Trabajo Fin de Máster
Máster en Ingeniería Aeronáutica

Analysis and Simulation of a Practical Quantum Key Distribution in Python for Aerospace applications

Autor: Juan Manuel Núñez Portillo
Tutora: María Ángeles Martín Prats

Dpto. de Ingeniería Electrónica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2020

Trabajo Fin de Máster
Máster en Ingeniería Aeronáutica

Analysis and Simulation of a Practical Quantum Key Distribution in Python for Aerospace applications

Autor:

Juan Manuel Núñez Portillo

Tutor:

María Ángeles Martín Prats
Profesora Titular

Dpto. de Ingeniería Electrónica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2020

Trabajo Fin de Máster: Analysis and Simulation of a Practical Quantum Key Distribution in Python for Aerospace applications

Autor: Juan Manuel Núñez Portillo

Tutora: María Ángeles Martín Prats

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2020

El Secretario del Tribunal

Resumen

Se presenta un estudio exhaustivo del estado del arte en la distribución cuántica de claves via satélite. Como resultado de dicho análisis, se simula el protocolo BB84 para ganar una mayor percepción. Este protocolo de distribución cuántica de claves ha sido ampliamente reportado en la literatura desde que fue publicado por primera vez y durante la última década, ha sido el más adoptado para experimentos en la atmósfera y en el espacio. Para añadir valor a los resultados que se obtienen en la simulación, algunas imperfecciones inherentes a los componentes comúnmente usados en tales experimentos son considerados, incluyendo los parámetros principales de la implementación. Adicionalmente, para el post procesamiento clásico, se emplean algoritmos típicos de corrección de error, verificación y amplificación de la privacidad. Por último, con respecto a la transmisión cuántica, la manipulación de los cúbits en la simulación se aborda de un modo cómodo mediante el uso de la librería de software de código abierto Cirq.

Abstract

An exhaustive study of the state of the art in satellite quantum key distribution is presented here. As a result of such analysis, the BB84 protocol is simulated to gain a further insight. This quantum key distribution protocol has been widely reported in the literature since it was first published and for the last decade, it has been the most adopted one for tests in the atmosphere and in space. In order to add value to the results which are obtained in the simulation, some imperfections inherent to the components commonly used in such tests are considered, including the main parameters of the implementation.Additionally, for the classical post-processing, typical algorithms of error correction, verification and privacy amplification are employed. Lastly, with respect to the quantum transmission, the manipulation of the qubits in the simulation is addressed in a confortable way by using the open-source software library Cirq.

Contents

Index of Figures

Index of Tables

Acronyms

APD	Avalanche Photo-Diode
BSC	Binary Symmetric Channel
CV	Continuous Variable
DC	Discrete Variable
ETSI	European Telecommunication Standards Institute
FEC	Forward Error Correction
FSO	Free-Space Optics or Free-Space Optical communication
FWHM	Full Width at Half Maximum
GEO	Geostationary Earth Orbit
IR	Intercept-Resend
ISO	International Organization for Standardization
LDPC	Low-Density Parity-Check
LEO	Low Earth Orbit
OGS	Optical Ground Station
PAT	Pointing, Acquisition and Tracking (PAT)
PNS	Photon-Number Splitting
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
RNG	Random Number Generator
SDT	Superdense Teleportation protocol
SNSPD	Superconducting Nanowire Single-Photon Detector
SPAPD	Single-Photon Avalanche Photo-Doiode
SPDC	Spontaneous Parametric Down-Conversion

1 Introduction

1.1 Introduction to quantum mechanics

Quantum mechanics is the part of physics that explains the behaviour of nature at the particle level. It was founded in the early 20th century and, since then, it is known for its counterintuitive statements as well as for the accuracy of its outcomes.

It all started with a series of explanations born from heuristic methods that were given to some bizarre phenomena:

- in 1900, Max Planck solved the problem of black-body radiation stating that bodies emit energy in discrete packets, or quanta, instead of continuously as traditionally thought;
- in 1905, Albert Einstein, to explain the photoelectric effect, concluded that light waves were made up of indivisible light quanta, later called photons;
- and in 1912, Ernest Rutherford proposed a new atomic model, according to which electrons orbit the nucleus like planets in the Solar System.

These descriptions introduced the new ideas of quantization, wave-particle duality and orbits, which were soon widely adopted and mathematically formulated through two approaches: Heisenberg's matrix mechanics and Schrödinger's wave mechanics [1]. However, the wave function concept (together with Max Born's probabilistic interpretation) turned out to be equivalent to Heisenberg's principle of uncertainty. While the former is related to the probability of finding an electron at a certain position at a specific time, the latter exhibits the impossibility of accurately determining its position and momentum at the same time [2].

The probabilistic approach rapidly led to the principle of superposition of states. At the quantum level, the state of a system, formed by one or more particles, defines its motion in a compatible way with the information that is accessible. For instance, the state of a single photon, part of a beam or the whole beam, may be given by the notion of its location, its energy (related to its momentum and, therefore, to its frequency or wavelength) and its polarization[1]. Note that, sometimes, several observations on a certain quantum state can yield different results. In this case, it is claimed that a general state of the states disclosed by the observations (two or more), is a superposition of all of them. This is essentially what is known as the principle of superposition and its statement deserves three clarifications. First, the possible measurement outcomes are always the same, i.e. there are not any intermediate resultant states. Second, prior to observing the result, there exists a certain probability that the system is in one state or in another, but it cannot be simultaneously in two states.

[1] Polarization of light is the property that makes its electric field oscillate perpendicularly to the direction of propagation.Light is unpolarized when such a direction presents random fluctuations in time. Otherwise, it is called polarized and there are three types of polarizations: linear, circular and elliptical.

Third, although the mathematical formulation of the principle allows to extend the number of outcomes up to the infinity, this must be contrasted with the physics on a case-by-case basis [3 pp. 4-14]. See Figure 1.1 to gain a further insight.

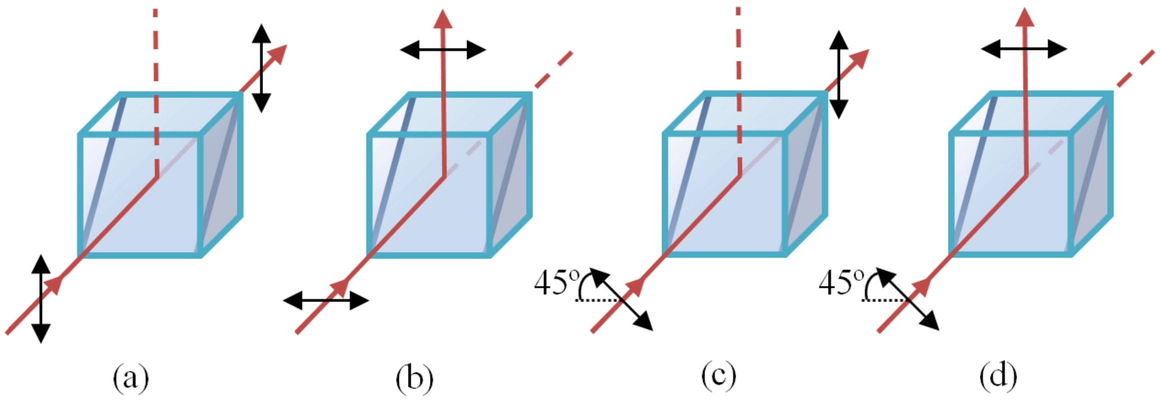

Figure 1.1 – Schematic illustration of an ideal polarizing beamsplitter cube and four linearly polarized single photons passing through it: (a) the photon is transmitted because it has an electric field whose polarization is parallel to the plane of incidence (formed by the incident and the reflected directions); (b) the photon is reflected because the polarization direction is perpendicular to the same plane; (c) and (d) the photon is either transmitted or reflected, respectively, with equal probability because its polarization direction forms 45º with both parallel and perpendicular directions. In this last case, there exists a superposition where the two possible resultant states after an observation (e.g. placing a photodetector after the beamsplitter in each direction) are the parallel and the perpendicular polarization directions.

If the quantum superposition of states is a bit counterintuitive, the quantum entanglement may be all the more. This phenomenon involves at least two particles in superposition and occurs when it is not possible to express the state of the ensemble in terms of the previous general states of each particle. In other words, the current state of one particle of the ensemble cannot be given by the state that it had before the entanglement, but only by the current state of the other entangled particles. In the case of two particles, they are called an entangled pair and have a special property known as the monogamy of entanglement. As one might infer by the name, when two particles are entangled, they cannot share the entanglement with a third party[2]. A second property of interest is the maximal coordination. When a number of particles, say two, are entangled, naturally or by means of a certain laboratory operation, and then become separated, if their states are measured, the result of the second one will be immediately correlated with the result of the first one [4]. An example of generation of entangled photons is illustrated in Figure 1.2.

Needless to say, all the revolutionary ideas that triggered the creation of quantum mechanics, gave rise to a long debate among the physicians. Fortunately, the pressure was relieved with the advancement in experimentation throughout the second half of the past century, and the focus turned to the development of exciting applications.

[2] Say an eavesdropper who tries to obtain any information from the entangled pair.

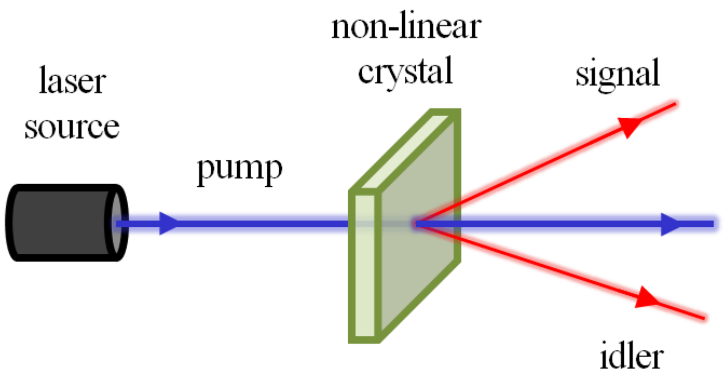

Figure 1.2 – Schematic set-up for the generation of polarization entangled photon-pairs via spontaneous parametric down-conversion (SPDC). As a pump laser beam passes through a non-linear crystal, one photon can spontaneously split into two photons, usually called signal and idler photons. These two photons can hold the same or a different polarization between them, depending on parameters such as the incident electric field, the crystal material, etc. Additionally, the new pair must satisfay the energy and momentum conservation laws with respect to the original photon, having thus a lower frequency and symmetrical directions. Despite its inefficiency, it is one of the most popular methods for the entanglement of photons [5].

1.2 Motivation and Related work

From 1940s to 1990s, quantum physics made it possible to engineer technologies such as the transistor, the laser and the atomic clock [6 pp. 5-13]. With this kind of technologies, many applications surfaced and changed the human life. However, the search of new quantum technologies did not stop and received a boost from the physician Richard Feynman in 1959 and in 1981, announcing a non-minor new revolution. For a few decades, this second generation of quantum technologies has been taking shape. This time, unlike the first generation, the focus is on the control of individual quantum particles [6 p. 18], exploiting the phenomena of superposition and entanglement.

Typically, quantum technologies are classified into four categories: sensors, communication, simulators and computers; amazingly, they share a close relationship with the aerospace industry. For instance, in the field of sensors, there exists a fervent interest in quantum clocks that outperform previous atomic clocks used in the GPS systems [7]; in quantum gravimeters for monitoring the Earth [8]; and in other sensors for fundamental science in space [9]. Regarding the communication category, the main applications are the quantum cryptography and the quantum internet [10]. Quantum simulators, on the other hand, should be understood as a potential powerful tool to, for example, design ligther and stronger materials as well as more aerodynamic parts [11]. Last but not least, the quantum computer is a promising way of accelerating the calculations in very complex problems or accessing an authentic artificial intelligence [12].

The above-mentioned attractive applications, and many others, together with the effort of the scientific community, have awakened a worldwide interest. Private companies as well as research institutions do not want to fall behind and neither do the goverments of the world powers, due to the potential geopolitical implications. In this context, in 2018 the European Commission decided to launch a one-billion-euro initiative on a ten years timeline, in response to the Quantum Manifesto signed by scientists in 2016 [13]. Note that this initiative, known as the Quantum Flagship, must persue an additional goal. As happens with other large-scale initiatives strongly related to science, say the construction of the nuclear fusion reactor ITER, the recruitment of a suitable engineering workforce is vital to succeed.

Whether the investment in all kinds of quantum infrastructures and training programs is justified or not is beyond the scope of this work. Only time will tell the real supremacy of quantum computers or the deployment of a quantum network. Nevertheless, what is a reality today is the quantum cryptography, particularly the Quantum Key Distribution (QKD). In fact, there are a few companies such as ID Quantique or QinetiQ that already commercialise it through optical fiber and terrestrial free-space optical (FSO) links.

The progress made in QKD comes together with the enormous dependency on data of the society and the threat that a quantum computer breaks the currently used public key cryptosystems. One of the most popular methods to send a secret message between two parties is the RSA[3] cryptosystem. It involves the use of a public key and a private key created by one of the parties following an algorithm. The public key is shared with the other party, who uses it to encrypt a certain message and send it to the first party. Then, this party decrypts it with the help of the secret key. Even though this method seems to be secure based on the experience, there are not any security proofs and the last barrier against an eavesdropper is the time-consuming factoring on a classical computer [14 pp. 640-644]. However, this task could be quickly performed by a quantum computer and a quantum algorithm[4].

On the contrary, the security of cryptographic protocols that make use of QKD rests on physical phenomena. QKD permits to share an unconditionally secret key between two parties and even to reveal the presence of an eavesdropper. The exchange of a raw key takes place through an untrusted quantum channel, whereas an authenticated classical channel is required to transform the raw key into a secure key. Unfortunately, the distribution of the key through the quantum channel, e.g. optical fiber or terrestrial free-space links, has important losses. In this way, the secret key rate hardly reaches 10 kbps if the distance is longer than 100km[5]. A solution may be the introduction of quantum repeaters along the trajectory, but this would never allow key distributions on an intercontinental scale. To overcome these limitations, the use of a quantum satellite network sounds very promising [18 p. 1]. In fact, several experimental missions in space have already been executed or proposed around the world[6].

However, the longer distances of satellite QKD is not the only point for the motivation of this work. Equipping future satellites with QKD components may make their designs simpler and lighter. For instance, large memories onboard to store the instructions would no longer be needed [19 p. 31]. Instead, the satellite operator could send such instructions in a secure manner as required, what constitutes a problem that has not been solved yet. This functionality would have a clear impact on the satellite in terms of adaptability as well. It could perform a wider variety of tasks and even to live longer. On the other hand, the technological trend towards a high interconnectedness and autonomy cannot be left behind, where security in the involved communications will play a central role, enabling trusted designs against external attacks.

1.3 Purpose and Scope

The aim of this work is to analyse the state of the art in satellite QKD, simulating some basic results to consolidate learning. In particular, the BB84 protocol is analysed. With reference to the related

[3] Rivest, Shamir and Adleman invented it, hence the acronym.

[4] As of July 2020, Shor's algorithm (1994) could solve the factoring problem for 2048-bit RSA integers in a matter of hours, with the help of a quantum computer with millions or billions of noisy qubits, depending on the version of the algorithm (see Table 2 of [15]). On the other hand, and to the best of my knowledge, neither Google, IBM nor Intel has announced a quantum processor with more than 72 qubits yet.

[5] As of July 2020, and to the best of my knowledge, the distance records are: 502km with a secret key rate of 0.118bps by optical fiber [16]; and 144km with a secret key rate of 24bps by terrestrial free-space link [17].

[6] Later, in Section 3.2, some information will be provided on this subject.

works presented at the end of Section 1.2, this work aspires to model the main steps of the entire QKD protocol, including the effects of imperfections, noise and eavesdropping. The main contribution, however, is the use of Cirq[7], a Python library specifically designed to run quantum circuits against quantum computers and simulators.

On the other hand, the scope of this work is limited by the duration of the project. For this reason, the authentication is not simulated. Furthermore, those imperfections inherent to the QKD implementation that require an additional classical post-processing to treat them (e.g. timing jitter, dark counts, etc.) are not included; and only the intercept-resend is considered (without quantum memory). Lastly, a deep study of optimal error-correcting codes and privacy amplification is not covered by this document either. However, the main ideas behind the later and the former are introduced at the appropriate instant.

1.4 Structure of the work

In order to detail how the desired goals have been achieved, this document is structured in chapters.

In Chapter 2, the QKD problem is mathematically formulated. Both quantum communication and classical post-processing are introduced. First, the Dirac notation, the concept of qubit and its evolution through noiseless and noisy channels are described. Secondly, some tools from the information theory field are presented, laying the foundation to understand later in Chapter 3 how the security proof of a QKD protocol is addressed.

In Chapter 3, the theoretical framework of QKD is presented. A detailed explanation of the steps and the security issues of a QKD protocol are given. Moreover, various general classifications of QKD protocols are exposed, focusing on the BB84 protocol.

In Chapter 4, some ideas for the implementation of the BB84 protocol are mentioned, together with the state-of-the-art of the main technologies. With this content, the ground is prepared for the simulation of some of the main imperfections of the QKD components.

In Chapter 5, an overview of the numerical modelling is presented. All the contents of the previous chapters are met here.

Next, in Chapter 6, a number of basic, but interesting, results of the simulations are collected.

Finally, in Chapter 7, the results of this work are discussed, providing a summary and a proposal for future research.

Note that this document is organized in a slightly different way from the traditional structure of introduction, methods, results and discussion. The multidisciplinary nature of QKD makes it complicated to decide the best order for the presentation of the contents. The author of this work truly hopes that the reader will find it easy to follow.

[7] It is difficult to say whether Cirq has already been used in the area of QKD or not, but, to the best of my knowledge, any studies including the non-idealities have not been published as of July 2020.

2 Mathematical formulation

2.1 Quantum states

2.1.1 State vectors

The state of a certain system at the quantum level can be represented by different ways. Typically, some representations are more suitable than others depending on the application. In quantum computation and quantum information, the use of the Dirac notation, or the bra-ket notation, is widespread. Therefore, only familiar linear algebra written in a user-friendly notation will be required to cope with quantum mechanics.

Getting back to the idea introduced in Section 1.1 that a system is completely described by the definition of its state, the mathematical formulation emerges naturally. According to the first postulate of quantum mechanics, a physical system is linked with a Hilbert space $\mathbb{C}^d$ called state space of the system, where d denotes its dimension[8]. Thus, its state is given by a column vector in $\mathbb{C}^d$, also known as state vector [14 p. 80]. In the context of quantum information, if d is equal to 2, the state vector receives the name of qubit (or quantum bit), whereas for a general dimension the term qudit is used.

