^{X,Z}. \tag{4.46}$$

Tough tighter upper bounds on $\overline{N}_{\mathrm{R,mp}}^{X,Z}$ could in principle be used, potentially based on the "factorial moment" [129] or the Klar bounds [130]. However, practically, the scope for potential improvement is minimal in the non-decoy protocol and only possible for the highest tolerable losses of each finite block. These alternate bounds are also less amenable for numerical evaluation for the parameter ranges typical in QKD.

Next, the phase error rate in the key generation basis ϕ^X needs to be upper bounded based on the observed number of errors m_Z and the lower bound of the observed non-multiphotons $\underline{\mathrm{N}}_{R,nmp}^{Z}$ both in the Z (parameter estimation) basis. We conservatively assume that all Z basis errors occur on the received non-multiphoton fraction, hence

we have a first estimate of the phase error rate in the X,

$$\phi^X \leq \frac{m_Z}{\underline{\mathrm{N}}^Z_{R,nmp}}. \tag{4.47}$$

However, this estimate is the result of N_R^Z samples in the Z basis and it is not sufficient to upper bound the phase error rate in the unannounced N_R^X samples in the X (key generation) basis in the finite-key analysis as it is in the asymptotic limit, see Eq. (4.25). Hence, for this random sampling without replacement problem and a tail bound error ε', the upper bound of the unobserved value $\overline{\phi}^X$ can be estimated from the observed value $m_Z/\underline{\mathrm{N}}^Z_{R,nmp}$ using the gamma function of Eq. (3.47)

$$\overline{\phi}^X = \frac{m_Z}{\underline{\mathrm{N}}^Z_{R,nmp}} + \gamma\left(N_R^X, N_R^Z, \frac{m_Z}{\underline{\mathrm{N}}^Z_{R,nmp}}, \varepsilon_{\mathrm{PE}}\right), \tag{4.48}$$

where the parameter estimation error is $\varepsilon_{\mathrm{PE}} = \varepsilon_{sec}/6$.

Incorporating this entire finite-key analysis in Eq. (4.45), the final secure key length extracted from a finite block of statistics is given by

$$\ell^{(\mathrm{SPS})}_{\mathrm{ND}} = \underline{N}^X_{\mathrm{R,nmp}}\left[1 - h_2\left(\overline{\phi}^X\right)\right] - \lambda_{\mathrm{EC}} - 2\log\frac{3}{\varepsilon_{\mathrm{sec}}} - \log\frac{2}{\varepsilon_{\mathrm{cor}}}. \tag{4.49}$$

Note we set a phase error threshold of $\phi^X_{\mathrm{thld}} = 0.11$ (11% errors), and if it is exceeded, $\overline{\phi}^X > \phi^X_{\mathrm{thld}}$, the parties abort the protocol, resulting in zero key length. To estimate the key rate, one simply divides the secure key length by the sent signals $R^{(\mathrm{SPS})}_{\mathrm{ND}} = \ell^{(\mathrm{SPS})}_{\mathrm{ND}}/N_{\mathrm{S}}$.

In our method, we lump together the vacuum and single-photon detection events into the non-multi-photon estimation. An alternative approach is to include a vacuum distribution to estimate these events separately. Hence, we aim to explore if this additional vacuum state can considerably enhance the key generation. To evaluate it, we consider two new scenarios. First, Bob exactly knows the vacuum contribution, $N^{X,Z}_{\mathrm{R},0} = N_{\mathrm{S}} p^2_{X,Z} p_0^{(\mathrm{att})} p^{X,Z}_{\mathrm{click}}$. Second, Bob estimates a lower bound of the vacuum events. For the latter, using the mean photon number definition, we estimate the lower bound of the pre-attenuated vacuum emission probability as $p_0^{(\mathrm{att})} \geq \underline{p}_0^{(att)} = 1 - \langle n \rangle_{\mathrm{att}} =$

$1-\eta_{\mathrm{tr}}\langle n\rangle$ and then the vacuum events as $\underline{N}_{\mathrm{R},0}^{X,Z}=N_{\mathrm{S}}p_{X,Z}^{2}\underline{p}_{0}^{(att)}p_{\mathrm{click}}^{X,Z}$. consequently, the secure key length with of a non-decoy SPS protocol with a vacuum distribution reads as

$$\ell_{\mathrm{ND+vac}}^{(\mathrm{SPS})}=\underline{N}_{\mathrm{R},0}^{X}+\underline{N}_{\mathrm{R},1}^{X}\left[1-h_{2}\left(\frac{m_{Z}}{\underline{N}_{\mathrm{R},1}^{Z}}\right)\right]-\lambda_{\mathrm{EC}}-2\log\frac{3}{\varepsilon_{\mathrm{sec}}}-\log\frac{2}{\varepsilon_{\mathrm{cor}}}. \tag{4.50}$$

where $\underline{N}_{\mathrm{R},1}^{X,Z}=\underline{N}_{\mathrm{R,nmp}}^{X,Z}-\underline{N}_{\mathrm{R},0}^{X,Z}$. To compute the case of the exact vacuum estimate simply replace $\underline{N}_{\mathrm{R},0}^{X,Z}$ for $N_{\mathrm{R},0}^{X,Z}$. In Section 4.5.1, we discuss the results of this non-decoy with a vacuum state and demonstrate that adding an extra vacuum decoy state to separately estimate vacuum and single-photon events does not provide any advantage in key performance.

4.4.2.2 Previous Secure Key Rate Analysis

The finite-key analysis proposed by Cai and Scarani in [37] builds upon the Devetak-Winter formula outlined in Eq. (3.11), which estimates the sifted key in the asymptotic limit. To account for finite-key effects, they implemented several corrections to the asymptotic key rate of Devetak-Winter of Eq. (3.11).

The first correction involves replacing conditional von Neumann entropy of Eq. (3.11), $S(A|E)$, which represents Eve's uncertainty about Alice's key, with the smooth min-entropy, $H_{\mathrm{min}}^{\varepsilon}(A|E)$, that operates in the finite-key regime.

Assuming Eve has partial information about the shared key, privacy amplification (PA) is employed to extract a secure key that ensures its non-correlation with Eve's information by sacrificing some key bits. To measure Eve's side information, i.e. its probability of guessing the key bits, we use the smooth min-entropy. Note that higher smooth min-entropy values indicate greater security in the key extraction process during PA.

We aim to guarantee a lower bound for the smooth min-entropy of the raw key. Therefore, for any $\varepsilon>0$, the smooth min-entropy in terms of the conditional von

Neumann entropy is bounded as

$$H_{\min}^{\varepsilon}\left(A|E\right) \geq N_{\mathrm{R}}^{X}\left(S\left(A|E\right)-\delta\right) \tag{4.51}$$

where N_{R}^{X} is the sifted key, and δ is the correction term of the unconditional security proof in [131]. Applying that to the Corollary 3.3.7 of [132], we obtain

$$\begin{aligned}\delta &= 2\log\left(\mathrm{rank}(\rho_X)+tr\left(\rho_{AE}^{2}\left(\mathbb{1}_{\rho_X}\otimes\rho_{E}^{-1}\right)\right)+2\right)\sqrt{\frac{\log(2/\varepsilon)}{N_{\mathrm{R}}^{X}}}\\ &= 2\log\left(\mathrm{rank}(\rho_X)+3\right)\sqrt{\frac{\log(2/\varepsilon)}{N_{\mathrm{R}}^{X}}}\\ &\leq 2\left\{\log\left[\mathrm{rank}(\rho_X)\right]+\frac{3}{2}\right\}\sqrt{\frac{\log(2/\varepsilon)}{N_{\mathrm{R}}^{X}}}.\end{aligned} \tag{4.52}$$

Given that the dimension of Alice's density operator ρ_A is $\mathrm{rank}(\rho_A)=4$, as Alice can send four possible polarised states, we find

$$\delta \leq 7\sqrt{\frac{\log(2/\varepsilon)}{N_{\mathrm{R}}^{X}}}. \tag{4.53}$$

The second correction involves adding a numerical term which quantifies Eve's uncertainty for a finite block of N_{R}^{X} bits, provided by δ, plus the PA step,

$$\Delta_{N_{\mathrm{R}}^{X}} \leq 7\sqrt{\frac{\log(2/\varepsilon)}{N_{\mathrm{R}}^{X}}}+\frac{2}{N_{\mathrm{R}}^{X}}\log\left(\frac{1}{\varepsilon_{PA}}\right). \tag{4.54}$$

Incorporating this expanded correction term into Eq. (4.51), we obtain

$$H_{min}^{\varepsilon}\left(X|E\right) \geq N_{\mathrm{R}}^{X}\left\{\Delta_{\mathrm{nmp}}^{X}\left[1-h_2(\phi^{X})\right]-\Delta_{N_{\mathrm{R}}^{X}}\right\}. \tag{4.55}$$

where $\Delta_{\mathrm{nmp}}^{X}=1-\overline{p}_{\mathrm{m}}^{(att)}/p_{\mathrm{click}}^{X}$ represents the non-multiphoton fraction, i.e. the probability that a secure non-multiphoton causes a detection event on Bob's apparatus.

Finally, the third correction is the replacement of $S(A|B)$, which is the second von Neumann entropy of Eq. (3.11), with $S(A|B)=N_{\mathrm{R}}^{X}\mathrm{leak}_{\mathrm{EC}}$, which denotes the fraction of information sacrificed in error correction (EC). While this quantity is precisely

known in practical applications when applying the EC code, in theoretical analysis, it is approximately estimated as

$$\text{leak}_{\text{EC}} \approx f_{\text{EC}} h_2(e_X) + \frac{1}{N_{\text{R}}^X} \log\left(\frac{2}{\varepsilon_{\text{EC}}}\right) \quad \text{with} \quad f_{\text{EC}} > 1 \tag{4.56}$$

where $f_{EC} > 1$ is the efficiency error correction factor and $e^X = p_{\text{err}}^X / p_{\text{click}}^X$ is the quantum bit error rate (QBER) in the X basis.

To estimate the secure key rate for a finite block size, we must divide Eq. (3.11) by the number of signals sent by Alice, acknowledging that this quantity is finite and it does tend to infinity, and introducing the smooth min-entropy to characterise the information leaked to Eve from Alice's system. Thus, we have

$$R_{\text{ND-SPS}}^{(Cai)} \geq \frac{1}{N_{\text{S}}} \left(H_{min}^{\varepsilon}(A|E) - S(A|B)\right). \tag{4.57}$$

As explained, we replace Eq. (4.55) for the min-entropy and $S(A|B) = N_{\text{R}}^X \text{leak}_{\text{EC}}$ for the second conditional entropy using Eq. (4.56) in Eq. (4.57), to obtain the finite key rate of this non-decoy SPS model based on [37]

$$\begin{aligned} R_{\text{ND-SPS}}^{(Cai)} &\geq \frac{N_{\text{R}}^X}{N_{\text{S}}} \left\{ \Delta_{\text{nmp}}^X \left[1 - h_2(\phi^X)\right] - \Delta_{N_{\text{R}}^X} - f_{\text{EC}} h_2(e_Z) - \frac{1}{N_{\text{R}}^X} \log\left(\frac{2}{\varepsilon_{\text{EC}}}\right) \right\} \\ &\geq p_X^2 p_{\text{click}}^X \Bigg\{ \Delta_{\text{nmp}}^X \left[1 - h_2(\phi^X)\right] - 7\sqrt{\frac{\log(2/\varepsilon)}{N_{\text{R}}^X}} - \frac{2}{N_{\text{R}}^X} \log\left(\frac{1}{\varepsilon_{PA}}\right) \\ &\quad - f_{\text{EC}} h_2(e_X) - \frac{1}{N_{\text{R}}^X} \log\left(\frac{2}{\varepsilon_{\text{EC}}}\right) \Bigg\}. \end{aligned} \tag{4.58}$$

In the finite-key scenario, observed and estimated parameters such as the phase error rate ϕ^X or the multiphoton states $N_{\text{R,mp}}^{X,Z}$ experience statistical fluctuations, as discussed in Section 4.4.2.1. These fluctuations are quantified by introducing a deviation in the probabilities or rates associated with these parameters. Let λ_n be one of these probabilities and suppose that n signals have been used to estimate λ_n. The difference

with the asymptotic probability λ_∞ is given by

$$|\,\lambda_n - \lambda_\infty\,| \leq \xi(n,d) = \sqrt{\frac{2\ln(1/\varepsilon_{\mathrm{PE}}) + d\,\ln(n+1)}{n}}, \tag{4.59}$$

where d is the number of outcomes of a POVM. The lower and upper bounds of the probability considering this deviation are, $\underline{\lambda}_n = \max[\lambda_n - \xi(n,d), 0]$ and $\overline{\lambda}_n = \min[\lambda_n + \xi(n,d), 1]$, respectively.

These deviations are applied to the multiphoton probability $\overline{p}_{\mathrm{m}}^{(att)}$ and to the QBER e^Z in the Z basis. For the sifted events in the key generation basis $N_{\mathrm{R}}^X = N_{\mathrm{S}} p_X^2 p_{\mathrm{click}}^X$, there are statistical fluctuations on the multiphoton probability $\overline{p}_{\mathrm{m}}^{(att)}$, which was already bounded from our previous SPS characterisation model (Section 4.1). To ensure security in our key estimate, we must apply to $\overline{p}_{\mathrm{m}}^{(att)}$ a deviation to obtain an upper bound. Therefore, we derive the lower bound of the non-multiphoton fraction in the key generation basis as follows

$$\underline{\Delta}_{\mathrm{nmp}}^X = 1 - \frac{\min\left[\overline{p}_{\mathrm{m}}^{(att)} + \xi(N_{\mathrm{R}}^X, 2), 1)\right]}{p_{\mathrm{click}}^X}. \tag{4.60}$$

where in QKD, $d = 2$, since the only two possible outcomes are either Alice = Bob or Alice $\neq$ Bob.

As in the previous finite-key model, here the error in the parameter estimation basis is also used to calculate the phase error rate ϕ^X in the X (key generation) basis. This rate is subjected to the fluctuations in the block formed by the number of signals used in the Z basis, $N_{\mathrm{R}}^Z = N_{\mathrm{S}} p_Z^2 p_{\mathrm{click}}^Z$. Hence, applying the deviation to the error rate in the parameter estimation basis, $e^Z = p_{\mathrm{err}}^Z / p_{\mathrm{click}}^Z$, we obtain the following upper bound on the phase error rate

$$\overline{\phi}^X = \frac{\min\left[e^Z + \xi(N_{\mathrm{R}}^Z, 2), 1\right]}{\overline{\Delta}_{\mathrm{nmp}}^Z}, \tag{4.61}$$

where now we use the upper bound of the non-multiphoton fraction in the Z basis, which is given by

$$\overline{\Delta}_{\mathrm{nmp}}^Z = 1 - \frac{\max\left[\overline{p}_{\mathrm{m}}^{(att)} - \xi(N_{\mathrm{R}}^Z, 2), 0)\right]}{p_{\mathrm{click}}^Z}. \tag{4.62}$$

Introducing these bounds of the finite-key analysis, Eqs. (4.60) and (4.61) as $\phi^X \leq \overline{\phi}^X$ and $\Delta^X_{\text{nmp}} \geq \underline{\Delta}^X_{\text{nmp}}$ into the secure key rate of Eq. (4.58), we obtain the final expression to estimate secure key rates from finite blocks that account for statistical fluctuations. Furthermore, one can also assume that the click and error probability is the same for each of the four detectors, i.e. $p_{\text{click}} \equiv p^X_{\text{click}} = p^Z_{\text{click}}$ and $p_{\text{err}} \equiv p^X_{\text{err}} = p^Z_{\text{err}}$, hence $\Delta_{\text{nmp}} \equiv \Delta^X_{\text{nmp}} = \Delta^Z_{\text{nmp}}$, and compute the Eq. (4.58) to estimate finite key rates.

4.5 Secure Key Rate Performance: A Comparative Analysis

Here, we first show the substantial key generation enhancement within the finite-key framework comparing our non-decoy SPS protocol, described in Section 4.4.2.1, to the previous work of [126], whose secret key rate formula is derived in Section 4.4.2.2. We also elucidate the reasons behind this key rate performance improvement. Second, we compare our non-decoy SPS with the 2-decoy weak coherent pulse protocol of Section 3.6.2.1, under different channel losses and for varying signal accumulation times. We find that SPSs with moderate performance can achieve higher key rates in certain parameter regimes of low loss and short integration times. The results also provide guidance for SPS performance targets for QKD applications.

4.5.1 Non-Decoy Single-Photon Source Models

Analysing the two non-decoy SPS models, we observe significant improvements in the finite key rate of our protocol for an optical fibre channel. This key enhancement can be understood in two different ways: at long distances, where the block size required to produce the same key rate is massively reduced, see Figure 4.3 (a); alternatively, for a fixed acquisition time, our non-decoy SPS tolerates a considerably wider range of losses, see Figure 4.3 (b), where the maximum tolerable loss, i.e. the highest channel loss that produces a non-zero key, has significantly increased for our non-decoy SPS model.

The key rate enhancement is quantified by comparing the number of signals required

Description	**Parameter**	**Value**
Mean photon number	$\langle n \rangle$	0.0142
Second-order correlation function	$g^{(2)}(0)$	0.036
Source repetition rate	R_{rate}	160.7 MHz
Misalignment probability	p_{mis}	0.003
Dark count probability	p_{dc}	3.67×10^{-8}
Detector efficiency	η_{det}	0.6525
Fibre loss	l	0.1904 dB/km
Parameter estimation failure probability	ε_{PE}	$2 \times 10^{-10}/3$
Privacy amplification failure probability	ε_{PA}	$10^{-10}/6$
Correctness failure probability	ε_{cor}	10^{-15}
Secrecy failure probability	ε_{cor}	10^{-10}
Error correction leakage	λ_{EC}	Eq. 3.51 or $1.16 N_{\text{R}}^{X} h_2(e_X)$

Table 4.1: Baseline QKD system parameters for the finite-analysis of the quantum dot of [40]. Note the error correction leakage can be characterised differently depending on the block size. The detector efficiency and dark count probability are considerably close amongst four detectors in the experiment of [42], hence we take their average and assume the same for each detector. Thus, we assume $p_{\text{click}} \equiv p_{\text{click}}^{X} = p_{\text{click}}^{Z}$ and $p_{\text{err}} \equiv p_{\text{err}}^{X} = p_{\text{err}}^{Z}$. In particular, the total detector efficiency is estimated as the relative efficiency on average due to the measured losses of each detector ($\approx 87\%$) and the estimated quantum efficiency of the detectors ($\approx 75\%$). The channel transmittance is given by $\eta_{ch} = 10^{-l/10}$.

to approach the asymptotic key rate. To approach the asymptotic key rate with the method of [126], the received block size, N_{R}, has to be on the order of 10^{15}, dotted purple curve Figure 4.3 (a). Our results indicate a factor 10^8 improvement, with the finite key rate curve reaching the asymptotic limit with just 10^7 received signals when Alice's pre-attenuation is applied. Considering a block size defined by the sent signals N_{S}, the integration time required to approach the asymptotic key rate is drastically reduced from 10^4 years, dotted purple curve Figure 4.4, to just one hour, solid red line in the same figure.

In terms of fixed acquisition time, previous security analysis of Section 4.4.2.2 restricts the maximum distance for key exchange after one second of acquisition time to less than 1 km, see Figure 4.3 (b) and the dotted green line Figure 4.4. In contrast, our calculations show a maximum tolerable loss of 26.9 dB which is equivalent to over 140 km of fibre (solid green line in Figure 4.4). For all acquisition times considered, our non-decoy SPS analysis achieves the same key rate over an additional 25 dB of channel loss. Furthermore, in Figure 4.4), we also highlight the impact of Alice's pre-

attenuation, showing how it increases the range of tolerable losses, i.e. generating keys under higher losses, by comparing the asymptotic case with pre-attenuation (solid blue line) and without pre-attenuation (dashed blue line). Detailed explanations for this impact are provided in Sections 4.1 and 4.2. Note that the asymptotic key rates are estimated using Eq. (4.32) and the model of Section 4.4.1.

Furthermore, for each channel loss, we optimise the basis bias P_X and the pre-attenuation of Alice's source, quantitatively expressed as the transmissivity η_{tr}, to achieve the highest key rate. In Figure 4.5, we show the optimal values of these parameters for two block sizes defined as the number of Bob's detection events (received signals), which are exactly the same block sizes depicted in Figure 4.3 (a) for our QKD analysis.

Our key length formula of Eq. (4.49) represents a more up-to-date version for a non-decoy SPS analysis compared to previous studies, since we introduce an adapted SKL derivation and tight finite-key bounds for the the non-multiphoton events and phase error rate due to the random sampling without replacement problem. This enhancement of the finite key rate is due to the improved bounds of the statistical fluctuations achieved using the Chernoff bound applied to the number of events, as opposed to the bounding method applied to probabilities and rates in [126]. The deviations of these probabilities, Eq. (4.59), might seem to be relatively small when expressed as probabilities, however, they become magnified when expressed in the total number of events, such as the number of multiphoton emissions. Therefore, the Chernoff bound on events provides tighter estimates of the maximum number of multiphoton emissions, thereby increasing the number of non-multiphoton events at longer distances and consequently enhancing the key rate.

We have demonstrated that fibre-based QKD with a frequency-converted quantum dot is possible at high rates for distances and acquisition times relevant to metropolitan communication networks. The source performance of the quantum dot in [42] with the QKD parameters of Table 4.1, exceeds other single-photon emitters suggested for use in QKD systems in terms of key rate and maximum tolerable loss. These results raise the following question, combining state-of-the-art QD performance in brightness [107] and

multiphoton suppression [133], with the frequency conversion demonstrated in [40] into one device, would it allow the generation of key rates comparable to decoy-state QKD with weak coherent pulses? Ultimately, surpassing weak coherent pulse implementations requires sources much closer to the ideal performance of unity collection efficiency with multiphoton emission probabilities approaching zero. However, we need further analysis, which will be developed in the following sections, to determine if practical SPSs have the potential to enhance the key performance of weak coherent pulses.

Finally, we evaluate the idea of an additional vacuum decoy state for the original non-decoy SPS in Figure 4.6. The key enhancement shown in these two scenarios with a vacuum decoy state is negligible for all channel losses. In particular, in the high-loss regime, even assuming Bob has complete knowledge of the vacuum contribution, the maximum tolerable loss increases by only 0.05 dB for one minute of acquisition time. Therefore, due to its modest key rate increase, the extra experimental endeavour, considering the usual difficulty of creating a perfect decoy vacuum state in practice [93, 134], and the need for additional detector characterisation to estimate the vacuum contribution, is not a worthwhile consideration. Thus, we also demonstrate the lower bound of the non-multi-photon events is not underestimated compared to estimating the vacuum and single-photon events separately. As a result, we take this conservative approach and assume that Eve gains the same amount of information from the vacuum states as from the single-photon states.

4.5.2 Optimal Non-Decoy Single-Photon Source and 2-Decoy Weak Coherent Pulse

Here, we analyse the impact of different SPS characteristics on the secure key and the maximum tolerable loss for several finite blocks. The block size used to extract the secure key is defined by the number of signals sent by Alice $N_{\mathrm{S}} = N_{\mathrm{rate}}t$, which depends on the acquisition time of the experiment t and the source repetition rate R_{rate}.

First, we analyse the results of our non-decoy SPS protocol in the finite-key analysis, Section 4.4.2.1, for various acquisition times and time-zero second-order correlation functions $g^{(2)}(0)$, while also considering the asymptotic case, Section 4.4.1. Subse-

quently, we compare it with a 2-decoy WCP protocol based on Section 3.6.2.1.

Description	**Parameter**	**Value**
Source repetition rate	R_{rate}	160.7 MHz
Misalignment probability	p_{mis}	0.003
Dark count probability	p_{dc}	3.67×10^{-8}
Detector efficiency	η_{det}	0.6525
Fibre loss	l	0.1904 dB/km
Secrecy failure probability	ε_{sec}	10^{-10}
Correctness failure probability	ε_{cor}	10^{-15}

Table 4.2: Baseline QKD protocol parameters for both protocols, non-decoy SPS and 2-decoy WCP, based on the experiment of the quantum dot in [42].

Figure 4.7 illustrates the impact of $g^{(2)}(0)$ on the secure key performance for channel losses (optical fibre distances) in the non-decoy SPS protocol. As expected, fixing the dark count probability means that the $g^{(2)}(0)$ value determines the drop-off of the secure key curves and hence the maximum tolerable loss. For a one-second time block (dotted curves), the improvement in the maximum tolerable loss is approximately 1 dB between the three $g^{(2)}(0)$ values, which is modest. However, for one minute of acquisition time (dashed curves), the difference in the range of tolerable losses among the $g^{(2)}(0)$ values exhibits a considerable increment, as the secure key performance is already close to the asymptotic regime. The asymptotic key of $g^{(2)}(0) = 3.6\%$ (solid blue curve) is approached at one minute of acquisition time by halving the $g^{(2)}(0)$ (dashed orange line). Notably, one hour of acquisition time is required for $g^{(2)}(0) = 3.6\%$ to approach its asymptotic key rate. Thus, halving the $g^{(2)}(0)$ from 3.6% to 1.8% yields similar key rates but for vastly different block sizes, resulting in a reduction of approximately 98% in the acquisition time.

In Figure 4.9, we show the maximum tolerable channel loss varying the mean photon number $\langle n \rangle$ while fixing $g^{(2)}(0)$. A higher $\langle n \rangle$ corresponds to a lower vacuum emission and higher single-photon and multiphoton emissions. Therefore, the higher $\langle n \rangle$, the less acquisition time (number of sent signals) is required for the pre-attenuation of Alice's source to kick in. The SPS with $\langle n \rangle = 0.5$ (red curve) introduces the pre-attenuation even for the smallest acquisition time. This indicates that any other source with a mean photon number $\langle n \rangle > 0.5$ will not increase the maximum tolerable loss, as the

SPS distribution will be pre-attenuated by Alice regardless. The point at which each curve converges to the curve with $\langle n \rangle = 0.5$ represents its first acquisition time in which the pre-attenuation is introduced.

For acquisition times above one second, all the key curves reach the secure key of $\langle n \rangle = 0.5$ and their asymptotic limit is achieved above 100 seconds, where the maximum loss is constant despite the rise of time. In particular, for the SPS of [42] (blue curve), there is an increase between 0.1 and 0.2 dB on the maximum tolerable loss for acquisition times within the interval of $[0.01, 0.1]$ seconds. A greater mean photon number than $\langle n \rangle > 0.0142$ is needed to tolerate higher losses than the 2-decoy state protocol for times below 0.62 seconds (10^8 sent signals). Consequently, an SPS with $\langle n \rangle > 0.0142$ would extend the range of tolerable losses compared to a decoy WCP system with a maximum tolerable channel loss of 20 dB or below. SPSs with greater $\langle n \rangle$ extend this to 26.5 dB, however, beyond this regime at high losses, the superiority of the 2-decoy WCP is evident. It is worth mentioning the SPS with the highest mean photon number, $\langle n \rangle = 0.5$, for extremely short acquisition times of 0.01 seconds, tolerates up to 9 dB (47 km) more channel loss (fibre distance) than the 2-decoy with WCP. Note that the fixed QKD parameters to both protocols, non-decoy SPS and 2-decoy WCP, are shown in Table 4.2. These common parameters are consistent with the parameters used in Section 4.5.1, see Table 4.1.

We also fix the channel loss and show the secure key rate versus time blocks. Note that for the fixed losses in Figure 4.8, a higher mean photon number than $\langle n \rangle = 0.5$ (red curve) would produce the same key rate, since it would be pre-attenuated and $g^{(2)}(0)$ does not dominate in this low-loss regime. Therefore, $\langle n \rangle = 0.5$ shows the highest possible secure key generation for the SPS protocol at these particular channel losses. This principle is illustrated in Figure 4.8 (b) with 20 dB of channel loss, where the key results of $\langle n \rangle = 0.5$ (red curve) overlap with the secure key curve of $\langle n \rangle = 0.142$ (purple curve). However, in Figure 4.8 (a) with 10 dB of channel loss, within the regime where the block size is large enough to approach the asymptotic key, i.e. the number of key bits is almost constant even though the acquisition time increases, the highest secure key bits (red curve) scales by a factor of 9.7 compared to the key bits of the lowest

$\langle n \rangle = 0.0142$.

Furthermore, non-decoy SPS only shows an advantage over the 2-decoy WCP at 20 dB loss for extremely small acquisition times, where the 2-decoy method is unable to generate key. In Figure 4.8 (a) with a 10 dB of channel loss, the non-decoy SPS of $\langle n \rangle = 0.142$ (purple line) and $\langle n \rangle = 0.5$ (red line) outperform the secure key generation of the 2-decoy WCP (orange curve) for block sizes approximately below 0.03 seconds ($4.8 \cdot 10^6$ sent signals) and 29 seconds ($4.66 \cdot 10^9$ sent signals), respectively.

We demonstrate that the non-decoy SPS may enhance the key rate performance of the 2-decoy WCP for short acquisition times (small number of sent signals) in the low-loss regime. Additionally, the range of acquisition times where the non-decoy SPS surpasses the 2-decoy WCP can potentially be wider for channel losses below 10 dB (52.5 km of fibre). Within the same regime, at least a mean photon number as the quantum dot in [42], i.e. $\langle n \rangle \geq 0.0142$ is required to tolerate higher losses over the 2-decoy WCP. Complementary SPS characteristics for both improvements include a $g^{(2)}(0) \leq 3.6\%$ and a source repetition rate of $R_{\text{rate}} \geq 160.7$ MHz.

Through our theoretical key estimates, we present SPSs as a valid quantum source for short-range QKD, performing an efficient BB84 protocol with one unique source at Alice's side, thus avoiding experimental complexity associated with decoy methods. Nevertheless, further research is necessary to establish a fair comparison between WCPs and SPSs within the decoy method framework. Concretely, a decoy analysis using a Fock basis notation that aligns with the SPS approach outline here would be beneficial [136]. This idea will be the aim of the next chapter.

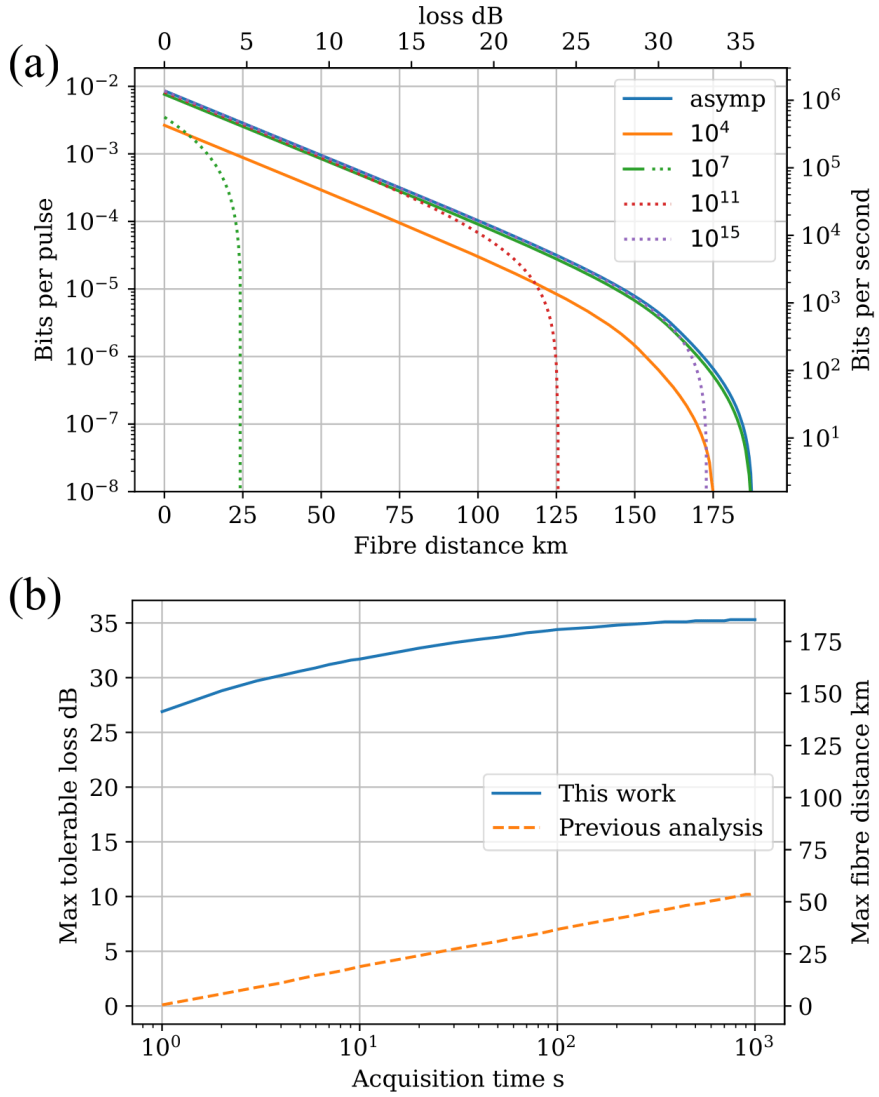

Figure 4.3: Comparison of finite key rate in a semi-log scale based on our non-decoy SPS analysis using the Chernoff bound, estimated using Eq. (4.49), and previous finite-key analysis based on [37], calculated using Eq. (4.58), for the quantum dot source of [42]. The finite key rate for different block sizes, defined as the number of received signals by Bob N_{R}, is shown in Figure (a). This work (our analysis in Section 4.4.2.1) is shown with solid lines and the previous analysis (presented in Section 4.4.2.2) with dotted lines. For both versions, Alice's pre-attenuation, characterised by transmissivity η_{tr}, and p_X are optimised for every distance (channel loss) of each block. Note the asymptotic results follow the analysis of Section 4.4.1. The bound presented in this work results in substantially higher finite key rates using smaller block sizes. Figure (b) shows the maximum tolerable loss achievable as a function of the acquisition time t. This can also be interpreted in terms of the number of sent signals $N_{\mathrm{S}} = R_{\mathrm{rate}}t$, where R_{rate} is the source repetition rate, see Table 4.1. This work remarkably improves the distance over which a key can be generated compared to [126], particularly for short acquisition times.

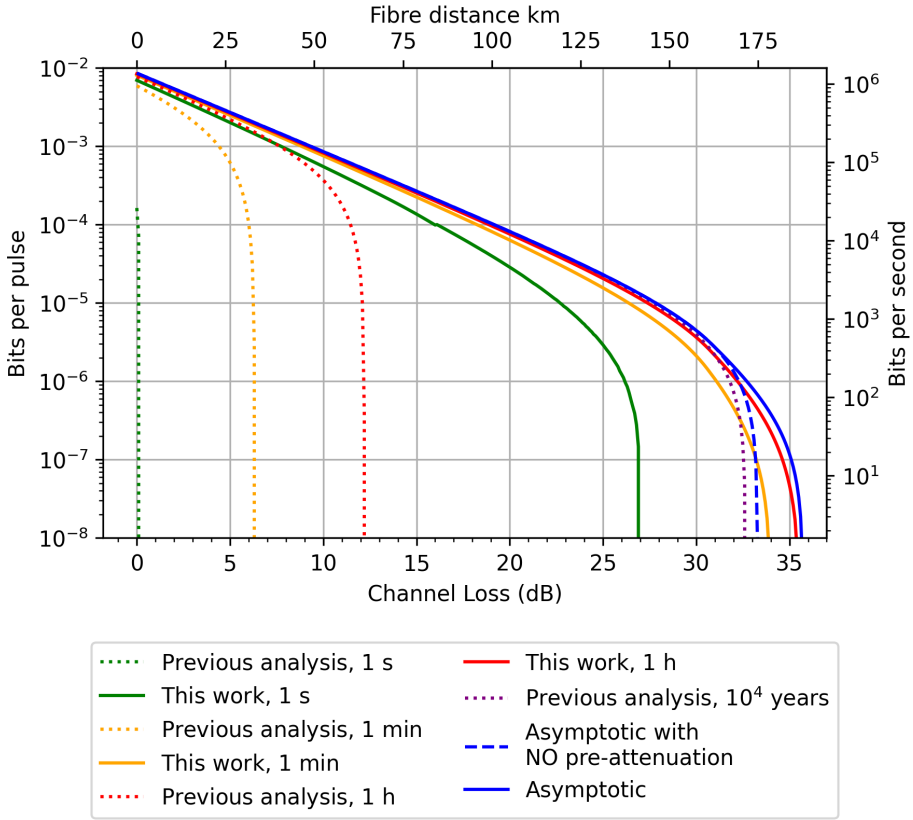

Figure 4.4: Comparison of finite key in a semi-log scale based on our non-decoy SPS analysis using the Chernoff bound, calculated using Eq. (4.49), and previous finite-key analysis based on [126], estimated using Eq. (4.58), for the quantum dot source of [42]. Here it is shown the finite key rate for different block sizes, defined as the number of sent signals by Alice N_{S}. This work (our analysis in Section 4.4.2.1) is shown with solid lines and the previous analysis (presented in Section 4.4.2.2) with dotted lines. Note the asymptotic results follow the analysis of Section 4.4.1. The blue dashed line represents the asymptotic limit of our non-decoy SPS model with no pre-attenuation of Alice's source. For the remaining key curves, Alice's pre-attenuation and p_X are optimised for each channel loss (distance). The acquisition times (number of sent signals) evaluated are 1 second (1.607×10^9), 1 minute (9.642×10^9), 1 hour (5.785×10^{11}) and 10^4 years (5.067×10^{19}). The bound presented in this work results in substantially greater finite key rates using the same block sizes as [126]. Whereas for the previous work of [126] reaching the asymptotic key rate was unattainable (dotted purple line), this work (our non-decoy SPS) massively reduces the required block size to approach it.

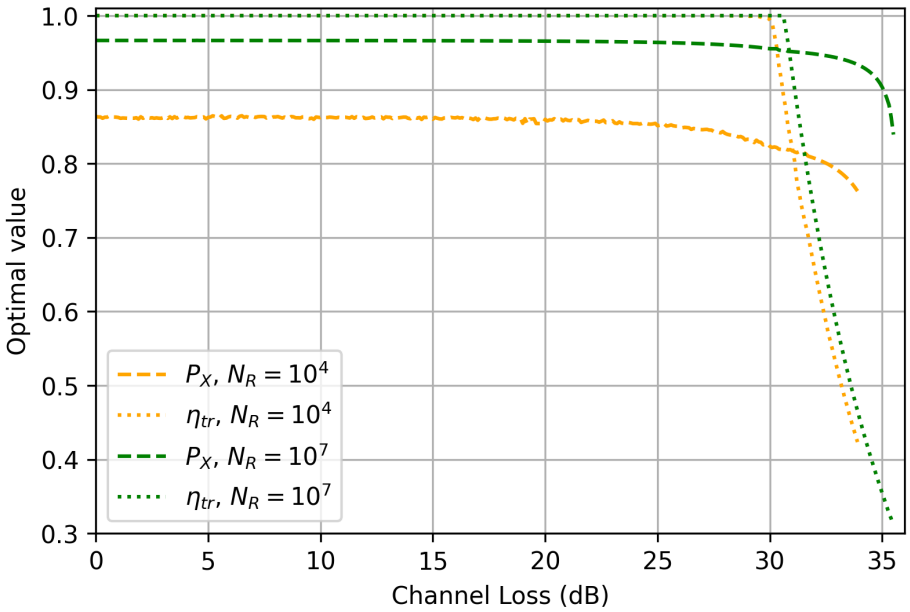

Figure 4.5: The optimal values for the basis bias P_X (dashed lines) and Alice's transmissivity η_{tr} (dotted lines) versus channel losses for block sizes of 10^4 (orange) and 10^7 (green) received signals by Bob. As shown in Figure 4.3 (a), the maximum tolerable loss of each block size is different.

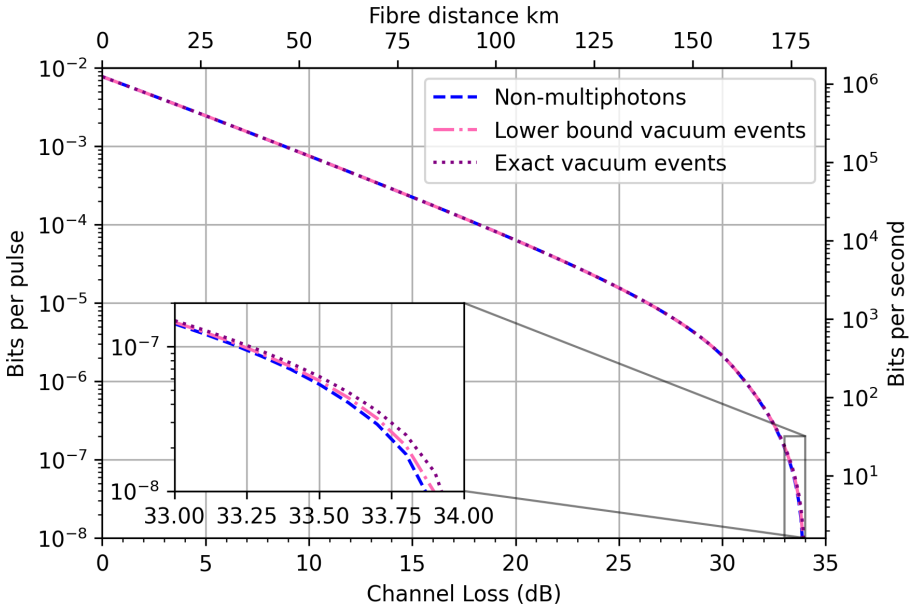

Figure 4.6: The secure key of the non-decoy SPS protocol with a vacuum decoy state, using Eq. (4.50), as a function of the channel loss (fibre distance) in a semi-log scale with optimised p_X and pre-attenuation, defined by transmissivity η_{tr}, for 1 minute of acquisition time. The dashed blue curve represents the finite secure key using the non-multiphoton estimation, Eq. (4.49), and the other two curves estimate separately the vacuum and single-photon events, the green dotted curve uses a lower bound on the vacuum events $\underline{N}_{\mathrm{R},0}^{X,Z}$ and the dashed purple curve uses the exact number of vacuum events $N_{\mathrm{R},0}^{X,Z}$, see Eq. (4.50) for further details.

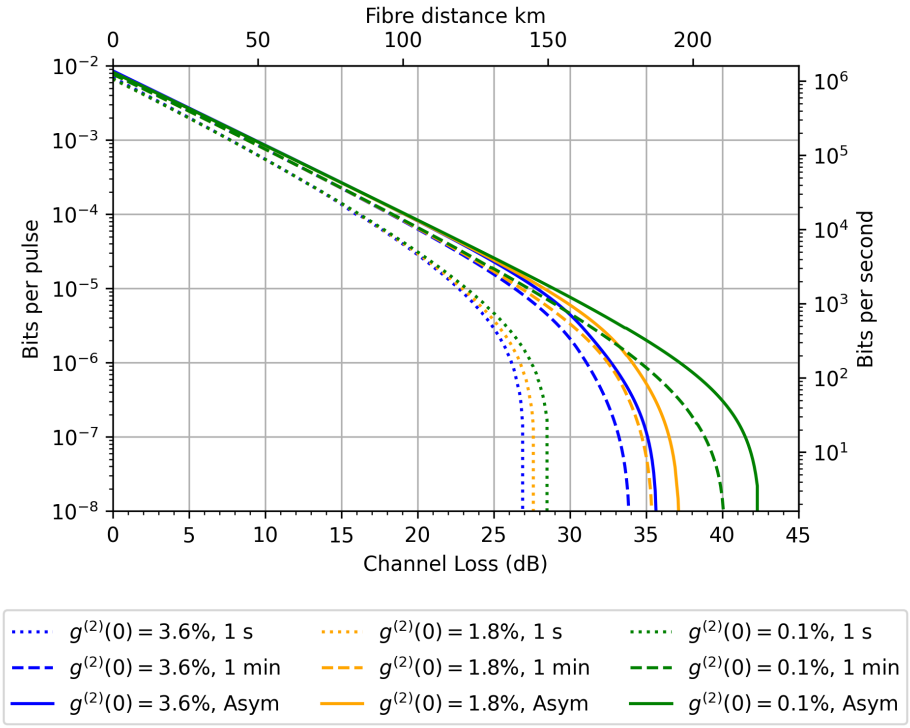

Figure 4.7: Comparison of the secure key in a semi-log scale for the non-decoy SPS protocol with several second-order correlation functions $g^{(2)}(0)$ and block sizes, optimising the basis bias p_X and the transmissivity η_{tr} associated with Alice's source pre-attenuation for each channel loss. The SKR $R_{\mathrm{ND}}^{(\mathrm{SPS})}$ and SKL $\ell_{\mathrm{ND}}^{(\mathrm{SPS})}$, Eq. (4.49), are represented by the bits per pulse and the bits per second, respectively. The $g^{(2)}(0) = 3.6\%$ (blue curves) corresponds to the quantum dot used in the QKD analysis of [42]. The $g^{(2)}(0) = 1.8\%$ (orange curves) is based on [135] and $g^{(2)}(0) = 0.1\%$ (green curves) is considered an optimistic case. The mean photon number is fixed to $\langle n \rangle = 0.0142$, which corresponds to the quantum dot of [42]. We consider two acquisition times (number of sent signals) of 1 second ($1.607 \cdot 10^8$), dotted curves, and 1 minute ($9.642 \cdot 10^9$), dashed curves, plus the asymptotic limit, solid curves.

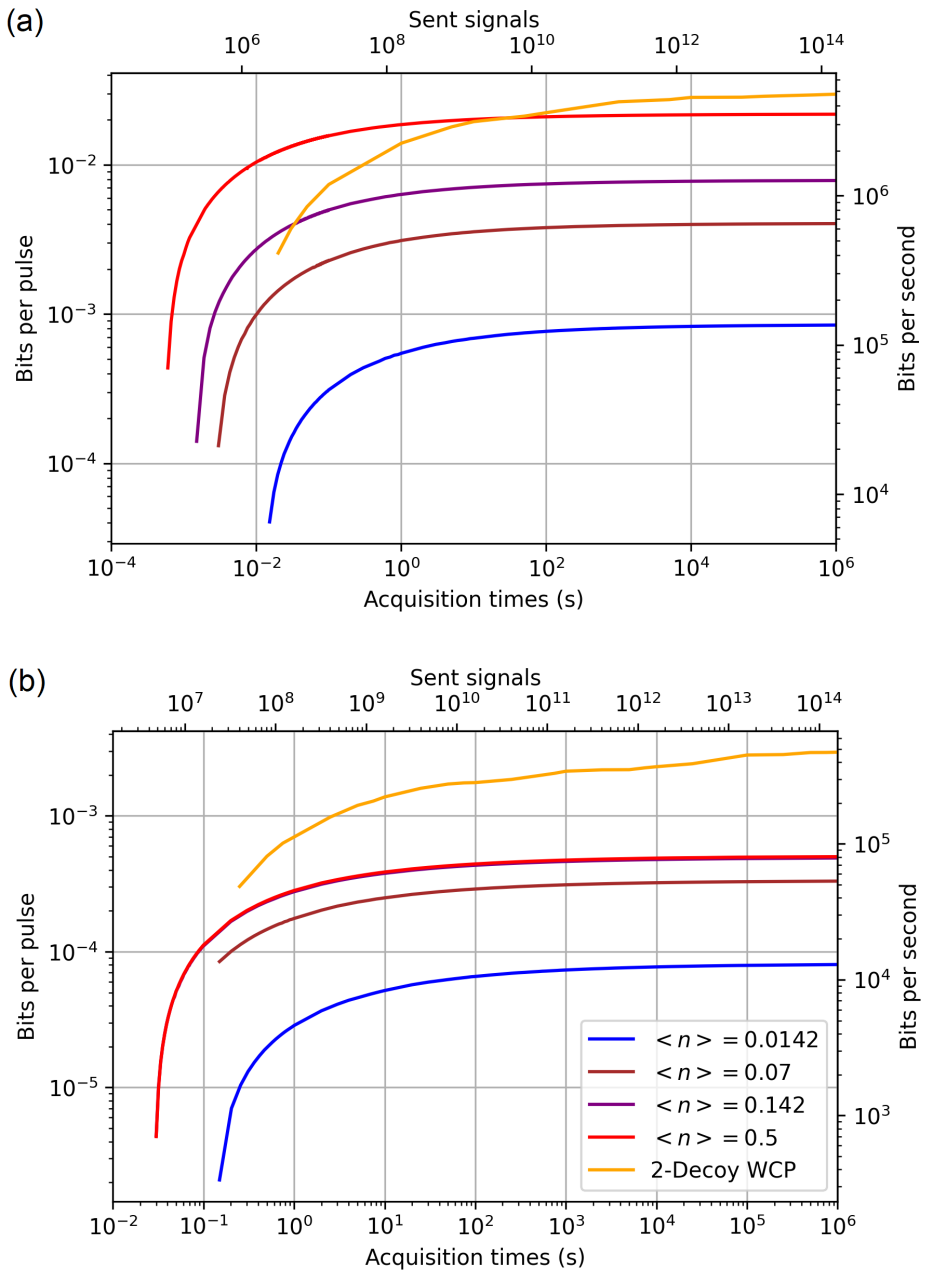

Figure 4.8: Secure key as a function of the acquisition times (sent signals) in log-log scale for (a) 10 dB and (b) 20 dB of channel loss for the optimised non-decoy SPS protocol with various mean photon numbers $\langle n \rangle$ and the optimised 2-decoy WCP method (orange curve). Here the $g^{(2)}(0) = 0.036$.

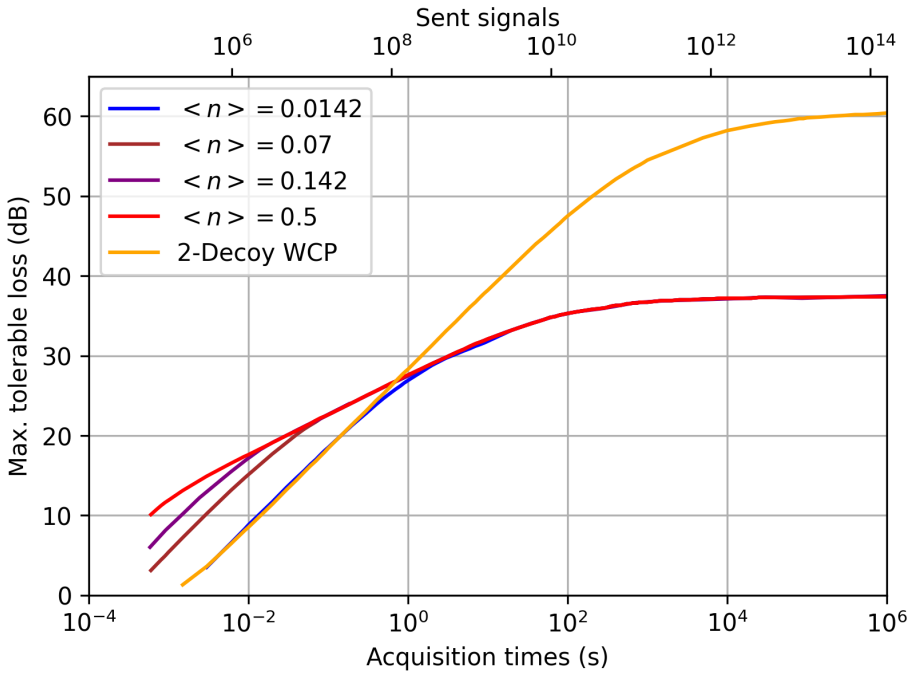

Figure 4.9: Comparison of the maximum tolerable channel loss as a function of the acquisition time in a semi-log scale for the non-decoy SPS protocol with several mean photon numbers $\langle n \rangle$ and the 2-decoy WCP protocol (orange curve), optimising the free parameters in both protocols. The maximum loss is displayed as a function of the block size represented by the acquisition time or the number of sent signals by Alice. Here the second-order correlation function is fixed to $g^{(2)}(0) = 3.6\%$.

Chapter 5

Decoy Efficient-BB84 Protocols with Single-Photon Sources

As discussed previously, the recent advancement of low-$g^{(2)}(0)$ single-photon sources (SPSs) have established them as an increasingly viable alternative source for prepare-and-measure QKD experiments [105, 106]. Experimental studies with a unique SPS have shown their secure key generation without the use of decoy method [124, 137]. In Chapter 4, we conducted a theoretical study on a non-decoy SPS protocol, by updating the state-of-the-art analysis with more advanced QKD techniques, shown in our works [42] and [116]. Our studies provide more optimal bound estimates, hence higher key rates, compared to previous research. Nevertheless, the advantages of the decoy method are indisputable regardless of the quantum source implemented, providing a key enhancement compared to non-decoy methods. Hence, in this chapter, we present two decoy protocols that can be applied to any experimental SPS. Furthermore, in this chapter, we aim to address what SPS characteristics are necessary to see a surpass of SPSs over WCPs in a decoy BB84 protocol and the extent of this potential key enhancement.

In the traditional decoy method, the form of the probabilities of the source distributions determine how to bound the yields, i.e. the vacuum and single-photon events, and it works as follows. The methodology involves deriving the exact formula for the yield and finding an inequality that bounds the multiphoton summation to lower bound

the yield. To ensure this inequality is satisfied, a condition that relates elements of the different photon number emission distributions must arise. For instance, in the 2-decoy with WCPs, the inequality of Eq. (3.32) is used to lower bound the single-photon events. The conditions on the intensities of the different Poissonian distributions, i.e. $\mu_1 > \mu_2 + \mu_0$ and $\mu_2 > \mu_0$, is what ensures the inequality to bound the number of single-photon events is met. This approach is distribution-specific, making it challenging to find a general inequality that works for any statistical distribution. Moreover, as explained in Section 4.1, the diverse and intricate nature of SPSs, based on various quantum-mechanical systems, complicates the establishment of a general photon emission distribution that captures the behaviour of any practical SPS. Therefore, it seems that general inequalities for the decoy method or arbitrary distributions for SPS are inadequate to elaborate a decoy SPS model.

Despite these complexities, previous studies have sought to generalise the decoy method for arbitrary photon number statistics [136,138,139], which may be potentially applicable to practical SPSs. However, these works exhibit several issues or gaps. First, they lack methods for characterising photon emissions for their arbitrary distribution, requiring the assumption of access to the true photon statistics of the source. This is problematic for sources not conforming to common statistical distributions, such as Poissonian, binomial, or thermal distributions, which is the case for practical SPSs. Second, since they are not tied to a particular statistical distribution, their derived inequalities for deriving lower bounds of the yields are expressed in terms of photon emission probabilities in the Fock basis. Consequently, the absence of a method to characterize sources with arbitrary statistics implies a lack of tools to ensure photon emission conditions are satisfied in an infinite Hilbert space, leading to the necessity of assuming these conditions as true.

To address the first issue, we adopt the non-decoy method approach of partially characterizing SPS statistics using the time-zero second-order correlation function $g^{(2)}(0)$ and the mean photon number $\langle n \rangle$ as for our non-decoy SPS model. Although now we exploit Alice's pre-attenuation of her SPS, defined by the transmissivity factor, to generate several photon number distributions (Section 5.1). Inspired by the decoy method

with WCPs, of setting various intensity levels to generate different Poisonian distributions, we introduce multiple source pre-attenuations to create the signal and the decoy-state distributions, defined in the Fock basis by a set of transmissivities. However, to ensure protocol security, the yields for the decoy SPS need additional bounds on Alice's vacuum and single-photon emission probabilities (Section 5.3) compared to non-decoy SPS where the multiphoton upper bound was sufficient. Additionally, we extend the receiver model of non-decoy SPSs to include these three employed SPS distributions in Section 5.2 and discuss the optimisation of the protocol parameters (Section 5.4).

To address the second issue, under certain assumptions, we relate the pre-attenuations to the photon emission probability conditions that must be satisfied to lower bound the yields, as it occurs with the intensities in decoy WCP. This approach provides a method to verify these conditions while partially relaxing the assumptions of decoy studies for arbitrary photon statistics. In particular, we review the strengths and weaknesses of several previous decoy studies with a Poissonian or arbitrary photon number distribution and compare them to our decoy SPS protocols in Section 5.6.1. Furthermore, we also point out any inconsistencies in the photon emission probability conditions stated in earlier works.

Specifically, we present the security bounds of the yields for a 2-decoy (Section 5.5.1.1) and a 1-decoy (Section 5.5.1.2) efficient BB84 SPS protocols. We provide detailed explanations on how the transmissivity conditions of the pre-attenuation emerge for our decoy SPS protocols. We also addressed their critical role in the security bounds of the yields, analogous to the intensity conditions in 2-decoy WCPs. Note that we analyse a 2-decoy SPS considering one decoy state as a vacuum distribution as well as for the 2-decoy WCP. We retain all tight bounds of the finite-key analysis introduced in Section 3.6.2.1 and 4.4.2.1 to account for finite key effects, leading to the derivation of the final key length estimation in Section 5.5.2.

Finally, we compare the key performance of the decoy SPS protocols presented here to the 2-decoy WCP method of Section 3.6.2.1 over an optical fibre channel (Section 5.6.2). To perform a fair comparison, we apply identical fixed protocol parameters to all

methods. For consistency and to facilitate comparison with our previous quantum dot of [42] in the non-decoy SPS method, we set the same source repetition rate, $R_{\text{rate}} = 160.7$ MHz, for both decoy SPS and the 2-decoy WCP. However, we are aware that higher rates in the order of GHz are possible for both SPSs [140–142] and WCPs [143]. Additionally, we keep the same $g^{(2)}(0) = 0.036$ of the quantum dot for our decoy SPS method while varying the mean photon number. Finally, we highlight the SPS characteristics necessary to either outperform or match decoy WCP methods. A notable strength of our decoy SPS model is that can be computed for any conceivable SPS with a measurable $g^{(2)}(0)$ and $\langle n \rangle$.

5.1 Sender Model: Multiple Statistical Distributions

Introducing a variable attenuator allows us to set different transmissivities, i.e. the fraction of the signal passing through the attenuator, enabling the generation of multiple photon number distributions. Since the true emission probabilities of the single-photon source (SPS) are unknown, we partially characterise them. In the sender model for non-decoy SPS presented in Section 4.2, we established a reliable upper bound of Alice's multiphoton emission probability. Here this bounded distribution is subsequently utilized after applying two transmissivities to generate both the signal and decoy distributions. We also present further bounds on the vacuum and single-photon emission probabilities, which are essential for estimating the lower bound of the yields.

Unlike the conventional 2-decoy with WCPs, here is no mathematical expression available that describes the statistical distribution of the source across the entire infinite Hilbert space. Consequently, the true photon number distribution of the SPS is written in the Fock basis as $\delta^{(SPS)} \equiv \{P_k^{(SPS)}\}_{k\in\mathbb{N}}$ where $P_k^{(SPS)}$ represents the k-photon emission probabilities, and $P_{\text{m}}^{(SPS)} = \sum_{k\geq 2} P_k^{(SPS)}$ the multiphoton emission probability. By applying different transmissivities $\eta_{tr}^{(j)}$, we obtain the following probabilities of each pre-attenuated distribution

$$P_n^{(j)} = \sum_{k=n}^{\infty} \binom{k}{n} \left(\eta_{tr}^{(j)}\right)^n \left(1-\eta_{tr}^{(j)}\right)^{k-n} P_k^{(SPS)}, \tag{5.1}$$

which form the pre-attenuated distributions with the true emission probabilities $\delta_{\text{att}}^{(j)(SPS)} = \{P_n^{(j)}\}_{n\in\mathbb{N}}$. Thus, these transmissivities are analogous to the intensities of the Poissonian distributions used in the decoy WCP.

However, we do not have access to the true probabilities of $\delta^{(SPS)}$. To simulate Alice's emissions, we must use the same bounded distribution as in the non-decoy method, ensuring protocol security through an upper bound on the multiphotons. This partial characterisation of $\delta^{(SPS)}$ is formed by Eqs. (4.9), (4.10) and (4.11), represented by $\delta^{(bound)} \equiv \{p_k\}_{k=0,1,2}$. Then we pre-attenuate $\delta^{(bound)}$ using Eq. (5.1) and use them in our simulation model for Alice's sent states, which can be condensed in the following notation $\delta_{\text{att}}^{(j)(bound)} = \{p_n^{(j)}\}_{n=0,1,2}$. It is important to highlight how relevant it was to conclude which photon states are involved in the multiphoton emissions to reach its upper bound (see Section 4.1). Note that throughout this entire chapter, the upper case P represents the true photon emission probabilities of the SPS and p corresponds to a bounded estimate.

5.2 Receiver Model: Detection Events Simulation

To show the performance of our method, we simulate the observed values that would be acquired in a real QKD experiment. Here, we describe our model, similar to Section 4.2, to estimate the click and error probabilities that simulate the observed events.

First, the click probability for a given j-distribution is given by

$$p_{\text{c}|\delta^{(j)}} = \sum_{n=0}^{\infty} p_n^{(j)} \left[1 - (1 - p_{\text{dc}})\,(1 - \eta_{\text{ch}}\eta_{\text{det}})^n\right].$$

For simplicity, we assume that the dark count probability p_{dc} and the efficiency η_{det} of the detectors associated with each basis are identical. The channel efficiency is given by $\eta_{\text{ch}} = 10^{-l/10}$ where l is the channel loss in dB.