Before carrying on with the mathematical description of quantum systems, two things deserve to be clarified. First, a Hilbert space is but a generalization for a dimension d of the well-known concept of Euclidean space. It is equipped with an inner product, that is, a generalization of the dot product. Secondly, the difference between the mathematical qubit (or qudit) and its physical realization must be remarked. As happens with the bit, which can be either zero or one and be built by means of an electrical signal, the qubit is, in general, the term used to refer to the abstract object, which can be physically built by a variety of methods. An example, which is of interest in the case of this work, is a photon with a variable polarization. However, it is true that, in practice, both mathematical and physical connotations are widespread.

To express the principle of superposition, once the notion of state vector has been introduced, it is not difficult to imagine the construction. In $\mathbb{C}^2$

$$\boldsymbol{q} = \alpha_1 \boldsymbol{q}_1 + \alpha_2 \boldsymbol{q}_2 \tag{2.1}$$

where $\boldsymbol{q}$ is the general state given by the superposition of the resultant states $\boldsymbol{q}_1$ and $\boldsymbol{q}_2$. Note that $\boldsymbol{q}_1$ and $\boldsymbol{q}_2$ must be unitary and linearly independent. In fact, they span the vector space $\mathbb{C}^2$ forming one of many possible bases. In particular, only orthonormal bases are interesting for this study. After this, it is time to start using the Dirac notation:

[8] For this work, a finite dimension can be perfectly assumed.

$$|q\rangle = \alpha_1 |q_1\rangle + \alpha_2 |q_2\rangle \tag{2.2}$$

The symbol $|\cdot\rangle$ is used to indicate the column vector nature and it is typically called a ket. If the basis is a canonical basis, then the use of $|0\rangle$ and $|1\rangle$ to refer to the transposes of $\begin{bmatrix}1 & 0\end{bmatrix}$ and $\begin{bmatrix}0 & 1\end{bmatrix}$, respectively, is widely adopted. This basis is usually known as standard basis or computational basis. In the case of a photon containing the information in its polarization, $|0\rangle$ and $|1\rangle$ are reserved for the horizontal and the vertical polarization, respectively. Another basis that will be used in this work is the diagonal basis, which is the spanning set formed by the transposes of $\left(1/\sqrt{2}\right)\begin{bmatrix}1 & 1\end{bmatrix}$ and $\left(1/\sqrt{2}\right)\begin{bmatrix}1 & -1\end{bmatrix}$. The notation is also abbreviated with the symbols $|+\rangle$ and $|-\rangle$, respectively. Note that this set is but the result of rotating the standard basis an angle of 45º. In fact, one can easily express any vector of one basis in terms of the vectors of the other basis and vice versa:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.3}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.4}$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \tag{2.5}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{2.6}$$

With respect to the complex[9] coefficients α_1 and α_2, they are called amplitudes and must satisfy the normalization condition:

$$\langle q|q\rangle = |\alpha_1|^2 + |\alpha_2|^2 = 1 \tag{2.7}$$

The symbol $\langle\cdot|\cdot\rangle$ represents the inner product between the bra $\langle\cdot|$ and the ket $|\cdot\rangle$, where the bra is but the dual vector to $|\cdot\rangle$. On the other hand, it is also important to remark the physical meaning of these amplitudes. Each $|\alpha_i|^2$ stands for the probability that a measument yields the outcome $|q_i\rangle$. For that reason, the normalization is a key condition.

So far only single qubits (or qudits[10]) have been considered, but the case of multiple qubits is also interesting. The joint state of a composite system is given by the tensor product, which in the case of two qubits is

$$|qu\rangle \equiv |q\rangle|u\rangle \equiv |q\rangle \otimes |u\rangle = \begin{bmatrix} \alpha_1 \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} \\ \alpha_2 \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \end{bmatrix} \tag{2.8}$$

The introduction of composite systems makes it necessary to talk about at least two aspects. First, the dimension of the joint state is 2^n, with n being the number of qubits. Second, taking into consideration the definition of entanglement given in Section 1.1, an entangled pair of qubits cannot be described by the tensor product. Otherwise, it is clear that the individual states could be perfectly recovered from the four equations of Eq. (2.8). The most famous examples of entangled qubits are known as the Bell states or EPR pairs for historical reasons. More precisely, there are four states:

[9] Although a complex number is defined by two parameters, the two complex coefficients α_1 and α_2 present only two degrees of freedom. This is because two conditions are also imposed: the normalization condition and the assumption that the state vector remains unchanged when it is multiplied by whichever (complex) factor [3 p. 17].

[10] Hereinafter only qubits will be considered. The generalization for *d* dimensions is not difficult at all.

$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \tag{2.9}$$

$$\frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \tag{2.10}$$

2.1.2 Density operators

Another useful, and equivalent to the state vector, approach to describe the state of a quantum system is by way of the density operator. This formulation is built up from the set of possible general states in which one can find the system and their corresponding probabilities p_k. Mathematically, the definition of the density operator (for a general qubit) is

$$\rho \equiv \sum_k p_k |q^k\rangle\langle q^k| \tag{2.11}$$

where $|\cdot\rangle\langle\cdot|$ denotes the outer product, which is but the product between a column vector and a row vector, i.e. a matrix.

Again, it is important to clarify three aspects. First, note the intentional use of a superscript k instead of a subscript i. This is to make the distinction between a possible general state and the orthonormal vectors of a certain basis. Second, the generalization allows to consider the case with a unique qubit, where p equals one. Third, the introduction of the density operator is motivated by its capacity to comtemplate mixed states. While each $|q^k\rangle$ is a pure state, that is, there exists exact information about its state, ρ represents a mixed state. The additional randomness of a mixed state must not be confused with the randomness around a pure state, which can be in superposition and its amplitudes can be unkown. Since a picture is worth a thousand words, see Figure 2.1.

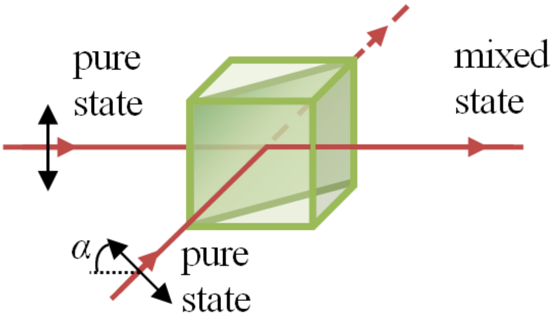

Figure 2.1 – Schematic illustration of an ideal non-polarizing beamsplitter cube and two single photons with different polarization directions going through it. This picture aims at helping separate the probability distribution of a mixed state from the probability distribution of a pure state in superposition. For instance, a pure state can be vertically polarized and polarized in a specific direction (i.e. in superposition), whose angle can be unknown (that is to say, its amplitudes can be unkown).

As is the case with the state vector formulation, a composite system can be defined by the density operator as well. It is enough to use the tensor product. If two bidimensional systems A and B are being studied, the joint state is

$$\rho^{AB} = \rho^{A} \otimes \rho^{B} = \begin{bmatrix} \rho_{11}^{A}\begin{bmatrix} \rho_{11}^{B} & \rho_{12}^{B} \\ \rho_{21}^{B} & \rho_{22}^{B} \end{bmatrix} & \rho_{12}^{A}\begin{bmatrix} \rho_{11}^{B} & \rho_{12}^{B} \\ \rho_{21}^{B} & \rho_{22}^{B} \end{bmatrix} \\ \rho_{21}^{A}\begin{bmatrix} \rho_{11}^{B} & \rho_{12}^{B} \\ \rho_{21}^{B} & \rho_{22}^{B} \end{bmatrix} & \rho_{22}^{A}\begin{bmatrix} \rho_{11}^{B} & \rho_{12}^{B} \\ \rho_{21}^{B} & \rho_{22}^{B} \end{bmatrix} \end{bmatrix} = \\ = \begin{bmatrix} \rho_{11}^{A}\rho_{11}^{B} & \rho_{11}^{A}\rho_{12}^{B} & \rho_{12}^{A}\rho_{11}^{B} & \rho_{12}^{A}\rho_{12}^{B} \\ \rho_{11}^{A}\rho_{21}^{B} & \rho_{11}^{A}\rho_{22}^{B} & \rho_{12}^{A}\rho_{21}^{B} & \rho_{12}^{A}\rho_{22}^{B} \\ \rho_{21}^{A}\rho_{11}^{B} & \rho_{21}^{A}\rho_{12}^{B} & \rho_{22}^{A}\rho_{11}^{B} & \rho_{22}^{A}\rho_{12}^{B} \\ \rho_{21}^{A}\rho_{21}^{B} & \rho_{21}^{A}\rho_{22}^{B} & \rho_{22}^{A}\rho_{21}^{B} & \rho_{22}^{A}\rho_{22}^{B} \end{bmatrix} \qquad (2.12)$$

The last mathematical object that will be presented in this subsection is the reduced density operator. Imagine that there is a system formed by the combination of the systems *A* and *B*. Then, the state of one of the subsystems, say *A*, is described by

$$\rho_{A}^{AB} \equiv \mathrm{tr}_{B}\left(\rho^{AB}\right) \qquad (2.13)$$

where $\mathrm{tr}_{B}\left(\cdot\right)$ denotes the partial trace over system *B*. Before seeing its definition, if ρ^{AB} can be expressed in terms of $\rho^{A} \otimes \rho^{B}$, where ρ^{j} , making use of Eq. (2.11), consists of addends like $p_{k,j}\left|q^{k,j}\right\rangle\left\langle q^{k,j}\right|$ (with *j*=*A*,*B*), and each $\left|q^{k,j}\right\rangle$ is, in turn, $\alpha_{1}^{k,j}\left|q_{1}^{j}\right\rangle + \alpha_{2}^{k,j}\left|q_{2}^{j}\right\rangle$ without loss of generality, then it is not complicated to visualize that ρ^{AB} is but a sum of terms like $\left|q_{i}^{A}\right\rangle\left\langle q_{l}^{A}\right| \otimes \left|q_{r}^{B}\right\rangle\left\langle q_{s}^{B}\right|$ (with *i*,*l*,*r*,*s*=1,2) multiplied by some factor. Now, the partial trace over system *B* is by definition

$$\mathrm{tr}_{B}\left(\left|q_{i}^{A}\right\rangle\left\langle q_{l}^{A}\right| \otimes \left|q_{r}^{B}\right\rangle\left\langle q_{s}^{B}\right|\right) \equiv \left|q_{i}^{A}\right\rangle\left\langle q_{l}^{A}\right| \mathrm{tr}\left(\left|q_{r}^{B}\right\rangle\left\langle q_{s}^{B}\right|\right) \qquad (2.14)$$

Therefore, recalling that this is linear algebra, the following result is obtained:

$$\rho_{A}^{AB} = \rho^{A}\mathrm{tr}\left(\rho^{B}\right) = \rho^{A} \qquad (2.15)$$

In words, the reduced density operator for system *A* provides the connection between the state of the subsystem *A* in *AB* and the system *A*, as one could intuit. Notice that $\mathrm{tr}\left(\rho^{B}\right)$ equals one has been used but not proved. Without wishing to set a precedent, the proof is left to the curious reader. To start, use Eq. (2.11) and Eq. (2.2), with a symbolic probability distribution and amplitudes. At the end, Eq. (2.7) and the sum of probabilities equals one need to be applied.

Unfortunately, this document only outlines the essentials of quantum states. More details about density operators and reduced density operators can be found in [14 pp. 98-106]. Also, the concept of Bloch sphere, typically used to deal with single (pure or mixed) qubits, is described in [14 pp. 15, 89].

2.2 Evolution and Measurement

Once the state of a quantum system has been introduced, it is time to see how to go from one state to another. To do so, suppose the existence of a closed[11] quantum system. According to the second postulate of quantum mechanics, the evolution of a closed quantum mechanical system after a certain time interval is governed by a unitary transformation [14 p. 81]. In symbols for the two viewed representations of states,

[11] Strictly speaking, a real closed quantum system does not exist. However, this is not an impediment as long as the environmental conditions are under control. In other words, the external parameters are not any noise sources, but working conditions.

$$|q'\rangle = U|q\rangle \tag{2.16}$$

$$\rho' = U\rho U^\dagger \tag{2.17}$$

where $|q\rangle$ (or ρ) and $|q'\rangle$ (or ρ') are the previous and the subsequent states, respectively, to the linear transformation given by the unitary operator *U* or, in terms of matrices, by the unitary matrix *U*. This means that $U^\dagger U = UU^\dagger = I$, with $U^\dagger \equiv \left(U^*\right)^T$.

Notice that for the goals of this work, there is no necessity to deal with the Schrödinger equation and Hamiltonian. It is sufficient to cope with unitary matrices. Some examples of unitary matrices for single qubits that will be of interest are shown in Figure 2.2.

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Figure 2.2 – Examples of well-known unitary matrices. From left to right: the first three matrices are called the Pauli matrices (*X* and *Z* are also known as the bit flip and the phase flip matrices, respectively); whereas *H* is the matrix representation of the Hadamard operator, which can be understood as the change-of-basis matrix from the standard basis to the diagonal basis and vice versa.

On the other hand, after the evolution of the system, it is sometimes interesting to perform a measurement. In general, this measument disturbs the state of the system, because it is as if someone has opened it to the outside. Therefore, the mathematical description of a measurement can no longer be a unitary transformation. In other terms, it must be compatible with its irreversible nature. In this direction, imagine a system is prepared in a certain state, whose possible resultant states are given by the index *m*. For instance, if the state is $\alpha_0|0\rangle + \alpha_1|1\rangle$, then the possible resultant states are $|0\rangle$ and $|1\rangle$, with *m*={0,1}. Quantum measurements are formulated by the set of operators {M_m}, in such a way that if the state of the system prior to the measurement is $|q\rangle$(or ρ), the state after the measurement is

$$|q_m\rangle = \frac{M_m|q\rangle}{\sqrt{p(m)}} \tag{2.18}$$

$$\rho_m = \frac{M_m \rho M_m^\dagger}{p(m)} \tag{2.19}$$

where *p(m)* is the probability of yielding the outcome related to the index *m*. This probability can be calculated by the following expressions, depending on the representation:

$$p(m) = \langle q|M_m^\dagger M_m|q\rangle \tag{2.20}$$

$$p(m) = \mathrm{tr}\left(M_m^\dagger M_m \rho\right) \tag{2.21}$$

Note that the sum of probabilities must be equal to one for all $|q\rangle$, that is

$$\sum_m p(m) = \sum_m \langle q|M_m^\dagger M_m|q\rangle = \langle q|\sum_m M_m^\dagger M_m|q\rangle = 1 \Rightarrow \sum_m M_m^\dagger M_m = I \tag{2.22}$$

It remains to be clarified how the operators M_m are defined. For the sake of time, consider this situation: if one measures in the standard basis, then $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. At this point, it may be useful for future sections to pause and think about the following example.

Example 2.1 – *Imagine a situation in which a person called Bob receives a packet. It contains a qubit with a brief letter from his friend Alice. She tells him that the qubit is prepared in one of the two* *states* $\{|0\rangle, |+\rangle\}$*. However, she prefers not to disclose the state and challenges him to guess it. In a few days' time, she will call him to say whether he is right or wrong.*

Almost immediately, Bob starts thinking how to know the state. Before performing the measurement, he wants to check if there exists a vulnerability that leaks some information. In this sense, the first thing he does is to decide which basis he should use for the measurement, either the standard basis or the diagonal basis. For instance, if the standard basis is chosen, the possible states are $|0\rangle$ *and* $\left(|0\rangle+|1\rangle\right)/\sqrt{2}$*, and the measurement operators are* $M_0=|0\rangle\langle 0|$ *and* $M_1=|1\rangle\langle 1|$*. So the probability that a measurement yields* $|0\rangle$ *given that the initial state was* $|0\rangle$ *or* $|+\rangle$ *is*

$$p\left(|0\rangle \,|\, |0\rangle\right)=\langle 0|M_0^\dagger M_0|0\rangle=\langle 0|0\rangle\langle 0|0\rangle\langle 0|0\rangle=1\cdot1\cdot1=1 \tag{2.23}$$

$$\begin{aligned}
p_0(|0\rangle \,|\, |+\rangle) &= \frac{1}{\sqrt{2}}\left(\langle 0|+\langle 1|\right)M_0^\dagger M_0\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)=\frac{1}{2}\left(\langle 0|+\langle 1|\right)|0\rangle\langle 0|0\rangle\langle 0|\left(|0\rangle+|1\rangle\right)=\\
&=\frac{1}{2}\left(\langle 0|0\rangle\langle 0|0\rangle\langle 0|0\rangle+\langle 0|0\rangle\langle 0|0\rangle\langle 0|1\rangle+\langle 1|0\rangle\langle 0|0\rangle\langle 0|0\rangle+\langle 1|0\rangle\langle 0|0\rangle\langle 0|1\rangle\right)=\\
&=\frac{1}{2}\left(1\cdot1\cdot1+1\cdot1\cdot0+0\cdot1\cdot1+0\cdot1\cdot0\right)=\frac{1}{2}
\end{aligned}\tag{2.24}$$

Therefore, $p\left(|1\rangle \,|\, |0\rangle\right)=1-p\left(|0\rangle \,|\, |0\rangle\right)=1-1=0$ *and* $p\left(|1\rangle \,|\, |+\rangle\right)=1-p\left(|0\rangle \,|\, |+\rangle\right)=1-1/2=1/2$*. In other words, if a measurement is performed in the standard basis, and the result is* $|1\rangle$*, it can be assured with certainty that the initial state was* $|+\rangle$*. Nevertheless, if the result is* $|0\rangle$*, it cannot be said anything because the state* $|+\rangle$ *expressed in the standard basis is a superposition of* $|0\rangle$ *and* $|1\rangle$*.*

Let us see what happens if the diagonal basis is chosen. In this case, the possible states are $\left(|+\rangle+|-\rangle\right)/\sqrt{2}$ *and* $|+\rangle$*, and the measurement operators are* $M_+=|+\rangle\langle +|$ *and* $M_-=|-\rangle\langle -|$*. So the probability that a measurement yields* $|+\rangle$ *given that the initial state was* $|0\rangle$ *or* $|+\rangle$ *for both possible states is*

$$\begin{aligned}
p(|+\rangle \,|\, |0\rangle) &= \frac{1}{\sqrt{2}}\left(\langle +|+\langle -|\right)M_+^\dagger M_+\frac{1}{\sqrt{2}}\left(|+\rangle+|-\rangle\right)=\frac{1}{2}\left(\langle +|+\langle -|\right)|+\rangle\langle +|+\rangle\langle +|\left(|+\rangle+|-\rangle\right)=\\
&=\frac{1}{2}\left(\langle +|+\rangle\langle +|+\rangle\langle +|+\rangle+\langle +|+\rangle\langle +|+\rangle\langle +|-\rangle+\langle -|+\rangle\langle +|+\rangle\langle +|+\rangle+\langle -|+\rangle\langle +|+\rangle\langle +|-\rangle\right)=\\
&=\frac{1}{2}\left(1\cdot1\cdot1+1\cdot1\cdot0+0\cdot1\cdot1+0\cdot1\cdot0\right)=\frac{1}{2}
\end{aligned}$$

(2.25)

$$p(|+\rangle \,|\, |+\rangle)=\langle +|M_+^\dagger M_+|+\rangle=\langle +|+\rangle\langle +|+\rangle\langle +|+\rangle=1\cdot1\cdot1=1 \tag{2.26}$$

Therefore, $p\left(|-\rangle \,|\, |0\rangle\right)=1-p\left(|+\rangle \,|\, |0\rangle\right)=1-1/2=1/2$ *and* $p\left(|-\rangle \,|\, |+\rangle\right)=1-p\left(|+\rangle \,|\, |+\rangle\right)=1-1=0$*. Similarly to the former basis, if a measurement is performed in the diagonal basis, and the result is* $|-\rangle$*, it can be assured with certainty that the initial state was* $|0\rangle$*. Nevertheless, if the result is* $|+\rangle$*, it cannot be said anything because the state* $|0\rangle$ *expressed in the diagonal basis is a superposition of* $|+\rangle$ *and* $|-\rangle$*.*

In conclusion, unless Bob has the luck to select the wrong basis and to obtain the outcome that allows him to discard one of the options, he cannot be sure that he obtained the right state with the measurement. Additionally, it is not possible to rely on any bias since one basis is the result of rotating 45^{o} *the other; that is, if he chooses the wrong basis, the probability of obtaining the wrong state is 1/2. For all of the above reasons, and taking into consideration that he has only one opportunity before disturbing the initial state with the measurement, he decides to make the choice of the basis at random.*

Example 2.1 brings to light the indistinguishability of non-orthogonal quantum states, which prevents a person without further information from knowing the state of a quantum system [14 pp. 70-71, 56-57]. At this point, it seems natural to ask why one cannot simply take the qubit whose state is unkown, make a number of copies in the laboratory, perform that number of measurements and then analyse the statistical results. Unfortunately, it is not physically possible to reproduce exactly a qubit in an unkown state, unless only orthogonal states are considered, but this is not the case. This statement is known as the no-cloning theorem. More details can be found in [14 pp. 24-25, 529-532].

With respect to the evolution (or the measurement) of a composite quantum system, it is immediate to extrapolate Eqs. (2.16-19). It is enough to use a property of the tensor product which involves the tensor product of linear transformations. Suppose a composite system *AB* formed by the systems *A* and *B*. If $U^{AB} = U^A \otimes U^B$, then

$$\left|q^{A'}q^{B'}\right\rangle = U^{AB}\left|q^A q^B\right\rangle = U^A \otimes U^B\left(q^A \otimes q^B\right) = U^A q^A \otimes U^B q^B \tag{2.27}$$

$$\begin{aligned}\rho^{AB'} &= U^{AB}\rho^{AB}\left(U^{AB}\right)^{\dagger} = U^A \otimes U^B\left(\rho^A \otimes \rho^B\right)\left(U^A\right)^{\dagger} \otimes \left(U^B\right)^{\dagger} = \\ &= U^A\rho^A\left(U^A\right)^{\dagger} \otimes U^B\rho^B\left(U^B\right)^{\dagger}\end{aligned} \tag{2.28}$$

Finally, it is important to make the connection between this section and some aspects from quantum computing[12], due to the simulation tool used in this work. In the field of quantum computing, a quantum gate corresponds to what has been mathematically defined here as a unitary operator or unitary matrix *U*. Typically, a quantum gate acts on one or a few qubits and the combination of various quantum gates operating on a number of qubits forms a quantum circuit. This quantum circuit represents the set of operations behind a quantum algorithm. For instance, consider the quantum teleportation algorithm shown in Figure 2.3, which permits to send a quantum state from one party to another located far apart by using the entanglement phenomenon.

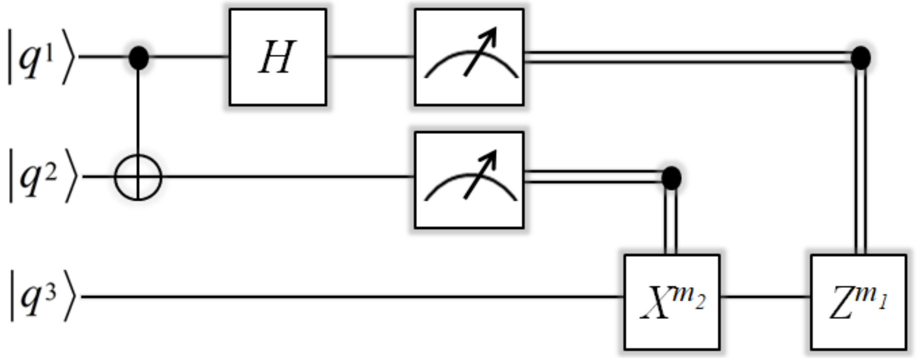

Figure 2.3 – Quantum circuit for the quantum teleportation algorithm. There are three qubits: the first and the second ones are at one location, whereas the third one is somewhere else. The second and the third qubits are previously entangled (one of the EPR pairs presented in Eq. (2.9)). Each horizontal single line represents the evolution of its respective qubit. There are different quantum gates, acting on one or two qubits. There are also two measurements performed on the first and the second qubits. The results of these measurements are communicated to the other party via a classical channel

2.3 Quantum noise

This section is the natural extension of the previous one. In Section 2.2, the evolution of a quantum

[12] In turn, it is easy to see the connection between quantum computing and classical computing.

system and the measurement of its state were studied without taking into account the interaction with the environment. However, from a more realistic viewpoint, this interaction does exist and needs to be considered. To do so, the constraint that the system is closed must be relaxed. In fact, only the system in conjunction with the environment can be treated as closed.

The formulation of the effect that the environment E has on the quantum system Q can be undertaken by different approaches. The most common one is the operator-sum representation. Its main features are the mathematical foundations, the simplicity of the representation and the direct physical interpretation. A detailed deduction of the operator-sum representation using concepts and equations already seen is provided in Appendix A. For this section, it is enough to know the result:

$$\varepsilon\left(\rho^{Q}\right)=\sum_{k}E_{k}\rho^{Q}\left(E_{k}\right)^{\dagger} \tag{2.29}$$

where ρ^{Q} is the initial state of the system Q (given by its density operator), $\varepsilon\left(\rho^{Q}\right)$ denotes the state of the system Q after its interaction with the environment and E_k are the so-called Kraus operators or operation elements for the quantum operation ε.

The physical complexity behind the quantum noise is extraordinarily reduced to the mathematical compactness of Eq. (2.29). This representation can become even more tangible by means of some particular quantum noise models (sometimes called noisy quantum channels). More precisely, for a system Q of dimension two, that is, a qubit, the operation elements for different quantum operations can be found in the literature. For instance, in [14 pp. 376-385] the main types of quantum noise are described. See Table 2.1 for a summary. It is useful in order to get a general insight of the quantum noise mechanisms.

Table 2.1 – Summary of some of the most common quantum noise models.

QUANTUM CHANNEL	KRAUS OPERATORS	DESCRIPTION
Bit flip	$E_0=\sqrt{p}\begin{bmatrix}1&0\\0&1\end{bmatrix}, E_1=\sqrt{1-p}\begin{bmatrix}0&1\\1&0\end{bmatrix}$	It changes the state of a qubit from $\left\|0\right\rangle$ to $\left\|1\right\rangle$ (and viceversa) with probability 1-p.
Phase flip	$E_0=\sqrt{p}\begin{bmatrix}1&0\\0&1\end{bmatrix}, E_1=\sqrt{1-p}\begin{bmatrix}1&0\\0&-1\end{bmatrix}$	When p=1/2, it corresponds to a measurement of the qubit in the standard basis.
Depolarizing	$E_0=\sqrt{1-\frac{3p}{4}}\begin{bmatrix}1&0\\0&1\end{bmatrix}, E_1=\sqrt{\frac{p}{4}}\begin{bmatrix}0&1\\1&0\end{bmatrix},$ $E_2=\sqrt{\frac{p}{4}}\begin{bmatrix}0&-i\\i&0\end{bmatrix}, E_3=\sqrt{\frac{p}{4}}\begin{bmatrix}1&0\\0&-1\end{bmatrix}$	With probability p, the single qubit is depolarized, i.e. replaced by the entirely mixed state I/2.
Amplitude damping	$E_0=\begin{bmatrix}1&0\\0&\sqrt{1-\gamma}\end{bmatrix}, E_1=\begin{bmatrix}0&\sqrt{\gamma}\\0&0\end{bmatrix}$	Associated with the energy dissipation, γ could represent the probability of losing a photon.

Phase damping	$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}, E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}$	Associated with the loss of quantum information, λ could be understood as the probability that a photon from the quantum system has been scattered. This process has been historically known as decoherence, but today the terms decoherence and quantum noise are indistinguishable.

Two important remarks must be made about the noise models presented in Table 2.1. First, note that all of them are defined by a single parameter, which can be though of as a probability. Unfortunately, this parameter is not known unless one has perfect knowledge of his experimental platform. For this reason, these models seem to be more useful for a parameter sweep analysis. Second, thinking specifically about the connection between these types of quantum noise and the physics behind the QKD in specific working conditions, it turns out that a rigorous applicability of these quantum noise models is not easy at all. Without going into details and with the aim of being consistent with the goals and the scope of this work, a high-level approach to take into consideration the imperfections and the error sources is required. Considering various quantum noise models on the one hand, and attenuation sources on the other hand, might be tedious as well as unnatural. Instead, this work will model all the photon losses by the transmission from the source to the detector on the one hand, and will use only the bit flip channel to introduce errors at the receiver side. An additional comment will be made in Section 5.1.2.

2.4 Fundamentals of information theory

While in Sections 2.1 through 2.3 the focus is on the mathematical support of the operation of a QKD, this section is about the tools that are used to prove the security of that operation[13]. The necessity of introducing these tools appears when, from the implementation viewpoint, the length of the final key must be decided. To make it compatible with the agreed level of security, it is important to estimate how much information about the key has been leaked throughout the whole process. Within this context, the field of information theory comes into play.

2.4.1 Information entropy

In order to estimate the leakage of information in the execution of a QKD, or equivalently the knowledge an unwelcome party might have obtained, the first step is to have a magnitude that quantifies the information in terms of probabilities. This magnitude is the entropy. Assuming for now that all the quantum states have already been measured and that, therefore, the discussion is only about classical information (a comment in this regard will be made later in this section), the magnitude is called the Shannon entropy[14].

The Shannon entropy (and the rest of the ideas) can be more easily introduced with the help of the

[13] Recall that all this effort is to build up an infrastructure that provides unconditional security. Therefore, the security implications cannot be left behind. Otherwise, time, money and material resources would be being wasted.

[14] This concept was originally introduced by Claude Shannon in 1948, when he published a paper about the successful transmission of bits over a noisy classical channel [20]. He based the use of the word entropy on the analogy with the entropy formula defined in statistical thermodynamics.

fictional characters Alice, Bob and Eve[15]. Imagine that Alice is able to generate a n-bit string X, statistically modelled as a random variable with a probability distribution $p_1, \ldots, p_N$ (N=2^n). For instance, if n=3, the possible values of X are 000, 001, 010, 011, 100, 101, 110 and 111. The Shannon entropy of X represents the average quantity of information one has gained after learning the value of X, or from a complementary viewpoint, how much uncertainty one had before learning the value of X [20 p. 11]. Mathematically,

$$H(X) \equiv H(p_1, \ldots, p_N) \equiv -\sum_x p_x \log_2(p_x) \tag{2.30}$$

A special case of the Shannon entropy occurs when there are only two possible outcomes. In this case, the Shannon entropy is called the binary entropy. Although these two outcomes could also be two n-bit strings (e.g. if n=3, 001 and 110), the case of a single bit is of more interest here. The formula becomes

$$H(X) \equiv H(p) \equiv H_{bin}(p) \equiv h(p) \equiv -p\log_2 p - (1-p)\log_2(1-p) \tag{2.31}$$

Pay attention to three details: first, the use of $h(\cdot)$ is frequently used instead of $H(\cdot)$; second, the existence of a single parameter p since there are just two possible outcomes; third, the binary entropy illustrates more easily the fact that the Shannon entropy is zero[16] when the variable is deterministic, that is, when either p or (1-p) is 1, and, on the contrary, is maximum if p=1/2 (maximum uncertainty).

Now, think of Bob and Eve. Bob wants to receive correctly the n-bit string sent by Alice, whereas Eve attempts to obtain the same but illegally. It is important to know the mutual information between Alice and Bob as well as between Alice (or Bob) and Eve. In symbols,

$$I_{ij} \equiv H(X_i : X_j) \equiv H(X_i) + H(X_j) - H(X_i, X_j) \tag{2.32}$$

where I_{ij} is the mutual information between i and j (i,j=A, B, E, standing for Alice, Bob and Eve), X_i and X_j are the random variables at disposal of i,j and $H(X_i, X_j)$ is called the joint entropy, because it is defined by the joint probability distribution of X_i and X_j, which is, in turn, related to the conditional entropy by

$$H(X_i \mid X_j) \equiv H(X_i, X_j) - H(X_j) \tag{2.33}$$

Although the expressions have not been proved, it is not difficult to do it by means of some basic properties of the probability theory [20 p. 12]. The most useful aspect is to understand these magnitudes with the help of their meanings (knowledge gained after the measurement or uncertainty existent before the measurement). Without going into details, it is obvious that the aim is to maximize I_{AB} and to minimize I_{AE} and I_{BE}.

After having introduced the Shannon entropy, it is time to clarify why the discussion turned into classical information. The reason is the scope of this work once again. It is assumed that the avesdropper perfoms the measurement right after intercepting the quantum signal, therefore, at the point of the post-processing, the eavesdropper only holds classical information. In the case of being able to store the quantum signals waiting for a privileged position, the study should make use of the so-called Von Neumann entropy. Just to show that it represents a generalization of the Shannon entropy, see its expression (using the letter S instead of H)

[15] These characters, and others such as Charlie, are typically used in the fields of cryptography and physics for the sake of understanding. Each one has a specific function: Alice and Bob are the sender and the receiver, respectively, of certain message; Eve plays the role of an eavesdropper; and Charlie sometimes appears to help Alice and Bob carry out their secure communication.

[16] Defining $0\log_2 0 \equiv 0$.

$$S(\rho) = -\mathrm{tr}(\rho \log_2 \rho) \tag{2.34}$$

When the involved quantum states are orthogonal, the Von Neumann's entropy coincides with the Shannon entropy, as one might infer by remembering that the measurement of the states $|0\rangle$ and $|1\rangle$ always yields $|0\rangle$ and $|1\rangle$ respectively, as classically expected. As well as the Shannon entropy and the Von Neumann entropy, there are other entropy definitions such as the Rényi entropy, the min-entropy or the max-entropy, which are used in the security proofs to deduce unconditional security bounds. Definitely, the definitions of those entropies and the relations among them are out of scope. However, take the so-called Holevo bound (upper bound on the accessible information) [14 p. 531] as an example:

$$I_{ij} \equiv H(X_i : X_j) \leq S(\rho) - \sum_x p_x S(\rho_x) \equiv \chi \tag{2.35}$$

where χ is known as the Holevo quantity and $\rho = \sum_x p_x \rho_x$.

2.4.2 The coding problem

The concept of information entropy is mainly useful at the end of the QKD protocols. This step is called the privacy amplification and will be explained later in Section 3.6. However, there is another step that uses the information entropy but from a slightly different perspective. More precisely, this step is the information reconciliation or error correction (explained in Section 3.4), which makes use of the idea behind the coding problem.

The coding problem sets out the situation of a sender with a classical information source able to generate the sequential random variables X_1, X_2, …, which are independent and identically distributed [14 p. 537]. This sender wonders how short the encoding of X_i could become allowing an eventual receiver to reliably reconstruct the original message. The answer of this problem is given by the Shannon's noiseless channel coding theorem, according to which any compression scheme will be realible as long as the rate R is greater than $H(X)$ [20 p. 16]. In other words, $H(X)$ is the minimal number of bits which is necessary to faithfully reproduce the message.

At this point, there are four things that may sound confusing. First, X is a random variable that follows the same probability distribution as X_1, X_2, … Second, each X_i represents a single bit, whose value is a priori unkown, therefore $H(X)$ is here the binary entropy (in this case, the symbol $H(\cdot)$ is typically used). Third, it is common to refer to R and $H(\cdot)$ as rates. However, the rates are not bits per second, but rates of compression, that is, the ratio between the lengths of the encoded message and the original message. For instance, if a sequence of n bits is considered, then the length of the initial message is n, the length of the encoded (or compressed) message is nR and the minimal length of the encoded message so that it can be reconstructed is $nH(X)$. Fourth, the application of this theorem in the information reconciliation step makes sense because the classical channel is assumed noiseless, as described later in Section 3.1.

Nevertheless, the situation mentioned in the penultimate paragraph is not exactly the one that is relevant for information reconciliation, although it is a good starting point. Instead of only one classical information source, imagine that there are two. One belongs to Alice and the other to Bob. The sequence of random variables associated with each source are again independent and identically distributed, and, in addition, correlated between them. Expressed in a different but more familiar way, this is equivalent to say that Alice sends her sequence of bits to Bob, who receives the same sequence except for the errors. If both of them are interested in correcting the errors, it is important to know the minimal number of bits that are required for this additional noiseless communication. The answer to this generalized question was provided by Slepian and Wolf in [21] with the idea that the encoding of X_A must be at least $H(X_A \mid X_B)$ in order to be successful. This limit can be further transformed assuming that the behaviour of the difference between X_A and X_B can be modelled by a binary symmetric channel (BSC) with parameter the quantum bit error rate (QBER). Have a look at Figure 2.4.