The error probability for a given j-distribution is then given by

$$p_{\mathrm{err}|\delta^{(j)}} = \frac{p_0^{(j)} p_{dc}}{2} + \sum_{n=1}^{\infty} p_n^{(j)} \left[1 - (1 - p_{dc})\left(1 - \eta_{\mathrm{ch}}\eta_{\mathrm{det}}\right)^n\right] p_{\mathrm{mis}},$$

where p_{mis} is the probability of error due to the misalignment of the set-up.

After sifting, given Alice's number of sent states N_{S}, the number of detection events when both parties choose either the X or the Z basis for a j-distribution is given by

$$N_{X,\delta^{(j)}} = N_{\mathrm{S}} p_X^2 p_{\delta^{(j)}} p_{\mathrm{c}|\delta^{(j)}} \tag{5.2}$$

$$N_{Z,\delta^{(j)}} = N_{\mathrm{S}} p_Z^2 p_{\delta^{(j)}} p_{\mathrm{c}|\delta^{(j)}}, \tag{5.3}$$

respectively, where $p_{\delta^{(j)}}$ is the probability of Alice selecting a particular j-distribution. Similarly, the errors in the X and Z basis for each j-distribution are simulated as $m_{X,\delta^{(j)}} = N_{\mathrm{S}} p_X^2 p_{\delta^{(j)}} p_{\mathrm{err}|\delta^{(j)}}$ and $m_{Z,\delta^{(j)}} = N_{\mathrm{S}} p_Z^2 p_{\delta^{(j)}} p_{\mathrm{err}|\delta^{(j)}}$, respectively. Since the Z basis is exclusively used for parameter estimation, the parties publicly analyse their Z outcomes to determine the total number of errors amongst all distributions $m_Z = \sum_j m_{Z,\delta^{(j)}}$. These events are observed values in a real experiment. However, note that one cannot determine the errors in the X basis $m_X = \sum_j m_{X,\delta^{(j)}}$, since the events in the key generation basis are not revealed. In fact, the errors in X are corrected by implementing an error correction code and form part of the final secure key. We just hypothetically use them to theoretically estimate the number of bits used to perform the error correction code.

5.3 Bounds on the Photon Emission Probabilities

In this section, we present lower and upper bounds for the vacuum and single-photon emission probabilities for any generic distribution, $P_0^{(j)}$ and $P_1^{(j)}$ respectively, and a lower bound for the probability of sending a single-photon state p_1. These bounds are relevant to maintain the lower bounds of the yields and avoid any potential overestima-

tion due to unnecessary assumptions on Alice's emissions. Therefore, they are not used to simulate Bob's counts, they are introduced in the yields, see Section 5.5.1. To derive the bounds, we employ the definitions of the SPS characteristics, which are the second-order correlation function $g^{(2)}(0)$ and mean photon number $\langle n\rangle_{\delta^{(j)}}$. Note that when the pre-attenuation is applied to the original SPS distribution, $g^{(2)}(0)$ stays invariant, while the mean photon number linearly decreases with respect to the transmissivity $\langle n\rangle_{\delta^{(j)}} = \eta_{tr}^{(j)} \langle n\rangle$, where $\langle n\rangle$ is the measured mean photon number of the SPS with no pre-attenuation.

Let us assume that there is a positive $g^{(2)}(0)$ and $g^{(3)}(0)$ while higher kth-order correlation functions are null. This provides us with two equations plus the definition of $\langle n\rangle_{\delta^{(j)}} = g^{(1)}(0)$ and the condition on the sum of all n-photon emission probabilities, hence we have the following system of equations

$$g^{(2)}(0) = \frac{\sum_{n=2}^{\infty} n(n-1)P_n^{(j)}}{\langle n\rangle_{\delta^{(j)}}^2} \tag{5.4}$$

$$g^{(3)}(0) = \frac{\sum_{n=3}^{\infty} n(n-1)(n-2)P_n^{(j)}}{\langle n\rangle_{\delta^{(j)}}^3} \tag{5.5}$$

$$\langle n\rangle_{\delta^{(j)}} = \sum_{n=0}^{\infty} nP_n^{(j)} \tag{5.6}$$

$$\sum_{n=0}^{\infty} P_n^{(j)} = 1. \tag{5.7}$$

$P_n^{(j)}$ represent the true n-photon emission probabilities. We derive an estimate of the true probabilities, denoted by $p_n^{(j)}$, as a bound to the true ones. To obtain exact solutions for this system we need to impose that all $p_{n\geq 4}^{(j)} = 0$, hence we assume the set of emission probabilities $\{p_0^{(j)}, p_1^{(j)}, p_2^{(j)}, p_3^{(j)}\}$. Solving the system for the vacuum probability

$$p_0^{(j)} = 1 - \langle n\rangle_{\delta^{(j)}} + \frac{g^{(2)}\langle n\rangle_{\delta^{(j)}}^2}{2} - \frac{g^{(3)}\langle n\rangle_{\delta^{(j)}}^3}{6}. \tag{5.8}$$

Consider the SPS shows a monotonic decrease of its kth-order correlation functions as the order k increases, i.e. $g^{(k)}(0) \geq g^{(k+1)}(0)\ \forall k \in [2,\infty)$, which was firstly introduced in Section 4.1. In this case $g^{(2)}(0) \geq g^{(3)}(0)$, and considering the worst-case scenario

we take $g^{(2)}(0) = g^{(3)}(0)$, then the term depending on $g^{(2)}(0)$ of Eq. (5.8) is positive, $\langle n\rangle^2_{\delta^{(j)}} \left(3 - \langle n\rangle_{\delta^{(j)}}\right)/6 > 0$.

Let us explore how this term evolves if we generalise the problem to the space with infinite kth-order correlation functions. We have

$$p_0^{(j)} = 1 - \langle n\rangle_{\delta^{(j)}} + \sum_{k=2}^{\infty}(-1)^k \frac{g^{(k)}(0)\,\langle n\rangle^k_{\delta^{(j)}}}{k!}. \tag{5.9}$$

We can upper bound $p_0^{(j)}$ using the monotonic decrease on the kth-order correlation functions $g^{(k)}(0) \leq g^{(k-1)}(0) \leq \cdots \leq g^{(2)}(0)$

$$p_0^{(j)} \leq 1 - \langle n\rangle_{\delta^{(j)}} + g^{(2)}(0) \sum_{k=2}^{\infty}(-1)^k \frac{\langle n\rangle^k_{\delta^{(j)}}}{k!}.$$

Solving the summation of the even k values for $0 < \langle n\rangle_{\delta^{(j)}} \leq 1$ (other values for the mean photon number are forbidden)

$$\sum_{k=1}^{\infty} \frac{\langle n\rangle^{2k}_{\delta^{(j)}}}{(2k)!} = \cosh\langle n\rangle_{\delta^{(j)}} - 1,$$

and of the odd k values

$$\sum_{k=1}^{\infty} \frac{\langle n\rangle^{2k+1}_{\delta^{(j)}}}{(2k+1)!} = \sinh\langle n\rangle_{\delta^{(j)}} - \langle n\rangle_{\delta^{(j)}}\,.$$

Thus, the upper bound of the true probability $P_0^{(j)}$ reads as

$$P_0^{(j)} \leq \overline{p}_0^{(j)} = 1 - \langle n\rangle_{\delta^{(j)}} + g^{(2)}(0)\left(\langle n\rangle_{\delta^{(j)}} - 1 + \frac{1}{e^{\langle n\rangle_{\delta^{(j)}}}}\right). \tag{5.10}$$

It is worth noticing that the unique case in which this upper bound does not hold is when $g^{(2)}(0)$ is the only positive correlation function. Hence, to use the bound of Eq. (5.10) we need at least $g^{(3)}(0) > 0$. Moreover, setting $g^{(2)}(0) = 1$ the bound obtained is $\overline{p}_0^{WCP} = 1/e^{\langle n\rangle_{\delta^{(j)}}}$, which reaches the behaviour of the vacuum emissions in a Poissonian distribution as expected, and it is a valid upper bound when all $g^{(k\geq 3)}(0) = 0$ (or simply unknown). In our analysis, we use the tight bound of Eq. (5.10) since we

consider most realistic SPSs can potentially provide a positive $g^{(3)}(0)$. Also, since $(\langle n\rangle_{\delta^{(j)}} - 1) + 1/e^{\langle n\rangle_{\delta^{(j)}}} > 0$, we present the lower bound of the true probability

$$P_0^{(j)} \geq \underline{p}_0^{(j)} = 1 - \langle n\rangle_{\delta^{(j)}}\,. \tag{5.11}$$

Moreover, it is straightforward to upper bound $P_1^{(j)}$ using the definition of the mean photon number, Eq. (5.6),

$$P_1^{(j)} \leq \overline{p}_1^{(j)} = \langle n\rangle_{\delta^{(j)}} \tag{5.12}$$

and finally, the lower bound on the true $P_1^{(j)}$ can be estimated by simply $\underline{p}_1^{(j)} = 1 - \overline{p}_m - \overline{p}_0^{(WCP)}$ using Eq. (4.6), which leads to

$$P_1^{(j)} \geq \underline{p}_1^{(j)} = 1 - \frac{g^{(2)}(0)\,\langle n\rangle_{\delta^{(j)}}^2}{2} - \frac{1}{e^{\langle n\rangle_{\delta^{(j)}}}}. \tag{5.13}$$

Note here we needed to use the upper bound $\overline{p}_0^{(WCP)}$, otherwise the lower bound is not met.

The true probability of Alice sending a particular n-photon state is defined as $P_n = \sum_j p_{\delta^{(j)}} \underline{P}_n^{(j)}$. We lower bound the true probability of sending single-photons for any pre-attenuated distribution

$$P_1 \geq \underline{p_1} = \sum_j p_{\delta^{(j)}} \underline{p}_1^{(j)}, \tag{5.14}$$

where the probabilities of selecting each distribution $p_{\delta^{(j)}}$ are known by the legitimate parties and $\underline{p}_1^{(j)}$ is the lower bound in Eq. (5.13) but denoted for each pre-attenuated distribution $\delta^{(j)}$.

5.4 Optimisation of Protocol Parameters

We implement two protocols: (1) the 2-decoy SPS protocol where there are three pre-attenuated distributions involved. Explicitly, $\delta^{(0)} = \{1, 0, 0\}$, $\delta_{\text{att}}^{(1)} = \{p_0^{(1)}, p_1^{(1)}, p_2^{(1)}\}$, and $\delta_{\text{att}}^{(2)} = \{p_0^{(2)}, p_1^{(2)}, p_2^{(2)}\}$, where $\delta_{\text{att}}^{(0)}$ is fixed as a vacuum distribution; and (2) the 1-decoy SPS protocol where there are only two pre-attenuated distributions, $\delta_{\text{att}}^{(1)}$ and

$\delta_{\text{att}}^{(2)}$. For all the protocols, we calculate the maximum lower bound of the key length for each channel loss (fibre distance) by optimising over the protocol parameters: (1) $\{p_X, p_{\delta^{(1)}}, p_{\delta^{(2)}}, \eta_{\text{tr}}^{(1)}, \eta_{\text{tr}}^{(2)}\}$ where $\eta_{\text{tr}}^{(0)} = 0$ and (2) $\{p_X, p_{\delta^{(1)}}, \eta_{\text{tr}}^{(1)}, \eta_{\text{tr}}^{(2)}\}$.

5.5 Decoy Protocols: Security Analysis

In this section, we provide the derivation of the security bounds of the yields, i.e. the bounds on the single-photon and vacuum events, for both protocols. Our upper bounds of the phase errors caused by single-photons in one basis are not presented since when computed they did not give a lower estimate than the total number of errors in one basis. Therefore, we consider all errors to be due to sent single-photons in both decoy protocols. We also present the finite-key analysis and illustrate the main steps of the protocol starting with the 2-decoy SPS and carrying on with the 1-decoy SPS. Finally, the secure key length formula is introduced with its security analysis based on [96] for the 2-decoy protocol and on [95] for the 1-decoy protocol using uncertainty relations of the smooth entropies (Section 2.2.3).

5.5.1 Security Bounds: Yields

In conventional decoy methods, the form of conditional probabilities that rely on the source distribution is exploited to establish analytical bounds on the yields. Note that for every distribution applied in a decoy protocol, there must be an associated bound of the multiphoton terms involved in the yield expressions. We cannot replicate the derivations already proposed by QKD studies that use particular statistical distributions, since it does not suit our SPS case. Therefore, we aim for our own security bounds of the yields that suit our pre-attenuated distributions on the Fock basis. Although we first derive the yield bounds using the true pre-attenuated emission probabilities $\delta_{att}^{(j)(SPS)} \equiv \{P_n^{(j)}\}_{n\in\mathbb{N}}$ derived from the actual SPS distribution $\delta^{(SPS)} \equiv \{P_k^{(SPS)}\}_{k\in\mathbb{N}}$, and then we will introduce our bounded estimate of Alice's emission probabilities presented in Section 5.3. Note that the probabilities of $\delta_{att}^{(j)(SPS)}$ are not the same as the estimated probabilities of $\delta_{att}^{(j)(bound)} = \{p_n^{(j)}\}_{n=0,1,2}$ with an upper bounded multiphoton

probability, which is simply used for Alice's simulation model in Section 5.1.

It is instructive to start working with probabilities and convert them into numbers of detection events at the end. First, we introduce the true click probability of Bob's detectors for each given j-distribution

$$P_{\mathrm{c}\,|\,\delta^{(j)}} := \sum_{n=0}^{\infty} P_n^{(j)} P_{\mathrm{c}\,|\,n}, \tag{5.15}$$

where $P_{\mathrm{c}\,|\,n}$ is the click probability on Bob's side when an n-photon state is sent. Note that for simplicity and clarity in the next derivations, we denote $P_{\mathrm{c}\,|\,\delta^{(j)}} \equiv P_{\mathrm{c}\,|\,\delta_{att}^{(j)(SPS)}}$ and $\delta^{(j)} \equiv \delta_{att}^{(j)(SPS)}$. We assume the click probability $P_{\mathrm{c}\,|\,n}$ is completely under Eve's control while what Alice sends is not. Note that the true pre-attenuated emission probabilities amongst the j-distributions $P_n^{(j)}$ are unknown and generated through the different transmissivities $\eta_{tr}^{(j)}$ as explained in Section 5.1.

5.5.1.1 2-Decoy Method

In the 2-decoy SPS protocol, we use a total number of three distributions, traditionally known as the signal state and the two decoy states Hence, the superscript of the distributions are $j = 0, 1, 2$. We evaluate the case where the pre-attenuated distribution of $\delta^{(0)} \equiv \delta^{(vac)}$ is set as the vacuum distribution, hence $\eta_{\mathrm{tr}}^{(0)} = 0$, and its true photon emission probabilities are

$$P_n^{(0)} = \begin{cases} 1, \text{if } n = 0. \\ 0, \forall n \in [1, \infty). \end{cases} \tag{5.16}$$

However, we first derive exact expressions for the click probability for a given sent single-photon $P_{\mathrm{c}\,|\,1}$ and then for a sent vacuum state $P_{\mathrm{c}\,|\,0}$ with generality, i.e. without imposing $\delta^{(0)}$ is a vacuum distribution. These conditional probabilities are usually called yields. Additionally, in Section 4.5.2, we discuss the reasons for setting one distribution as a vacuum state. Finally, we express these click probabilities as single-photon and vacuum detection events.

The click probability for each particular j-distribution expanding the terms with

non-multiphoton probabilities read as

$$P_{\mathrm{c}\,|\,\delta^{(0)}} = P_0^{(0)} P_{\mathrm{c}\,|\,0} + P_1^{(0)} P_{\mathrm{c}\,|\,1} + \sum_{n=2}^{\infty} P_n^{(0)} P_{\mathrm{c}\,|\,n} \tag{5.17}$$

$$P_{\mathrm{c}\,|\,\delta^{(1)}} = P_0^{(1)} P_{\mathrm{c}\,|\,0} + P_1^{(1)} P_{\mathrm{c}\,|\,1} + \sum_{n=2}^{\infty} P_n^{(1)} P_{\mathrm{c}\,|\,n} \tag{5.18}$$

$$P_{\mathrm{c}\,|\,\delta^{(2)}} = P_0^{(2)} P_{\mathrm{c}\,|\,0} + P_1^{(2)} P_{\mathrm{c}\,|\,1} + \sum_{n=2}^{\infty} P_n^{(2)} P_{\mathrm{c}\,|\,n}, \tag{5.19}$$

which in the current context, the transmissivity conditions among the three distributions are not yet established. The selection of distributions in the upcoming sections may seem arbitrary at first, but its logic will become clear later. It is crucial to recognize that the click probabilities given a selected j-distribution $P_{\mathrm{c}\,|\,\delta^{(j)}}$ are known. These probabilities are linked to the observed detection events on Bob's apparatus and to the probabilities we aim to lower bound $P_{\mathrm{c}\,|\,1}$ and $P_{\mathrm{c}\,|\,0}$. Here, we introduce one of the fundamental principles of a decoy method, which is that the yields must be equal amongst the pre-attenuated distributions, hence $P_{\mathrm{c}\,|\,n} \equiv P^{(0)}_{\mathrm{c}\,|\,n} = P^{(1)}_{\mathrm{c}\,|\,n} = P^{(2)}_{\mathrm{c}\,|\,n}\ \forall n \in \mathbb{N}$.

Lower Bound on the Single-Photon Events

To calculate $P_{\mathrm{c}\,|\,1}$, we choose Eq. (5.19) and replace the unknown $P_{\mathrm{c}\,|\,0}$. Therefore, we first solve for the vacuum click probability $P_{\mathrm{c}\,|\,0}$ in Eq. (5.17)

$$P_{\mathrm{c}\,|\,0} = \frac{1}{P_0^{(0)}} \left(P_{\mathrm{c}\,|\,\delta^{(0)}} - P_1^{(0)} P_{\mathrm{c}\,|\,1} - \sum_{n=2}^{\infty} P_n^{(0)} P_{\mathrm{c}\,|\,n} \right),$$

and then introduce it into Eq. (5.19)

$$\begin{aligned} P_{\mathrm{c}\,|\,\delta^{(2)}} = \frac{P_0^{(2)}}{P_0^{(0)}} \left(P_{\mathrm{c}\,|\,\delta^{(0)}} - P_1^{(0)} P_{\mathrm{c}\,|\,1} - \sum_{n=2}^{\infty} P_n^{(0)} P_{\mathrm{c}\,|\,n} \right) \\ + P_1^{(2)} P_{\mathrm{c}\,|\,1} + \sum_{n=2}^{\infty} P_n^{(2)} P_{\mathrm{c}\,|\,n}. \end{aligned}$$

We move the known click probabilities $P_{\mathrm{c}\,|\,\delta^{(j)}}$ to the left-hand side of the equation leaving the terms with unknown probabilities on the right-hand side

$$P_0^{(0)} P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(2)} P_{\mathrm{c}\,|\,\delta^{(0)}} = \left(P_0^{(0)} P_1^{(2)} - P_0^{(2)} P_1^{(0)}\right) P_{\mathrm{c}\,|\,1} + \sum_{n=2}^{\infty} \left(P_0^{(0)} P_n^{(2)} - P_0^{(2)} P_n^{(0)}\right) P_{\mathrm{c}\,|\,n}.$$

Solving for the click probability given a sent single-photon state, we obtain

$$P_{\mathrm{c}\,|\,1} = \frac{1}{P_0^{(0)} P_1^{(2)} - P_0^{(2)} P_1^{(0)}} \left[P_0^{(0)} P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(2)} P_{\mathrm{c}\,|\,\delta^{(0)}} + \sum_{n=2}^{\infty} \left(P_0^{(2)} P_n^{(0)} - P_0^{(0)} P_n^{(2)}\right) P_{\mathrm{c}\,|\,n}\right],$$

and it can be lower bounded as

$$P_{\mathrm{c}\,|\,1} \geq \frac{1}{P_0^{(0)} P_1^{(2)} - P_0^{(2)} P_1^{(0)}} \left(P_0^{(0)} P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(2)} P_{\mathrm{c}\,|\,\delta^{(0)}} - P_0^{(0)} \sum_{n=2}^{\infty} P_n^{(2)} P_{\mathrm{c}\,|\,n}\right). \tag{5.20}$$

The final term of the inequality contains the emission and detection probabilities by multiphotons, $P_n^{(2)}$ and $P_{\mathrm{c}\,|\,n}$ for $n \geq 2$, respectively. Both probabilities are unknown, and although the sum of the first probability can be upper bounded as shown in Eq. (4.6), it is unhelpful here when it is part of a probability product. Furthermore, the second probability is unreliable since we assume it is entirely controlled by Eve. Thus, this multiphoton term must be bounded by probabilities accessible by Alice and Bob, such as the unused click probability of distribution $\delta^{(1)}$, Eq. (5.18). To establish this relation while maintaining the lower bound on $P_{\mathrm{c}\,|\,1}$, the multiphoton emission probabilities between distributions must fulfill $P_{n\geq 2}^{(2)} < P_{n\geq 2}^{(1)}$. To meet this multiphoton probability condition, we must make assumptions about the photon emission probabilities of the original SPS distribution and establish a relationship between its emission probabilities and its corresponding Kth-order correlation functions.

As in Section 5.3, we consider the time-zero Kth-order correlation functions with

$K \geq 2$ of the SPS monotonically decrease as the order K increases, i.e. $g^{(K+1)}(0) \leq g^{(K)}(0)$. Any of these Kth-order correlation functions is defined as

$$g^{(K)}(0) = \frac{\sum_{k=K}^{\infty} k(k-1)\cdots[k-(K-1)]\, P_k^{(SPS)}}{\langle n \rangle^K}, \tag{5.21}$$

where $P_k^{(SPS)}$ are the true emission probabilities for any kth-photon of the SPS with no pre-attenuation applied. Suppose we experimentally measure all the positive $g^{(K)}(0)$ function, i.e. for any higher order than a certain N, we obtain $g^{(K>N)}(0) = 0$. Hence, any corresponding kth-photon emission probability $P_{k>N}^{(SPS)} = 0$. Thus, we truncate the infinite-dimensional Hilbert space of photon emissions to a finite Hilbert space with a maximum N-photon state. For a fixed K, we can estimate its associated Kth-photon emission probability using the definition of Eq. (5.21) as

$$P_K^{(SPS)} = \frac{1}{K!}\left\{ g^{(K)}(0)\, \langle n \rangle^K - \sum_{k=K+1}^{N} k(k-1)\cdots[k-(K-1)]\, P_k^{(SPS)} \right\}. \tag{5.22}$$

Since the Hilbert space is finite, this allows us to exactly solve the system of equations for the finite set of $\{P_K^{(SPS)}\}_{K\in[2,N]}$, which are related to their corresponding $g^{(K)}(0)$. These photon emission probabilities are pre-attenuated applying Eq. (5.1), obtaining a finite collection of pre-attenuated probabilities $\{P_n^{(j)}\}_{n\in[2,N]}$. Any of these pre-attenuated probabilities fulfilled $P_n^{(j)} \leq P_K^{(SPS)}$. Furthermore, for a fixed transmissivity $\eta_{\mathrm{tr}}^{(j)}$, any particular multiphoton probability of $\{P_n^{(j)}\}_{n\in[2,N]}$ experience a exponential decay when $\eta_{\mathrm{tr}}^{(j)}$ decreases (the pre-attenuation increases). Hence, applying two transmissivities $\eta_{tr}^{(2)} < \eta_{tr}^{(1)} \leq 1$ to $\{P_K^{(SPS)}\}_{K\in[2,N]}$, we can ensure $P_n^{(2)} < P_n^{(1)}$ for any $n \in [2, N]$. The pre-attenuated single-photon emission probability for a particular j-distribution using the mean photon number definition as $P_1^{(j)} = \langle n \rangle_{\mathrm{att}} - \sum_{n=2}^{N} P_n^{(j)} = \eta_{\mathrm{tr}}^{(j)} \langle n \rangle - \sum_{n=2}^{N} P_n^{(j)}$, can also be estimated. Similarly to the behaviour of any $P_{n\geq 2}^{(j)}$, $P_1^{(j)}$ also shows a decay when $\eta_{\mathrm{tr}}^{(j)}$ decreases (pre-attenuation increases), although in this case it is a linear decay. Hence applying the previous transmissivity condition of $\eta_{tr}^{(2)} < \eta_{tr}^{(1)}$, we can ensure $P_1^{(2)} < P_1^{(1)}$. Finally, the pre-attenuated vacuum emission probability can also be calculated as $P_0^{(j)} = 1 - \sum_{n=1}^{N} P_n^{(j)}$, which they show a linear

increase when the $\eta_{\mathrm{tr}}^{(j)}$ decreases. Therefore, under the same transmissivity conditions, the pre-attenuated vacuum probabilities satisfy $P_0^{(2)} < P_0^{(1)}$. This is summarised in the following theorem.

Theorem 2 *(Photon emission probability inequalities). Suppose time-zero Kth-order correlation functions with $K \geq 2$ of the SPS monotonically decrease as the order K increases, i.e. $g^{(K+1)}(0) \leq g^{(K)}(0)$, and there exists a finite set of positive $g^{(K)}(0)$, being the highest order $g^{(N)}(0)$. Assuming there are no emissions of photon states that contain more than N photons, hence $P_{k>N}^{(SPS)} = 0$. Applying two pre-attenuations, that satisfy the condition $\eta_{tr}^{(j)} < \eta_{tr}^{(i)} \leq 1$, to the set of finite emission probabilities $\{P_k^{(SPS)}\}_{k\in[0,N]}$, it generates two sets of pre-attenuated probabilities that fulfill $P_n^{(j)} < P_n^{(i)}$ for any $n \in [2, N]$, $P_1^{(j)} < P_1^{(i)}$ and $P_0^{(j)} > P_n^{(i)}$.*

One can be convinced of this theorem due to the following. For any finite space being N the maximum number of photons contained in a state, one can set all the Kth-order correlation functions the same value, e.g. $g^{(K)}(0) = 0.036$ for all $K \in [2, N]$ as the quantum dot of [42], which is considered the worst-case scenario. Then, solve the system of equations for $\{P_K^{(SPS)}\}_{K\in[2,N]}$ and obtain their pre-attenuated version $\{P_n^{(j)}\}_{n\in[2,N]}$ by applying Eq. (5.1). For each one of them, one can build a vector with possible values of the transmissivity $0 < \eta_{tr}^{(j)} < 1$ with a small step between the elements of the vector. Since we do not know the true probabilities, we represent each bounded pre-attenuated probability of $\{p_n^{(j)}\}_{n\in[2,N]}$ versus the vector with all possible values of $\eta_{tr}^{(j)}$, one sees the exponential decay when $\eta_{tr}^{(j)}$ decreases for each representation. The estimate of pre-attenuated single-photon and vacuum emission probabilities, $p_1^{(j)}$ and $p_0^{(j)}$, can also be plotted for each element of the transmissivity vector. When $\eta_{tr}^{(j)}$ decreases, the single-photon probabilities show a linear decay while the vacuum probabilities depict a linear increase. We take a simple example using the parameters of the quantum dot in [42] (analysed in Section 4.5.1) to illustrate Theorem 2. Since $\langle n \rangle = 0.0142$ and $g^{(2)}(0) = 0.036$ for the quantum dot, we assume the same value for $g^{(3)}(0) = 0.036$ and for simplicity $g^{(K>3)}(0) = 0$. In Figures 5.1 and 5.2, we can see the previously described behaviour for the pre-attenuated probabilities, i.e. $P_3^{(j)}$, $P_2^{(j)}$, $P_1^{(j)}$

and $P_0^{(j)}$, but before the pre-attenuation is applied using Eq. (5.1), first, the previous emission probabilities are calculated by solving the system of Eq. (5.22), i.e. $P_3^{(\mathrm{SPS})}$, $P_2^{(\mathrm{SPS})}$, $P_1^{(\mathrm{SPS})}$ and $P_0^{(\mathrm{SPS})}$.

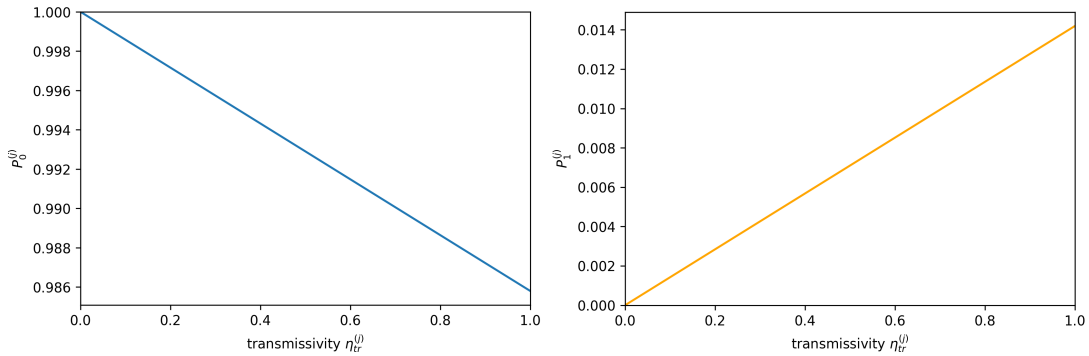

Figure 5.1: Pre-attenuated vacuum (left-hand side) and single-photon (right-hand side) emission probabilities of Theorem 2 considering $g^{(K>3)}(0) = 0$ as a function of the transmissivity.

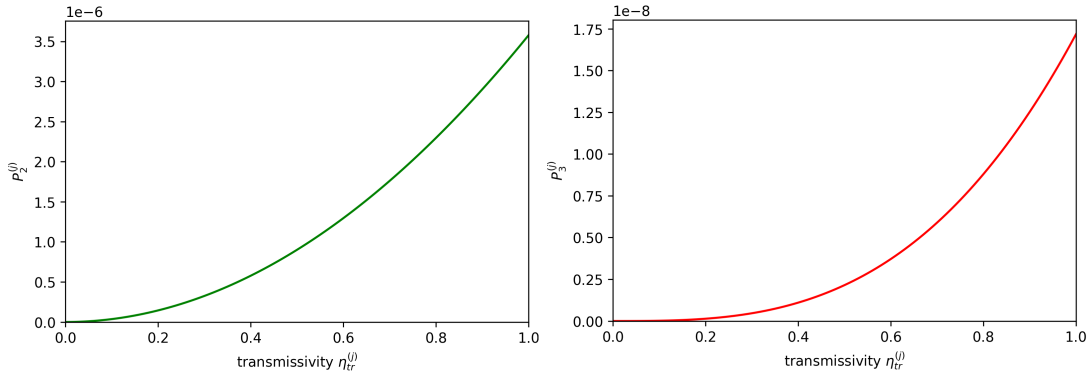

Figure 5.2: Pre-attenuated two-photons (left-hand side) and three-photons (right-hand side) emission probabilities of Theorem 2 considering $g^{(K>3)}(0) = 0$ as a function of the transmissivity.