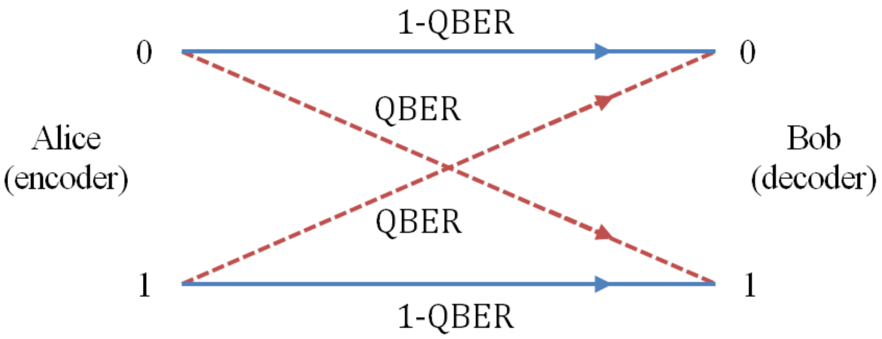

Figure 2.4 – Binary symmetric channel. In this model, a bit flip happens with a crossover probability QBER, whereas the correct bit value is sent with a probability 1-QBER.

Although this simple model is widely used in the field of classical communications, it is also common in QKD, where the used parameter is the one that has already been introduced, the QBER, which represents the ratio between the number of erroneous bits and the total number of bits received by Bob. This model permits to express $H\left(X_A \mid X_B\right)$ as simply h(QBER) (in this case, the use of the small letter h is widespread to refer to the binary entropy). The proof of this equivalence can be found in Appendix B.

Before going to the next chapter, a final comment is necessary.The concepts covered in this section, (in particular, the combination of the different uses of the Shannon entropy, the various entropy definitions, the classical communication notions right after having read many ideas about quantum objects, the introduction to error correction through a noiseless classical channel, etc.) may sound confusing and even shocking the first time. The information theory is not easy at all, and much less when there is a mixture of quantum and classical aspects. However, the detailed description of QKD presented in Chapter 3 will make it easier to understand the *whens* and *whys* of this section.

3 Theoretical framework of QKD

3.1 Principle of QKD

The purpose of QKD is to exchange an unconditionally secure key between two separated parties, typically Alice and Bob. This distribution is completed after two phases. The first phase demands that Alice and Bob are connected through a quantum channel. Alice encodes her raw key bits in light[17] degrees of freedom and sends them to Bob through this channel, which may be untrusted because of the presence of an eavesdropper Eve, as well as being noisy. Afterwards, Bob receives a part of the quantum signals sent by Alice due to the losses along the optical path and decodes them, obtaining a raw key. For the second phase, it is necessary that Alice and Bob have access to an authenticated[18] classical channel. Traditionally, it is assumed that this channel is also noiseless without loss of generality. With the help of a one-way or two-way classical communication[19], a classical information post-processing is carried out to transform the raw keys into a shared secret key. If that is not possible, the protocol is aborted. See Figure 3.1 to get a picture of this description.

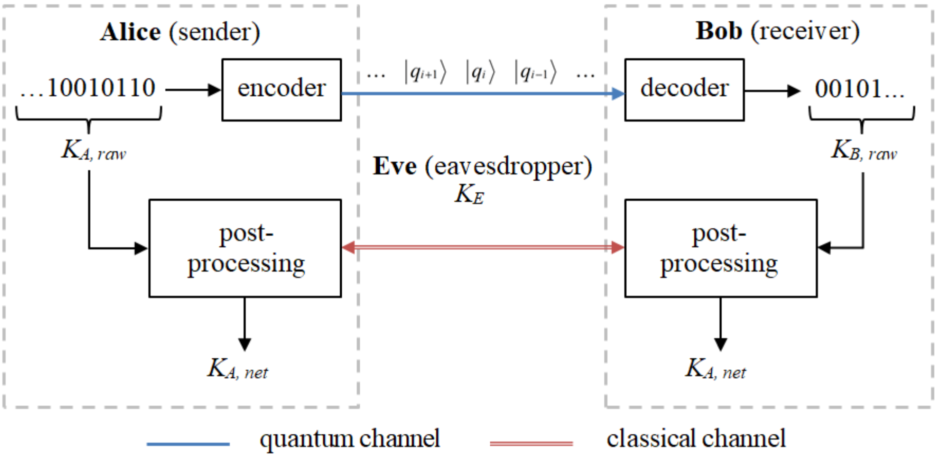

Figure 3.1 – Schematic illustration of a generic QKD protocol. $K_{i,\,raw}$ denotes the non-secret key before the post-processing (with i=A, B), K_E is the knowledge Eve has of $K_{i,\,raw}$ and $K_{A,\,net}$ denotes the shared secret key after the post-processing. On the other hand, pure states are plotted over the quantum channel without loss of generality.

[17] Light is the usual information carrier because it permits a separation between the parties and suffers from fewer interactions with matter.

[18] The authentication implies that Eve might listen to the conversation, but she could never take part in it [22 p. 3].

[19] Unlike in two-way post-processing, in one-way procedures only one of the agents involved in the QKD (typically Alice) can send information to the other, without feedback [22 p. 21].

Unlike traditional cryptographic protocols, the security of QKD protocols is guaranteed by physics. The fact that the signals can become modified by Eve's actions through the quantum channel reveals the leakage of information. Additionally, quantum states cannot be copied as happens with bits in a classical computer, according to the no-cloning theorem [22 p. 3].

In relation to the post-processing, the errors in Bob's raw key are corrected and the leaked information is addressed. With all the estimated information thoughout the different steps, Alice and Bob generate a key that is probabilistically secure at the cost of a key which is shorter than Bob's raw key [22 p. 9].

3.2 Classification of QKD protocols

QKD can be implemented following a variety of protocols. There exist different classifications of such QKD protocols. One of them divides the protocols into discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD), depending on the nature of light. The DV-QKD protocols deal with the particle nature of light, whereas the CV-QKD protocols use its wave nature [23 p. 1]. More precisely, in DV-QKD protocols, the information carrier is the photon by means of its degrees of freedom (polarization, energy, phase, arrival time, orbital angular momentum, entanglement, etc.). In contrast, in CV-QKD protocols, information is randomly encoded in the quadrature components of an optical field [24 p. 2], that is, in the terms Q and P of the following expression:

$$\boldsymbol{E}(\boldsymbol{r},t)=\boldsymbol{e}\|\boldsymbol{E}\|\left[Q\cos(\boldsymbol{kr}-\omega t)-P\sin(\boldsymbol{kr}-\omega t)\right] \tag{3.1}$$

Eq. (3.1) represents an electric field which is solution of Maxwell's equations for the case of monochromatic[20] plane[21] waves. $\boldsymbol{E}$ is the electric field vector, $\|\boldsymbol{E}\|$ is its norm, $\boldsymbol{e}$ is the polarization orientation, $\boldsymbol{k}$ is the wave vector, $\boldsymbol{r}$ is the position vector, ω is the angular frequency, Q is the position quadrature and P is the momentum quadrature.

As for the measurement techniques, while a single photon detector is used in DV-QKD, either homodyne or heterodyne detection[22] are employed in CV-QKD [23 p.1]. The use of these detection methods presents various advantages and disadvantages. On the one hand, single photodetectors require cooling and are commonly expensive and sensitive to stray light. On the contrary, homodyne receivers do not need cooling, are cost-effective, insensitive to stray light and, in addition, exhibit higher key rates[23] [23 p. 1; 27 p.5]. These arguments might make the choice easy, but unfortunately, CV-QKD has two major disadvantages: the distance is more limited due to the poor reconciliation efficiency and the excess noise[24] [29 p. 1] and the security proof is less advanced [30]. Despite the fact that an exhaustive analysis of the security proofs is beyond the scope of this work, one could easily infer the main reason: it is impossible to divide a single photon in DV-QKD, whereas the amplitude may be reduced by an eavesdropper in CV-QKD, in such a way that there is no difference between her action and a lossy quantum channel [23 p.2]. A general outline of the security proofs will be provided for the case of DV-QKD in Section 3.5.

Additionally, there exists a difference between the security of the DV-QKD schemes and the CV-QKD schemes. On the one hand, the unconditional security of DV-QKD is based on the

[20] In monochromatic waves, only one wavelength (or frequency) component exists.

[21] In plane waves, the propagation direction does not depend on the spatial coordinates.

[22] Without going into details, both homodyne and heterodyne detection techniques are ways of demodulating phase-encoded (and/or frequency-encoded) signals by the comparaison with a local oscillator signal [25].

[23] It is difficult to compare key rates for both DV-QKD and CV-QKD, since the experiments have not been performed in similar years and distances, and once a goal is achieved, the next goal is usually much more ambitious. Nevertheless, according to Figure 5 of [26], CV-QKD offers key rates in the range 0-20km that are ten times higher than in DV-QKD.

[24] At the time of working on this project, a new distance record by optical fiber has been published, doubling the previous distance, with 202.81km and a secret key rate of 6.214 bps [28]. More details about the space missions using CV-QKD can be found later in this section.

indistinguishability of non-orthogonal quantum states and the no-cloning theorem (already viewed in Section 2.2). On the other hand, the unconditional security of CV-QKD is supported by Heisenberg's uncertainty principle (mentioned in Section 1.1), which prevents Eve from having full knowledge of both quadratures at the same time [31 p. 214].

Although this work focuses on a particular DV-QKD protocol, the so-called BB84, it is interesting to remark the existence of various protocols. In the case of DV-QKD, some of the most known protocols are[25] BB84 [32], E91 [33], B92 [34] and BBM92 [35]. Somehow, most of them present similarities with the BB84, which was the first QKD protocol published in 1984. More details about this protocol will be provided in the next section. The same BB84 protocol can be implemented by using different degrees of freedom[26] of the photon as mentioned in the first paragraph of the current section. Moreover, there are additional versions of the BB84 protocol which include improvements against specific attacks such as the decoy-state BB84 [38] for the photon-number splitting attack. In the case of CV-QKD, on the other hand, the protocols can be subdivided into coherent state-based and squeezed state-based[27]. This last group presents the difficulty that the generation of squeezed states is technologically challenging [27 p.5]. In turn, there exists a lower classification into discrete protocols (e.g. the four-state protocol [23]) and Gaussian[28] protocols (e.g. the GG02 protocol [41]), whose practical implementation and security study are more advanced [23 p. 2].

Another classification of the protocols is possible considering how Alice and Bob obtain their raw keys. If Alice creates her own raw key by randomly generating a bit string and then she encodes it into optical signals, which are sent to Bob, who decodes them, finally obtaining his raw key, the protocol is refered as prepare-and-measure. In contrast, one finds the entanglement-based[29] protocols. In this case, a third party typically called Charlie distributes entangled quantum states to both Alice and Bob. As they receive them and perform the measurements, they obtain their corresponding raw keys [22 p. 8]. Notice that the entanglement-based protocols present an additional level of security because there is no need for untrusted nodes [43 p. 31]. A case in between occurs when it is Alice who generates the entangled states, keeping one part, and sending the other to Bob. By convention, this type of protocols is also known as prepare-and-measure.

Focusing on the DV-QKD schemes, the two most known prepare-and-measure protocols are the BB84 and the B92. In fact, the B92 is a simplification (at the expense of being less secure) of the BB84, considering only two states instead of four as will be described in the following section. On the other hand, the two most known entanglement-based protocols are the E91 and the BBM92. In particular, the BBM92 is the entanglement-based version of the BB84 [42 p. 2].

With all the former information in mind, it is time to see the state of the art in the QKD missions in space and in the atmosphere. To that end, see first Figure 3.2, where several examples of satellite QKD are illustrated. The same applies for different vehicles such as airplanes or hot-air balloons. And now, go to Table 3.1 to gain a general insight.

[25] The name of a protocol is formed by the initials of its authors and the year it was published.

[26] Typically, only one degree of freedom, say polarization or phase, is employed. However, with the objective of increasing the key rate, the photon can be exploited by using more than one (e.g. time and phase [36]), but also with degrees of freedom which span a higher-dimension Hilbert space (e.g. orbital angular momentum [37]). In any case, the dimension of the Hilbert space spanned by these two options is higher than two, i.e. the quantum state vectors are in $\mathbb{C}^d$ (recall the term qudit). This has a second effect, consisting of d (or even d+1) possible bases (not only the standard and the diagonal ones), what means a higher level of security [37 p. 2].

[27] The basic difference between coherent states and squeezed states comes from the fact that, while coherent states present the same fluctuations in both quadrature components, squeezed states have more noise in one quadrature than in the other [39].

[28] In a Gaussian protocol both quadratures behave as two random variables following zero-centred normal distribution [27 p. 9]. In contrast, in a discrete protocol, a set of states (e.g. four, eight…) around the zero is used for encoding the information [40].

[29] In the vast majority of cases where entanglement has been used, the technique employed for the generation of entangled photon-pairs was SPDC (go back to Figure 1.2) [42 p. 4].

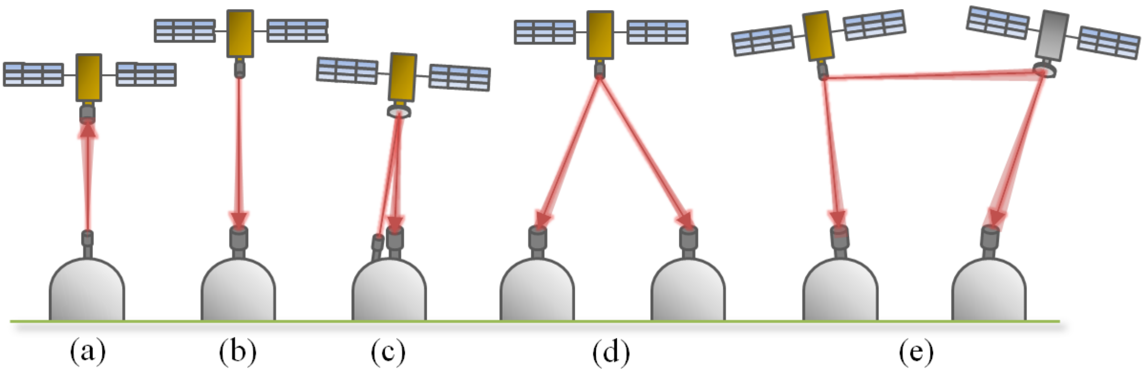

Figure 3.2 – Schematic illustration with various scenarios of satellite QKD. In scenario (a), a ground-to-satellite QKD is shown (uplink); in scenario (b), a satellite-to-ground QKD is represented (downlink); in scenario (c), a downlink is simulated with the help of retroflectors in the satellite; in scenario (d), a satellite distributes entangled photon pairs to Alice and Bob (different ground stations); and in scenario (e), an example of satellite-satellite interaction is depicted.

Table 3.1 – Summary of aerospace missions related to the implementation of QKD protocols.

LAUNCH/ FLIGHT YEAR	COUNTRIES	VEHICLES (NAMES)	QKD PROTOCOL	SCENARIO (see Figure 3.2)	REF.
2008	Italy	Satellites (Jason-2, Larets, Starlette and Stella)	Feasibility tests for decoy-state BB84	LEO (c)	[44]
2010	China	Hot-air balloon (-)	Decoy-state BB84	100km approx. (b)	[45]
2011	Germany	Airplane (Dornier 228)	BB84	20km approx. (b)	[46]
2016	Germany	Satellite (Alphasat I-XL)	Feasibility tests for DV-QKD using phase encoding and CV QKD using coherent states with Gaussian modulation	GEO (b)	[47]
2016	China	Satellite (Tiangong-2)	Decoy-state BB84	LEO (b)	[48]
2016	China	Satellite (Micius)	Decoy-state BB84, BBM92	LEO (b) (d)	[49-50]
2016	Canada	Airplane	Decoy-state BB84	3km, 5km, 7km,	[51]

		(DHC-6 Twin Otter)		10km (a)	
2016	Japan	Satellite (Socrates)	B92	LEO (b)	[52]
2019	Singapore	Satellite (SpooQy-1)	Feasibility tests for BBM92	LEO (d), but onboard receivers	[53]
2020	Germany	Satellite (QUBE)	BB84	LEO (b)	[54]
2021	UK, Singapore	Satellite (QKD Qubesat)	Not found	Not found	[55]
2021	Canada	Satellite (NanoQEY)	BBM92	LEO (a)	[56]
2022	France, Austria	Satellite (NanoBob)	BB84, decoy-state BB84, E91	LEO (a)	[57]
Funded mission	Canada	Satellite (QEYSSat)	BB84, BBM92	LEO (a) (b)	[58]
Funded mission	Singapore	Satellite (SpooQy-2)	Not found	Not found	[59]
Funded mission	Germany, Luxembourg, Austria, Switzerland, the Czech Republic, the Netherlands (public-private partnership)	Satellite (QUARTZ)	Not found	Not found	[60]
Funded mission	UK	Satellite (QKDSat)	Not found	Not found	[61]
Proposal	Belgium, Germany, Italy, Luxembourg, Malta, the Netherlands, Spain, Croatia, Cyprus, Greece, France, Lithuania, Slovakia, Slovenia, Sweden, Finland	One or several satellites	Not found	Not found	[62]

	(public funding)				
Proposal	US	Satellite (ISS)	Superdense teleportation (SDT)[30]	LEO (d)	[64]
Proposal	Switzerland, Germany, UK (private partnership)	Stratospheric long endurance vehicles	Not found	Not found	[65]
Proposal	UK, Singapore, Italy, Germany, the Netherlands, Switzerland, Austria	Satellite	BB84, BBM92	LEO (b)	[66]

Needless to say, there are many more tests that have been perfomed in relation to satellite QKD but are not shown in Table 3.1. Only those missions focused on the implementation of QKD protocols were considered here.

On the other hand, from Table 3.1, a few ideas can be extracted. First, much more effort has been devoted to the demonstration of DV-QKD protocols. Second, BB84 (its decoy-state version), and its entanglement-based counterpart BBM92, have been widely implemented. Third, there is a trend towards entanglement-based protocols, satellites which are capable of running more than one protocol and quantum superdense coding (exploiting the photon). Additionally, the agreements among companies and countries are more and more frequent.

For all the above-mentioned reasons, the choice of BB84 is a good starting point for this work. In particular, the BB84 with polarization encoding will be used, because it has been widely adoped since it was proved that polarization is preserved through free-space [52 p. 504]. The major issue of this encoding is, however, the fact that polarization depends on a reference frame and every misalignment is a source of error. On this matter, the use of alternative or additional degrees of freedoms, such as time bins or orbital angular momentum is being studied [53; 63], but is entirely beyond the scope of this work.

3.3 The Bennett-Brassard protocol (BB84)

As was pointed out in the previous section, the first QKD protocol was published by Charles H. Bennet and Gilles Brassard in 1984 [32]. This protocol is known as BB84 and since then, it has been widely implemented. When single polarized photons are used for coding, two non-orthogonal states (that is to say, two different bases) are used to encode each bit, 0 and 1 (in total four non-orthogonal states). Using the symbols $|H\rangle$ and $|V\rangle$ for the horizontally and vertically polarized photons instead of $|0\rangle$ and $|1\rangle$, and the symbols $|+45\rangle$ and $|-45\rangle$ for the diagonally polarized photons instead of $|+\rangle$ and $|-\rangle$, the coding of bits is built up as shown in Table 3.2.