Consequently, we analyse the implications of this theorem in the single-photon yield. First, let us apply one of the required assumptions in Theorem 2. We assume there is a maximum N-photon state with a positive $g^{(N)}(0) > 0$ and any correlation function with a higher order than N is null, i.e. any $g^{(K>N)}(0) = 0$, hence $P_{k>N}^{(SPS)} = 0$ and likewise for the pre-attenuated probabilities $P_{n>N}^{(j)} = 0$. Hence, our infinite-dimensional space of Eq. (5.20) is reduced to a finite Hilbert space, then the click probability of a

single-photon reads as

$$P_{\mathrm{c}\,|\,1} \geq \frac{1}{P_0^{(0)}P_1^{(2)} - P_0^{(2)}P_1^{(0)}}\Bigg(P_0^{(0)}P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(2)}P_{\mathrm{c}\,|\,\delta^{(0)}} - P_0^{(0)}\sum_{n=2}^{N}P_n^{(2)}P_{\mathrm{c}\,|\,n}\Bigg). \tag{5.23}$$

Considering that to create the distribution $\delta^{(2)}$ from the original truncated SPS distribution $\{P_K^{(SPS)}\}_{K\in[2,N]}$ we apply a lower transmissivity than for generating $\delta^{(1)}$ probabilities, i.e. $\eta_{tr}^{(2)} < \eta_{tr}^{(1)}$, hence $\delta^{(2)}$ is more pre-attenuated than $\delta^{(1)}$. We can use the Theorem 2 to conclude that $P_n^{(2)} < P_n^{(1)}$ for each n-photon state with $n \in [2, N]$. Introducing this in Eq. (5.23), we have

$$P_{\mathrm{c}\,|\,1} > \frac{1}{P_0^{(0)}P_1^{(2)} - P_0^{(2)}P_1^{(0)}}\Bigg(P_0^{(0)}P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(2)}P_{\mathrm{c}\,|\,\delta^{(0)}} - P_0^{(0)}\sum_{n=2}^{N}P_n^{(1)}P_{\mathrm{c}\,|\,n}\Bigg).$$

Finally introducing the multiphoton emission probabilities of $\delta^{(1)}$ for a finite Hilbert space with a maximum N-photon state emission, similar to Eq. (5.18), the multiphoton summation can be replaced as

$$P_{\mathrm{c}\,|\,1} > \frac{1}{P_0^{(0)}P_1^{(2)} - P_0^{(2)}P_1^{(0)}}\Bigg[P_0^{(0)}P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(2)}P_{\mathrm{c}\,|\,\delta^{(0)}} + P_0^{(0)}\Big(P_0^{(1)}P_{\mathrm{c}\,|\,0} + P_1^{(1)}P_{\mathrm{c}\,|\,1} - P_{\mathrm{c}\,|\,\delta^{(1)}}\Big)\Bigg].$$

Solving again for the click probability of single-photons, we obtain

$$P_{\mathrm{c}\,|\,1} > \underline{P}_{\mathrm{c}\,|\,1} = \frac{1}{P_0^{(0)}\left(P_1^{(1)} - P_1^{(2)}\right) + P_0^{(2)}P_1^{(0)}}\Bigg[P_0^{(0)}\Big(P_{\mathrm{c}\,|\,\delta^{(1)}} - P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(1)}P_{\mathrm{c}\,|\,0}\Big) + P_0^{(2)}P_{\mathrm{c}\,|\,\delta^{(0)}}\Bigg]. \tag{5.24}$$

Imposing the distribution $\delta^{(0)} \equiv \delta^{(vac)}$ as a vacuum distribution, which follows Eq.

(5.16), the lower bound of the single-photon yield reduces to

$$P_{\mathrm{c}\,|\,1} > \underline{P}_{\mathrm{c}\,|\,1} = \frac{1}{P_1^{(1)} - P_1^{(2)}} \left(P_{\mathrm{c}\,|\,\delta^{(1)}} - P_{\mathrm{c}\,|\,\delta^{(2)}} - P_0^{(1)} P_{\mathrm{c}\,|\,0} + P_0^{(2)} P_{\mathrm{c}\,|\,\delta^{(0)}} \right). \tag{5.25}$$

From this final expression, we can extract the other photon emission condition, which is $P_1^{(1)} > P_1^{(2)}$. This additional inequality arises from the denominator of $\underline{P}_{\mathrm{c}\,|\,1}$ and it is important since it ensures the denominator is not zero, otherwise $\underline{P}_{\mathrm{c}\,|\,1}$ becomes infinity. Additionally, this condition determines which terms contribute positively or negatively to $\underline{P}_{\mathrm{c}\,|\,1}$, which will be useful in the finite-key analysis in Section 5.5.2. Notably, this condition is hold by Theorem 2 under the transmissivity condition of $\eta_{tr}^{(1)} > \eta_{tr}^{(2)}$ in a finite Hilbert space.

To relate these bounds with the observed values received by Bob, the click probabilities must be converted to the expected number of detection events on each basis. Thus, we multiply Eq. (5.15) by p_X^2 for the X basis (Alice and Bob choose the same basis bias) and by the number of states sent by Alice N_{S}

$$N_{\mathrm{S}} p_X^2 P_{\mathrm{c}|\delta^{(j)}} = N_{\mathrm{S}} p_X^2 \sum_{n=0}^{\infty} P_n^{(j)} P_{\mathrm{c}|n}.$$

Here we identify the true expected number of detection events for each j-distribution in the X basis, similarly to Eq. (5.2) but with the true conditional probabilities $N^*_{X,\delta^{(j)}} = N_{\mathrm{S}} p_X^2 p_{\delta^{(j)}} P_{\mathrm{c}|\delta^{(j)}}$, plus the number of events caused by a sent n-photon state in the X basis $s_{X,n} = N_{\mathrm{S}} p_X^2 P_n P_{\mathrm{c}|n}$. Finally, the relation in Eq. (5.15) expressed in terms of the number of events is given by

$$\frac{N^*_{X,\delta^{(j)}}}{p_{\delta^{(j)}}} = \sum_{n=0}^{\infty} P_n^{(j)} \frac{s_{X,n}}{P_n}. \tag{5.26}$$

Thus, it is straightforward to convert Eq. (5.24) to the lower bound on the single-photon events by multiplying both terms of the equation by N_{S} and p_X^2 and identifying

the terms with any $N^*_{X,\delta^{(j)}}$ and $s_{X,n}$,

$$s_{X,1} > \overline{s}_{X,1} = \frac{P_1}{P_0^{(0)}\left(P_1^{(1)} - P_1^{(2)}\right) + P_0^{(2)}P_1^{(0)}}\Bigg[P_0^{(0)}\Bigg(\frac{N^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - \frac{N^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} - P_0^{(1)}\frac{s_{X,0}}{P_0}\Bigg) + P_0^{(2)}\frac{N^*_{X,\delta^{(0)}}}{p_{\delta^{(0)}}}\Bigg]. \tag{5.27}$$

However, considering $\delta^{(0)} \equiv \delta^{(vac)}$ a vacuum distribution, we obtain

$$s_{X,1} > \overline{s}_{X,1} = \frac{P_1}{P_1^{(1)} - P_1^{(2)}}\Bigg(\frac{N^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - \frac{N^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} - P_0^{(1)}\frac{s_{X,0}}{P_0} + P_0^{(2)}\frac{N_{X,\delta^{(0)}}}{p_{\delta^{(0)}}}\Bigg), \tag{5.28}$$

where apart from the simplification of the emission probabilities associated with $\delta^{(0)}$, we set $N_{X,\delta^{(0)}}$ as an observed value. Since now $\delta^{(0)}$ exclusively sends vacuum, there is no variance in the photon states sent from the vacuum distribution, hence its detection events $N_{X,\delta^{(0)}}$ cannot cause statistical fluctuations on the yield estimates that depend on the finite block, see further details in Section 5.5.2. However, to compute the single-photon events we need to bound the unknown true pre-attenuated emission probabilities involved, i.e. $P_0^{(j)}$ and $P_1^{(j)}$. Hence, we introduce lower and upper bounds of these probabilities, shown in Section 5.3, to hold the lower bound, which makes the lower bound of the single-photon events for the 2-decoy SPS protocol with a vacuum distribution as

$$s_{X,1} > \overline{s}_{X,1} = \frac{\underline{p}_1}{\overline{p}_1^{(1)} - \underline{p}_1^{(2)}}\left(\frac{N^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - \frac{N^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} - \overline{p}_0^{(1)}\frac{\overline{s}_{X,0}}{\underline{p}_0} + \underline{p}_0^{(2)}\frac{N_{X,\delta^{(0)}}}{p_{\delta^{(0)}}}\right). \tag{5.29}$$

The upper bound of the vacuum events is expressed in the following section, Eq. (5.31). Note that by simply replacing the index X by Z all these estimations can also be calculated in the Z (parameter estimation) basis. This also applies to the subsequent bounds.

Bounds on the Vacuum Events

To estimate the vacuum events, i.e. the detection events caused when a vacuum state is sent, we exploit the vacuum distribution $\delta^{(vac)} \equiv \delta^{(0)}$ that purely sends vacuum states.

Thus, we aim to bound $P_{c,0} = P_{c,\delta^{(0)}} P_0 / p_{\delta^{(0)}}$, which comes from the click probability of the vacuum distribution in Eq. (5.17) after replacing the probabilities of the vacuum distribution in Eq. (5.16). Expanding the probability of Alice sending a vacuum state

$$P_{c,0} = P_{c,\delta^{(0)}} \left(1 + \frac{p_{\delta^{(1)}}}{p_{\delta^{(0)}}} P_0^{(1)} + \frac{p_{\delta^{(2)}}}{p_{\delta^{(0)}}} P_0^{(2)} \right).$$

Here we introduce the bound of the vacuum emission probability presented in Section 5.3, and express it in terms of detection events, the lower bound is given by

$$s_{X,0} \geq \underline{s}_{X,0} = N_{X,\delta^{(0)}} \left(1 + \frac{p_{\delta^{(1)}}}{p_{\delta^{(0)}}} \underline{p}_0^{(1)} + \frac{p_{\delta^{(2)}}}{p_{\delta^{(0)}}} \underline{p}_0^{(2)} \right), \tag{5.30}$$

and the upper bound is

$$s_{X,0} \leq \overline{s}_{X,0} = N_{X,\delta^{(0)}} \left(1 + \frac{p_{\delta^{(1)}}}{p_{\delta^{(0)}}} \overline{p}_0^{(1)} + \frac{p_{\delta^{(2)}}}{p_{\delta^{(0)}}} \overline{p}_0^{(2)} \right). \tag{5.31}$$

Note the events caused by the vacuum distribution are not bounded as in the lower bound for the single-photon events. Furthermore, this upper bound on the vacuum events is introduced in the lower bound on the single-photon events, Eq. (5.29).

5.5.1.2 1-Decoy Method

In the 1-decoy SPS protocol, we remove one distribution and we use a total of just two, commonly known as the signal and the decoy state, hence we use $j = 1, 2$ to denote each distribution, i.e. $\delta^{(1)}$ and $\delta^{(2)}$. We first derive the single-photon yield and then the vacuum yield. We also expressed both of them in terms of the number of events using the same approach as in the 2-decoy SPS method in Section 5.5.1.1.

Lower Bound on the Single-Photon Events

We first solve for $P_{c\,|\,1}$ using the two expressions of click probability involved in the protocol, Eqs. (5.18) and (5.19),

$$\begin{aligned} P_{c\,|\,1} =& \frac{1}{P_0^{(1)}P_1^{(2)} - P_0^{(2)}P_1^{(1)}} \Bigg[P_0^{(1)} P_{c\,|\,\delta^{(2)}} - P_0^{(2)} P_{c\,|\,\delta^{(1)}} \\ &+ \sum_{n=2}^{\infty} \left(P_0^{(2)} P_n^{(1)} - P_0^{(1)} P_n^{(2)} \right) P_{c\,|\,n} \Bigg] \end{aligned} \tag{5.32}$$

where $\sum_{n=2}^{\infty} \left(P_0^{(2)} P_n^{(1)} - P_0^{(1)} P_n^{(2)} \right) > 0$, which is expected to be positive in our pre-attenuated SPS characterisation model, must be lower bounded, hence we introduce the inequality

$$P_0^{(2)} P_n^{(1)} - P_0^{(1)} P_n^{(2)} > P_0^{(2)} P_n^{(1)} - P_0^{(1)} P_n^{(1)} = \left(P_0^{(2)} - P_0^{(1)} \right) P_n^{(1)} \quad \text{with } n \geq 2, \tag{5.33}$$

since again we aim to bound the multiphoton summation with the pre-attenuated emission probabilities of distribution $\delta^{(1)}$, $P_n^{(1)}$, to then be able to replace the whole summation. Applying the same Theorem 2 presented in Section 5.5.1.1 and assuming a finite Hilbert space with a maximum N-photon state and the transmissivity condition $\eta_{tr}^{(1)} > \eta_{tr}^{(2)}$, it implies the condition $P_n^{(1)} > P_n^{(2)}$ is met, which makes the condition of Eq. (5.33) hold. Hence, the lower bound of the click probability of single-photons is given by

$$\begin{aligned} P_{c\,|\,1} >& \frac{1}{P_0^{(1)}P_1^{(2)} - P_0^{(2)}P_1^{(1)}} \Bigg[P_0^{(1)} P_{c\,|\,\delta^{(2)}} - P_0^{(2)} P_{c\,|\,\delta^{(1)}} \\ &+ \left(P_0^{(2)} - P_0^{(1)} \right) \sum_{n=2}^{N} P_n^{(1)} P_{c\,|\,n} \Bigg]. \end{aligned}$$

Replacing the multiphoton summation of distribution $\delta^{(1)}$ using the Eq. (5.18) but for a finite Hilbert space, we obtain

$$P_{c\,|\,1} > \frac{1}{P_0^{(1)}P_1^{(2)} - P_0^{(2)}P_1^{(1)}}\Big[P_0^{(1)}P_{c\,|\,\delta^{(2)}} - P_0^{(2)}P_{c\,|\,\delta^{(1)}} + \left(P_0^{(2)} - P_0^{(1)}\right)\left(P_{c\,|\,\delta^{(1)}} - P_0^{(1)}P_{c\,|\,0} - P_1^{(1)}P_{c\,|\,1}\right)\Big].$$

Finally, solving for $P_{c\,|\,1}$

$$P_{c\,|\,1} > \underline{P}_{c\,|\,1} = \frac{1}{P_1^{(1)} - P_1^{(2)}}\left[P_{c\,|\,\delta^{(1)}} - P_{c\,|\,\delta^{(2)}} + \left(P_0^{(2)} - P_0^{(1)}\right)P_{c\,|\,0}\right]. \tag{5.34}$$

The denominator is always positive, i.e. $P_1^{(1)} > P_1^{(2)}$, which is also ensured by the transmissivity condition $\eta_{tr}^{(1)} > \eta_{tr}^{(2)}$ applying Theorem 2.

Finally, using the same process as in Eq. (5.28), the lower bound of the single-photon events is given by

$$s_{X,1} > \underline{s}_{X,1} = \frac{P_1}{P_1^{(1)} - P_1^{(2)}}\left[\frac{N^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - \frac{N^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} + \left(P_0^{(2)} - P_0^{(1)}\right)\frac{s_{X,0}}{P_0}\right]. \tag{5.35}$$

Lower Bound on the Vacuum Events

Here we solve for $P_{c\,|\,1}$ in Eq. (5.18), we replace it in Eq. (5.19) and we obtain the following exact expression for the click probability for a given sent vacuum state

$$P_{c\,|\,0} = \frac{1}{P_1^{(1)}P_0^{(2)} - P_1^{(2)}P_0^{(1)}}\Big[P_1^{(1)}P_{c\,|\,\delta^{(2)}} - P_1^{(2)}P_{c\,|\,\delta^{(1)}} \tag{5.36}$$

$$+ \sum_{n=2}^{\infty}\left(P_1^{(2)}P_n^{(1)} - P_1^{(1)}P_n^{(2)}\right)P_{c\,|\,n}\Big] \tag{5.37}$$

Assuming $P_1^{(2)}P_n^{(1)} > P_1^{(1)}P_n^{(2)}$ for all $n \geq 2$, a lower bound may be potentially met by applying $\eta_{tr}^{(1)} > \eta_{tr}^{(2)}$ and the assumptions required in Theorem 2. However, one must be careful and should check this condition for every n-photon state till the maximum N-photon state associated with the last positive $g^{(K=N)}(0)$. While Theorem 2 with the mentioned transmissivity condition implies $P_n^{(1)} > P_n^{(2)}$ for any $n \geq 2$, under the same

transmissivities it holds $P_1^{(1)} > P_1^{(2)}$. However, as explained in Section 5.5.1.1, the difference $P_n^{(1)} - P_n^{(2)}$ should be bigger than the difference $P_1^{(2)} - P_1^{(1)}$ since the multiphoton ($n \geq 2$) emission probabilities experience a exponential decay when the transmissivity $\eta_{tr}^{(j)}$ decreases while the single-photon probabilities decays linearly. Experimentally, one should verify the photon emission condition stated for every k-photon state with a positive $g^{(k)}(0)$. In particular, in our simulation model for Alice's source, since we do not have access to the true emission probabilities, we consider the worst-case scenario where the multiphoton probability is upper bounded and only two-photon states are involved as it was proved in Section 4.1. Thus, for our model, we can ensure $p_1^{(2)} p_2^{(1)} > p_1^{(1)} p_2^{(2)}$ is met, which represent our estimates of the pre-attenuated probabilities, see Section 5.1.

In general, assuming the emission probability condition is met, one can compute the following lower bound

$$P_{c\,|\,0} \geq \frac{1}{P_1^{(1)} P_0^{(2)} - P_1^{(2)} P_0^{(1)}} \left(P_1^{(1)} P_{c\,|\,\delta^{(2)}} - P_1^{(2)} P_{c\,|\,\delta^{(1)}} \right). \tag{5.38}$$

The condition $P_1^{(1)} P_0^{(2)} > P_1^{(2)} P_0^{(1)}$, which arises from the denominator, is ensured by the transmissivity condition $\eta_{tr}^{(1)} > \eta_{tr}^{(2)}$ by applying Theorem 2, since it implies $P_1^{(1)} > P_1^{(2)}$ and $P_0^{(2)} > P_0^{(1)}$.

Since the parties do not have access to the true emission probabilities represented by the uppercase P, we introduce the bounds of Section 5.3, exploiting the measurable SPS characteristics, to derive the final lower bound of the vacuum events, which can be expressed in terms of the number of events as

$$s_{X,0} \geq \underline{s}_{X,0} = \frac{\underline{p}_0}{\overline{p}_1^{(1)} \overline{p}_0^{(2)} - \underline{p}_1^{(2)} \underline{p}_0^{(1)}} \left(\underline{p}_1^{(1)} \frac{\underline{N}^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} - \overline{p}_1^{(2)} \frac{\overline{N}^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} \right). \tag{5.39}$$

5.5.2 Finite-Key Analysis: Secure Key Length Estimation

It is worth noticing that for the secure key length (SKL) estimation, we must blind ourselves to the simulation of Bob's counts (Section 5.2) which also involves the partial characterisation of Alice's source (Section 5.1) and directly work with the observed

outcomes as if we were in a real QKD experiment. In particular, the key is generated from the observed statistics on the X basis. These observed values do not correspond to the true expected values in Eq. (5.27) or (5.28). Only in the asymptotic limit, the observed values will be directly applicable to the $s_{X,1}$ bound, since the number of observed events converges to the expected value. However for our finite sample, we bound those unknown expected values (denoted with *) by applying the Chernoff bounds of Eq. 3.37, to the given observed values as

$$N^*_{X,\delta^{(1)}} \geq \underline{N}^*_{X,\delta^{(1)}} = N_{X,\delta^{(1)}} - \Delta^- \text{ and } N^*_{X,\delta^{(1)}} \leq \overline{N}^*_{X,\delta^{(1)}} = N_{X,\delta^{(1)}} + \Delta^+ \tag{5.40}$$

$$N^*_{X,\delta^{(2)}} \geq \underline{N}^*_{X,\delta^{(2)}} = N_{X,\delta^{(2)}} - \Delta^- \text{ and } N^*_{X,\delta^{(2)}} \leq \overline{N}^*_{X,\delta^{(2)}} = N_{X,\delta^{(2)}} + \Delta^+, \tag{5.41}$$

where the upper and lower deviations, Δ^+ and Δ^-, are defined in Eq. (3.37). and depend on the number of events and the parameter estimation $\varepsilon_{\text{PE}} = \varepsilon_{\text{sec}}/21$ (2-decoy) or $\varepsilon_{\text{PE}} = \varepsilon_{\text{sec}}/19$ (1-decoy). Note that we do not write the bounds for the observed errors of each distribution $m_{X,\delta^{(j)}}$, since we do not use them to derive a bound for the single-photon errors. We assume the total number of errors in the parameter estimation basis are caused by single-photons.

As explained in Section 3.6.2.1, if we were to use the observed values directly to estimate the number of detection events caused by single-photons or vacuum states, it could potentially lead to an overestimation of the vacuum or single-photon events, compromising the security of the protocol. Therefore, for finite blocks, the parties must bound their observed outcomes, ensuring that the tail probabilities are bounded with an arbitrarily small error, despite not knowing the exact statistical distribution.

Additionally, while Eve may know the number of photons in each sent state due to her ability to perform nondemolition measurements, the parties are unaware of this information. However, Eve does not know which distribution is being used to send the state when she intercepts it. This statement relies on the security of the decoy method since the parties build the set of outcomes for each distribution after the quantum communication has concluded, during the basis reconciliation step.

In the 2-decoy protocol, one of the decoy states is chosen to be a vacuum distribu-

tion, denoted by $\delta^{(0)}$. The detection events at Bob's side of this distribution $N_{X,\delta^{(0)}}$ are observed as the detector dark counts and since $\delta^{(0)}$ is purely sending vacuum state, the vacuum events are not influenced by statistical fluctuation, as there is no variation in photon states contributing to the observed events of $\delta^{(0)}$ for a given size of the block. In other words, the parties know with certainty that a click on Bob's detector when Alice chooses $\delta^{(0)}$ must be caused by a vacuum state. Hence, we do not apply the Chernoff bound to $N_{X,\delta^{(0)}}$.

The lower (upper) bound on the expected events of either $N^*_{X,\delta^{(1)}}$ or $N^*_{X,\delta^{(2)}}$ is selected when the term contributes positively (negatively) to either the single-photon $s_{X,1}$ or vacuum events $s_{X,0}$, which are positive terms of the key formula. The analysis of the denominators of $s_{X,1}$ and $s_{X,0}$ for each decoy SPS protocol tells us which terms are positive or negative. Finally, using Eqs. (5.40) and (5.41) we obtain the final expression of the single-photon and vacuum events, which read as follows.

The lower bound of the single-photon events in the 2-decoy SPS with a vacuum distribution is given by

$$s_{X,1} \geq \frac{\underline{p}_1}{\overline{p}_1^{(1)} - \underline{p}_1^{(2)}} \left(\frac{\underline{N}^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - \frac{\overline{N}^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} - \overline{p}_0^{(1)} \frac{\overline{s}_{X,0}}{\underline{p}_0} + \underline{p}_0^{(2)} \frac{N_{X,\delta^{(0)}}}{p_{\delta^{(0)}}} \right). \tag{5.42}$$

Note that the lower and upper bound of the vacuum events in the 2-decoy remains the same, see Eqs. (5.30) and (5.31), since it just depends on $N_{X,\delta^{(0)}}$ which are perfectly characterised by the parties for each finite block.

For the 1-decoy SPS protocol, the lower bound of the single-photon events is given by

$$s_{X,1} \geq \underline{s}_{X,1} = \frac{\underline{p}_1}{\overline{p}_1^{(1)} - \underline{p}_1^{(2)}} \left[\frac{\underline{N}^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - \frac{\overline{N}^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} + \left(\underline{p}_0^{(2)} - \overline{p}_0^{(1)} \right) \frac{\underline{s}_{X,0}}{\overline{p}_0} \right]. \tag{5.43}$$

and for the vacuum events,

$$s_{X,0} \geq \underline{s}_{X,0} = \frac{\underline{p}_0}{\overline{p}_1^{(1)} \overline{p}_0^{(2)} - \underline{p}_1^{(2)} \underline{p}_0^{(1)}} \left(\underline{p}_1^{(1)} \frac{\underline{N}^*_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} - \overline{p}_1^{(2)} \frac{\overline{N}^*_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} \right). \tag{5.44}$$

In this work, we do not introduce any novel methods for deriving the secure key lengths using the smooth min- and max-entropies as described in Section 2.2.3. The derivation in the WCP case has already been addressed by [96][add another] for the 2-decoy protocol and by [95] for the 1-decoy protocol, which is also based in [96]. Our unique contribution lies in the utilization of the vacuum distribution to estimate the lower bound of vacuum events $\underline{s}_{X,0}$ but discard the vacuum events of the vacuum distribution $N_{X,\delta^{(0)}}$ to form the final secure key length of our 2-decoy SPS protocol. This exclusion is motivated by the fact that correcting errors associated with vacuum events incur a higher bit cost than the contribution these events make to the key, hence their inclusion is detrimental to key generation. The rationale is as follows, the distribution $\delta^{(0)}$ only sends vacuum states, hence there is no quantum correlation between its sent vacuum states and its detection events in Bob's apparatus (dark counts). Consequently, half of these events are correct but the other half cause errors, i.e. $\mathrm{QBER}_{X,\delta^{(0)}} = 0.5$ (see the explanation of efficient BB84 in Section 3.6 for a better understanding). As a result, the bit cost for error correction exceeds the number of bits provided by $\delta^{(0)}$. For instance, if the contribution to the key is $N_{X,\delta^{(0)}} = 100$ bits, the information needed to perform the error correction code over those 100 bits is $1.16\, N_{X,\delta^{(0)}}\, h(\mathrm{QBER}_{X,\delta^{(0)}}) = 116$ bits. Therefore, in a protocol that includes a vacuum distribution, we demonstrate that discarding the detection events of $\delta^{(0)}$ and exclusively using them to estimate $s_{X,0}$, results in a greater secure key length. In particular, in our model, $N_{X,\delta^{(0)}}$ events are discarded such as the mismatched events and only the vacuum events from distributions $\delta^{(1)}$ and $\delta^{(2)}$ contribute to the key. Consequently, we subtract $N_{X,\delta^{(0)}}$ from the lower bound of the vacuum events and the leakage due to error correction in the secure key length formula. Thus the SKL of our 2-decoy SPS protocol with a vacuum distribution is given by

$$\ell_{2\mathrm{D}}^{(\mathrm{SPS})} = \underline{s}_{X,0} - N_{X,\delta^{(0)}} + \underline{s}_{X,1}\left[1 - h(\overline{\phi}^{X})\right] \tag{5.45}$$

$$- 1.16\left(N_X - N_{X,\delta^{(0)}}\right) h(\mathrm{QBER}_X) \tag{5.46}$$

$$- 6\log_2\frac{21}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}. \tag{5.47}$$

For our 1-decoy SPS protocol, the SKL formula remains identical to previous studies and it is given by

$$\ell_{1\mathrm{D}}^{(\mathrm{SPS})} = \underline{s}_{X,0} + \underline{s}_{X,1}\left[1 - h(\overline{\phi}_X)\right] - 1.16\, N_X h(\mathrm{QBER}_X) \tag{5.48}$$

$$- 6\log_2\frac{19}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}. \tag{5.49}$$

The secure key rate (SKR) is estimated as $R = \frac{\ell}{N_{\mathrm{S}}}$ for both protocols. The upper bound on the phase error rate in the X (key generation) basis for both protocols is estimated using the events in the Z (parameter estimation) basis as $\overline{\phi}_X = m_Z/\underline{s}_{Z,1} + \gamma(\underline{s}_{X,1}, \underline{s}_{Z,1}, m_Z/\underline{s}_{Z,1}, \varepsilon_{\mathrm{PE}})$, where the expression for the gamma function is shown in Eq. (3.47).

5.5.3 Description of the Protocols

The 2-decoy efficient BB84 SPS uses three pre-attenuated photon number emission distributions $\delta^{(j)} = \{p_n^{(j)}\}_{n,j=0,1,2}$ with $\delta^{(0)}$ representing the vacuum distribution. For each preparation of a quantum state, Alice selects one of the three transmissivities $\eta_{tr}^{(j)}$ associated with $\delta^{(j)}$, being two of them, $\eta_{tr}^{(1)}$ and $\eta_{tr}^{(2)}$, which are optimised, plus the remaining fixed $\eta_{tr}^{(0)} = 0$. This variety of distributions with different transmissivity levels is used to overcome a PNS attack when the quantum channel is subjected to high losses. All the pre-attenuated distributions are used for the key generation (efficient BB84).

Alice transmits secure photon states, i.e. single-photons or vacuum states (whose classical bits are flipped with the error correction code), and unsecured multiphoton states from any $\delta^{(j)}$ distribution. Consequently, Bob expects to obtain a proportion of the emissions from the key generation basis N_X due to channel losses. Here, $N_X = \sum_{n=0}^{\infty} s_{X,n}$ is the total detection events in the X basis given the states sent by Alice on the same basis. These X basis events come from the selected distributions by Alice $N_{X,\delta^{(0)}}, N_{X,\delta^{(1)}}$ and $N_{X,\delta^{(2)}}$. An eavesdropper cannot distinguish between the states from different $\delta^{(j)}$, hence Eve is forced to intercept them all. Both legitimate parties estimate the number of events caused by single-photons $s_{X,1}$ and vacuum states $s_{X,0}$,

i.e. the yields, using $N_{X,\delta^{(j)}}$. They also calculate the single-photon errors $e_{Z,1}$ in the parameter estimation basis, i.e. the phase errors on Bob's side caused by sent single-photons, although here they correspond to the total number of errors $e_{Z,1} = m_Z$. The phase error rate ϕ^X is subsequently estimated. The parties have agreed on a threshold that cannot be exceeded, $\phi^X < \phi^X_{\text{thld}}$, otherwise they must abort the protocol.

The essence of the decoy method for efficient BB84 is that the phase error rate of the two bases must be equal. This condition holds only in the asymptotic regime, as observed errors in each basis cannot be assumed to be identical in the finite key regime, despite the expected errors in the X and Z bases being identical. Specifically, in the asymptotic limit, where the data block size is considered arbitrarily large, the number of observed events assigned to each distribution $N_{X,\delta^{(j)}}$ tends to the expected number of events $N^*_{X,\delta^{(j)}}$. However, with finite samples, statistical fluctuations occur, as explained in Section 5.5.2.

It is instructive to summarise the main steps followed in our protocols, especially the actions involving the observed quantities which shall be bounded. First, Alice prepares the states, selecting a basis choice $b_i^{\text{A}} \in \{X, Z\}$ and a distribution $\delta_i^{(j)} \in \{\delta^{(j)}\}_{j=0,1,2}$ for every time she sends a state to Bob, represented by index i. Bob measures in basis $b_i^{\text{B}} \in \{X, Z\}$. Alice and Bob obtain two strings of outcomes, N_i^{A} and N_i^{B} respectively, with the length of the number of signals sent by Alice $i = 1, \cdots, N_{\text{sent}}$ including the non-detections of Bob. During basis reconciliation, the parties build two sets formed by instances where their basis choice coincide while discarding Bob's non-detections $N_i^{\text{B}} = \emptyset$. For the 2-decoy protocol with vacuum distribution $\delta^{(0)}$, the parties also discard Bob's detections caused by this distribution and use them to estimate the bounds on the remaining vacuum events. Therefore, Alice and Bob identify the following sets, $X^{\text{A}}_{\delta^{(j)}} := \{N_i^{\text{A}} : b_i^{\text{A}} = b_i^{\text{B}} = X, N_i^{\text{B}} \neq \emptyset\}$, $X^{\text{B}}_{\delta^{(j)}} := \{N_i^{\text{B}} : b_i^{\text{A}} = b_i^{\text{B}} = X, N_i^{\text{B}} \neq \emptyset\}$, and $Z^{\text{A}}_{\delta^{(j)}} := \{N_i^{\text{A}} : b_i^{\text{A}} = b_i^{\text{B}} = Z, N_i^{\text{B}} \neq \emptyset\}$, $Z^{\text{B}}_{\delta^{(j)}} := \{N_i^{\text{B}} : b_i^{\text{A}} = b_i^{\text{B}} = Z, N_i^{\text{B}} \neq \emptyset\}$ $\forall i, j$, respectively. In a real experiment, the sets of the parties would not be identical $X^{\text{A}}_{\delta^{(j)}} \neq X^{\text{B}}_{\delta^{(j)}}$ and $Z^{\text{A}}_{\delta^{(j)}} \neq Z^{\text{B}}_{\delta^{(j)}}$, due to errors. However, in our theoretical analysis, we directly calculate the total number of events for each set. Therefore, we assume $X^{\text{A}}_{\delta^{(j)}} = X^{\text{B}}_{\delta^{(j)}} = X_{\delta^{(j)}}$ and $Z^{\text{A}}_{\delta^{(j)}} = Z^{\text{B}}_{\delta^{(j)}} = Z_{\delta^{(j)}}$. To proceed with the protocol, these sets have

to be greater than a threshold of counts for each j-distribution, i.e. $|X_{\delta^{(j)}}| \geq N^{block}_{X,\delta^{(j)}}$ and $|Z_{\delta^{(j)}}| \geq N^{block}_{Z,\delta^{(j)}}$. This step is also addressed in the WCP version of Section 3.6.2.1. Since we do not conduct an actual experiment, we have to assume that our calculated observed events meet the required block size.

To generate the key, the parties select a random sample of the set $X_{\delta^{(j)}}$ with size $N_X = \sum_{j\in\delta^{(j)}} N_{X,\delta^{(j)}}$, creating a raw key pair. The parties also compute the number of bit errors $m_{Z,\delta^{(j)}}$ of each block $N_{Z,\delta^{(j)}}$ to calculate the total number of errors m_Z. Successively, they calculate the bounds on the number of the single-photon events $s_{X,1}$ and vacuum events $s_{X,0}$, Eqs. (5.42) and (5.30) for the 2-decoy and Eqs. (5.43) and (5.44) for the 1-decoy, where the Chernoff bound is applied to obtain the expected values, Eqs. (5.40) and (5.41). They also estimate the upper bound of the phase error rate as $\overline{\phi}^X$ including the γ^U function due to the random sampling without replacement problem. Finally, they verify that the phase error rate is below the predetermined threshold $\overline{\phi}_X < \phi^X_{\text{thld}}$. Otherwise, they abort the protocol. Note that for the 1-decoy protocol, any steps involving the vacuum distribution are omitted.

In classical post-processing, the parties perform an error correction code that sacrifices bits of the shared key. As noted, the sets formed by the outcomes where Alice and Bob chose the same basis and Bob obtained a click, $X^{\text{A}}_{\delta^{(j)}}$, $X^{\text{B}}_{\delta^{(j)}}$, $Z^{\text{A}}_{\delta^{(j)}}$ and $Z^{\text{B}}_{\delta^{(j)}}$, are extremely unlikely to be identical in practice. Consequently, discrepancies between Alice and Bob's sets persist when the raw key pair is randomly selected. To reconcile these sets, they perform an error-verification step using universal hash functions. Finally, they carry out privacy amplification, again employing universal hash functions to minimise the information leaked to Eve.

5.6 Secure Key Performance: A Comparative Analysis

The main challenges in adapting the decoy method to SPSs are developing optimised yield security bounds for photon number distributions in the Fock basis while relaxing the assumptions on the distributions. Moreover, finding a relation between their emission probabilities and easy-to-measure SPS characteristics, to provide partial but

sufficient knowledge to estimate the secure key length under a security parameter

5.6.1 Relaxation of the Required Photon Emission Probability Conditions

The formalism of [136, 138, 139] which considers arbitrary photon number statistics for decoy methods, seems suitable for the intricate nature of SPSs at first glance. However, it presents several issues for practical SPSs, which we aim to improve with our presented decoy protocols. Here we explore the derivation of the single-photon events lower bound $\underline{s}_{X,1}$ to highlight the important aspects that must be met to achieve an optimised and adapted decoy method for practical SPSs. These aspects are summarised in Tables 5.1 and 5.2, comparing our decoy SPS protocols with previous decoy studies using arbitrary distributions or Poissonian distributions (WCPs) [95, 96].

First, we consider which statistical distribution is used, shown in the third column of Tables 5.1 and 5.2. The first issue with the studies that employ a formalism for an arbitrary distribution is that they do not relate the emission probabilities to any measurable SPS characteristics. Hence, one must either fully characterize the photon number distribution of the practical SPS, which is experimentally challenging, or make strong assumptions about the SPS emission probabilities. In this work, we propose a partial characterisation of the SPS using the second-order correlation function and the mean photon number, providing a method to estimate the key rate from an experimental SPS under more relaxed assumptions compared to previous studies.

Second, we examine the number of emission probabilities in the Fock basis (studies with arbitrary distributions) or intensities (Poissonian studies) that are involved in the single-photon events estimation. Works for arbitrary distributions use three probabilities (vacuum, single-photon and two-photon) per pre-attenuated distribution. We reduce this to just two probabilities (vacuum and single-photon) per distribution, as in decoy WCP studies. This is shown in the fourth column of Table 5.1.

Third, we consider the number of distributions used for the single-photon events lower bound, shown in the fifth column of Table 5.1. We aim to use all available distributions in a protocol to estimate $\underline{s}_{X,1}$. However, in the 2-decoy studies for arbitrary

Paper	**Protocol**	**Source Distribution**	$P_n^{(j)}$ **or** μ_j **involved**	**Used** $P_{c\,\vert\,\delta^{(j)}}$ **or** $P_{c\,\vert\,\mu_j}$
[136, 138, 139]	2-Decoy	Arbitrary	$P_0^{(j)}, P_1^{(j)}, P_2^{(j)}$ $j=0,1,2$	$P_{c\,\vert\,\delta^{(1)}}, P_{c\,\vert\,\delta^{(2)}}$
[139]	1-Decoy	Arbitrary	$P_0^{(j)}, P_1^{(j)}, P_2^{(j)}$ $j=1,2$	$P_{c\,\vert\,\delta^{(1)}}, P_{c\,\vert\,\delta^{(2)}}$
[96]	2-Decoy	Poissonian	μ_0, μ_1, μ_2	$P_{c\,\vert\,\mu_0}, P_{c\,\vert\,\mu_1}, P_{c\,\vert\,\mu_2}$
[95]	1-Decoy	Poissonian	μ_1, μ_2	$P_{c\,\vert\,\mu_1}, P_{c\,\vert\,\mu_2}$
Our work	1-Decoy	Based on $g^{(2)}, \langle n\rangle$	$P_0^{(j)}, P_1^{(j)}$ $j=1,2$	$P_{c\,\vert\,\delta^{(1)}}, P_{c\,\vert\,\delta^{(2)}}$
Our work	2-Decoy with vac. dist.	Based on $g^{(2)}, \langle n\rangle$	$P_0^{(j)}, P_1^{(j)}$ $j=0,1,2$	$P_{c\,\vert\,\delta^{(0)}}, P_{c\,\vert\,\delta^{(1)}}, P_{c\,\vert\,\delta^{(2)}}$

Table 5.1: Comparison of state-of-the-art decoy papers using an arbitrary or Poissonian distribution with our decoy SPS protocols on lower bounding the single-photon click probability $\underline{P}_{c\,\vert\,1}$, which leads to the single-photon events lower bound $\underline{s}_{X,1}$. The colour red indicates that it is not suitable for our SPS characterisation approach in decoy protocols. Orange represents that the concept is suitable for our formalism but not directly applicable, hence some additional work is required. Finally, green represents the optimal condition. Here we show that we minimise the number of required photon emission probabilities to estimate $\underline{P}_{c\,\vert\,1}$, using less than the arbitrary distribution studies. We also maximise the used number of click probabilities for a given distribution, involving all of them, leading to tighter $\underline{P}_{c\,\vert\,1}$ than the decoy methods with arbitrary photon statistics. These ideas are inspired by the decoy WCP works, however, they cannot be directly applied to our decoy SPS models as they are tied to the Poissonian nature of the employed WCPs.

statistics, one distribution was not introduced for the single-photon events estimate, while for the 1-decoy protocol version, all the available distributions are used since it uses one distribution less than 2-decoy, which is highlighted in green in the cell corresponding to [139] of the fourth column. Although not immediately obvious, having more resources to bound $s_{X,1}$ by using one distribution to bound its multiphoton summation leads to a more optimal bound. In more detail, the exact expression of $P_{\mathrm{c}\,\vert\,1}$ is lower bounded by introducing an inequality of the multiphoton emission probabilities, called the multiphoton condition (fifth column of Table 5.2), which bounds the multiphoton summation of $P_{\mathrm{c}\,\vert\,1}$. Thus, this summation can be replaced by the unused distribution. This process is applied by the decoy WCP works and we achieve to adapt it for practical SPSs in our method.

Furthermore, another significant consideration in decoy WCP protocols is the intensity condition, an inequality relating to the intensity levels of the WCPs, implying the multiphoton condition. If the intensity condition is met, the multiphoton condition

Paper	Protocol	Source Distribution	Transmissivity (intensity) conditions	Multiphoton conditions	Conditions from $\underline{P}_{c\|1}$ ($\underline{s}_{X,1}$) denominator
[136, 138, 139]	2-Decoy	Arbitrary	None	$P_2^{(1)}P_n^{(2)} \leq P_2^{(2)}P_n^{(1)}$ for $n \geq 3$	$P_2^{(2)}P_1^{(1)} > P_2^{(1)}P_1^{(2)}$
[139]	1-Decoy	Arbitrary	None	$P_2^{(1)}P_n^{(2)} \leq P_2^{(2)}P_n^{(1)}$ for $n \geq 3$	$P_2^{(2)}P_1^{(1)} > P_2^{(1)}P_1^{(2)}$
[96]	2-Decoy	Poissonian	$\mu_1 > \mu_2 + \mu_0 > \mu_0$	$\mu_2^n - \mu_0^n < \left(\mu_2^2 - \mu_0^2\right)\mu_1^{n-2}$ for $n \geq 2$	$\mu_1 \geq \mu_2$
[95]	1-Decoy	Poissonian	$\mu_1 > \mu_2$	$\mu_1^2\mu_2^n < \mu_2^2\mu_1^n$ for $n \geq 2$	$\mu_1 > \mu_2$
Our work	1-Decoy	Based on $g^{(2)}, \langle n \rangle$	$\eta_{tr}^{(1)} > \eta_{tr}^{(2)}$	$P_n^{(2)} < P_n^{(1)}$ for $n \geq 2$	$P_1^{(1)} > P_1^{(2)}$
Our work	2-Decoy with vac. dist.	Based on $g^{(2)}, \langle n \rangle$	$\eta_{tr}^{(1)} > \eta_{tr}^{(2)} > \eta_{tr}^{(0)} = 0$	$P_n^{(2)} < P_n^{(1)}$ for $n \geq 2$	$P_1^{(1)} > P_1^{(2)}$

Table 5.2: Extension of the comparison of state-of-the-art decoy papers using an arbitrary or Poissonian distribution with our decoy SPS protocols on lower bounding the single-photon click probability $\underline{P}_{c|1}$ ($\underline{s}_{X,1}$). Note that the transmissivity (intensity) conditions must be strictly greater because otherwise, they would accept the case of the single-photon events $\underline{s}_{X,1}$ going to infinity. This is imposed by the conditions that come from the denominator of $\underline{P}_{c|1}$. The colours indicate the same as in Table 5.1. In our decoy SPS protocols, the transmissivity conditions plus certain assumptions ensure our multiphoton condition, $P_n^{(2)} < P_n^{(1)}$ for $n \geq 2$, and the condition from the denominator of the lower bound of the single-photon events, $P_1^{(1)} > P_1^{(2)}$, by applying Theorem 2. This is similar to the intensity conditions for decoy WCP studies, which are not suitable for the SPS statistical distribution. Notably, we relax the assumptions and conditions of the decoy with arbitrary distribution, although we do not achieve an assumption-free scenario regarding the photon emission probabilities as in decoy with Poissonian distributions. Note that the conditions of the decoy WCP study in [96] are explicitly derived in Section 3.6.2.1, whereas the conditions for the arbitrary distributions are derived in Section A of Appendix A, i.e. Eqs. (A.8) and (A.9). Note that considering $\mu_0 = 0$, i.e. vacuum distribution, for the 2-decoy Poissonian, one obtains the multiphoton condition of the 1-decoy Poissonian.

holds, satisfying the lower bound of $s_{X,1}$. Additionally, there is a condition on the emission probabilities that arises from the denominator of $\underline{s}_{X,1}$, which for decoy with Poissonian distributions is also held by the intensity conditions.

This idea is not present in the general formalism of decoy methods with arbitrary distributions. Although they state the same intensity conditions as decoy WCP, this is only used when they compute a particular statistical distribution and does not apply generally to their formalism. Thus, they must assume their multiphoton condition is true in the infinite-dimensional Hilbert space. In our decoy SPS protocols, we introduce a quantity analogous to intensity for decoy WCP methods. We select the transmissivities that defined the pre-attenuation of Alice's source, as it increases the tolerable distance range for key generation, as shown in the non-decoy SPS (Section 4.5.1), and allows us to generate different pre-attenuated distributions from the original SPS dis-

tribution. See our transmissivity conditions in Table 5.2. Although our transmissivities do not operate as smoothly as the WCP intensities in the decoy method, it relaxes the assumptions of the decoy with arbitrary distributions. Thus, considering the transmissivity condition of $\eta_{\mathrm{tr}}^{(1)} > \eta_{\mathrm{tr}}^{(2)} > \eta_{\mathrm{tr}}^{(0)} = 0$ and assuming the following: first, a monotonic decay of the Kth-order correlation functions $g^{(K+1)}(0) \leq g^{(K)}(0)$ for all $K \geq 2$, which is reasonable for practical SPSs; second, all the correlation functions above a certain Nth-order are null, i.e. $g^{(K>N)}(0) = 0$; and third, only the N-photon states contribute to the highest order correlation function $g^{(N)}(0)$ with a positive value, i.e. the emission probabilities of photon states with more than N photons are null $P_{k>N}^{(SPS)} = 0$. We ensure our multiphoton and denominator conditions extracted from deriving $\underline{s}_{X,1}$ are fulfilled, which implies $\underline{s}_{X,1}$ itself holds. Thus, compared to decoy studies with arbitrary distributions, instead of verifying a multiphoton condition in the infinite-dimensional Hilbert space (which is impractical), we provide a method to corroborate the needed conditions to achieve $\underline{s}_{X,1}$ under reasonable assumptions for an SPS, thereby relaxing the assumptions to ensure protocol security. In Table 5.2, this can be seen as the fact that the transmissivity (intensity) condition of the fourth column implies the multiphoton and denominator conditions on the last two columns of the right-hand side of the table under certain (no) assumptions. Note that for the decoy with arbitrary distributions, these types of implications do not exist at all, i.e. nothing facilitates the verification of their photon emission conditions, they simply recover the WCP case when computing a Poissonian distribution.

In particular, in [136, 138, 139], they do not mention any intensity conditions, they simply present their signal, decoy and vacuum distribution. Additionally, their multiphoton condition derived from the lower bound on the single-photon yield has to be satisfied by three-photon states or higher, see Table 5.2. The two-photon states do not need to be included, contrary to what is shown in Eq. (14) of their first paper [136]. That condition for two-photon states may be necessary for achieving a positive key but is not a security condition of the protocol. In their following paper, they state the same condition introducing bounds to the emission probabilities, Eq. (36) of [138]. However, their bounds are calculated using the Poissonian distribution by arbitrarily defining an

interval of the intensity of the coherent state $[\mu_j^L, \mu_j^U]$ for each distribution $\delta^{(j)}$, which is not a statistical behaviour that suits practical SPSs.

In [139], they do not specify which multiphoton conditions these generic statistical distributions must fulfil, however, we specifically show them in the fifth column of Table 5.2. Although, they do mention their inequalities from the $P_{c|1}$ denominator, Eq. (1) in [139]. Therefore, the emission probabilities of their generic distributions are subject to additional inequalities beyond the ones they assert. Then the claim that their decoy analysis can be applied to generic distributions may be questioned. First, not every type of quantum source has photon emission statistics that meet their multiphoton condition used to bound $P_{c|1}$. Second, while it is true they can ensure the fulfilment of their multiphoton conditions for Poissonian, thermal, and binomial distributions, the denominator condition from $\underline{P}_{c|1}$, shown in the sixth column of Table 5.2, is met by the Poissonian and thermal distribution but not by the binomial distribution. Seemingly, having an impact on obtaining the highest secure key rates for the binomial distribution in their decoy simulation.

5.6.2 Non-Decoy and Decoy Single-Photon Source versus 2-Decoy Weak Coherent Pulse

In the 2-decoy SPS protocol with a vacuum distribution, we implemented a methodology that exclusively exploits the vacuum distribution to bound the vacuum events without using any additional distribution. A similar technique was applied in [100], however, it is often not implemented in 2-decoy studies [96, 139]. Thus, we avoid further conditions for the multiphoton emission probabilities, avoiding the complexity of verifying them using Theorem 2 or extra artifices, as the true SPS distribution is unknown. To check the common parameters among the protocols see Table 5.3. Note that some of them are maintained from previous chapters to be consistent.

When the 2-decoy SPS is computed their optimal highest key rates are achieved when a vacuum distribution is considered. Therefore, we do not show the results for a more generic 2-decoy protocol without imposing a vacuum distribution for $\delta^{(0)}$, as its key performance is consistently worse. Additionally, we find that the key generation

Description	**Parameter**	**Value**
Source repetition rate	R_{rate}	160.7 MHz
Misalignment probability	p_{mis}	0.003
Dark count probability	p_{dc}	3.67×10^{-8}
Detector efficiency	η_{det}	0.6525
Optical fibre loss	l	0.1904 dB/km
Secrecy failure probability	ε_{sec}	10^{-9}
Correctness failure probability	ε_{cor}	10^{-15}

Table 5.3: Baseline QKD system parameters for both decoy SPS methods and the 2-decoy WCP protocol. These parameters are based on the experimental set-up of the quantum dot in [42].

performance between the 2-decoy SPS with vacuum and the 1-decoy SPS protocol is nearly identical for 1 hour of acquisition time, as shown in Figure 5.3 (b). However, the difference between them increases for a shorter acquisition time of 1 min, where the 2-decoy SPS gives a slightly higher key rate for the high-loss regime, see Figure 5.3 (a). Hence, we can conclude that the 2-decoy SPS has a higher key rate performance than the 1-decoy SPS at small block sizes. Increasing the block size, the difference in secure key rates between the 2-decoy WCP and the decoy SPS protocols diminishes. This was expected since we have already shown the SPS has more potential for short acquisition times as presented in Section 4.5.2.

Note that in the decoy SPS models of Figures 5.3 and 5.4 $g^{(2)}(0)$ is fixed, whose value is taken from the quantum dot of [40] analysed in Section 4.5. Our decoy SPS results highlight that for achieving parity with the key rate performance of the 2-decoy WCP and surpassing it in the high-loss regime, an SPS with a mean photon number of $\langle n \rangle = 0.2$ is required, see Figure 5.3. This observation underscores the advantageous position of SPSs with sufficiently high mean photon numbers ($\langle n \rangle \geq 0.2$) over WCPs in key generation within high-loss regimes for decoy protocols, owing to their ability to significantly reduce multiphoton emissions.

However, it is well known that WCPs can achieve higher repetition rates than SPS, which are more limited. In Figure 5.5, we show that even for our real SPS at a repetition rate of 160.7 MHz (dashed green line), a greater key generation than a high repetition rate WCP (10 GHz) is achieved for the decoy method. We also plot some other realistic

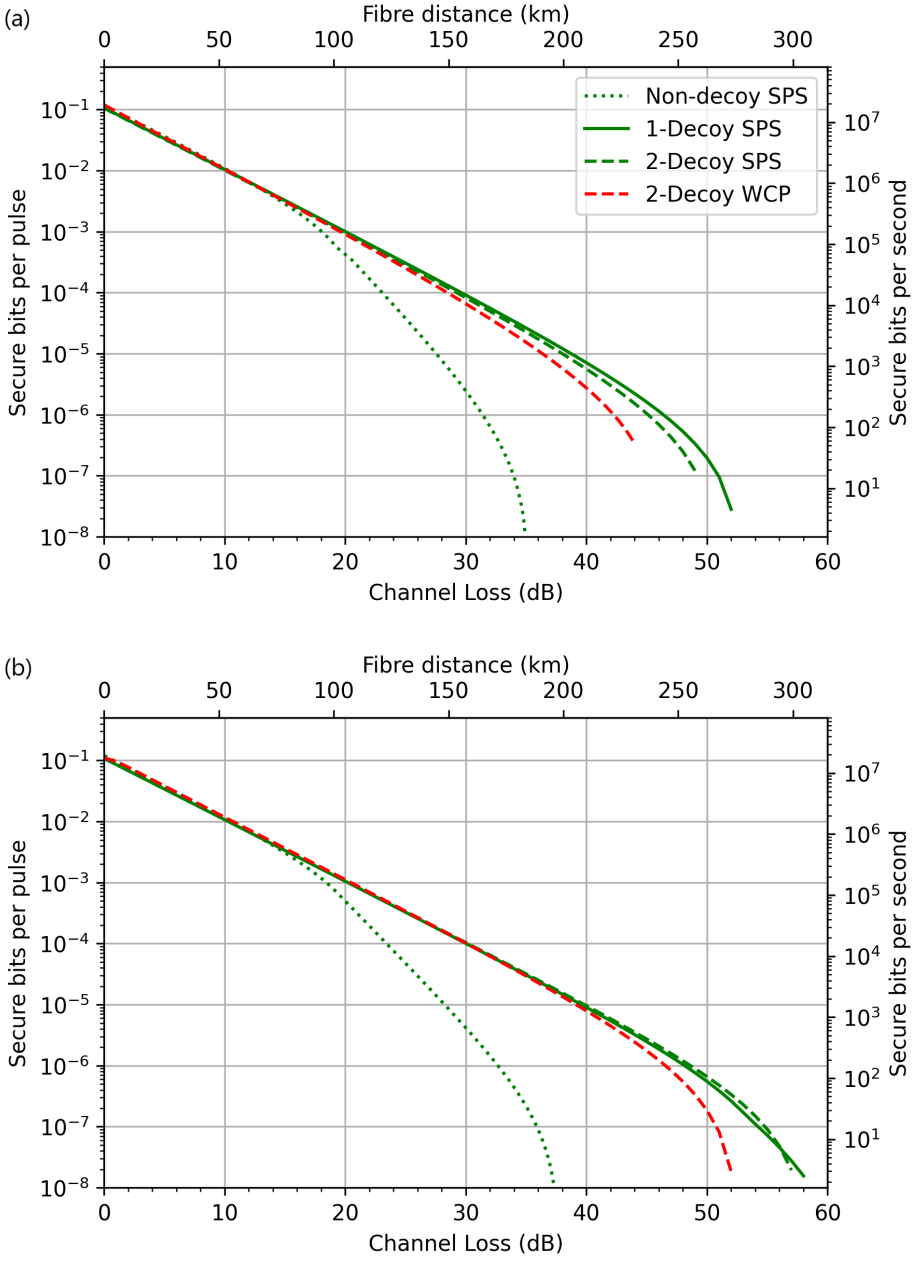

Figure 5.3: Comparison of the finite secure key amongst all the protocols with optimised parameters. The non-decoy SPS of Section 4.4.2.1, the 1-decoy and 2-decoy SPS of this chapter and the 2-decoy WCP protocol of Section 3.6.2.1. Here in (a) we consider a block size of 1 minute of acquisition time (9.642×10^9 sent signals) and in (b) 1 hour of acquisition time (5.7852×10^{11} sent signals). In both figures, the mean photon number of the SPS is $\langle n \rangle = 0.2$ and the second-order correlation function is $g^{(2)}(0) = 0.036$.

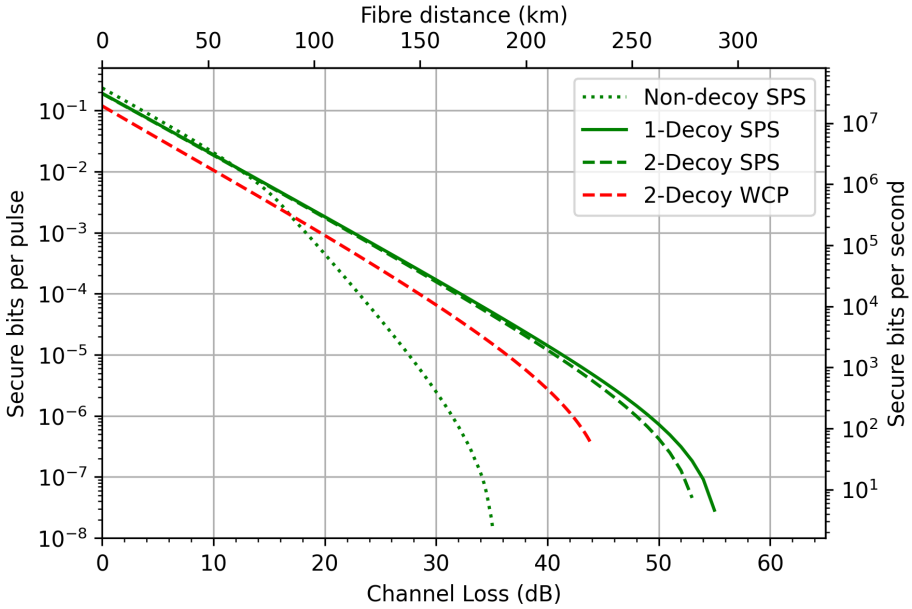

Figure 5.4: Comparison of the finite secure key amongst all the protocols with optimised parameters. Here is considered a block size of 1 minute of acquisition time (9.642×10^9 sent signals) and for the SPS a mean photon number of $\langle n \rangle = 0.4$ and $g^{(2)}(0) = 0.036$.

repetition rates for WCP and an optimistic scenario for SPS of 1 GHz.

Furthermore, we doubled the previous mean photon number ($\langle n \rangle = 0.4$) to illustrate the potentially achieved key rate increment between the decoy SPS protocols and the 2-decoy WCP, shown in Figure 5.4. In this figure, we reach a similar result for our non-decoy SPS, which is more generic and refined, compared to a previous analysis for a heralded SPS in [144], confirming a practical SPS can outperform a 2-decoy WCP in the low-loss regime. We can conclude the impact of low multiphoton emissions of SPSs with a sufficiently high mean photon number, $\langle n \rangle \geq 0.2$, in the high-loss regime is evident, extending the maximum tolerable loss of the decoy method compared to WCPs.

In general, it is clear than an SPS with mean photon number below $\langle n \rangle < 0.2$ cannot surpass the key generation of WCPs. In the finite regime, when the block size is less than 10^7 sent signals, the non-decoy SPS may have an advantage in the low-loss regime (less than 26.5 dB channel loss) when its $\langle n \rangle$ is sufficiently high (we refer to the previous section 4.5.2 for further discussion). In the scenario where all

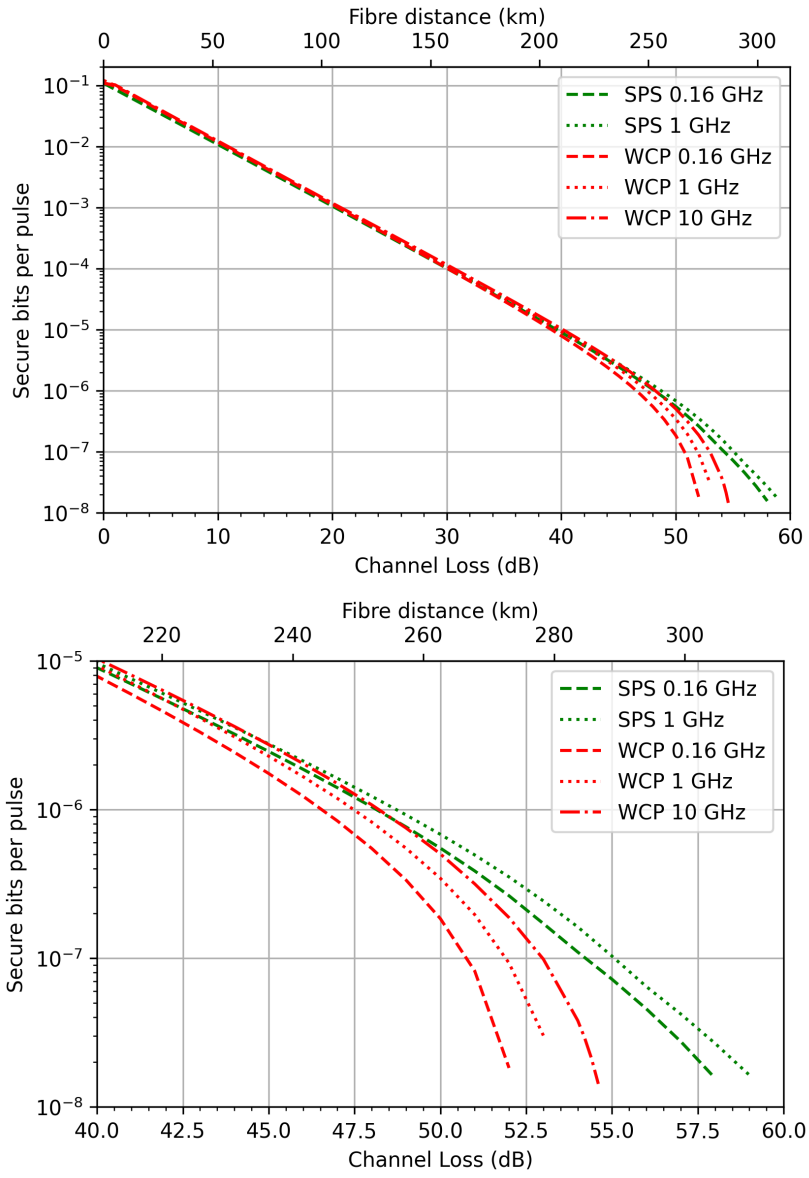

Figure 5.5: Comparison of the finite secure key of the 2-decoy protocol for WCP (red line) and SPS (green line) considering several repetition rates. Here we use a block size of 1 hour of acquisition time.

these detrimental conditions for the SPS QKD performance over WCPs are met (see Diagram **??** for further details), i.e. $\langle n \rangle < 0.2$ and more than 10^7 sent signals, we find it useful to provide a comparison between the non-decoy and 1-decoy method for SPSs, see Figure 5.6. We select 1 minute of acquisition time as the block size, since the relative difference of the protocols with other blocks must be equivalent and it is above 10^7 sent signals. Therefore, considering these number of sent signals, the 1-decoy method is a more optimal choice than the 2-decoy for SPSs (see Figure 5.3 a).