[30] SDT is a new entanglement-based protocol which uses the idea of high-dimension quantum states to generate photon pairs hyperentangled in polarization and orbital angular momentum (or time bins), overcoming the effects of noise and losses [63].

Table 3.2 – Coding of bits in the BB84 protocol.

BIT	BASIS	QUANTUM CODING
0	Standard $(+)$	$\|H\rangle$
	Diagonal $(\times)$	$\|+45\rangle$
1	Standard $(+)$	$\|V\rangle$
	Diagonal $(\times)$	$\|-45\rangle$

With the previous coding in mind, the quantum transmission is as follows [32 p. 177]:

1. Alice selects a random *n*-bit string (formed by ones and zeros) and a random sequence of *n* polarization bases (standard or diagonal).
2. She then encodes each bit of the string in the corresponding basis of the chosen sequence of bases (Table 3.2), sending the photons to Bob one after the other.
3. Bob receives each photon and performs a measurement in a randomly decided basis, which may be the same one as Alice chose or a different one. Depending on the outcome, Bob writes down a zero or a one (Table 3.2).

An example with all the possible combinations for the bit 0 is illustrated in Table 3.3. The case of bit 1 is analogous.

Table 3.3 – Examples of quantum transmission for the bit 0.

Alice's bits	0	0	0	0	0	0
Alice's sequence of bases	+	+	+	×	×	×
Quantum coding	$\|H\rangle$	$\|H\rangle$	$\|H\rangle$	$\|+45\rangle$	$\|+45\rangle$	$\|+45\rangle$
Bob's sequence of bases	+	×	×	+	+	×
Bits decoded by Bob	0	0	1	0	1	0

Observe that whenever Bob selects the same basis as Alice, he obtains the right bit. On the contrary, if he chooses a different basis from Alice, he obtains the right bit only fifty percent of the times. Taking such errors into account and also those due to the noisy quantum channel and the presence of an eavesdropper (it is not too difficult to imagine the consequences in Bob's string after having viewed Table 3.3), the necessity of an information post-processing is justified.

The classical information post-processing consists of several steps, namely: authentication, sifting (or basis reconciliation), error estimation, error correction (or reconciliation), confirmation and privacy amplification. The steps error estimation, error correction and confirmation are sometimes put together, but that does not make them less important. Figure 3.3 is a helpful diagram.

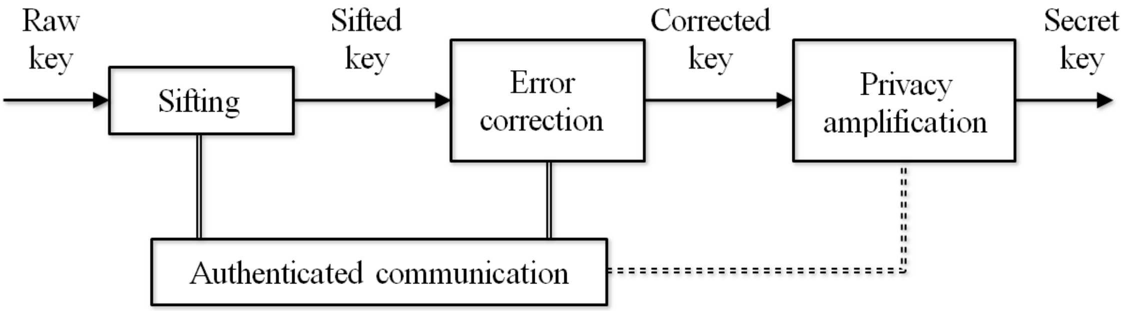

Figure 3.3 – Diagram with the steps of the classical information post-processing.

After more than thirty-five years since the publication of the BB84 protocol, the quantum transmission remains the same, but the classical post-processing has experienced some slight modifications with respect to Bennett and Brassard's first version. Basically, the changes concern the user who initiates the exchange of information, who sends it and who listens to the other, etc. Most times, they are just a matter of the technology which is in reach. Another important reason is that those modifications satisfy the necessity of minimizing the leakage of information. In any case, a detailed description of the above-mentioned steps is provided below.

First of all, the discussion in the post-processing needs to be authenticated as already stated in Section 3.1. There exist a variety of authentication methods. Among them, the uses of fingerprints, digital signatures, voice or facial recognition are options in ongoing research, whereas a shared secret key is usually employed. This key may be originated in the previous round of QKD, what introduces the need for a pre-shared key in the first round, and only has to be secure until the next round [22 p. 8]. The way to authenticate the communication with the help of a key is by appending a tag to each exchanged message (not only at the beginning of the post-processing). This tag is the result of some calculation over the key. Unfortunately, more details about the procedure are out of scope, although they can be found in [67].

Once Bob has his raw key, Alice and Bob share the bases they used to encode and decode the key bits, discarding those positions where they used different ones. Typically, it is Bob who sends his bases to Alice and she announces the ones that were correct, since, with the losses, he has much less information to exchange (also looking for efficiency). Anyway, it is vital not to disclose the values of the bits over the public channel, only the bases they employed. This stage is known as sifting or basis reconciliation, and at the end, the length of the sifted key is approximately half as large as Bob's raw key. If this condition is not met, either the length of Bob's raw key was clearly insufficient or the randomness was too poor. For these reasons, the raw key rate (in bits per second) or the sifted key rate (in bits per second) should be monitored.

After the sifting, Alice and Bob share the same sifted key, except for the errors in Bob's string. At this point, it is convenient to estimate these errors, commonly in the shape of the QBER parameter (errors over length of the sifted key). In order to make such estimation, a number of bits must be exchanged between Alice and Bob, and therefore, discarded. The size of this sacrifice of bits is not a petty matter, because the shorter the final key is, the less secure it becomes. In some papers such as [84], as a first approach, half the sifted-key length is used for the estimation. However, it is clear that a good estimation could be made with fewer bits so long as the sifted key is large enough, or with the help of a typical value of QBER. Each bit matters. In this sense, there are several methods that even allow an on-the-fly estimation of the QBER during the reconciliation [69]. In any case, the QBER must be estimated because of two reasons: the performance of the chosen error-correcting code depends on this value (in fact, it is an input to determine its main parameters); and the unconditional security of the BB84 (it also happens with the rest of protocols) is subject to the value of QBER (beyond a certain threshold[31], the privacy amplification is useless). In this work, a deep study of specific error-estimation methods is out of scope, and a sacrifice of half of the bits will be implemented for the sake of simplicity.

In relation to the reconciliation step, there are various criteria to select the best error-correcting method [70 pp. 3-6; 71 pp. 299-300]: efficiency, adaptability and robustness. It must be efficient from the viewpoint of the speed, what translates to minimal computational and communication resources, as well as in terms of the additional information revealed during the reconciliation protocol over the bare minimum. Typically, this last definition of efficiency is mathematically formulated as follows

$$f_{EC} = \frac{m}{nH\left(X_A \mid X_B\right)} \underset{\text{If BSC(QBER)}}{=} \frac{R}{h\left(\text{QBER}\right)} \tag{3.2}$$

where f_{EC} denotes the reconciliation efficiency, m is the number of bits exchanged between Alice and Bob in the reconciliation, n is the length of Alice and Bob's strings after sifting and error estimation (also known as frames), $R=m/n$ is the compression rate, X_A and X_B are random variables which represent single bits in Alice and Bob's strings respectively and $H\left(X_A \mid X_B\right)$ is the conditional entropy introduced in Subsection 2.4.1, which here represents the minimal amount of information that needs to be exchanged to correct a single bit, as exposed in Subsection 2.4.2. In the case of a BSC with parameter QBER, $H\left(X_A \mid X_B\right) = h\left(\text{QBER}\right)$, as proved in Appendix B.

Additionally, the error-correcting protocol should present some adaptability against changes in the length of the strings and in the QBER, and of course robustness. In practice, the robustness can be defined either as the probability that at least one error remains after the reconciliation or as the ratio between the number of remaining errors and the frame length (residual error rate).

In order not to make this section too long, the description of the error-correcting methods is left for the next section. Here it suffices to say that the reconciliation protocols are not exempt from a probabilistic nature. More concretely, depending on the chosen method, it might happen that either the error-correcting method fails, or it succeeds but yielding a wrong solution. For that reason, a confirmation step is vital. This confirmation is usually performed with the help of some pre-established hash function [72 p. 17]. This function takes as input the presumably corrected key and returns some set of bits. For instance, Bob sends his result to Alice, who compares it with hers. If they are coincident, she notifies Bob the confirmation. Otherwise, she announces that the reconciliation failed. The hash functions together with the confirmation step will be explained in Subsection 3.4.3.

Before explaining the last step, notice that, at this point, the corrected key should have approximately as many zeros as ones. If not, perhaps the randomness is too poor and the consequence is that the probability that an eavesdropper guesses the key is higher. In an ideal case, the probability that a bit is zero is the same as the probability that a bit is one. Therefore, the probability of guessing an n-bit key is $1/2^n$. However, when there exists a bias (e.g. the number of ones is much higher than the number of zeros), it is easy to see that the probability of guessing the key becomes higher. This fact brings into light once again the importance of a suitable random number generator to create Alice's raw key.

The former also helps introduce the probabilistic nature of the security of the final key. After all, the unconditional security of QKD announced so many times is limited by certain probability. Unfortunately, this probability (from the viewpoint of an eavesdropper) is higher than the value $1/2^n$

[31] A threshold of 11% is typically employed in one-way procedures. This value is obtained by using the notions of mutual information introduced in Subsection 2.4.1 together with an unconditional security bound. More details can be found in Appendix A of [22].

exposed in the previous paragraph. This is because of the information leaked throughout the discussion between Alice and Bob in the post-processing, as well as the information obtained by the eavesdropper through attacks. This increase in the probability of guessing the key can be controlled precisely by the privacy amplification. Taking the corrected key as input and making an estimation of the leaked information, this step returns a key that is probabilistically secure according to a specific security proof. The privacy amplification will be described in detail in Section 3.6, right after having explained the main ideas behind a security proof in Section 3.5.

3.4 Information reconciliation

The approaches typically used in QKD information reconciliation are two: the Cascade protocol and the Forward Error-Correction (FEC) technique. While the former was specifically proposed for QKD in 1994 [73], the latter was adapted from the classical communication context. The main difference between them is that the Cascade protocol is an interactive protocol (that is, a two-way protocol), which requires a number of communication rounds between Alice and Bob, unlike the FEC codes, which are one-way error-correcting protocols where, in general, only one communication round is required.

It is clear, according to the feature mentioned in the previous paragraph, that FEC codes are much more efficient in terms of computational and communication resources. From the viewpoint of a FSO QKD between a LEO satellite and an optical ground station (OGS), where the visibility window is short (e.g. less than 14min for an altitude of 1000km), the FEC approach is preferable. Nevertheless, FEC codes only work (if it does not fail) in a narrow range around the provided estimation of QBER [74], whereas the Cascade protocol shows robustness in the range between 0 and 15% [73 p. 419] even if the initial estimation turned out to be too poor [70 p. 15] (although it is true that it becomes a bottleneck when the error rate is high). For this reason, taking into consideration that the high dependency on the QBER estimation in the case of FEC codes means a higher cost of bits in the error-estimation step, and that the possibility of using higher-altitude satellites or a satellite constellation in the future might make the interactive behaviour of the Cascade protocol less significant, both approaches are implemented in this work. Do not confuse this decision with the intention of applying more than one error-correcting method in the same QKD round, which would be catastrophic from the viewpoint of the information leaked during the reconciliation.

Despite the many modifications (not necessarily improvements [70 p. 3]) the Cascade protocol has experienced since it was published, this work only covers the original version. On the other hand, among the number of variants of FEC codes already employed in QKD, this work focuses on Low-Density Parity-Check (LDPC) codes. More precisely, the LDPC code described in [71] is the chosen one, because it has already been used in space experiments such as [48] and the leakage of information during the reconciliation is only slightly higher than with the Cascade protocol.

A pragmatic description of the two above-mentioned protocols is provided below, leaving the technical explanaitions for the curious reader.

3.4.1 The Cascade protocol

For the sake of consistency with the notation already introduced, suppose Alice's n-bit frame is denoted by A and it is formed by the bits $X_{Ai}=\{0,1\}$. Similarly, Bob's n-bit frame is denoted by B and it is formed by the bits $X_{Bi}=\{0,1\}$.

The basic idea behind this protocol is to divide the frames into blocks, comparing the parities in Alice and Bob's blocks. In the case of being coincident, Bob can claim that his corresponding block has either an even number of errors or not a single one. In the case of paritiy mismatch, Bob can find one error with the help of the auxiliary search function BINARY, making that block contain either an even number of errors or not a single one after having corrected it. This process is repeated several times, updating the size of the blocks in each pass and shuffling the bits randomly to find new errors.

In the passes subsequent to the first one, this protocol takes advantage of the implication of correcting a new error over the parity of Bob’s blocks that contained that bit in the previous passes. It is obvious that if the parities of those blocks were left being coincident with the corresponding parities of Alice’s blocks, the correction of a new error in the last pass makes those parities become different and, therefore, new errors can be found in all those blocks by using BINARY. Notice that these new corrections unmask, in turn, additional errors for the same reason, producing thus a cascade of corrections which give rise to the name of the protocol.

The function BINARY works similarly to how Bolzano’s theorem allows to find one root of an equation in a certain interval. The main difference lies in comparing parities instead of signs. A flowchart describing the interactive process from Bob’s perspective is illustrated in Figure 3.4.

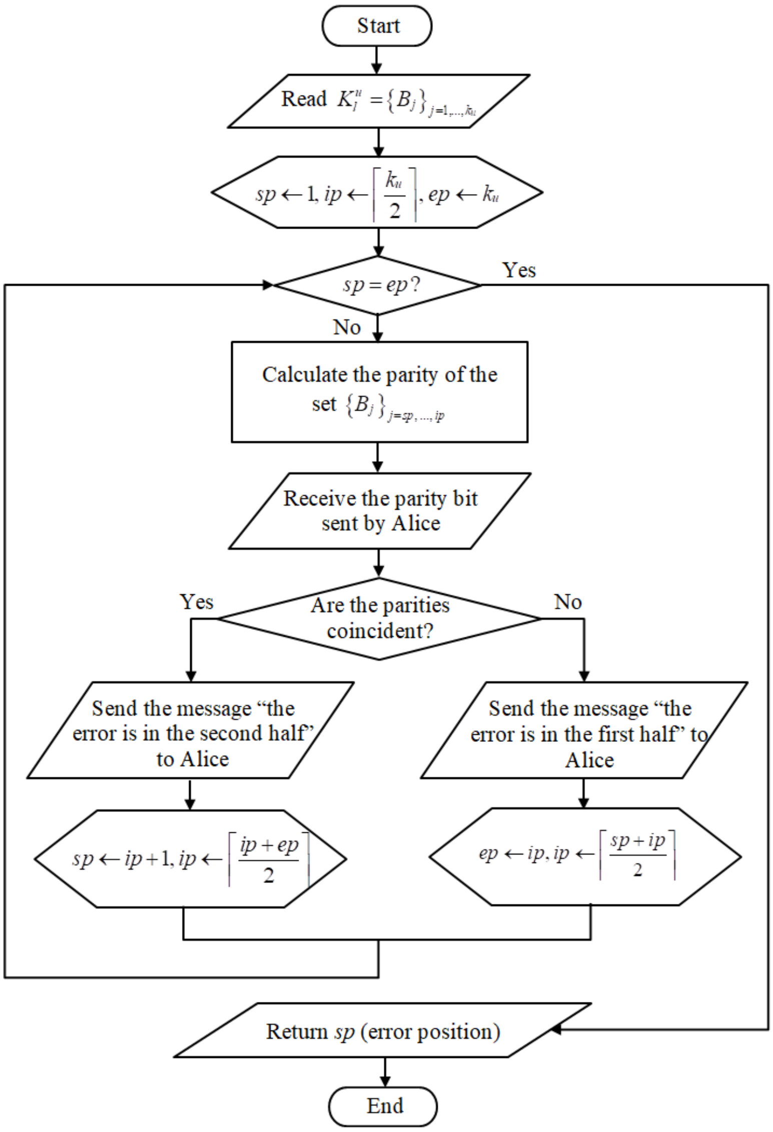
Start
Read $K_l^u = \{B_j\}_{j=1,\dots,k_u}$
$sp \leftarrow 1, ip \leftarrow \left\lceil \frac{k_u}{2} \right\rceil, ep \leftarrow k_u$
$sp = ep?$
Yes
No
Calculate the parity of the set $\{B_j\}_{j=sp,\dots,ip}$
Receive the parity bit sent by Alice
Yes
Are the parities coincident?
No
Send the message “the error is in the second half” to Alice
Send the message “the error is in the first half” to Alice
$sp \leftarrow ip+1, ip \leftarrow \left\lceil \frac{ip+ep}{2} \right\rceil$
$ep \leftarrow ip, ip \leftarrow \left\lceil \frac{sp+ip}{2} \right\rceil$
Return *sp* (error position)
End

Figure 3.4 – Flowchart showing how to perform the binary search. K_l^u denotes the block *l* in pass *u*; k_u denotes the size of the blocks in pass *u*; *sp*, *ip* and *ep* represent the starting, intermediate and ending positions, respectively; and *j* may be different from *i* if the bits were randomly shuffled.

An important remark about the binary search is that the information leak is at most $\lceil \log_2 k_u \rceil$ bits.

With respect to the values of the parameters involved in the Cascade protocol, the same paper [73 pp. 420-422] provides almost all of them. In the first pass, the size of the blocks is k_1 (the last one can be smaller). Pass after pass, the size of the blocks doubles, that is, $k_u=2k_{u-1}$ where u depicts the index of passes. Moreover, the necessary number of passes is given by the experience of the authors and is equal to 4 (as long as the size of the block is smaller than the size of the frame, obviously).