Finally, in Figure 5.7, we present the key results for the quantum sources experimentally developed by our collaborators, which are the quantum dot of [42] and the hexagonal boron nitride (hBN) source, which we theoretically analysed for a free-space QKD implementation in [145] (discussed in the following chapter). Clearly, we observe that the mean photon number of the quantum dot is not sufficiently high to approach the 2-decoy WCP key performance. In contrast, the hBN source emerges as a promising candidate to surpass traditional WCPs in the decoy method, thanks to its high mean photon number of $\langle n \rangle = 0.513$ However, this value of the mean photon number is estimated under certain assumptions explained in [145], hence, further experimental characterisation is needed to ensure this particular hBN source can outperform decoy WCP.

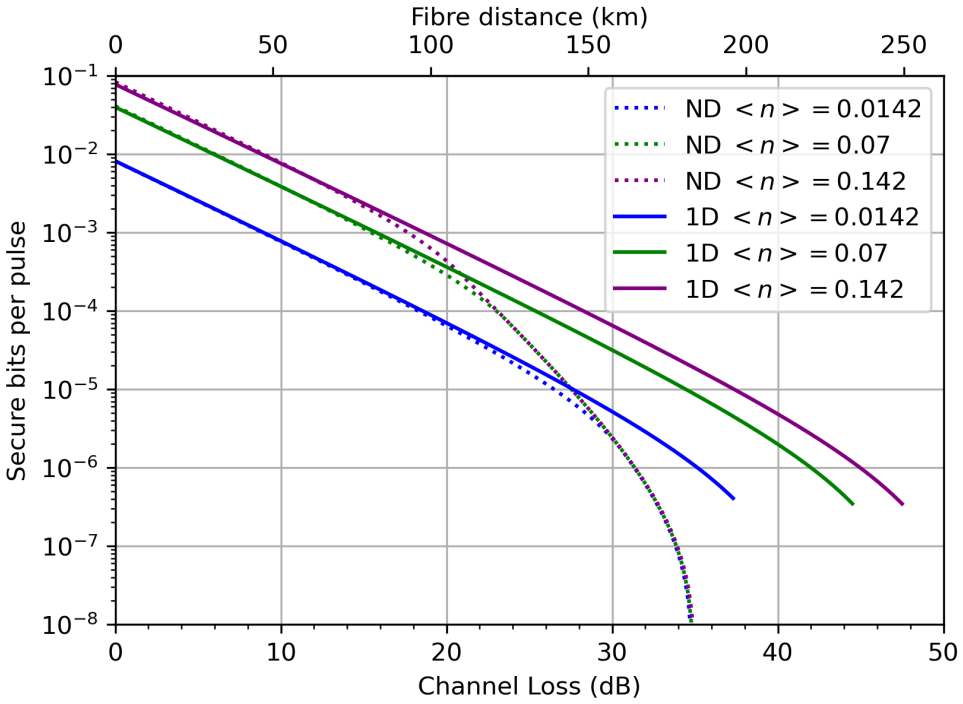

Figure 5.6: Comparison of the finite key rates in a semi-log scale for SPSs with different mean photon numbers $\langle n \rangle$ for the non-decoy (dotted lines) and 1-decoy (solid lines) protocols. The fixed block size is 1 minute of acquisition time (9.642×10^9 sent signals).

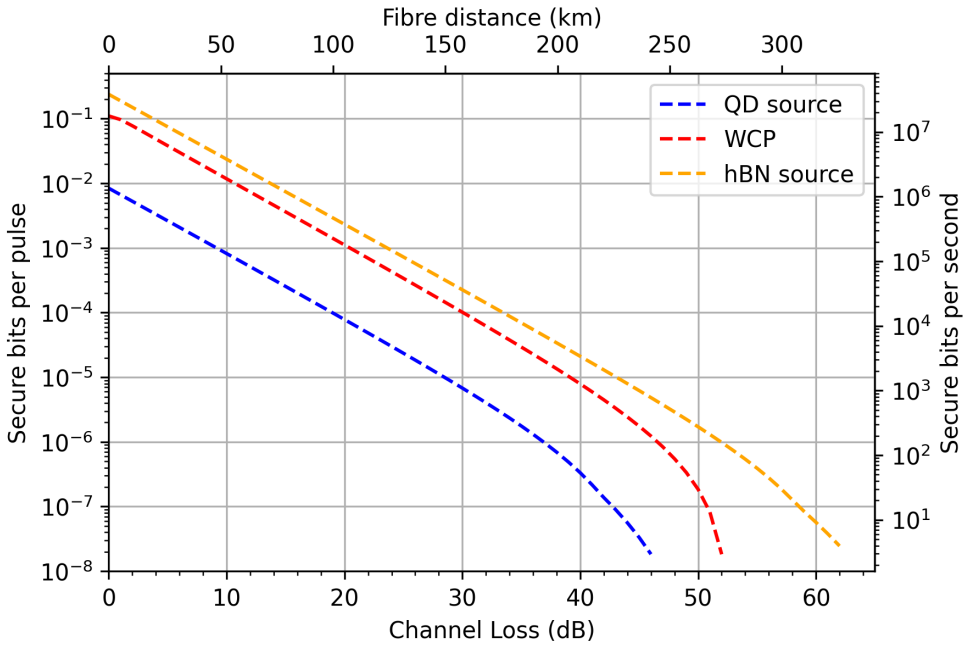

Figure 5.7: Comparison of the finite secure key for the 2-decoy protocol (dashed lines) with different optimised quantum sources. The quantum dot of [42] with $\langle n \rangle = 0.0142$ and $g^{(2)}(0) = 0.036$ (blue line), the widely employed WCP (red line) with optimised intensities and an SPS based on a 2D material, which is a hexagonal boron nitride (hBN) (orange line), with $\langle n \rangle = 0.513$ and $g^{(2)}(0) = 0.0064$. Note the hBN source will be analysed for free-space QKD in the next chapter. Here is considered a block size of 1 hour of acquisition time (5.7852×10^{11} sent signals).

Chapter 6

Satellite-To-Ground Quantum Key Distribution

The transmission loss of a free-space channel is extremely lower than in optical fibre, where the loss scales exponentially and it is unattainable to go far beyond 1000 km [20, 146]. In fact, the current distance record over fibre is 1002 km using a twin-field QKD protocol [147]. Hence, there is a clear motivation to move to free-space QKD and avoid the exponential scattering and absorption losses in fibres. The losses for twin-field QKD protocols enter with the square root into the rate-distance relationship, unlike conventional protocols that scale linearly. However, the scaling remains exponential. Overcoming global distances and maintaining sufficiently high data rates require satellite links [148] or quantum repeaters [149–152]. However, stringent performance requirements render quantum repeaters impractical by themselves for scaling to intercontinental ranges [153]. Therefore, given that the attenuation in the atmosphere becomes negligible above 10 km [154], satellite QKD provides a promising alternative to quantum repeaters [153, 155, 156]. The first space-to-ground QKD protocol has been demonstrated by the Micius satellite using the BB84 protocol with decoy states [157, 158]. The link to Micius was only operational during the night to avoid sunlight saturating the single-photon detectors in the ground station.

Near future quantum networks will require daylight operation for continuous availability. Several studies have explored daytime QKD using weak coherent states pro-

duced by pulsed lasers [159–165]. The wavelengths were chosen in the atmospheric transmission windows in the range of 700-900 nm or in the telecom C-band at 1550 nm [163–165]. The latter has the appeal of intrinsically lower solar irradiance, at the expense of less efficient single-photon avalanche diodes (SPADs) based on e.g. InGaAs/InP (compared to silicon-based SPADs) or very expensive, although efficient, superconducting nanowire single-photon detectors (SNSPDs). Another major drawback when using longer wavelengths is the linear scaling of the divergence with the wavelength. The diffraction losses can be compensated by larger telescopes, however, this drastically increases the cost of satellites and optical ground stations. Quantum communication using visible wavelengths is therefore desirable. In this chapter, we propose several wavelength candidates for satellite QKD and we characterise their total transmission efficiency in free space using the model presented in Section 6.1.

The solar background can be suppressed by spectral, spatial, and temporal filtering. However, a natural opportunity is offered by the Fraunhofer lines, i.e. the set of dark lines in the solar spectrum caused by absorption in the Sun's or the Earth's atmosphere. When classical information is encoded in polarised light at these wavelengths, it can be separated from the sunlight by spectral filtering at Bob's side. This scheme was originally proposed in 2006 [166], although it was never actually realised due to the requirement of a tunable short pulse laser and either a fast polarization modulator for visible light or multiple lasers that are spatially overlapped. This initial work employed a wavelength of 656.448 nm as the broadest Fraunhofer line. Thus, we aim to explore which wavelength is the most optimal for daylight QKD communication and which quantum source can perform more efficiently in this scenario. We propose two Fraunhofer lines suitable for daylight operation and we evaluate a weak coherent pulse and a single-photon source as the possible QKD sources.

To estimate the secure key lengths, we perform the same up-to-date techniques shown in previous chapters, such as smooth entropies and improved finite-key bounds. We have already reviewed the importance of the finite key effect, nevertheless, it is worth highlighting that here its significance is also relevant due to the restrictive transmission times between the satellite and ground station, which impose a limit on the secure

key generation. The optimisation of the protocol parameters is also crucial to extract the maximum secure key for each satellite overpass, which is presented in Section 6.2. In particular, we analyse the finite secure key for the 2-decoy WCP protocol of Section 3.6.2.1 and the non-decoy SPS method of Section 4.4.2.1 in a satellite QKD scenario for a range of zenith and non-zenith overpasses and satellite altitudes. To simulate satellite-to-ground QKD communication and optimise the parameters, we use our SatQuMa simulation toolkit [1], which was firstly used for simulating the 2-decoy WCP with a vacuum distribution [97], here we expand the model to the non-decoy SPS to evaluate both of them. Further analysis on the 2-decoy satellite QKD model is examined in [167].

We also provide a method to estimate the annual secure key length, which can be interpreted as a long-term key volume at a particular latitude of the optical ground station (OGS) (Section 6.3). Our final aim is to identify the optimal wavelength for daylight free-space QKD amongst our proposed wavelength candidates, although we also examine them during night communication. These candidates are the Hα line (656.448 nm), the Ca II line (854.445 nm) and the telecom C-band (1550.027 nm) and they were selected by our collaborators after evaluating asymptotic secure key rates for wavelengths ranging from 400 to 1700 nm. Depending on the wavelength the free-space channel model acquires a different transmission efficiency. Here we do not cover the details of this selection process. However, it can be found in our published collaborative paper [145], as well as the contributions of this chapter. The practical single-photon source used in our model assumes the parameters from a tunable microcavity-coupled colour centre in hexagonal boron nitride (hBN) [168, 169], previously developed in [170]. This SPS operates at room temperature and has been implemented on a satellite platform, hence, it is suitable for space-to-ground QKD [106].

6.1 System Model

We consider a satellite in a circular Sun-synchronous orbit (SSO) and we vary its altitude h and maximum elevation angle of the overpass $\theta_{\text{elev}}^{\max}$ to analyse the key generation in different scenarios. Our satellite model performs downlink QKD to an OGS at sea

level, which has been proven more robust than uplink QKD in handling atmospheric extinction [148]. The elevation and range are calculated as a function of time for different overpass geometries representing different ground track offsets and maximum elevations for the overpass, see Figure 1 of [97]. The ground track offset represents the distance between the plane of the satellite overpass and the location of the OGS when the satellite is at its maximum elevation, thus it is an analogous quantity to the maximum elevation angle of the pass. Furthermore, the quantum link is restricted to be above $\theta_{\text{elev}}^{\text{min}} = 10^{\circ}$, since any elevation below that angle is not feasible.

Internal transmitter losses are not included since they can be countered by adjusting the WCP source to maintain the desired exit aperture intensities. We also do not explicitly consider time-varying transmittance, modelling the average change in channel loss due only to the change in elevation with time. For protocols such as BB84, channel transmission fluctuations do not directly impact the secure key rate, in contrast to continuous variable QKD where this appears as excess noise leading to key reduction.

The ideal overpass corresponds to the satellite passing over the zenith of the OGS, see Figure 1 (b) of [97], giving the longest transmission time with the highest transmission efficiency of the free-space channel. However, an overpass usually does not pass directly overhead most times and it reaches a maximum elevation $\theta_{\text{elev}}^{\text{max}} < 90^{\circ}$, as represented in Figure 1 (b) of [97]. We model the total transmission efficiency of the free-space channel considering the following aspects.

6.1.1 Geometric Considerations

Here we present the geometric considerations of our satellite-to-ground communication model, see Figure 6.1. The orbital period of the satellite is given by

$$T = 2\pi\sqrt{\frac{(R_{\text{E}} + h)^3}{G m_{\text{E}}}} \tag{6.1}$$

where R_{E} is the radius of the Earth, h is the satellite altitude, G is the gravitational constant and m_{E} is Earth's mass. Using this period is straightforward to calculate the frequency orbital period as $\omega = 2\pi/T$. For each transmission time of the overpass

t, we define the corresponding angle $\phi = \omega t + \pi/2$. Furthermore, we consider that the satellite pass starts at the transmission time $t = -\Delta t$ and elevation angle $-\theta_{\text{elev}}$, reaches $t = 0$ at the maximum elevation angle of the pass $\theta_{\text{elev}}^{\max}$, i.e. $\phi = \pi/2$, and finishes at time $t = \Delta t$ and elevation angle θ_{elev}. Note the maximum elevation angle can be below 90°, i.e. a non-zenith pass. The coordinates of the satellite are defined as

$$S_x = (R_{\text{E}} + h)\cos\phi \tag{6.2}$$

$$S_y = 0 \tag{6.3}$$

$$S_Z = (R_{\text{E}} + h)\sin\phi. \tag{6.4}$$

The ground track offset depends on the maximum elevation angle of the overpass and it is defined as

$$d(\theta_{\text{elev}}^{\max}) = R_{\text{E}}\left[\pi/2 - \theta_{\text{elev}}^{\max} - \arcsin\left(\frac{R_{\text{E}}\sin\left(\theta_{\text{elev}}^{\max} + \frac{\pi}{2}\right)}{R_{\text{E}} + h}\right)\right], \tag{6.5}$$

and the coordinates of the OGS are calculated as

$$x_{\text{ogs}} = 0 \tag{6.6}$$

$$y_{\text{ogs}} = R_{\text{E}}\sin\left(\frac{d(\theta_{\text{elev}}^{\max})}{R_{\text{E}}}\right) \tag{6.7}$$

$$z_{\text{ogs}} = R_{\text{E}}\cos\left(\frac{d(\theta_{\text{elev}}^{\max})}{R_{\text{E}}}\right), \tag{6.8}$$

where the x-coordinate is zero because we are considering a terrestrial ground station.

The slant distance $z(h, \phi)$, defined as the distance between the satellite and the OGS, can be calculated as the norm of the difference between the previous coordinates

$$z(h, \phi) = (S_x - x_{\text{ogs}})^2 + (S_y - y_{\text{ogs}})^2 + (S_z - z_{\text{ogs}})^2. \tag{6.9}$$

The angle associated with the arc of the orbital path is defined as

$$\alpha = \arccos\left(\frac{R_{\text{E}} + (R_{\text{E}} + h)^2 - z(h, \phi)^2}{2R_{\text{E}}(R_{\text{E}} + h)}\right). \tag{6.10}$$

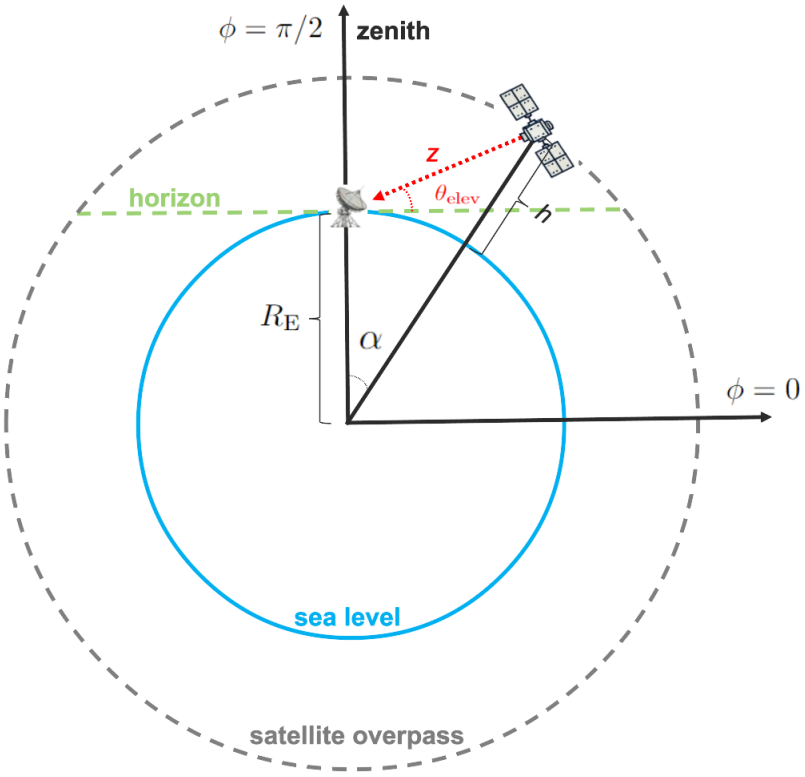

Figure 6.1: Geometry of a zenith satellite overpass around the Earth communicating with an optical ground station (OGS) located at sea level. θ_{elev} represents the elevation angle of the pass, α is the angle between the satellite position and the zenith, and $\phi = \omega t + \pi/2$ where ω is the frequency orbital period and t the transmission time of the satellite, hence when $t = 0$ (at zenith) $\phi = \pi/2$. The transmission time of the satellite starts at $-\delta t$ and ends at $+\delta t$. Here there is no ground track offset since it is a zenith pass, hence $\theta_{\text{elev}}^{\max} = 90°$, which implies $d(\theta_{\text{elev}}^{\max}) = 0$.

Finally, we can calculate the elevation angle for each time of the overpass as

$$\theta_{\text{elev}}(\phi) = \arccos\left(\frac{(R_{\text{E}} + h)\sin(\alpha)}{z(h,\phi)}\right), \tag{6.11}$$

note that $\phi = \phi(t)$.

6.1.2 Diffraction-Induced Transmission

We assume that free-space quantum communication is based on a quasi-monochromatic optical mode represented by a Gaussian beam with waist w_0 and infinitely large curva-

ture. The spot size matches the telescope's clear aperture, hence the aperture does not induce any diffraction. Alice transmits the quantum states through free space and after a distance $z(h, \phi)$, they are detected by Bob whose telescope has a circular aperture with radius a_{G}. For the satellite's telescope, we assume a diameter of 10 cm, which is compatible with CubeSats. For the OGS, we take the telescope diameter from the Micius experiment (1 m), hence $a_{\mathrm{G}} = 0.5$ m [157]. To minimize the impact of turbulence, which can be compensated for using adaptive optics in the ground station [171], we consider downlink communication. In particular, the elevated dark count rate resulting from space radiation must be acknowledged and adequately mitigated. [172–174].

Inevitably, the waist of the beam expands while propagating due to free-space diffraction. Hence, after traveling for a distance $z = z(h, \phi)$, the beam has expanded to

$$w_{\mathrm{G}}(z) = w_0 \sqrt{1 + \frac{z^2}{z_R^2}}, \tag{6.12}$$

where $z_R = \pi w_0^2 \lambda^{-1}$ is the Rayleigh range and $w_0 = 5$ cm is the beam radius at the exit of the satellite's telescope. The transmission efficiency through the receiver telescope's aperture a_{G} is given by

$$\eta_{\mathrm{G}}(z) = 1 - \exp\left(-2\frac{a_{\mathrm{G}}^2}{w_{\mathrm{G}}^2}\right). \tag{6.13}$$

In this work, we neglect the refraction effect of the atmosphere on the elongation of the beam path for different angles.

6.1.3 Atmospheric Extinction

The atmospheric extinction is caused by both aerosol absorption and Rayleigh/Mie scattering, resulting in free-space propagation loss. To estimate the atmospheric transmission as a function of wavelength and elevation angle θ_{elev}, we use an open-source code, called libRadtran [175], and we obtain as an outcome the atmospheric transmission η_A results. We interpolate them to have steps of 1 second (approximately 0.14°) within the entire transmission time (elevation angles) of the overpass.

6.1.4 Pointing and Tracking Losses

The satellite is presumed to orient its telescope towards the ground station and maintain tracking throughout its pass. This tracking typically utilizes a beacon laser emitted from the ground station. Given the considerable distances involved, it is necessary to account for a point ahead angle to compensate for the finite speed of light. This point ahead angle, derived from the satellite's orbital data [176], is then applied as an offset to the incidence angle of the beacon beam. For example, for an orbit at an altitude of 500 km, the point ahead angle can reach up to 53 μrad. Both the beacon beam sensing and the point ahead mechanism are prone to errors. However, these errors are assumed to be independent and normally distributed with zero means.

For these conditions, the link efficiency due to pointing and tracking errors, η_{pt}, can be modelled as [177, 178]

$$\eta_{\mathrm{pt}} = \exp(-G_{\mathrm{tx}}\theta_{\mathrm{pt}}^2), \tag{6.14}$$

with the transmit antenna gain $G_{\mathrm{tx}} = (\frac{2\pi a_{\mathrm{S}}}{\lambda})^2$ and the combined pointing and tracking error angle θ_{pt} of the satellite. Note, $a_{\mathrm{S}} = 5$ cm is the clear transmitter aperture radius. For the calculation of the corresponding loss, a pointing and tracking error of 1 μrad is assumed [157].

6.1.5 Temporal Filtering

Since dark counts occur randomly, they can be mitigated by temporally filtering the detection events [162]. This can be achieved either actively by gating the detectors or through post-selection. In the following analysis, we consider the temporal width of the photons to be $\tau = 3$ ns, which is determined by the excited state lifetime or the laser pulse length, depending on the light source. For a fair comparison, we assume that the filtering efficiency for a laser pulse and a single-photon emitter is identical, although, in practice, it depends on the precise temporal distribution. For a single-photon emitter, the spontaneous emission process follows an exponential distribution. The filtering

efficiency for a gating time δt is given by the cumulative distribution function,

$$\eta_{\text{temp}} = 1 - \exp\left(-\frac{\delta t}{\tau}\right). \tag{6.15}$$

For each wavelength and quantum source, we consider the same $\delta t = 1$ ns to have a fair comparison between them. This is the most commonly employed getting time for WCPs in decoy protocols.

6.1.6 Total Transmission

The link efficiency of the free-space channel not considering the receiver model, is given by the product of the previous transmission terms,

$$\eta_{\text{link}} = \eta_{\text{G}}\eta_{\text{A}}\eta_{\text{pt}}\eta_{\text{temp}}. \tag{6.16}$$

Multiplying by the detector efficiency η_{det}, we finally obtain the total transmission of the free-space communication link considering Bob's side,

$$\eta_{\text{tot}} = \eta_{\text{link}}\eta_{\text{det}}. \tag{6.17}$$

Note that we have neglected internal optical losses in the sender and receiver unit, which are typically small compared to the other link losses due to anti-reflection coatings and high-quality optics.

In Figure 6.2, we present the total link loss in dB calculated by $l_{\text{tot}} = -10\log_{10}\eta_{\text{tot}}$ and the diffraction-induced transmission losses using $l_{\text{G}} = -10\log_{10}\eta_{\text{G}}$ versus the transmission time of a zenith overpass. There is a significant difference of approximately 6 dB (5 dB) between the Hα line (Ca II line) and the C-band. Although variations exist among the three wavelengths for all the parameters involved in η_{tot}, the diffraction-induced loss shows similar differences to l_{tot} between the wavelengths, as depicted in Figure 6.2. This suggests that diffraction-induced transmission has a greater impact on the total loss compared to the other parameters. Therefore, for the total losses in our specific model, we observe a clear disadvantage of the C-band compared to the other

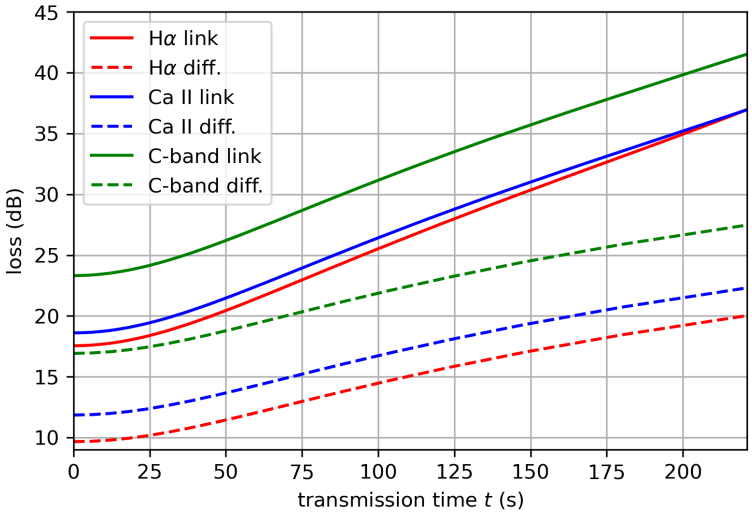

Figure 6.2: Total transmission dB losses l_{tot}(solid lines) and diffraction-induced dB losses l_{G} (dashed lines) of the communication link represented as a function of the transmission time of the satellite, for the three wavelength candidates: Hα (656.448 nm), Ca II (854.445 nm), and C-band (1550.027 nm). This is calculated for a zenith pass, hence the time origin $t = 0$ represents the maximum elevation angle of the pass $\theta_{\text{elev}}^{\text{max}} = 90°$.

wavelengths. This greater loss for the C-band due to diffraction was anticipated, as an increase in wavelength λ leads to greater bream broadening w_{G}, thereby reducing the efficiency of the diffraction-induced transmission η_{G}. Furthermore, Hα experiences 1 dB less total loss than Ca II at time $t = 0$ seconds (maximum elevation angle of the pass). However, they both reach similar total link losses at long transmission times (low elevation angles).

6.1.7 Background Noise

As explained in the previous section, the maximum tolerable loss of a prepare-and-measure QKD system is limited by the extraneous count rates that cause the typical cutoff in the key rate curves together with the intrinsic multiphoton contribution of the used quantum source. These extraneous count rates are the sum of the dark count of the detector, which is fixed for the entire transmission time and occur with probability p_{dc}, and the background counts caused by the sun during daylight, which depend on the transmission time of the overpass. In particular, this background noise also

depends on the receiver's aperture size a_{G} and field of view Ω_{fov}. Many QKD systems use temporal filtering [162], which reduces the extraneous counts as the detectors are active for a certain short time δt when a photon sent by Alice is expected.

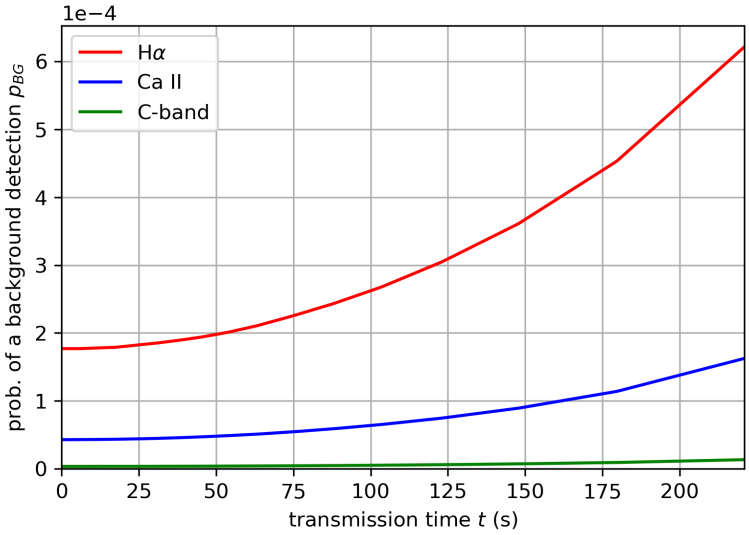

Figure 6.3: Representation of the probability of detecting background light p_{BG} for the three wavelength candidates: Hα (656.448 nm), Ca II (854.445 nm), and C-band (1550.027 nm).

The solar background is dependent on the wavelength λ and spectral filter bandwidth $\Delta\lambda$. Hence, we can define the parameter

$$\Gamma_R = \Delta t \Omega_{fov} a_{\mathrm{G}}^2. \tag{6.18}$$

We assume $\Omega_{fov} = 10^{-10}$ sr [171] and $a_{\mathrm{G}} = 50$ cm for the receiving telescope [157]. The extraneous count probability is then given by

$$p_{\mathrm{ec}}(\lambda) = \eta_{\mathrm{det}}(\lambda)\Gamma_R H_\lambda^{\mathrm{sun}} + p_{\mathrm{dc}}(\lambda)\delta t = \eta_{\mathrm{det}}(\lambda)p_{\mathrm{BG}}(t) + p_{\mathrm{dc}}(\lambda)\delta t, \tag{6.19}$$

where $p_{\mathrm{BG}}(t)$ accounts for the detection probability of background light due to solar irradiance and is dependent on the transmission time of the satellite overpass. The detector efficiencies of each wavelength $\eta_{\mathrm{det}}(\lambda)$ are extracted from commercially available single-photon detectors. Specifically, they are $\eta_{\mathrm{det}}(\mathrm{H}\alpha) = \eta_{\mathrm{det}}(\mathrm{CaII}) \approx 85\%$ and

$\eta_{\text{det}}(\text{C}-\text{band}) \approx 73\%$. For more details about the selected detector for each wavelength see the Supplementary Material of [145]. In addition, we take the detector dark count rate from the detector with the highest efficiency for each wavelength, which are $p_{\text{dc}}^{\text{H}\alpha} = 6 \times 10^{-8}$, $p_{\text{dc}}^{\text{CaII}} = 4.5 \times 10^{-8}$ and $p_{\text{dc}}^{\text{C-band}} = 10^{-6}$. Moreover, H_{λ}^{sun} is the solar spectral irradiance integrated over the spectral filter bandwidth. We take $\Delta\lambda = 0.5$ nm for all wavelengths due to technological reasons. We acknowledge the potential benefits of using ultra-narrow bandpass filters, particularly for wavelengths like the Hα Fraunhofer line, which exhibits a notably narrow width. Our assumption of a 0.5 nm filter width is intended to standardize the comparison across all wavelengths in the finite-key analysis between the two protocols. However, we recognize the importance of exploring more nuanced filter selections for specific Fraunhofer lines. Further analysis on this and the calculation of the solar spectral irradiance using libRadtran is included in the asymptotic study and the Supplementary Material of [145].

In Figure 6.3, we illustrate the evolution of the background probability p_{BG} as a function of the transmission time during a zenith pass. This figure highlights the advantage of the C-band, where background light counts are expected to be significantly lower than for other wavelengths. Conversely, Hα line is the wavelength more affected by the solar irradiance, especially at low elevation angles (long transmission times). In summary, Figure 6.2 and 6.3 provide a comprehensive overview of the parameters that most significantly impact the key generation results of the wavelength candidates, which are thoroughly analysed in Section 6.4.

6.2 Optimisation of Protocol Parameters

In this section, to maximize the attainable secure key the efficient BB84 protocol is implemented. Thus, in the 2-decoy WCP the highest key length is generated by optimizing the following parameters, the basis bias p_X, the intensities of the two sources μ and ν_1, the probabilities of choosing each source p_μ and p_{ν_1}, and the transmission time window δt of the satellite overpass. Notice that we set the other decoy-state intensity as vacuum $\nu_2 = 0$. For the non-decoy SPS, there are fewer protocol parameters, hence, we

Description	**Parameter**	**Value**
Intrinsic QBER	e_{int}	0.03
Source repetition rate	R_{rate}	10^8 Hz
Detection time window	δt	1 ns
Secrecy failure probability	ε_{sec}	10^{-9}
Correctness failure probability	ε_{cor}	10^{-15}

Table 6.1: Fixed QKD system parameters for both protocols, the non-decoy SPS and the 2-decoy WCP. The intrinsic error and the source repetition rate are set conservatively compared to other QKD demonstrations.

generate an optimized secure key length (SKL) by finding the optimal p_X, δt and the pre-attenuation of Alice's source η_{att}. For both protocols, 2-decoy WCP and non-decoy SPS, the number of sent pulses N_{S} is determined by the source repetition rate which is set to 100 MHz. To perform a fair comparison, we consider a detection time window $\Delta t = 1$ ns for all wavelengths and both QKD protocols. We also consider a fixed e_{int}, which is the intrinsic quantum bit error rate (QBER) and combines errors arising from source quality, receiver measurement fidelity, basis misalignment, and polarisation fluctuations. Baseline QKD system parameters are summarised in Table 6.1.

The optimization works as follows: first, the satellite altitude h and the maximum elevation angle of the overpass $\theta_{\text{elev}}^{\max}$ are fixed. Thus, we obtain a fixed total transmission time for the single overpass and an associated link efficiency for each time slot. Then, the optimization of the SKL over the protocol parameters, $\{p_X, \mu_1, \mu_2, p_{\mu_1}, p_{\mu_2}\}$ for the 2-decoy WCP with a vacuum decoy state ($\mu_0 = 0$) and $\{p_X, \eta_{\text{att}}\}$ for the non-decoy SPS, is run for each possible time windows, from $-\delta t$ to $+\delta t$ (the time of the whole overpass is the maximum window), to find the one resulting in the highest SKL. This δt optimization is done because when the QBER is extremely high at lower elevation angles taking a shorter finite block than the whole pass gives us greater SKL.

6.3 Annual Secure Key Length Estimation

The expected annual secure key length is defined as the generated key during a whole Earth's rotation around the sun equivalent to $t_{\text{ER}} \approx 31558140$ s and here we use the estimation method of [97]. For a given satellite altitude (that we set at 500 km) we

estimate the maximum SKL for each non-zenith overpass (maximum elevation angle $\theta_{\text{elev}}^{\max} < 90°$). The maximum elevation angle of the pass can be expressed as the ground track offset d, i.e., the distance from the ground station to where the satellite ground track crosses the longitudinal circumference that goes through the station. Thus, we represent the SKL vs. d for single passes, and we integrate the area below each curve as

$$\text{SKL}_{\text{int}}^{\text{Day(Night)}} = 2 \int_0^{d_{\max}} \text{SKL}_d^{\text{Day(Night)}} \, \text{d}d \tag{6.20}$$

where $\text{SKL}_d^{\text{Day(Night)}}$ is the SKL per pass as a function of the ground tack offset $d(\theta_{\text{elev}}^{\max})$, and $d_{\max}$ is the maximum tolerable ground track offset [97]. This integral represents the area below the secure key curve in bits-meter (bm) units. The factor 2 comes from the fact that we have negative values for the ground track offset that generates the same key as the positive d. Thus, since we do not model the orbits over time, we estimate the average SKL of a single orbit by dividing this area by the line of longitude of the station latitude L_{lat}.

Assuming a satellite in a sun-synchronous orbit and neglecting weather, we estimate the annual secure key using blocks formed by single passes during either daylight or night as

$$\overline{\text{SKL}}_{\text{annual}}^{\text{Day(Night)}} = \frac{N_{\text{orbits}}^{\text{annual}}}{L_{\text{lat}}} \text{SKL}_{\text{int}}^{\text{Day(Night)}}. \tag{6.21}$$

If the ground station latitude is close to the poles the previous approximation to estimate the annual SKL is not valid [179]. In this work, we consider the location of the station at the equator. This corresponds to the longitudinal circumference of the station latitude $L_{\text{lat}} \approx 4.008 \times 10^7$ m, modeling the Earth as a world geodetic system (WGS) 84 ellipsoid. Lastly, the total number of orbits during the earth's rotation around the sun is $N_{\text{orbits}}^{\text{annual}} = t_{\text{ER}}/T_{\text{S}} \approx 5567$ [1]. In one orbit, the satellite crosses the line of latitude of the ground station twice, once during daylight and once during the night. Therefore, to calculate the total annual secure key we add together the SKL

[1] For simplicity in our notation we use the word annual, we refer to the time earth takes to do a whole rotation around the sun, not to the 365 days approximation

during daylight and night

$$\overline{\mathrm{SKL}}_{\mathrm{annual}} = \overline{\mathrm{SKL}}^{\mathrm{Day}}_{\mathrm{annual}} + \overline{\mathrm{SKL}}^{\mathrm{Night}}_{\mathrm{annual}}. \tag{6.22}$$

6.4 Secure Key Performance: Non-Decoy Single-Photon Source and 2-Decoy Weak Coherent Pulse

Here are presented the key generation results for the 2-decoy WCP of Section 3.6.2.1 and the non-decoy SPS of Section 4.4.2.1 but now they are implemented within SatQuMa, which simulates satellite-to-ground QKD communication. We examine the secure key length generation for a satellite within a range of altitudes and non-zenith passes (varying the maximum elevation angle) for both daylight and night operation. Note that for nighttime we do not consider any background light, hence $p_{\mathrm{BG}} = 0$ and the extraneous counts are caused exclusively by detector dark counts. Furthermore, we neglect weather conditions in our model.

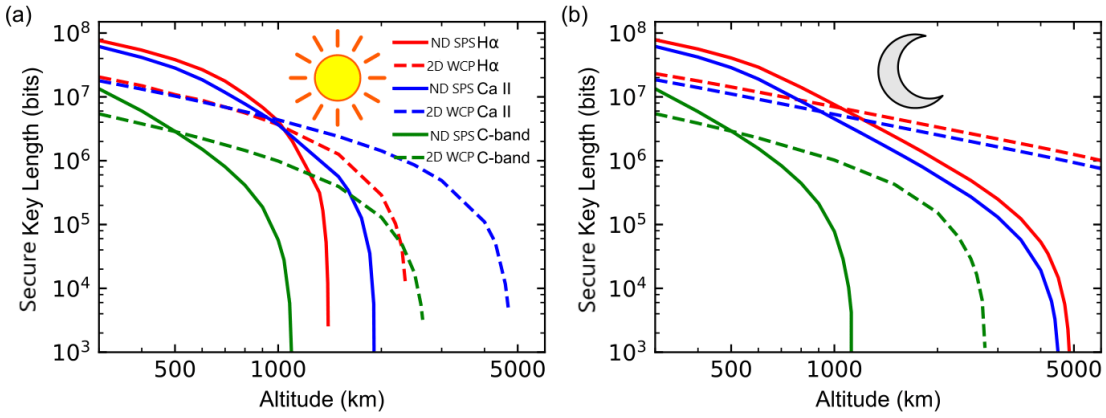

Figure 6.4: The secure finite key length (bits) as a function of the satellite altitude considering a zenith pass for our non-decoy single-photon source (ND SPS) protocol (solid lines) and the 2-decoy weak coherent pulses (2D WCP) protocol (dashed lines), emitting at Hα (656.448 nm), Ca II (854.445 nm), and C-band (1550.027 nm) (a) in daylight and (b) at night.

Figure 6.4 illustrates the secure key length (SKL) versus the satellite altitude ex-

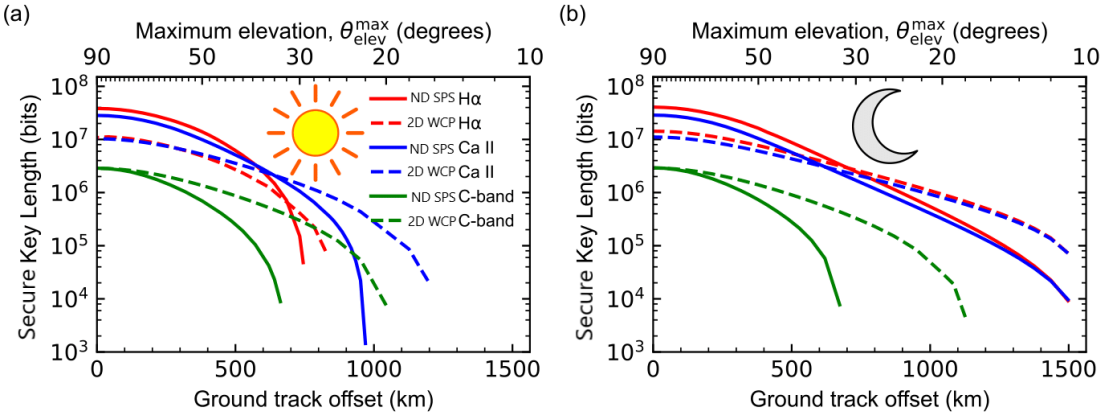

Figure 6.5: The secure finite key length (bits) as a function of the ground track offset of Eq. (6.5) (maximum elevation, $\theta_{\text{elev}}^{\text{max}}$) for our non-decoy single-photon source (ND SPS) protocol (solid lines) and the 2-decoy weak coherent pulse (2D WCP) protocol (dashed lines), emitting at Hα (656.448 nm), Ca II (854.445 nm), and C-band (1550.027 nm) (a) in daylight and (b) at night.

clusively considering zenith passes, i.e. when the maximum elevation angle $\theta_{\text{elev}}^{\text{max}} = 90°$, for our non-decoy SPS and the 2-decoy WCP emitting at Hα, Ca II, and C-band wavelengths, both during the daylight and night communication. During daytime operations, Figure 6.4 (a), it is evident that Hα and Ca II Fraunhofer lines supersede the telecom C-band in key performance for altitudes smaller than 1240 km. Notably, our non-decoy SPS surpasses the 2-decoy WCP up to an altitude of 1000 km for both Hα and Ca II lines. If we consider the C-band, our non-decoy SPS performs better than the 2-decoy WCP up to 500 km altitude. This pattern is also observed during nighttime operations, since the counts due to background light at the C-band are extremely low, see Figure 6.3. However, at overly high altitudes, the 2-decoy WCP surpasses our non-decoy SPS for both day and night. Moreover, in daylight, there is an advantage of the 2-decoy WCP C-band for altitudes higher than 1240 km for non-decoy SPS Hα, 1500 km for non-decoy SPS Ca II, and 2000 km for 2-decoy WCP Hα. The improvement of the C-band in these regions during daylight occurs because it has the lowest background probability, see Figure 6.3, e.g. $p_{\text{BG}}^{\text{C-band}} \approx 3.52 \times 10^{-6}$ at zenith, amongst the three wavelengths for 1 ns of detection time, e.g. $p_{\text{BG}}^{\text{H}\alpha} \approx 1.77 \times 10^{-4}$ and $p_{\text{BG}}^{\text{CaII}} \approx 4.29 \times 10^{-5}$

Protocol - Wavelength	$\eta_{\text{loss}}^{\text{sys}}$ **(dB)**	$\overline{\text{SKL}}_{\text{annual}}^{\text{Day}}$ **(Gb)**	$\overline{\text{SKL}}_{\text{annual}}^{\text{Night}}$ **(Gb)**	$\overline{\text{SKL}}_{\text{annual}}^{\text{equator}}$ **(Gb)**
ND SPS - Hα	17.55	3.4829	4.0934	7.5763
2D WCP - Hα	17.55	1.1411	1.8912	3.0323
ND SPS - Ca II	18.60	2.6308	2.7958	5.4266
2D WCP - Ca II	18.60	1.2383	1.4972	2.7355
ND SPS - C-band	23.31	0.2215	0.2278	0.4493
2D WCP - C-band	23.31	0.3204	0.3308	0.6512

Table 6.2: Expected annual secure key length with the ground station at the equator, i.e. $\overline{\text{SKL}}_{\text{annual}}^{\text{equator}} = 13.89 \times 10^{-4} \left(\overline{\text{SKL}}_{\text{annual}}^{\text{Day}} + \overline{\text{SKL}}_{\text{annual}}^{\text{Night}} \right)$ for the non-decoy (ND) SPS and the 2-decoy (2D) WCP protocol operating at each wavelength during daylight and night time operation.

at the zenith. This together with the 2-decoy method makes C-band tolerate higher altitudes in daylight communication. Similarly, at night, Figure 6.4 (b), our non-decoy SPS with either Hα or Ca II achieves better results compared to the 2-decoy WCP with the same wavelengths for up to 1000 km. The maximum altitude to have an operational quantum channel for an SPS is beyond 4000 km. However, for long distances, 2-decoy WCP becomes extremely more efficient during the night.

Most satellite overpasses will not cross over the zenith of the ground station. To extract the maximum amount of secure key for each overpass, the QKD system needs to operate even at low maximum elevation angles $\theta_{\text{elev}}^{\max}$, although we impose a minimum elevation angle $\theta_{\text{elev}}^{\min} = 10^\circ$ (ground track offset $d_{\min} \approx 1563$ km) for transmission. To evaluate all possible non-zenith passes, we represent the SKL vs the ground track offset and the maximum elevation angle of the overpass, see Figure 6.5. As expected, when $\theta_{\text{elev}}^{\max}$ decreases the extracted key is reduced. During the night, Figure 6.5 (b), the 2-decoy WCP for C-band does not show any improvement over its non-decoy SPS version. During daylight operation, Figure 6.5 (a), our non-decoy SPS emitting at Hα line outperforms all other alternatives up to a 600 km ground track offset ($\theta_{\text{elev}}^{\max} > 40^\circ$). This superior key performance extends up to about 800 km during nighttime operations. Furthermore, during daylight, even though the 2-decoy WCP C-band tolerates lower $\theta_{\text{elev}}^{\max}$ angles than others, non-decoy SPS Hα and Ca II continue to outperform the 2-decoy WCP C-band up to 750 km and 950 km ground track offset, respectively. This SPS advantage is clearly displayed when we estimate the key length volume over a year.

Table 6.2 presents $\overline{\text{SKL}}_{\text{annual}}^{\text{equator}}$, the expected annual secure key length, using Eqs.

Protocol - Wavelength	$\eta_{\text{loss}}^{\text{sys}}$ **(dB)**	$\text{SKL}_{\text{int}}^{\text{Day}}$ **(bm)**	$\text{SKL}_{\text{int}}^{\text{Night}}$ **(bm)**
ND SPS - Hα	17.55	2.51×10^{13}	2.94×10^{13}
2D WCP - Hα	17.55	8.21×10^{12}	1.36×10^{13}
ND SPS - Ca II	18.60	1.89×10^{13}	2.01×10^{13}
2D WCP - Ca II	18.60	8.91×10^{12}	1.08×10^{13}
ND SPS - C-band	23.31	1.59×10^{12}	1.64×10^{12}
2D WCP - C-band	23.31	2.31×10^{12}	2.38×10^{12}

Table 6.3: Integral of the secure key length curve in bits-meter unit for 500 km of satellite altitude for each protocol and wavelength during daylight and night time operation.

(6.21) and (6.22), for the proposed wavelengths and sources during daylight and nighttime operation assuming the ground station at the equator. We associate each wavelength with a system loss metric $\eta_{\text{sys}}^{\text{loss}}$, defined as the total dB loss of the quantum link at the zenith. To obtain those SKLs we integrate the SKL in Figure 6.5 using Eq. (6.20). The corresponding outcomes in bits-meter unit are given in Table 6.3. Operating a 2-decoy WCP at night, Hα shows higher annual SKL than Ca II and C-band, while during daylight Ca II outperforms the other two operating wavelengths. Considering our non-decoy SPS, the Hα line is superior to the other two candidates during daylight and nighttime operations. Overall, we estimate that our non-decoy SPS Hα generates the highest SKL of 7.5763 Gb per year among all the combinations of protocols and wavelengths.

In general, the Hα line has the lowest system loss metric amongst all wavelengths, and total link losses for a zenith pass as shown in Figure 6.2, while C-band clearly starts with a considerable disadvantage compared to the visible and infrared candidates, see the $\eta_{\text{sys}}^{\text{loss}}$ in Table 6.2 or Figure 6.2. This gap of approximately 6 and 5 dB loss in relation to Hα and Ca II, respectively, is mainly due to a higher diffraction loss of the C-band, again shown in Figure 6.2, since longer wavelengths experience higher beam broadening and consequently the transmission efficiency through the ground station telescope is lower. Albeit the channel loss difference between these wavelengths decreases during the satellite zenith pass depicted in Figure 6.2, the secure key length for the C-band does not exceed the other wavelengths in most scenarios.

Even if the channel loss assumptions made in this study might seem idealistic when contrasted with the Micius satellite implementation, they remain within the realm

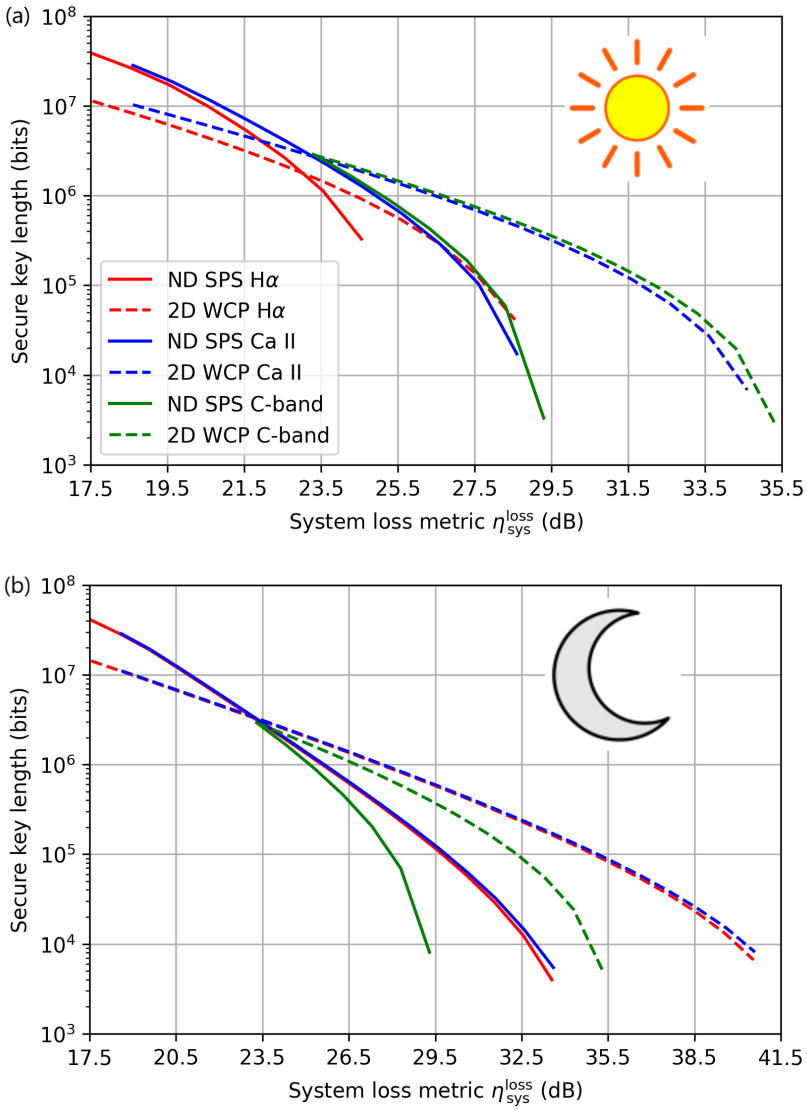

Figure 6.6: The secure finite key length (bits) as a function of the system loss metric for our non-decoy single-photon source, denoted by SPS, and the 2-decoy WCP, denoted by two-decoy source (TDS), emitting at Hα (656.448 nm), Ca II (854.445 nm), and C-band (1550.027 nm) (a) in daylight and (b) at night. Note that every wavelength starts at the dB of the system loss metric shown in Table 6.2 and we compute steps of 1 dB.

of feasibility given the constant advancement in satellite communication technologies, targeting lower losses. However, we also explore scenarios with higher losses (system loss metric) to determine which combination of source, protocol and wavelength is more resistant. Figure 6.6, illustrates the secure key length as a function of the system loss metric $\eta_{\text{sys}}^{\text{loss}}$, which we employ as the most representative loss of the entire zenith pass. If $\eta_{\text{sys}}^{\text{loss}}$ increases, we see that the most resilient wavelengths are Ca II and C-band for daylight, and Hα and again Ca II for nighttime operation. In particular, both of these pairs of optimal wavelengths, either at night or in daylight, practically tolerate the same range of system loss. As expected, when $\eta_{\text{sys}}^{\text{loss}}$ is higher than the system loss metric of C-band (23.31 dB), the non-decoy SPS protocol loses its advantage over the 2-decoy WCP for the Fraunhofer lines. Additionally, if a real-life implementation of the QKD system for any of these wavelengths experiences greater losses than those predicted by our theoretical model, the aperture of the telescope can be increased to reduce the system loss metric and ensure that it continues operating within the favourable regime for the non-decoy SPS protocol, below 23.31 dB.

Chapter 7

Conclusion

In the non-decoy SPS protocol, we have drastically reduced the required size of the block to generate high keys that approach the asymptotic limit, thereby increasing the maximum tolerable loss of the system. These results were primarily achieved by introducing tighter bounds to account for the statistical fluctuations due to finite key effects. This approach also allows us to extend the range of tolerable channel losses by introducing a pre-attenuation on Alice's source, overcoming the limitations of previous non-decoy analyses where loose bounds prevented pre-attenuation from enhancing the maximum tolerable loss. For our non-decoy SPS, successfully generate non-zero keys over 175 km of fibre using an actual quantum dot source for a block of 10^7 received signals. In contrast, using the previous non-decoy analysis found in the literature, non-zero key generation is only achievable up to a maximum distance of 25 km for the same block size, due to its loose deviations applied to the expected probabilities and rates in the finite-key analysis.

Thus, we demonstrate that SPSs with sufficiently high brightness and low second-order correlation function can serve as a viable alternative source for short-range QKD networks operating at short acquisition times. These results encourage experimentalists to implement practical SPSs in a BB84 protocol, avoiding the experimental complexity of building decoy states. Additionally, we show that an extra decoy vacuum state is not beneficial for the non-decoy SPS. Ultimately, we provide an easy-to-compute model for experimentalists, enabling them to estimate the key generation rates of their

practical SPSs with minimal effort, requiring only the characterization of the time-zero second-order correlation function, which is typically performed, and the mean photon number.

However, as expected, we demonstrate that 2-decoy WCP is superior to non-decoy SPS in most scenarios, particularly where small block sizes and the low-loss regime are avoided. In response, we present two novel and adapted decoy methods for practical SPSs, inspired by the traditional 1-decoy and 2-decoy models with WCPs. These methods retain the simplicity of partially characterizing the SPS distribution using two measurable quantities, once again providing a model that can be straightforwardly computed. We demonstrate an SPS with a mean photon number $\langle n \rangle \geq 0.2$ enhances key generation over the decoy WCP with optimised intensity levels, specifically in the high-loss regime. Therefore, we conclude that, since practical SPSs have already achieved a sufficiently low $g^{(2)}(0)$, further efforts to optimize SPSs in order to surpass WCPs in QKD should focus on increasing their mean photon number rather than further reducing $g^{(2)}(0)$.

In the diagram shown in Figure 7.1, we synthesise the analysis regarding the parameter regimes in which SPSs outperform WCPs for the implementation of BB84 QKD. This comparison was discussed in detail in Sections 4.5.2 and 5.6.2. The optimal choice of source depends on the parameters defining the QKD scenario, including the source repetition rate, channel loss, and the mean photon number (intensity) of the emitted states.

Our results indicate that the principal advantage of SPSs in terms of secret key generation arises when they operate at a mean photon number $\langle n \rangle \geq 0.2$. In this regime, SPSs can achieve higher key rates than WCPs. For lower mean photon numbers, however, the performance gap narrows substantially, and any advantage of SPSs is restricted to small block sizes and low-loss channels. Moreover, within the decoy protocol for a SPS with $\langle n \rangle \geq 0.2$, the key rate enhancement of SPSs over WCPs becomes more pronounced as the block size decreases.

Therefore, our results suggest that the shorter the finite block, the better the SPS protocols handle the statistical fluctuations of observed values while exhibiting a greater

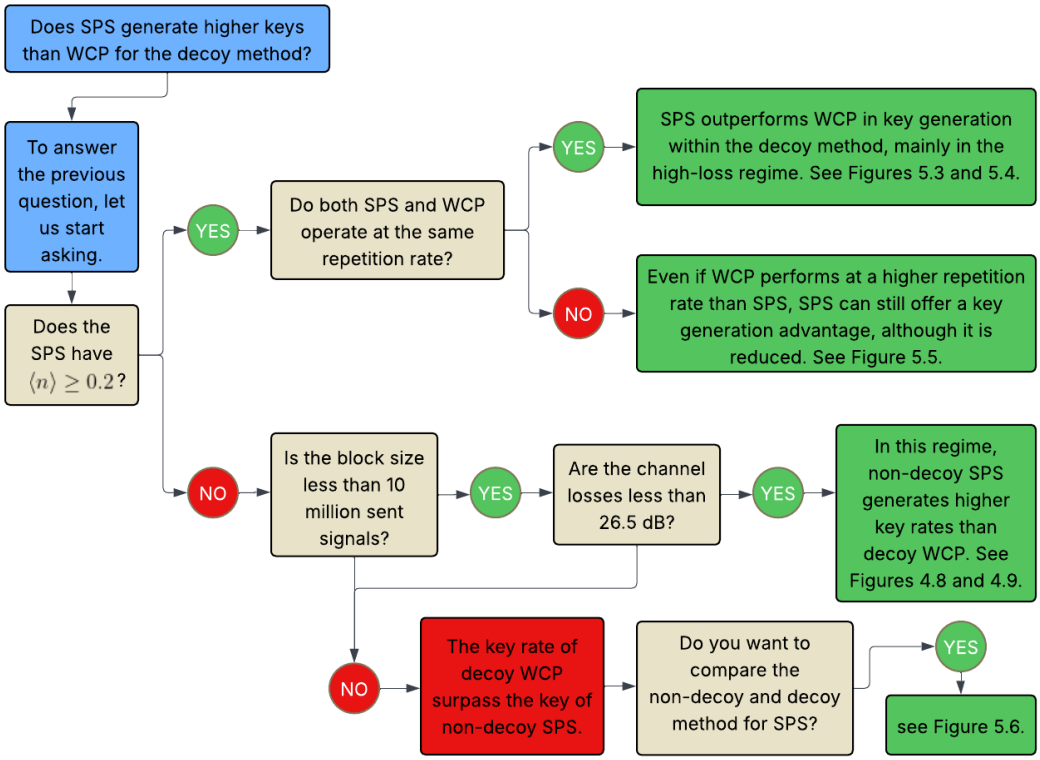

Figure 7.1: Summary of the optimal QKD protocol selection between SPSs and WCPs depending on different parameter scenarios.

capacity than WCPs to reduce multiphoton emissions. However, note that the assumptions made in the SPS distribution for our decoy methods are not present in decoy WCP. Although we relax the required conditions on the photon emission probabilities compared to previous decoy studies with arbitrary distributions, further research is needed to relax these assumptions even more. This could be achieved by developing a more comprehensive method to characterise and handle the photon emissions of the SPS in the estimation of vacuum and single-photon detection events.

Regarding the second-order correlation function for SPS applied to QKD. An extremely low $g^{(2)}(0)$ is advantageous for non-decoy SPS protocol, even though the pre-attenuation of the source consistently extends the range of tolerable losses. However, in decoy SPS protocols, since the multiphoton contribution is already bounded by the decoy method, which provides a tighter estimate of the secure events than the non-decoy

SPS, decreasing $g^{(2)}(0)$ does not yield significant improvement. In fact, the decoy state is already extremely attenuated for block sizes below one hour of acquisition time.