In order to explain how to calculate k_1, it is useful to introduce two concepts before. First, the probability that after the pass $u \geq 1$, $2e$ errors remain in K_l^1 (block l in pass 1) is represented by $\delta_u(e)$. To determine $\delta_1(e)$, the following expression can be used

$$\delta_1(e) = p(X = 2e) + p(X = 2e+1) \tag{3.3}$$

where X is approximated by a random variable that follows a binomial distribution with parameters k_l and $\overline{\text{QBER}}$ (estimation of the QBER). Second, the expected number of errors in the block K_l^1 after the pass u is denoted by E_u. Again, for pass 1 the following expression is used

$$E_1 = k_1\overline{\text{QBER}} - \frac{\left(1-\left(1-2\overline{\text{QBER}}\right)^{k_1}\right)}{2} \tag{3.4}$$

So the parameter k_u should be chosen in such a way that the next two inequalities are met:

$$\sum_{e=j+1}^{\left\lfloor \frac{k_1}{2} \right\rfloor} \delta_1(e) \leq \frac{1}{4}\delta_1(j) \tag{3.5}$$

$$E_1 \leq -\frac{\ln\frac{1}{2}}{2} \tag{3.6}$$

Although it is not explicitly specified in the text, one should see that $2j+1$ can be at most k_u, because in a block of size k_u there cannot be more than k_u errors. On the other hand, although the former way to obtain k_u is implemented in this work, in practice it is common to use the expression $k_u \approx 0.73/\overline{\text{QBER}}$ for the sake of time [70 p. 6].

In relation to the statement made at the beginning of the page about the characterization of the parameters involved in the protocol, there exists one aspect that is not well clarified in the text. Apparently, the type of functions to shuffle the bits randomly is to be decided by the user. In this work, a pre-shared seed between Alice and Bob is employed, since it seems to be an easy-to-use choice.

Finally, an idea of the robustness of the Cascade protocol can be provided in terms of bounds. If the inequalities (3.5) and (3.6) are used, after the fourth pass: $\delta_4(1) \leq 2\%$ and $E_4 \leq 0.043$, approximately for any value of $\overline{\text{QBER}}$.

3.4.2 An LDPC code

In order to be pragmatic and not to fall into the misleading explanations from the perspective of classical linear codes[32], a different approach is here adopted to describe the method. It is assumed

[32] Recall that what can be used in the cotext of QKD is not a classical linear error-correcting code per se, but an adaptation of it. A helpful example to keep in mind is the sort of analogies used in mechanics of materials, to determine e.g. the stress distribution along some structure subjected to certain loads, just because the form of the equations is the same. However, the problem here is that the difference is not always clear due to the similarities, what becomes an obstacle for those who are not too familiar with the reconciliation in QKD.

that the reader is not interested in knowing how to perform the error correction in classical communication, but wants to learn how to carry out the information reconciliation in the post-processing of the QKD.

Once again, suppose Alice's n-bit frame is denoted by A and it is formed by the bits $X_{Ai}=\{0,1\}$. Similarly, Bob's n-bit frame is denoted by B and it is formed by the bits $X_{Bi}=\{0,1\}$. A clever strategy to correct the errors without leaking too much information consists in doing some calculation over Alice's frame and sending the results to Bob, who must check if his frame fulfills the constraints, that is to say, if doing the same calculation over his frame yields Alice's outcomes. If not, he must find the way to obtain the right frame by using all the information that he already knows. At this point, it is clear that this error-correcting protocol is formed by two parts: first, the construction of the set of operations that both Alice and Bob have to perform; and second, the decoding that takes place at Bob's side.

With respect to the first step, the set of operations can be summed up in the multiplication (in modulo 2) between a matrix H (typically called the parity-check matrix, with its rows being also known as simply checks) and a vector (Alice or Bob's frames). How to make Alice and Bob construct the same parity-check matrix, leaking as little information as possible, is crutial. It is easy to understand that the construction rules must be previously shared. More precisely, according to [71 p. 301], whose description matches the one in [75 p. 1645], the parity-check matrix can be constructed as follows:

1. create an $p \times n$ matrix full of zeros, where p is the number of parity checks (it will be determined later) and n is the length of the frames;
2. and column by column, replace a number of random positions (e.g. 5, as recommended by [71 p. 301]) with ones, in such a way that the rows are more or less unirformly filled and that the inner product between two columns (or two rows) is at most 1.

The procedure deserves three remarks. First, to make Alice and Bob distribute the ones in the same manner, [71 p. 301] recommends using a pseudo-random number generator with a pre-shared seed. Second, notice that H is a sparse matrix, hence the expression low density is justified. Third, the number of parity checks is determined by fixing the reconciliation efficiency already defined in Eq. (3.2). According to [71 p. 301], a percentage of 25% higher than the bare minimum should work. That is,

$$f_{EC} = \frac{p/n}{h\left(\overline{\text{QBER}}\right)} = 1.25 \tag{3.7}$$

After creating the matrix, Alice performs the multiplication and sends the p-bit resultant string to Bob, who, with the matrix also constructed, checks if his frame is correct. If not, he starts the decoding. To do so, [71 p. 301] suggests the sum-product algorithm (with one modification depending on the value of the parity bits) and refers to [75 p. 1646] for the description. An important comment here is that [71] does not warn about the use of a BSC instead of a Gaussian channel as implemented in [75]. A synthetic description is found next.

1. Initialize the variables q_{ji}^{0} and q_{ji}^{1} (probabilities that the bit[33] $X_{Bi,corr}$ is 0 and 1, respectively, given the information obtained from the checks where this bit participates[34], except for the check j) in the following manner:

[33] To distinguish Bob's bits before the reconciliation from the corresponding ones after the reconciliation, the subscript *corr* is used for the latter. Obviously, if the error correction is confirmed later, $X_{Bi,corr}$ is equal to X_{Ai}.

[34] In symbols, the components H_{ji} that equals 1.

$$q_{ji}^{0} = p\left(X_{Bi,corr} = 0 \mid X_{Bi}\right) = \begin{cases} 1 - \overline{\text{QBER}} \text{ if } X_{Bi} = 0 \\ \overline{\text{QBER}} \quad \text{ if } X_{Bi} = 1 \end{cases} \tag{3.8}$$

$$q_{ji}^{1} = 1 - q_{ji}^{0} \tag{3.9}$$

2. Calculate the variables r_{ji}^{0} and r_{ji}^{1} (probabilities that the check j is fulfilled if the bit $X_{Bi,corr}$ is supposed fixed at 0 and 1, respectively, and the rest of bits follow a distribution given by the probabilities q_{jl}^{0} and q_{jl}^{1}). To indicate the set of bits that participate in the check j other than the bit $X_{Bi,corr}$, the symbol Ω is used. Be careful with the r_{ji}^{0} and r_{ji}^{1} where the bit $X_{Bi,corr}$ does not participate in the check j, because it cannot affect the rest of steps.

$$r_{ji}^{0} = \frac{1}{2}\left(1 + \prod_{l \in \Omega}\left(q_{jl}^{0} - q_{jl}^{1}\right)\right) \tag{3.10}$$

$$r_{ji}^{1} = \frac{1}{2}\left(1 - \prod_{l \in \Omega}\left(q_{jl}^{0} - q_{jl}^{1}\right)\right) \tag{3.11}$$

3. Calculate the normalized probabilities that the bit $X_{Bi,corr}$ is 0 and 1, i.e. q_{i}^{0} and q_{i}^{1}, respectively. Since these probabilities are obtained via the information that can be extracted from all the checks, they depend on whether the parity bit associated to each check is 0 or 1. To denote these parity bits, the variables P_j are used. In addition, to denote the set of checks where the bit $X_{Bi,corr}$ participates, the symbol Γ is used.

$$q_{i}^{0} = \lambda_{i}\, p\left(X_{Bi,corr} = 0 \mid X_{Bi}\right)\prod_{j \in \Gamma} r_{ji}^{x}, \text{ with } r_{ji}^{0} \text{ if } P_{j} = 0 \text{ else } r_{ji}^{1} \tag{3.12}$$

$$q_{i}^{1} = \lambda_{i}\, p\left(X_{Bi,corr} = 1 \mid X_{Bi}\right)\prod_{j \in \Gamma} r_{ji}^{x}, \text{ with } r_{ji}^{1} \text{ if } P_{j} = 0 \text{ else } r_{ji}^{0} \tag{3.13}$$

$$q_{i}^{0} + q_{i}^{1} = \lambda_{i}\left(\frac{q_{i}^{0}}{\lambda_{i}} + \frac{q_{i}^{1}}{\lambda_{i}}\right) = 1 \Rightarrow \lambda_{i} = \frac{1}{\left(\frac{q_{i}^{0}}{\lambda_{i}} + \frac{q_{i}^{1}}{\lambda_{i}}\right)} \tag{3.14}$$

4. Update the probabilities q_{ji}^{0} and q_{ji}^{1} with the help of the checks where the bit $X_{Bi,corr}$ participates, except for the check j (this set is denoted by Υ).

$$q_{ji}^{0} = \lambda_{ji}\, p\left(X_{Bi,corr} = 0 \mid X_{Bi}\right)\prod_{m \in \Upsilon} r_{mi}^{x}, \text{ with } r_{mi}^{0} \text{ if } P_{m} = 0 \text{ else } r_{mi}^{1} \tag{3.15}$$

$$q_{ji}^{1} = \lambda_{ji}\, p\left(X_{Bi,corr} = 1 \mid X_{Bi}\right)\prod_{m \in \Upsilon} r_{mi}^{x}, \text{ with } r_{mi}^{1} \text{ if } P_{m} = 0 \text{ else } r_{mi}^{0} \tag{3.16}$$

$$q_{ji}^{0} + q_{ji}^{1} = \lambda_{ji}\left(\frac{q_{ji}^{0}}{\lambda_{ji}} + \frac{q_{ji}^{1}}{\lambda_{ji}}\right) = 1 \Rightarrow \lambda_{ji} = \frac{1}{\left(\frac{q_{ji}^{0}}{\lambda_{ji}} + \frac{q_{ji}^{1}}{\lambda_{ji}}\right)} \tag{3.17}$$

5. Determine the value of every $X_{Bi,corr}$ based on the probabilities q_{i}^{0} and q_{i}^{1}. For instance, if $q_{i}^{0} \geq 0.5$, then $X_{Bi,corr}$ is set to 0, else $X_{Bi,corr}$ is set to 1.

6. Check if the parity constraints are satisfied. If so, the current value of the bits $X_{Bi,corr}$ with i=1, …, n is acceptable, waiting for the confirmation. Otherwise, repeat the steps 2-6 until either the parity constrains are met or a maximum of iterations (say 20, as in [71 p. 301]) is exceeded. In this case, a failure is declared.

3.4.3 Confirmation

Once the reconciliation has been concluded, the verification that it was successful is performed by way of a two-universal hash function. Mathematically, a class $\mathcal{F}$ of functions $\mathcal{X} \rightarrow \mathcal{Y}$ is two-universal if, for any x_1, x_2 in $\mathcal{X}$ such that $x_1 \neq x_2$, the probability of $f(x_1) = f(x_2)$ is at most $1/|\mathcal{Y}|$, as long as f is chosen at random from $\mathcal{F}$ with a uniform probability distribution. The symbol $|\mathcal{Y}|$ denotes the number of elements in the set $\mathcal{Y}$, that is, if it is $\{0,1\}^t$, then $|\mathcal{Y}| = 2^t$.

Alice and Bob's keys after the reconciliation protocol are in $\mathcal{X} = \{0,1\}^n$. With the previous decisions for the length of the hash value (i.e. t) and the hash function, both of them calculate the hash value, comparing the result. It is clear that Alice and Bob want to be sure enough about the reconciliation success, therefore the parameter t must be sufficiently high to make a failure of the verification step be extremely improbable. A typical value may be 50 bits [76 p. 2; 77 p. 3]. On the other hand, the choice of the hash function usually depends on the computational constraints. Since these functions were studied for the first time, there have been some contributions with faster and faster constructions. In this work, without covering a literature review, the family of hash functions proposed in [78] is chosen.

Succinctly, given t, one defines the parameter θ as the largest prime number below 2^t (e.g. 2^{50}-27 if t is set to 50 [77 p. 3]) and selects a value k from $\{0, 1, \ldots, \theta\text{-}1\}$ at random. Additionally, the binary strings A and B are divided into substrings a_i and b_i of length the floor of $\log_2 \theta$. With this in mind, the hash values are calculated as follows

$$f(A) = \text{int\_ to\_string}\left(\sum_i \text{string\_to\_int}(a_i)\, k^{i-1} \bmod \theta\right) \tag{3.18}$$

$$f(B) = \text{int\_ to\_string}\left(\sum_i \text{string\_to\_int}(b_i)\, k^{i-1} \bmod \theta\right) \tag{3.19}$$

where $\text{int\_to\_string}(\cdot)$ and $\text{string\_to\_int}(\cdot)$ are two functions that convert an integer into a binary string and a binary string into an integer, respectively.

3.5 Security issues

The reason why this section is located here is because the basic notions about security that are going to be introduced will have an effect on the way the privacy amplification is carried out. Indeed, this dependency was to be expected, since the widely-claimed unconditional security of QKD must be ensured after all.

Prior to the implications of the unconditional security, two remarks about the meaning of the word unconditional are needed. First, this characterization of the security refers to the fact that Eve's technology is assumed to be unlimited, contrary to the restrictions that the conventional cryptography imposes on the computational power of the adversaries [22 p. 9], although some constraints are created [22 p. 10]: Eve cannot access Alice and Bob's modules; a true random number generator must be employed; unconditional secure authentication in the classical channel is mandatory; and Eve cannot go beyond the limits of physics. Second, and as stated in Section 3.3, the unconditional security is actually of a probabilistic nature. Technically speaking, the key that is finally obtained in QKD is said to be ε-secure if the probability that an eavesdropper ends up knowing it is ε. Among the possible sources of the security parameter ε, one finds the different estimations that are made during the execution of the QKD protocol, concerning the physical implementation (e.g. the indistinguishability of the optical signals, the average number of photons per pulse, etc.) and the data (e.g. the symmetry of the key, the error rate, the leaked information, etc.), as well as the probability that Eve's attacks are successful [72 p. 9].

Whatever the origin of the security parameter ε is, it must be calculated in such a way that easily allows for the addition of tasks with failure probability ε', the total security parameter coming to

$\varepsilon+\varepsilon'$. This property is known as composability and is vital for many reasons. On the one hand, it is important because it simplifies the analysis of the different probabilities. On the other hand, the importance comes from the fact that a QKD system is typically built up to operate several times, not only one. Therefore, throughout the desired number of executions, say N, the total security parameter $N\varepsilon$ should be kept sufficiently low not to make the QKD too risky [72 p. 10].

Given the significance of the security parameter, it is not enough to roughly estimate it, but it must be carefully proved in specific operating conditions (e.g. losses, error rate, etc.) by means of a security proof [72 p. 9]. However, performing this kind of proofs is not an easy task at all, since any a priori negligible detail can lead to a side channel for the eavesdroppers. Additionally, one has to pay attention not only to the list of theoretical assumptions, but also to how they are put into practice. On this matter, an extraordinary effort to achieve standardization[35] for QKD is being made, and a special care of the security proofs is being taken [72].

Needless to say, a deep study of the state-of-the-art of security proofs is totally out of scope. One of the reasons is that, in spite of being very advanced from a theoretical viewpoint, the analysis still causes controversy when the practical implementation is addressed [81 p. 2]. A complete and recent description of the security analyses using entropic notions can be found in [81] and, therefore, its results will be used for the privacy amplification.

With respect to the current section, the classification of the eavesdropping strategies remains to be introduced.

3.5.1 Classification of the eavesdropping strategies

In general terms, the different strategies that an eavesdropper can adopt to extract information throughout the execution of the QKD can be classified into four categories [22 pp. 23-26; 31 pp. 229-233]: individual (or incoherent) attacks; collective attacks; coherent attacks; quantum hacking and side channel attacks.

In the first place, individual attacks consist in an interaction with each qubit transmitted over the quantum channel following the same strategy and measuring their states before the classical post-processing. The most known attack in this family is the intercept-resend (IR) attack, in which Eve catches each qubit on the fly, performs a measurement on it as Bob would do, prepares a qubit in the same state she obtained and sends it to Bob to go unnoticed.

In the second place, collective attacks are very similar to individual attacks. The main difference lies in the fact that this time, Eve can postpone the measurement of her ancilla qubits until the most convenient instant (typically, during the classical post-processing). To keep the quantum states, Eve needs to have access to a quantum memory.

A generalization of the former two categories leads to the coherent attacks, in which Eve can adapt her strategy depending on the events, her measurement outcomes, etc.

Finally, the quantum hacking attacks and side channel attacks take advantage of the weaknesses of practical implementations. Such weaknesses affect both Alice and Bob's sides as well as the quantum channel. Two examples of quantum hacking attacks are: in the so-called Trojan horse attack, Eve obtains information about the key by sending a bright laser beam towards Alice's module and measuring the reflected light; with the blinding attack, Eve makes Bob select the same basis as she does by exploiting the operation of the single photon counting modules. Regarding the side channel attacks, they are, in general, attacks that do not introduce differences between Alice and

[35] To the best of my knowledge, the two institutions that have made more progress in this sense are the European Telecommunication Standards Institute (ETSI), with a growing set of recommendations [79], and the International Organization for Standardization (ISO), with a publication of standards scheduled for 2022 [80].

Bob's keys. Consider, for instance, the existence of significant variations in the propagation wavelengths of the four quantum states, making them distinguishable. Other important examples are the beam-splitting attack, in which Eve takes part of the photons Alice sends to Bob and hiding them as losses, and the photon-number splitting (PNS) attack, in which Eve takes the extra photons emitted by Alice's module when a weak coherent state-based QKD system[36] is employed.

Among the above-mentioned attacks, the one which is covered by the scope of this work is the IR attack. In particular, it is interesting to see the effects of Eve's interaction and how her presence can be detected. Taking into consideration the notions about measuring a quantum state discussed in Section 2.2, it is clear that Alice and Bob obtain the same results providing that they select the same bases. However, this fact is distorted when there exists someone in between performing measurements in bases chosen at random. In probabilistic terms, the probability of detecting the IR attack is thus equivalent to the probability that Bob obtains the wrong result even if he chose the same basis as Alice did. In symbols,

$$\begin{aligned} p\left(X_A \neq X_B \mid Y_A = Y_B\right) = p\left(X_A \neq X_B \mid Y_A = Y_B = Y_E\right) p\left(Y_A = Y_B = Y_E\right) + \\ + p\left(X_A \neq X_B \mid Y_A = Y_B \neq Y_E\right) p\left(Y_A = Y_B \neq Y_E\right) \end{aligned} \tag{3.20}$$

where X_i denotes the bit obtained by the party i (Alice, Bob or Eve) after a measurement in the basis Y_i . If Eve decides her basis at random, it is easy to see that $p(Y_A = Y_B = Y_E) = p(Y_A = Y_B \neq Y_E) = 1/2$. Moreover, in the event of triple coincidence of bases, Bob always obtains the same result as Alice sent, that is, $p(X_A \neq X_B \mid Y_A = Y_B = Y_E) = 0$. However, if Eve selects the wrong basis, only half of the cases she obtains the right result (as remarked in Example 2.1), preparing and sending therefore the correct qubit to Bob. As a result,

$$p\left(X_A \neq X_B \mid Y_A = Y_B\right) = 0 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \tag{3.21}$$

The former means that the presence of an eavesdropper causes, on average, one error per four bits in Bob's sifted key. At first sight, one might think that this probability is not high enough to reveal Eve's interaction during the estimation of the QBER. For the same reason, one might wonder how many bits are necessary to estimate the QBER in such a way that the presence of the eavesdropper is fully disclosed. To know that, take a sample with n' bits. The probability that all those bits are correct is $(3/4)^{n'}$, therefore the probability of having at least one erroneous bit (i.e. of detecting Eve during the parameter estimation) is $1 - (3/4)^{n'}$. If $n' = 1$, this probability is 25%, whereas if $n' = 25$, the probability becomes 99.9%.