Finally, we demonstrate that practical SPSs could also offer an advantage in free-space QKD, particularly in downlink satellite communication. Our collaborators identified two favourable wavelengths, the Hα and Ca II Fraunhofer lines, for daylight operation, and we evaluated them together with the telecom C-band for satellite QKD in the finite-key analysis. Our channel model for each wavelength shows lower losses for the Hα and Ca II lines than for the C-band. This model does not consider any internal losses on the receiver side, which could be mitigated by implementing adaptive optics and further technological improvements. Notably, we show the greatest annual volume of key generation for the Hα line using our non-decoy SPS, surpassing the 2-decoy WCP protocol. This result is relevant as it demonstrates how alternative quantum sources and wavelengths can outperform WCPs and C-band in free-space QKD. Moreover, our analysis contributes significantly to the ongoing discussion on optimising the key generation for upcoming satellite missions that aim to employ an SPS.

However, to conduct a fair comparison with decoy WCP in our satellite-to-ground QKD simulation model, it is necessary to introduce the decoy SPS protocols presented in this work. Based on our results in fibre, one may certainly expect that decoy SPS would offer better key rate performance than non-decoy SPS, and potentially surpass the 2-decoy WCP for a broader range of non-zenith passes and satellite altitudes. Additionally, it is important to note that overall cloud cover notably reduces visibility, which is essential for effective QKD operations, a factor that varies considerably across different geographical locations, seasons, and specific weather conditions. Incorporating weather conditions into our model would be a clear progress towards simulating and analysing key performances that are feasible to reproduce in real-life QKD implementation.

Appendix A

Additional Lower bounds on the Single-Photon Events

Here, I reproduce the lower bound on the number of single-photon events for the decoy papers that used arbitrary photon statistics using our notation. For Wang's and Folletos's papers [136,138,139], the signal and one decoy state are used to derive the lower bound of $s_{X,1}$. Expressing Eq. (5.18) in terms of the number of events by multiplying by the basis bias squared p_X^2 and the sent signals N_{S}, we obtain

$$\begin{aligned} N_{X,\delta^{(1)}} &= \frac{p_{\delta^{(1)}}}{P_0} P_0^{(1)} s_{X,0} + \frac{p_{\delta^{(1)}}}{P_1} P_1^{(1)} s_{X,1} + \sum_{n=2}^{\infty} \frac{p_{\delta^{(1)}}}{P_n} P_n^{(1)} s_{X,n} \\ &= \frac{p_{\delta^{(1)}}}{P_0} P_0^{(1)} s_{X,0} + \frac{p_{\delta^{(1)}}}{P_1} P_1^{(1)} s_{X,1} + \frac{p_{\delta^{(1)}}}{p_{\delta^{(2)}}} \frac{P_2^{(1)}}{P_2^{(2)}} \lambda_{\mathrm{mp}} + \Delta_{\mathrm{mp}} \end{aligned} \tag{A.1}$$

where the terms related to multiphotons are

$$\lambda_{\mathrm{mp}} = \sum_{n=2}^{\infty} \frac{p_{\delta^{(2)}}}{P_n} P_n^{(2)} s_{X,n} \tag{A.2}$$

and

$$\Delta_{\mathrm{mp}} = \sum_{n=2}^{\infty} \frac{p_{\delta^{(1)}}}{P_n} P_n^{(1)} s_{X,n} - \frac{p_{\delta^{(1)}}}{p_{\delta^{(2)}}} \frac{P_2^{(1)}}{P_2^{(2)}} \lambda_{\mathrm{mp}}. \tag{A.3}$$

Similarly, expressing Eq. (5.19) in terms of the number of detection events, we obtain

$$N_{X,\delta^{(2)}} = \frac{p_{\delta^{(2)}}}{P_0} P_0^{(2)} s_{X,0} + \frac{p_{\delta^{(2)}}}{P_1} P_1^{(2)} s_{X,1} + \lambda_{\mathrm{mp}}. \tag{A.4}$$

Hence, this multiphoton term can be expressed as

$$\lambda_{\mathrm{mp}} = N_{X,\delta^{(2)}} - \frac{p_{\delta^{(2)}}}{P_0} P_0^{(2)} s_{X,0} - \frac{p_{\delta^{(2)}}}{P_1} P_1^{(2)} s_{X,1}. \tag{A.5}$$

Replacing it in Eq. (A.1) and solving for the single-photon events

$$\begin{aligned} s_{X,1} = & \frac{P_1}{P_2^{(2)} P_1^{(1)} - P_2^{(1)} P_1^{(2)}} \left[P_2^{(2)} \frac{N_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - P_2^{(1)} \frac{N_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} \right. \\ & \left. + \left(P_2^{(2)} P_0^{(1)} - P_2^{(1)} P_0^{(2)} \right) \frac{s_{X,0}}{P_0} + P_2^{(2)} \Delta_{\mathrm{mp}} \right]. \end{aligned} \tag{A.6}$$

These multiphoton terms may be confusing to understand the lower bound derivation. Therefore, to make it clearer, we can expressed Δ_{mp} as

$$\Delta_{\mathrm{mp}} = p_{\delta^{(1)}} \sum_{n=2} \left(P_n^{(1)} - \frac{P_2^{(1)}}{P_2^{(2)}} P_n^{(2)} \right) \frac{s_{X,n}}{P_n} \tag{A.7}$$

To derive the lower bound, we need to impose $\Delta \geq 0$, which implies the following inequality

$$P_2^{(1)} P_n^{(2)} \leq P_2^{(2)} P_n^{(1)} \quad \text{for } n \geq 2 \tag{A.8}$$

and the denominator must fulfilled

$$P_2^{(2)} P_1^{(1)} > P_2^{(1)} P_1^{(2)}. \tag{A.9}$$

Thus, the lower bound of the single-photon events is given by

$$\begin{aligned} s_{X,1} > & \frac{P_1}{P_2^{(2)} P_1^{(1)} - P_2^{(1)} P_1^{(2)}} \left[P_2^{(2)} \frac{N_{X,\delta^{(1)}}}{p_{\delta^{(1)}}} - P_2^{(1)} \frac{N_{X,\delta^{(2)}}}{p_{\delta^{(2)}}} \right. \\ & \left. + \left(P_2^{(2)} P_0^{(1)} - P_2^{(1)} P_0^{(2)} \right) \frac{s_{X,0}}{P_0} \right] \end{aligned} . \tag{A.10}$$

However, one can derive the same lower bound with less complex mathematical artifices first using Eqs. (5.18) and (5.19) and solving for $P_{c\,|\,1}$

$$P_{c\,|\,1} = \frac{1}{P_2^{(1)}P_1^{(2)} - P_2^{(2)}P_1^{(1)}}\Bigg[P_2^{(2)}P_{c\,|\,\delta^{(1)}} - P_2^{(1)}P_{c\,|\,\delta^{(2)}} + \left(P_2^{(2)}P_0^{(1)} - P_2^{(1)}P_0^{(2)}\right)P_{c\,|\,0} + \sum_{n=3}^{\infty}\left(P_2^{(2)}P_n^{(1)} - P_2^{(1)}P_n^{(2)}\right)P_{c\,|\,n}\Bigg], \tag{A.11}$$

and then applying the same conditions of eq (A.9) and a relaxed version of Eq. (A.8) for $n \geq 3$ instead of $n \geq 2$ to Eq. (A.11) and writing it in terms of the number of events, we obtain the same lower bound as Eq. (A.10).

Bibliography

[1] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, "Satellite quantum modelling & analysis software version 1.1: Documentation," *arXiv preprint arXiv:2109.01686*, 2021.

[2] A. Salomaa, "Public-key cryptography," 2013.

[3] E. Milanov, "The RSA algorithm," *RSA laboratories*, pp. 1–11, 2009.

[4] W. P. Wardlaw, "The RSA public key cryptosystem," in *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, pp. 101–123, Springer, 2000.

[5] R. P. Feynman, "Quantum mechanical computers," *Found. Phys.*, vol. 16, no. 6, pp. 507–532, 1986.

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

[7] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Reviews of Modern Physics*, vol. 68, no. 3, p. 733, 1996.

[8] I. L. Markov, A. Fatima, S. V. Isakov, and S. Boixo, "Quantum supremacy is both closer and farther than it appears," *arXiv preprint arXiv:1807.10749*, 2018.

[9] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[10] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[11] M. Kumar and P. Pattnaik, "Post quantum cryptography (PQC) - an overview," in *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–9, IEEE, 2020.

[12] C. Portmann and R. Renner, "Security in quantum cryptography," *Reviews of Modern Physics*, vol. 94, no. 2, p. 025008, 2022.

[13] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[14] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, pp. 7–11, 2014.

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[16] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum cryptography," *Scientific American*, vol. 267, no. 4, pp. 50–57, 1992.

[17] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," *Communications of the ACM*, vol. 62, no. 4, pp. 133–133, 2019.

[18] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[19] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, *et al.*, "Experimental measurement-device-independent quantum key distribution," *Physical review letters*, vol. 111, no. 13, p. 130502, 2013.

[20] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.

[21] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.

[22] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[23] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM (JACM)*, vol. 48, no. 3, pp. 351–406, 2001.

[24] U. Maurer, "Information-theoretic cryptography," in *Annual International Cryptology Conference*, pp. 47–65, Springer, 1999.

[25] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," *Quantum*, vol. 1, p. 14, 2017.

[26] W. K. Wootters and W. H. Zurek, "The no-cloning theorem," *Physics Today*, vol. 62, no. 2, pp. 76–77, 2009.

[27] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 72, no. 1, p. 012332, 2005.

[28] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, p. 1301, 2009.

[29] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," in *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, pp. 1–7, IEEE, 2017.

[30] H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution," *Physical Review A*, vol. 94, no. 1, p. 012325, 2016.

[31] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, *et al.*, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, no. 3, pp. 366–387, 2016.

[32] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical review letters*, vol. 85, no. 6, p. 1330, 2000.

[33] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, no. 5, p. 052304, 2000.

[34] H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, *et al.*, "Towards optimal single-photon sources from polarized microcavities," *Nature Photonics*, vol. 13, no. 11, pp. 770–775, 2019.

[35] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, 2003.

[36] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, "Security analysis of decoy state quantum key distribution incorporating finite statistics," *arXiv preprint arXiv:0707.3541*, 2007.

[37] R. Y. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.

[38] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, 2005.

[39] T. Vogl, Y. Lu, and P. K. Lam, "Room temperature single photon source using fiber-integrated hexagonal boron nitride," *Journal of Physics D: Applied Physics*, vol. 50, no. 29, p. 295101, 2017.

[40] C. L. Morrison, M. Rambach, Z. X. Koong, F. Graffitti, F. Thorburn, *et al.*, "A bright source of telecom single photons based on quantum frequency conversion," *Applied Physics Letters*, vol. 118, no. 17, 2021.

[41] S. Thomas, M. Billard, N. Coste, S. Wein, H. Ollivier, *et al.*, "Bright polarized single-photon source based on a linear dipole," *Physical review letters*, vol. 126, no. 23, p. 233601, 2021.

[42] C. L. Morrison, R. G. Pousa, F. Graffitti, Z. X. Koong, P. Barrow, *et al.*, "Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates," *Nature Communications*, vol. 14, no. 1, p. 3573, 2023.

[43] M. Toyoshima, Y. Shoji, C. Schaefer, Y. Takayama, H. Kunimori, *et al.*, "Comparison of free-space and fiber-based transmission systems in quantum cryptography," *Transactions of the japan society for aeronautical and space sciences, space technology japan*, vol. 7, no. ists26, pp. Pj_7–Pj_12, 2009.

[44] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," *Cambridge University Press*, 2000.

[45] M. M. Wilde, "Quantum information theory," *Cambridge University Press*, 2017.

[46] R. Wolf, "Quantum key distribution," *Lecture notes in physics*, vol. 988, 2021.

[47] F. Grasselli, "Quantum cryptography," *Quantum science and technology. Cham: Springer*, 2021.

[48] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, "Chain rules for smooth min- and max-entropies," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2603–2612, 2013.

[49] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[50] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018.

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

[52] S.-W. Ho and R. W. Yeung, "On the relation between the Shannon entropy and the von Neumann entropy," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, p. 42, IEEE, 2004.

[53] D. Partridge, "Information theory and redundancy," *Philosophy of Science*, vol. 48, no. 2, pp. 308–316, 1981.

[54] J. Von Neumann, *Mathematical foundations of quantum mechanics: New edition*, vol. 53. Princeton university press, 2018.

[55] N. J. Cerf and C. Adami, "Quantum extension of conditional probability," *Physical Review A*, vol. 60, no. 2, p. 893, 1999.

[56] R. Renner and S. Wolf, "Smooth Rényi entropy and applications," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, p. 233, IEEE, 2004.

[57] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography Conference*, pp. 407–425, Springer, 2005.

[58] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Transactions on Information theory*, vol. 55, no. 9, pp. 4337–4347, 2009.

[59] N. Datta, "Min- and max-relative entropies and a new entanglement monotone," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2816–2826, 2009.

[60] J. Ribeiro, G. Murta, and S. Wehner, "Fully device-independent conference key agreement," *Physical Review A*, vol. 97, no. 2, p. 022307, 2018.

[61] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Physical Review A*, vol. 54, no. 4, p. 2629, 1996.

[62] D. A. Lelewer and D. S. Hirschberg, "Data compression," *ACM Computing Surveys (CSUR)*, vol. 19, no. 3, pp. 261–296, 1987.

[63] M. Wilde, *Quantum information theory*. Cambridge university press, 2013.

[64] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A*, vol. 56, no. 1, p. 131, 1997.

[65] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 269–273, 1998.

[66] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels. I," *Information and Control*, vol. 10, no. 1, pp. 65–103, 1967.

[67] L. J. Schulman, "Communication on noisy channels: A coding theorem for computation," in *FOCS*, pp. 724–733, 1992.

[68] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, "Classical capacity of a noiseless quantum channel assisted by noisy entanglement," *arXiv preprint quant-ph/0106080*, 2001.

[69] B. Schumacher and M. D. Westmoreland, "Quantum mutual information and the one-time pad," *Physical Review A*, vol. 74, no. 4, p. 042305, 2006.

[70] A. S. Holevo, "Information capacity of a quantum observable," *Problems of Information Transmission*, vol. 48, no. 1, pp. 1–10, 2012.

[71] I. Devetak and A. Winter, "Classical data compression with quantum side information," *Physical Review A*, vol. 68, no. 4, p. 042301, 2003.

[72] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *problems of information transmission*, vol. 40, no. 4, pp. 318–336, 2004.

[73] D. Kahn, *The Story of Secret Writing*. Weidenfeld & Nicolson, 1968.

[74] M. E. Hellman, "An overview of public key cryptography," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 42–49, 2002.

[75] J. Grollmann and A. L. Selman, "Complexity measures for public-key cryptosystems," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 309–335, 1988.

[76] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[77] R. Lanjewar and G. Pande, "Implementation of AES-256 Bit: A Review," *Inventi Rapid: Information Security*, 2015.

[78] A. E. Omolara, A. Jantan, O. I. Abiodun, and H. Arshad, "An enhanced practical difficulty of one-time pad algorithm resolving the key management and distribution problem," in *proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, 2018.

[79] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *Journal of the AIEE*, vol. 45, no. 2, pp. 109–115, 1926.

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

[81] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," *Theoretical Computer Science*, vol. 560, pp. 27–32, 2014.

[82] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," *arXiv preprint arXiv:1409.3525*, 2014.

[83] U. Maurer, "Constructive cryptography–a new paradigm for security definitions and proofs," in *Joint Workshop on Theory of Security and Applications*, pp. 33–56, Springer, 2011.

[84] D. Aharonov, M. Ben-Or, and E. Eban, "Proceedings of innovations in computer science," 2010.

[85] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2*, pp. 386–406, Springer, 2005.

[86] T. Murayama, Y. Kabashima, D. Saad, and R. Vicente, "Statistical physics of regular low-density parity-check error-correcting codes," *Physical Review E*, vol. 62, no. 2, p. 1577, 2000.

[87] N. Agarwal, "Privacy amplification in quantum key distribution with machine learning," *channels*, vol. 2, p. 3, 2024.

[88] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2481–2485, 1999.

[89] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[90] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Info. Comput.*, vol. 4, no. 5, p. 325–360, 2004.

[91] V. B. Braginsky, Y. I. Vorontsov, and K. S. Thorne, "Quantum nondemolition measurements," *Science*, vol. 209, no. 4456, pp. 547–557, 1980.

[92] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[93] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, *et al.*, "Long-distance decoy-state quantum key distribution in optical fiber," *Physical review letters*, vol. 98, no. 1, p. 010503, 2007.

[94] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[95] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," *Applied Physics Letters*, vol. 112, no. 17, 2018.

[96] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Physical Review A*, vol. 89, no. 2, p. 022307, 2014.

[97] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, "Finite key effects in satellite quantum key distribution," *NPJ Quantum Inf.*, vol. 8, no. 1, p. 18, 2022.

[98] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[99] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, *et al.*, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature communications*, vol. 5, no. 1, p. 3732, 2014.

[100] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, *et al.*, "Tight security bounds for decoy-state quantum key distribution," *Sci. Rep.*, vol. 10, no. 1, p. 14312, 2020.

[101] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature communications*, vol. 3, no. 1, p. 634, 2012.

[102] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, "Fundamental finite key limits for one-way information reconciliation in quantum key distribution," *Quantum Information Processing*, vol. 16, no. 11, pp. 1–23, 2017.

[103] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr 2000.

[104] C.-Y. Lu and J.-W. Pan, "Quantum-dot single-photon sources for the quantum internet," *Nature Nanotechnology*, vol. 16, no. 12, pp. 1294–1296, 2021.

[105] R. Uppu, F. T. Pedersen, Y. Wang, C. T. Olesen, C. Papon, *et al.*, "Scalable integrated single-photon source," *Science advances*, vol. 6, no. 50, p. eabc8268, 2020.

[106] N. Ahmadi, S. Schwertfeger, P. Werner, L. Wiese, J. Lester, *et al.*, "QUICK3-design of a satellite-based quantum light source for quantum communication and extended physical theory tests in space," *Advanced Quantum Technologies*, p. 2300343.

[107] N. Tomm, A. Javadi, N. O. Antoniadis, D. Najer, M. C. Löbl, *et al.*, "A bright and fast source of coherent single photons," *Nature Nanotechnology*, vol. 16, pp. 399–403, Apr. 2021.

[108] H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, *et al.*, "Towards optimal single-photon sources from polarized microcavities," *Nature Photonics*, vol. 13, pp. 770–775, Nov. 2019.

[109] S. E. Thomas, M. Billard, N. Coste, S. C. Wein, Priya, *et al.*, "Bright polarized single-photon source based on a linear dipole," *Phys. Rev. Lett.*, vol. 126, p. 233601, Jun 2021.

[110] S. Strauf, N. G. Stoltz, M. T. Rakher, L. A. Coldren, P. M. Petroff, *et al.*, "High-frequency single-photon source with polarization control," *Nature Photonics*, vol. 1, pp. 704–708, Nov. 2007.

[111] C. L. Morrison, M. Rambach, Z. X. Koong, F. Graffitti, F. Thorburn, A. K. Kar, Y. Ma, S.-I. Park, J. D. Song, N. G. Stoltz, D. Bouwmeester, A. Fedrizzi, and B. D. Gerardot, "A bright source of telecom single photons based on quantum frequency conversion," *Applied Physics Letters*, vol. 118, no. 17, p. 174003, 2021.

[112] B. Da Lio, C. Faurby, X. Zhou, M. L. Chan, R. Uppu, H. Thyrrestrup, S. Scholz, A. D. Wieck, A. Ludwig, P. Lodahl, and L. Midolo, "A pure and indistinguishable single-photon source at telecommunication wavelength," *Advanced Quantum Technologies*, vol. 5, no. 5, p. 2200006, 2022.

[113] X. You, M.-Y. Zheng, S. Chen, R.-Z. Liu, J. Qin, *et al.*, "Quantum interference between independent solid-state single-photon sources separated by 300 km fiber," *arXiv:2106.15545*, 2021.

[114] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, pp. 133–165, 2005.

[115] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.

[116] R. G. Pousa, D. K. Oi, and J. Jeffers, "Comparison of non-decoy single-photon source and decoy weak coherent pulse in quantum key distribution," *arXiv preprint arXiv:2405.19963*, 2024.

[117] R. Alléaume, F. Treussart, J.-M. Courty, and J.-F. Roch, "Photon statistics characterization of a single-photon source," *New Journal of physics*, vol. 6, no. 1, p. 85, 2004.

[118] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-poisson light," *Physical Review A*, vol. 66, no. 4, p. 042315, 2002.

[119] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-poisson light," *Phys. Rev. A*, vol. 66, p. 042315, Oct 2002.

[120] D. Bunandar, L. C. Govia, H. Krovi, and D. Englund, "Numerical finite-key analysis of quantum key distribution," *npj Quantum Information*, vol. 6, no. 1, pp. 1–12, 2020.

[121] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, "Key generation analysis for satellite quantum key distribution," in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, vol. 11881, p. 1188106, SPIE, 2021.

[122] T. Brougham and D. Oi, "Medium-range terrestrial free-space QKD performance modelling and analysis," in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, vol. 11881, pp. 14–23, SPIE, 2021.

[123] T. Brougham and D. K. Oi, "Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD," *New Journal of Physics*, vol. 24, no. 7, p. 075002, 2022.

[124] T. Gao, L. Rickert, F. Urban, J. Große, N. Srocka, *et al.*, "A quantum key distribution testbed using a plug&play telecom-wavelength single-photon source," *Applied Physics Reviews*, vol. 9, no. 1, 2022.

[125] P. Chaiwongkhot, S. Hosseini, A. Ahmadi, B. L. Higgins, D. Dalacu, *et al.*, "Enhancing secure key rates of satellite QKD using a quantum dot single-photon source," 2020.

[126] R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics*, vol. 11, p. 045024, apr 2009.

[127] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Physical review letters*, vol. 106, no. 11, p. 110506, 2011.

[128] G. Vest, P. Freiwang, J. Luhn, T. Vogl, M. Rau, *et al.*, "Quantum key distribution with a hand-held sender unit," *Physical Review Applied*, vol. 18, no. 2, p. 024067, 2022.

[129] J. P. Schmidt, A. Siegel, and A. Srinivasan, "Chernoff–Hoeffding bounds for applications with limited independence," *SIAM Journal on Discrete Mathematics*, vol. 8, no. 2, pp. 223–250, 1995.

[130] B. Klar, "Bounds on tail probabilities of discrete distributions," *Probability in the Engineering and Informational Sciences*, vol. 14, no. 2, pp. 161–171, 2000.

[131] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Physical review letters*, vol. 100, no. 20, p. 200501, 2008.

[132] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[133] L. Schweickert, K. D. Jöns, K. D. Zeuner, S. F. Covre da Silva, H. Huang, *et al.*, "On-demand generation of background-free single photons from a solid-state source," *Applied Physics Letters*, vol. 112, no. 9, p. 093106, 2018.

[134] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," *Optics express*, vol. 16, no. 23, pp. 18790–18797, 2008.

[135] M. Rakhlin, A. Galimov, I. Dyakonov, N. Skryabin, G. Klimko, *et al.*, "Demultiplexed single-photon source with a quantum dot coupled to microresonator," *Journal of Luminescence*, vol. 253, p. 119496, 2023.

[136] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, "General theory of decoy-state quantum cryptography with source errors," *Physical Review A*, vol. 77, no. 4, p. 042311, 2008.

[137] M. Zahidy, M. T. Mikkelsen, R. Müller, B. Da Lio, M. Krehbiel, *et al.*, "Quantum key distribution using deterministic single-photon sources over a field-installed fibre link," *npj Quantum Information*, vol. 10, no. 1, p. 2, 2024.

[138] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, "Decoy-state quantum key distribution with both source errors and statistical fluctuations," *New Journal of Physics*, vol. 11, no. 7, p. 075006, 2009.

[139] G. Foletto, F. Picciariello, C. Agnesi, P. Villoresi, and G. Vallone, "Security bounds for decoy-state quantum key distribution with arbitrary photon-number statistics," *Physical Review A*, vol. 105, no. 1, p. 012603, 2022.

[140] E. Stock, W. Unrau, A. Lochmann, J. Töfflinger, M. Öztürk, *et al.*, "High-speed single-photon source based on self-organized quantum dots," *Semiconductor science and technology*, vol. 26, no. 1, p. 014003, 2010.

[141] A. Laucht, S. Pütz, T. Günthner, N. Hauke, R. Saive, *et al.*, "A waveguide-coupled on-chip single-photon source," *Physical Review X*, vol. 2, no. 1, p. 011014, 2012.

[142] K. Wakui, Y. Tsujimoto, M. Fujiwara, I. Morohashi, T. Kishimoto, *et al.*, "Ultra-high-rate nonclassical light source with 50 GHz-repetition-rate mode-locked pump pulses and multiplexed single-photon detectors," *Optics Express*, vol. 28, no. 15, pp. 22399–22411, 2020.

[143] G. Roberts, M. Lucamarini, J. Dynes, S. Savory, Z. Yuan, *et al.*, "A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution," *Quantum Science and Technology*, vol. 3, no. 4, p. 045010, 2018.

[144] Q. Wang, X.-B. Wang, and G.-C. Guo, "Practical decoy-state method in quantum key distribution with a heralded single-photon source," *Physical Review A*, vol. 75, no. 1, p. 012312, 2007.

[145] M. Abasifard, C. Cholsuk, R. G. Pousa, A. Kumar, A. Zand, *et al.*, "The ideal wavelength for daylight free-space quantum key distribution," *APL Quantum*, vol. 1, no. 1, 2024.

[146] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Physical review letters*, vol. 124, no. 7, p. 070501, 2020.

[147] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, p. 210801, 2023.

[148] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, p. 30, 2017.

[149] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, p. 5932, 1998.

[150] S. E. Vinay and P. Kok, "Practical repeaters for ultralong-distance quantum communication," *Phys. Rev. A*, vol. 95, no. 5, p. 052336, 2017.

[151] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, "Long-range big quantum-data transmission," *Phys. Rev. Lett.*, vol. 120, no. 3, p. 030503, 2018.

[152] M. Gündoğan, J. S. Sidhu, V. Henderson, L. Mazzarella, J. Wolters, *et al.*, "Proposal for space-borne quantum memories for global quantum networking," *npj Quantum Inf.*, vol. 7, no. 1, p. 128, 2021.

[153] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, *et al.*, "Advances in space quantum communications," *IET Quantum Commun.*, vol. 2, no. 4, pp. 182–217, 2021.

[154] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, p. 150501, 2005.

[155] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, *et al.*, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, p. 040502, 2015.

[156] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, *et al.*, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 839–894, 2022.

[157] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[158] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, "Micius quantum experiments in space," *Rev. Mod. Phys.*, vol. 94, no. 3, p. 035001, 2022.

[159] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, *et al.*, "Daylight quantum key distribution over 1.6 km," *Phys. Rev. Lett.*, vol. 84, no. 24, p. 5652, 2000.

[160] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, no. 1, p. 43, 2002.

[161] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," *New J. Phys.*, vol. 11, no. 4, p. 045007, 2009.

[162] H. Ko, K.-J. Kim, J.-S. Choe, B.-S. Choi, J.-H. Kim, *et al.*, "Experimental filtering effect on the daylight operation of a free-space quantum key distribution," *Sci. Rep.*, vol. 8, no. 1, pp. 1–7, 2018.

[163] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photon.*, vol. 11, no. 8, pp. 509–513, 2017.

[164] Y.-H. Gong, K.-X. Yang, H.-L. Yong, J.-Y. Guan, G.-L. Shentu, *et al.*, "Free-space quantum key distribution in urban daylight with the spgd algorithm control of a deformable mirror," *Opt. Express*, vol. 26, no. 15, pp. 18897–18905, 2018.

[165] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, *et al.*, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," *NPJ Quantum Inf.*, vol. 7, no. 1, p. 93, 2021.

[166] D. Rogers, J. C. Bienfang, A. Mink, B. Hershman, A. Nakassis, *et al.*, "Free-space quantum cryptography in the H-alpha Fraunhofer window," in *Free-Space Laser Communications VI*, vol. 6304, pp. 296–305, SPIE, 2006.

[167] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, "Finite key performance of satellite quantum key distribution under practical constraints," *Communications Physics*, vol. 6, no. 1, p. 210, 2023.

[168] T. T. Tran, K. Bray, M. J. Ford, M. Toth, and I. Aharonovich, "Quantum emission from hexagonal boron nitride monolayers," *Nat. Nanotechnol.*, vol. 11, pp. 37–41, 2016.

[169] T. Vogl, G. Campbell, B. C. Buchler, Y. Lu, and P. K. Lam, "Fabrication and deterministic transfer of high-quality quantum emitters in hexagonal boron nitride," *ACS Photonics*, vol. 5, no. 6, pp. 2305–2312, 2018.

[170] T. Vogl, R. Lecamwasam, B. C. Buchler, Y. Lu, and P. K. Lam, "Compact cavity-enhanced single-photon generation with hexagonal boron nitride," *ACS Photonics*, vol. 6, no. 8, pp. 1955–1962, 2019.

[171] S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," *Phys. Rev. Res.*, vol. 3, no. 2, p. 023130, 2021.

[172] F. Moscatelli, M. Marisaldi, P. Maccagnani, C. Labanti, F. Fuschino, *et al.*, "Radiation tests of single photon avalanche diode for space applications," *Nucl Instrum Methods Phys Res, Sect A, Accel Spectrom Detect Assoc Equip.*, vol. 711, pp. 65–72, 2013.

[173] Y. C. Tan, R. Chandrasekara, C. Cheng, and A. Ling, "Radiation tolerance of opto-electronic components proposed for space-based quantum key distribution," *J. Mod. Opt.*, vol. 62, no. 20, pp. 1709–1712, 2015.

[174] E. Anisimova, B. L. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, *et al.*, "Mitigating radiation damage of single photon detectors for space applications," *EPJ Quantum Technol.*, vol. 4, pp. 1–14, 2017.

[175] C. Emde, R. Buras-Schnell, A. Kylling, B. Mayer, J. Gasteiger, *et al.*, "The libRadtran software package for radiative transfer calculations (version 2.0. 1)," *Geosci. Model Dev.*, vol. 9, no. 5, pp. 1647–1672, 2016.

[176] H. Kaushal, V. Jain, and S. Kar, *Free space optical communication.* Springer, 2017.

[177] L. Valentini, A. Faedi, E. Paolini, and M. Chiani, "Analysis of pointing loss effects in deep space optical links," in *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2021.

[178] C. C. Chen and C. S. Gardner, "Impact of random pointing and tracking errors on the design of coherent and incoherent optical intersatellite communication links," *IEEE Trans. Commun.*, vol. 37, no. 3, pp. 252–260, 1989.

[179] L. Mazzarella, C. Lowe, D. Lowndes, S. K. Joshi, S. Greenland, *et al.*, "Quarc: Quantum research cubesat—a constellation for quantum communication," *Cryptography*, vol. 4, no. 1, p. 7, 2020.