Before concluding the current subsection, there is room for two additional comments about what is explained in the previous paragraph. First, one might immediately wonder how the errors introduced by an eavesdropper can be distinguished from the errors due to the noisy nature of the quantum channel or the imperfections in the QKD system. The answer is that they cannot be separated, assuming conservatively in practice that all the errors come from Eve's interaction. Second, a particular precaution must be taken to reproduce the numbers given in the previous paragraph. In order to avoid significant statistical fluctuations, the size of the sample should be sufficiently high.

3.6 Privacy amplification

The algorithm for the privacy amplification implemented in this work is the same as in [76 p. 3], which, in turn, is based on the security proof given in [81]. This algorithm has two parts: first, it checks the possibility of generating a specific secret key; and second, if possible, it transforms the

[36] More details about this will be provided in Section 4.2.

corrected key into a shorter but secure key. The resultant secret key is defined by its length l_{sec} and a security parameter ε_{pa}. Unlike other algorithms, this uses a secret key of fixed length as established by the security proof where it rests [81 p. 10].

The verification of the possibility to distill a secret key is based on the following inequality

$$2^{-\frac{1}{5}\left(n\left(1-h\left(\mathrm{QBER}_{\max}+v\right)\right)-p-t-l_{sec}\right)} \leq \varepsilon_{pa} \tag{3.22}$$

where n is the length of the corrected key, $h(\cdot)$ is the binary entropy, QBER$_{\max}$ is the threshold in the parameter estimation step, p is the number of parity checks[37], t is the length of the hash value that resulted in the confirmation step, l_{sec} is the length of the secret key and v is a quantity calculated as follows

$$v=\sqrt{\frac{2\left(n+n'\right)\left(n'+1\right)\ln\frac{1}{\varepsilon_{pa}}}{n\left(n'\right)^{2}}} \tag{3.23}$$

The parameter n' is the number of bits that were publicly announced and then discarded during the parameter estimation step. In this case, n' is equal to n.

Once the feasibility of obtaining a secure key is checked, the privacy amplification continues with the application of another hash function to shorten the key. In this case, the usual approach lies in the multiplication (modulo 2) between an $l_{sec} \times n$ matrix T_S and a vector formed by the corrected key. To construct the matrix in a simple and efficient manner, the shape of a Toeplitz matrix is employed:

$$T_S=\begin{bmatrix} s_0 & s_{-1} & s_{-2} & \cdots & s_{-(n-1)} \\ s_1 & s_0 & s_{-1} & \ddots & \vdots \\ s_2 & s_1 & \ddots & \ddots & s_{-2} \\ \vdots & \ddots & \ddots & s_0 & s_{-1} \\ s_{l_{sec}-1} & \cdots & s_2 & s_1 & s_0 \end{bmatrix}_{l_{sec}\times n} \tag{3.24}$$

As can be deduced from Eq. (3.24), a Toeplitz matrix presents the property $T_{i,j}=T_{i+1,j+1}=s_{i-j}$, where the elements s_{i-j} form part of a randomly chosen string $S=\left(s_{1-n}, s_{2-n}, \ldots, s_0, \ldots, s_{l_{sec}-2}, s_{l_{sec}-1}\right)$ of length $n+l_{sec}-1$. This string may be generated by Alice and then sent it to Bob, or created with the help of a pre-shared seed.

[37] As can be seen, this parameter only appears in the second error-correcting method described in this work (the LDPC code). The reason is that the considered security proof [97] assumes a one-way post-processing. Therefore, the Cascade protocol would not be compatible with it. However, this is not an obstacle to implement the Cascade protocol in this work, since it is always interesting to compare the performance of two different reconciliation methods, given the importance of this step in the final result.

4 BB84 Implementation

4.1 Generic implementation

So far the choice of the BB84 protocol via polarization encoding has been justified by the experience gained in free space throughout the last decade. Furthermore, the protocol (quantum transmission and public discussion) has been described right after explaining its main ingredients. This content would be sufficient to simulate a BB84-based quantum key distribution. However, this approach would present scant interest in practice, since it is worthless to simulate something that cannot be implemented because it does not include the inherent imperfections of the current technology. Consequently, it is interesting to address some of the main non-idealities (the ones permitted by the scope of the work) linked to the usually employed QKD components. In this sense, Figure 4.1 illustrates a generic architecture.

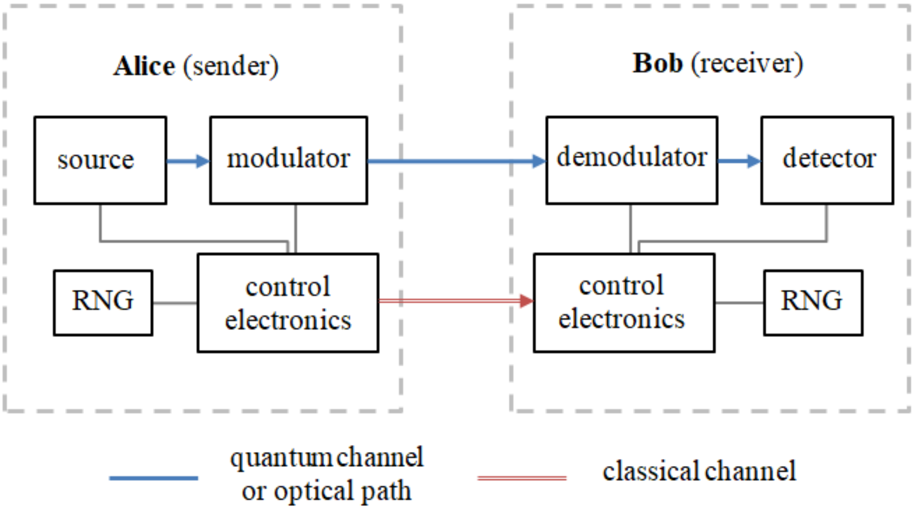

Figure 4.1 – Schematic illustration with the main parts of a QKD system and their interfaces. Succinctly, the photons generated in the source adapt in the modulator to carry the information along the quantum channel, down to the demodulator and finally the detector. The preparation of the quantum states is governed by the control electronics with the help of a random number generator (RNG), whereas the received information at Bob's side is stored until the classical post-processing starts, when both control electronics and RNGs are employed.

Even though both optics and electronics are included in Figure 1.1, only the former is of interest here. In particular, while the source, the quantum channel and the detector will be described in Sections 4.2 through 4.4, the main strategies for the modulator and the demodulator are briefly mentioned next.

For polarization encoding, the use of an electro-optic modulator is an option. Basically, this device controls the polarization of light (as well as optical power and phase) by applying a voltage to a non-linear crystal, what changes the refractive index in that direction. Unfortunately, this strategy to modify the polarization requires a high-voltage (in the order of kilovolts), what leads to an additional complexity and weight due to the necessity of a high-voltage amplifier, cooling, etc. In addition, it operates with a limited repetition frequency of the train of optical pulses (typically, a few megahertz), which may be insufficient to overcome the losses from sender to receiver. For these reasons, this option is only feasible in laboratory conditions. A different approach could lie in the use of polarization optics, namely: polarizing beamsplitters and/or linear polarizers together with an a priori rotary half-wave plate[38]. However, it is clearly impossible to rotate the half-wave plate with frequencies in the range of megahertz. Hence, a common solution to this bottleneck consists in generating four separated beams (one for every quantum state) and combining them in a non-polarizing beamsplitter. This is precisely the most adopted configuration and has been implemented in all the demonstrators in free-space. The demodulation, on the other hand, is carried out in a similar manner, with the only precaution that, to avoid possible misalignment between the reference frames of Alice and Bob's units, some actuator is needed in the receiver. To get a further insight into the typical architecture, read any of the papers indicated in Table 3.1.

Regarding the parameters that determine the operation of the QKD components, the sender module emits a train of optical pulses of duration Δt with a repetition rate f_{rep}, at the wavelength λ. The choice of the specific values for these parameters responds to the behavior of the QKD components and through the quantum channel. For instance, the wavelength is typically chosen to minimize the losses through the quantum channel (more details in Section 4.3). Depending on the decision, some components are more suitable than others and, of course, their performance may be function of it. Moreover, the higher the repetition frequency is, the larger the number of photons that reach the detector is and, therefore, the longer the final key can be; although it is limited in practice by the source, the RNG, the modulation strategy, the control electronics and the detector. As the repetition frequency becomes higher, it is easy to see that the duration of the pulses necessarily decreases. Practically speaking, this is not the unique reason, but it is also interesting to make the pulses as narrow as possible to achieve a better signal-to-noise ratio. However, narrower pulses constitute a technical problem from the perspective of the synchronization between Alice and Bob and, of course, may cause a lower counting rate [46 pp. 65-66].

In this work, tweaking the duration of the pulses is out of scope since it requires further post-processing techniques such as time filtering. The wavelength and the repetition frequency, on the contrary, can be modified more easily. In any case, it is useful to look at the choices made in the experiments of Table 3.1 where the BB84 protocol was implemented.

[38] A half-wave plate (or half-wave retarder) is a transparent plate that rotates the direction of linear polarization of the passing light a fixed angle.

Table 4.1 – Values for the main parameters of the optical signals used in those missions that implemented/will implement the BB84 protocol (or its decoy-state version).

LAUNCH/ FLIGHT YEAR	COUNTRIES	WAVELENGTH (nm)	REPETITION FREQUENCY (MHz)	PULSE DURATION (ns)	REF.
2008	Italy	1064	100	0.1	[44]
2010	China	850	100	1	[45]
2011	Germany	850	10	1	[46]
2016	China	850.15	50	0.5	[48]
2016	China	848.6	100	0.2	[49]
2016	Canada	785	400	Not found	[51]
2020	Germany	850	100	Not found	[54]
2022	France, Austria	808	Not found	Not found	[57]
Funded mission	Canada	780-795, 850	400	Not found	[58]
Proposal	UK, Singapore, Italy, Germany, the Netherlands, Switzerland, Austria	800	100	Not found	[66]

4.2 Source

For the generation of the single photons which are employed in the DV-QKD protocols, there exist three main options: single-photon sources, weak laser pulses and entangled photon-pair sources. The last one has already been described somehow when the entanglement was explained in Section 1.1 and is the least developed [43 p. 29]. However, this work is not focused on entanglement-based (or prepare-and-measure with entanglement) protocols, so this document will not provide further details. Regarding the other two options, they are explained next.

To better understand the difference between single-photon sources and weak laser pulses, it is worth introducing the idea that producing a train of optical pulses with real single photons may be quite challenging [43 p. 29]. Instead, it is more practicable to generate pulses where the number of photons n follows a probability distribution $p(n)$, with average number of photons per pulse μ. To specify this probability distribution, a parameter called second order correlation function at zero time delay, $g^{(2)}(0)$, is commonly used. This parameter, approximated as $2p(2)/p(1)^2$, gives the probability that a multiphoton event occurs. If, for instance, $g^{(2)}(0) = 1$, the light source is said to be coherent (as in the case of the laser), and perfectly coherent light presents Poissonian statistics, where the variance equals the mean value and the $p(n)$ is given by

$$p(n) = e^{-\mu}\frac{\mu^n}{n!} \tag{3.25}$$

By contrast, the lower $g^{(2)}(0)$ is, the closer the light source is to a true single-photon source ($g^{(2)}(0) = 0$), showing sub-Poissonian statistics (the variance is below the mean value). A helpful picture to visualize this idea is found in Figure 4.2.

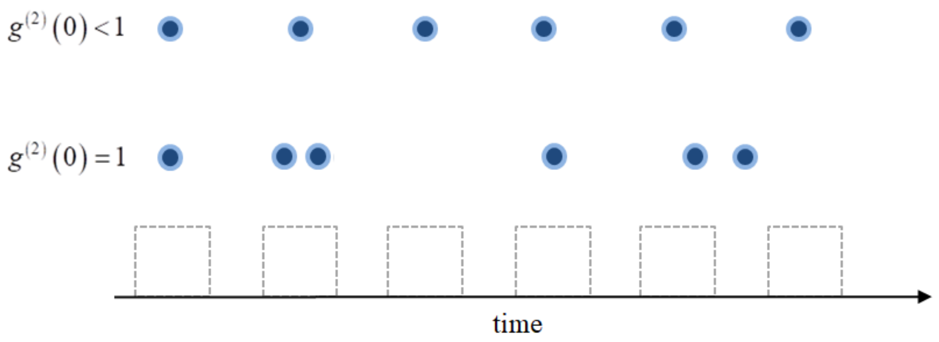

Figure 4.2 – Schematic illustration showing the different photon number statistics depending on the second order correlation function at zero time delay. When $g^{(2)}(0)<1$, the time interval between photons is approximately constant, whereas when $g^{(2)}(0)=1$, photons are randomly spaced in time [82 pp. 115-117].

In theory, single-photon sources would be the best decision to build up a DV-QKD system. However, it suffers from technical issues. The reason is that to be usable, it must simultaneously meet the stringent threefold criteria of [83 p. 734]: negligible probability of multiphoton event; indistinguishability of the emitted photons (e.g. same wavelength, phase or polarization); and high efficiency to make the photons propagate in a unique spatial mode (in other words, through the same quantum channel). Although a lot of research has been conducted over the last decades, these difficulties have not been overcome yet, being the quantum dots the most advanced technology [83 p. 735].

In view of the technical problems to fabricate a perfect single-photon source, the laser has turned out to be a very valid alternative. It certainly satisfies the last two conditions of the previous paragraph as well as being compatible with existing infrastructure. The objection is the non-vanishing probability that a pulse contains more than one photon. A solution employed in practice is the attenuation of the optical power down to the single-photon level. This strategy gives rise to the expression weak laser source [84 p. 34].

The question now is how much attenuation is required in practice. The answer to that comes from Eq. (3.25). With the aim of making $p(n)$ with $n \geq 2$ as low as possible, $\mu = 0.1$ is typically used, resulting $p(0) \approx 90.5\%$, $p(1) \approx 9\%$ and $p(n \geq 2) \approx 0.5\%$. A great disadvantage of $\mu = 0.1$ is that most of the sent pulses are empty. This can be solved by the use of a higher mean photon number together with decoy states to prevent the PNS attack, but this issue is not discussed here. If, additionally, one desires to calculate the attenuation coefficient, the following formula is used

$$\alpha = -10\log_{10}\frac{P_{out}}{P_{in}} \tag{3.26}$$

where α is the attenuation coefficient (in dB), P_{in} is the optical power before the attenuation and P_{out} is the optical power afterwards. A priori, P_{in} is known and P_{out} can be obtained in this way

$$P_{out} = h\frac{c}{\lambda}\frac{1}{f_{rep}}\mu \tag{3.27}$$

being h the Planck constant and c the speed of light (the rest of the symbols were already introduced).

4.3 Quantum channel

Generally speaking, the communication of information between a sender and a receiver suffers from the transmission losses inherent to the used channel, independently of both the communication protocol and the channel. However, such losses have a major impact when single photons are employed to transmit the data, since it may mean that the vast majority of photons never reach their destination. Taking into consideration that the quantum channel of interest for this work is free space, it is thus convenient to discuss the losses that affect photons through it.

In order to describe the losses, imagine the case of a ground-to-space (or vice versa) link. Depending on whether a lower link or an upper link is implemented, the space terminal is a satellite equipped with the corresponding QKD components as well as a telescope to emit or receive the optical beam. On the other hand, the OGS consists of the respective QKD equipment and also a receiving or a sending telescope. The link attenuation accounts for the losses that occur between the sending telescope and the receiving telescope and does not include the ones that take place inside the receiver unit. These losses can be grouped into geometric and atmospheric losses grosso modo [22 p. 18], considering that the decoherence of polarization is not significant as stated at the end of Section 3.2.

In the first place, geometric losses clearly include the beam diffraction and the aperture diameters of the telescopes. Additionally, the losses within the telescopes themselves may be considered here as well as the loss of the optical link [18 p. 3]. With respect to the latter, the relative motion between the satellite and the ground station requires a pointing, acquisition and tracking (PAT) system. The complexity of this system is high, especially if a LEO satellite is assumed.

In the second place, atmospheric losses take into account the effects of scattering, absorption and turbulence. Scattering refers to the deviation, in this case, of photons from their trajectory as a consequence of their interactions with particules (aerosols or smaller particules). This phenomenon depends on the wavelength and the visibility (i.e. weather conditions and time of day) as also happens with absorption [18 p. 9], which refers to the light absorbed by the existing particles in the atmosphere. Regarding scattering, there exist two main atmospheric windows exploited in practice, 780-850nm and 1520-1600nm [22 p. 18]. Although a QKD system using wavelengths around 800nm is constrained to operate almost in the night to avoid the sky radiance [85], the first spectral window has been almost unanimously used in the experiments up to now in accordance with Table 4.1. The reason is that the attenuation at 1550nm is significantly higher than at 800nm, as illustrated in Table 1 of [18]. For instance, in a LEO-to-ground scenario, the attenuation at 800nm is 6.4dB, in contrast to the 12.2dB at 1550nm[39].

The type of atmospheric loss known as turbulence refers to the random fluctuations in the refractive index. This happens as a result of the temperature gradient along the optical path of photons in the atmosphere. Such fluctuations have different effects; among them, the beam divergence, which is more or less significant for a ground-to-space link or a space-to-ground link, respectively. Since the atmosphere is closer to the ground station than to the satellite, it is easy to understand that the sooner the beam finds the fluctuations, the larger the beam spreading becomes. Numerically, while a LEO-to-ground link presents an attenuation of 6.4dB at 800nm, a ground-to-LEO link shows an

[39] Compare these attenuation values for a distance of 500km, with the ones obtained in optical fiber at the same wavelengths for a distance of 100km. With the attenuation coefficients of 2dB/km at 800nm and 0.2dB/km at 1550nm [22 p. 17], it results 200dB and 20dB, respectively.

attenuation of 27.4dB [18 p. 7].

After all the losses through the quantum channel, an important fact is that the photon number statistics continues being Poissonian [98 pp. 72-73]. To calculate the average number of photons at the end, the following reasoning can be used.

$$\alpha_{qch} = -10\log_{10}\frac{P_{out}}{P_{in}} \tag{3.28}$$

$$\begin{cases} P_{in} = h\dfrac{c}{\lambda}\dfrac{1}{f_{rep}}\mu_{in} \\ P_{out} = h\dfrac{c}{\lambda}\dfrac{1}{f_{rep}}\mu_{out} \end{cases} \Rightarrow \frac{P_{out}}{P_{in}} = \frac{\mu_{out}}{\mu_{in}} \tag{3.29}$$

$$\alpha_{qch} = -10\log_{10}\frac{P_{out}}{P_{in}} = -10\log_{10}\frac{\mu_{out}}{\mu_{in}} \Rightarrow \mu_{out} = \mu_{in}10^{-\frac{\alpha_{qch}}{10}} \tag{3.30}$$

where α_{qch} is the attenuation coefficient of the quantum channel, $\mu_{in} = \mu$ and μ_{out} is the mean photon number at the receiving telescope.

4.4 Detector

The measurement of single photons in the QKD context can be performed by two technologies [43 p. 29]: avalanche photo-diodes (APDs) and superconducting nanowire single-photon detectors (SNSPDs).

On the one hand, the working principle of single-photon APDs (SPAPDs) is the photoelectric effect followed by the so-called avalanche effect. When a photon is absorbed by the semiconductor material of the APD, an electron-hole pair is created and then accelerated through an intense internal electric field with some wavelength-dependent quantum efficiency η, triggering literally an avalanche of additional electrons which can be detected by suitable electronics. (see Figure 4.3 (a)). To make the detection of single photons possible, the gain needs to be sufficiently high; in other words, the applied electric field must be slightly higher than the breakdown voltage of the diode (Geiger mode). After each detection, the voltage is set below the breakdown limit in order to stop the avalanche of electrons, which otherwise would continue. This time interval is known as dead time (with symbol τ), since any new detection cannot be produced while it lasts [86]. Practically speaking, it limits the repetition rate of the photon counting detector. Other phenomena that might happen and also bounds the response of the APD are [84 pp. 21-23]: false or dark counts caused by the generation of electron-hole pairs by thermal fluctuations or secondary electrons instead of incoming photons; avalanches triggered by electrons that were trapped at internal defects in previous pulses (phenomeno known as after pulses); temporal fluctuations in the output of the electrical signal due to the random nature of the avalanche effect, also known as time jitter[40]; etc.

The technological alternative to the APD is the SNSPD [84 pp. 25-26]. As one might infer by its name, the SNSPD is basically a nanowire made of a superconducting material and cooled down to a point where it exhibits superconductivity. In these conditions, a bias current below its critical value is applied, in such a way that when an incoming photon is absorbed, a hotspot is formed in the nanowire. This hotspot shows a resistive effect, which makes the applied supercurrent flow around it, increasing thus the current density in the sideways. When this current density exceeds its threshold value, the total cross section transforms into a resistive barrier, generating a measurable voltage

[40] The light generated by the laser also presents time jitter, which can be similarly explained.

across the nanowire. This electrical resistivity vanishes after a while when the thermal energy is dissipated. In an analogous manner to the APD, the SNSPD presents a quantum efficiency, time jitter, etc. See Figure 4.3 (b) for a visual description.

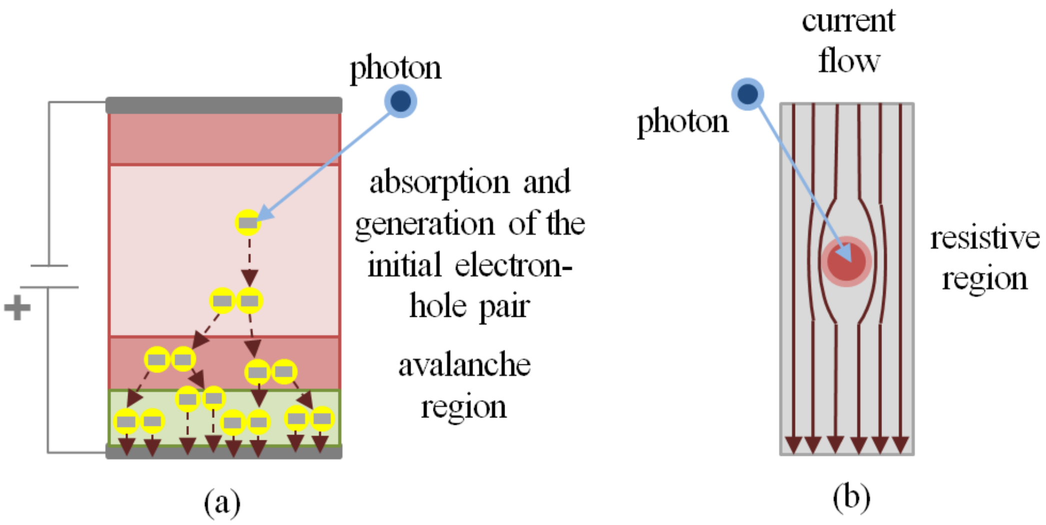

Figure 4.3 – Schematic illustration of the single-photon detectors. In (a), the principle of operation of an APD is depicted, with the generation and multiplication of electrons. In (b), it is shown how the resistive cross section is formed in a SNSPD.

Comparing the APD with the SNSPD, the latter exhibits higher quantum efficiency and a lower dark count rate at the expense of a demanding cooling down to a few kelvin. Even though the former also requires cooling, the operating temperatures are closer to room temperature [43 p. 29]. This reason together with its technological maturity justify the choice of APDs.

In view of the previous decision, it is interesting to mention some figures of the commercial APDs. First of all, they are made of different materials depending on the spectral operating range: silicon, from 260nm to 1100nm; germanium, from 800nm to 1600nm; and InGaAs, from 900nm to 1700nm [87]. In this work, the wavelengths of interest are between 780nm and 850nm, therefore, the typical specifications of Si APDs are the ones that are going to be shown. According to [88], in the cited spectral range, the quantum efficiency decreases approximately from 70% to 55%; a typical dead time is 50ns; and the dark count rate can reach the value of 15000cps at 830nm and 22ºC (maximum operating temperature). Unfortunately, this work only covers the use of the quantum efficiency and the dead time, since the rest of phenomena requires a deeper analysis. However, this does not mean that, for instance, the effect of the dark counts is negligible, but quite the opposite. A common optical error of 5% may increase to beyond 10% precisely because of the dark counts [22 p. 23].

5 Numerical modelling

In this work, the simulation of the BB84 protocol is entirely performed in Python and allows the user to modify the set of parameters and see the results that are listed in Figure 5.1.

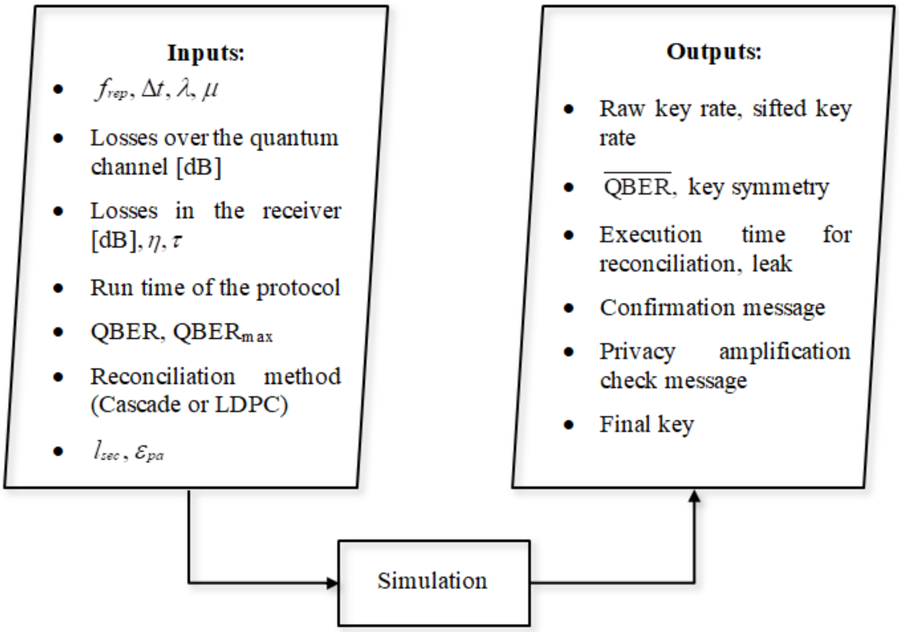
Inputs:
f_{rep}, Δt, λ, μ
Losses over the quantum channel [dB]
Losses in the receiver [dB], η, τ
Run time of the protocol
QBER, QBER_{max}
Reconciliation method (Cascade or LDPC)
l_{sec}, ε_{pa}
Outputs:
Raw key rate, sifted key rate
$\overline{\mathrm{QBER}}$, key symmetry
Execution time for reconciliation, leak
Confirmation message
Privacy amplification check message
Final key
Simulation

Figure 5.1 – List with the main inputs and outputs of the simulation code.

For the sake of organization, the code is divided into four modules:

1. Main module. It takes the inputs, generates the timing, calls the functions defined in the rest of modules, simulates the actions (losses, noise and IR attack) over the quantum channel and returns the resultant information.
2. Alice module. It contains the functions that simulate the random choices of the bits and the bases, and the preparation of the qubits.
3. Bob module. It contains the functions that simulate the demodulation and the measurements.
4. Post-processing module. It contains the functions for sifting, error estimation, error correction, confirmation and privacy amplification.

To obtain the results, the contents of the previous chapters have been employed. Only two aspects remain to be clarified: how to simulate the qubits and how to treat the statistical phenomena. What follows addresses such explainations.

5.1 Simulation of the quantum transmission with Cirq

Although the simulation of quantum systems could become extremely complex, the case of single qubits that only face changes of basis and measurements is quite simple actually. In this case, the simulation of the quantum particles is carried out classically, that is, by means of a classical computer. A quantum simulation would require a quantum computer. Basically, the main differences are related to the randomness and, of course, to the effect of the quantum noise on the results.

For the classical simulation of qubits, there are various options. On the one hand, one could perfectly write the lines of code in any programming language with the help of built-in functions for random sampling. After all, the evolution and the measurement outcomes of quantum systems are governed by linear algebra and probability theory as stressed in Chapter 2. On the other hand, there exists the alternative option of using open source software for quantum computing and quantum simulation. In this work, the latter is chosen because it further simplifies the treatment of the qubits. More concretely, the choice is Cirq, the Python library developed by Google to deal with quantum circuits. In the following subsections, the details about how to use Cirq to implement the QKD simulator are exposed. On this matter, it is useful to recall the comment made at the end of Section 2.2 with respect to quantum circuits. More information about how to install Cirq and other tutorials can be found in [89].

5.1.1 Preparation of the qubits

The preparation of each of the four quantum states $|H\rangle$, $|V\rangle$, $|+45\rangle$ and $|-45\rangle$ comprises two steps: the creation of the qubit and the modulation using the notions that were introduced in Section 2.2.

First of all, Cirq provides several ways for the definition of the qubit. In this work, the qubits are defined like this

```
import cirq
q = cirq.LineQubit(0)
```

By default, qubits are initialized to the state $|0\rangle$, independently of the number in parentheses (which indicates the position of the qubit in the quantum circuit). This must be taken into account in order to prepare the desired quantum states.

For the preparation of the state $|H\rangle$, nothing else has to be done since it coincides with the state of the initialization.

For the preparation of the state $|V\rangle$, a single bit flip is required to go from $|0\rangle$ to $|1\rangle$, what is done by applying the quantum gate equivalent to the bit flip matrix already presented in Figure 2.2. That is,

```
U1q = cirq.X(q)
```

For the preparation of the state $|+45\rangle$, the initial state $|0\rangle$ is expressed in a basis rotated 45° by applying the Hadamard gate (see Figure 2.2 again)

```
U1q = cirq.H(q)
```

Finally, for the preparation of the state $|-45\rangle$, a Hadamard gate followed by a phase flip gate are applied (see Figure 2.2), obtaining first the state $|+45\rangle$ and secondly the desired state $|-45\rangle$

```
U1q = cirq.H(q)
```

```
U2q = cirq.Z(q)
```

5.1.2 Modelling of noise sources

As already mentioned, the decoherence of polarization is almost negligible through free space (except in bad weather conditions) and, according to [46 p. 8], the errors in Bob's string are mainly due to background noise (stray light and dark counts) and polarization misalignments. Among them, only the polarization misalignments act on the qubits sent by Alice. These misalignments can be caused by an imperfect modulation or demodulation (e.g. due to an imperfect beamsplitter) or by a small rotation of the receiving module with respect to the sending module or vice versa. In any case, their effects on the measurement outcomes are the same. To understand the former, suppose that the quantum state to be prepared is $|H\rangle$, whereas the state that is actually generated is deviated an angle $\alpha \ll 1$, i.e. $\cos\alpha|H\rangle + \sin\alpha|V\rangle$. In these conditions, the probability of yielding the outcome $|V\rangle$ is different from zero as illustrated next:

$$\begin{aligned} p(|V\rangle) &= (\cos\alpha\langle H| + \sin\alpha\langle V|) M_V^\dagger M_V (\cos\alpha|H\rangle + \sin\alpha|V\rangle) = \\ &= \cos^2\alpha\langle H|V\rangle\langle V|V\rangle\langle V|H\rangle + \cos\alpha\sin\alpha\langle H|V\rangle\langle V|V\rangle\langle V|V\rangle + \\ &+ \sin\alpha\cos\alpha\langle V|V\rangle\langle V|V\rangle\langle V|H\rangle + \sin^2\alpha\langle V|V\rangle\langle V|V\rangle\langle V|V\rangle = \\ &= \cos^2\alpha\cdot 0\cdot 1\cdot 0 + \cos\alpha\sin\alpha\cdot 0\cdot 1\cdot 1 + \sin\alpha\cos\alpha\cdot 1\cdot 1\cdot 0 + \sin^2\alpha\cdot 1\cdot 1\cdot 1 = \\ &= \sin^2\alpha \neq 0 \end{aligned} \tag{3.31}$$

Regarding, the case of misalignment between sender and receiver, consider that the prepared state is $|H\rangle$, but the receiver performs a measurement in a basis slightly rotated, that is,

$$\begin{aligned} p(|V\rangle) &= \langle H|M_{V'}^\dagger M_{V'}|H\rangle = (\cos\alpha\langle H'| + \sin\alpha\langle V'|) M_{V'}^\dagger M_{V'} (\cos\alpha|H'\rangle + \sin\alpha|V'\rangle) = \\ &= \cos^2\alpha\langle H'|V'\rangle\langle V'|V'\rangle\langle V'|H'\rangle + \cos\alpha\sin\alpha\langle H'|V'\rangle\langle V'|V'\rangle\langle V'|V'\rangle + \\ &+ \sin\alpha\cos\alpha\langle V'|V'\rangle\langle V'|V'\rangle\langle V'|H'\rangle + \sin^2\alpha\langle V'|V'\rangle\langle V'|V'\rangle\langle V'|V'\rangle = \\ &= \cos^2\alpha\cdot 0\cdot 1\cdot 0 + \cos\alpha\sin\alpha\cdot 0\cdot 1\cdot 1 + \sin\alpha\cos\alpha\cdot 1\cdot 1\cdot 0 + \sin^2\alpha\cdot 1\cdot 1\cdot 1 = \\ &= \sin^2\alpha \neq 0 \end{aligned} \tag{3.32}$$

The most direct way to simulate all the error sources together is by the bit flip channel presented in Table 2.1, where the probability that a bit flip occurs would be the sum of the contributions of the stray light, the dark counts and the polarization misalignments ($\sin^2\alpha$). In Cirq, this can be done as follows

```
noisy_q = cirq.bit_flip(QBER).on(q)
```

where QBER represents the probability of flipping the qubit.

5.1.3 Demodulation and Measurements

Prior to the measurement, Bob needs to demodulate, that is, to choose the basis in which he performs the measurement. If he selects the standard basis, it is not necessary to do anything, but if he selects the diagonal basis, he applies another Hadamard gate on the incoming qubit. Aftewards, he measures the state. The measurement in Cirq can be done in this manner

```
Mq_probqm = cirq.measure(q)
```

Once all the quantum gates that are to be applied are shown, it is indispensable to remember that Cirq is designed to work with quantum circuits. Therefore, all the operations must be added to a certain circuit, previously defined. The process is like this

```
qtransmission = cirq.Circuit()
qtransmission.append(operation)
```

where `operation` may be any of the aforesaid operations.

Finally, the circuit has to be simulated to obtain the outcomes. The lines of code are

```
sim = cirq.Simulator()
bob_bit = sim.run(qtransmission)
```

5.2 Basic statistical tools

How to deal with statistics in this work is one of the most important parts. In particular, there are three aspects that can be remarked:

- To simulate the random decisions of bits and bases, the function `random.randint` is used.
- The Poissonian behaviour of the number of photons is modelled with the help of the function `np.random.poisson`. On this matter, it is important to run the function only at the end, when all the losses have already been considered. Otherwise, it would lead to wrong results, since something that is arbitrary becomes deterministic each time the function is run.
- In the simulation, as happens in real life, there exist statistical fluctuations. More precisely, the shorter the number of experiments (i.e. optical pulses), the more significant these fluctuations are. In the context of QKD, these fluctuations are known as finite-size effects. This work has not put too much emphasis on this matter, but it is certainly an issue in the security analyses. Here, to deal with these fluctuations, the so-called law of large numbers in probability theory is employed. Basically, the statement of this law is that the average of the outcomes should approach the expected value as long as the number of trials used to obtain the average is sufficiently large. In symbols, the weak form reads

  $$\lim_{n\to\infty} p\left(\left|\bar{x}_n - E\left(X\right)\right| > \varepsilon\right) = 0 \tag{3.33}$$

  In practice, this can be used as a criterion to stop, that is, to determine the number of optical pulses (i.e. the duration of execution of the protocol) which is necessary to return good averages (e.g. for the sifted key rate). That is,

  $$p\left(\left|\bar{x}_n - E\left(X\right)\right| > TOL\right) < \delta \tag{3.34}$$

  where TOL and δ are parameters to be chosen in advance. Assuming symmetry for $\bar{x}_n - E\left(X\right)$, rearranging a bit the expression inside parentheses, assuming that n is sufficiently large to apply the central limit theorem and approximating the standard deviation to the sample standard deviation, it results

  $$2\left[1-\phi\left(\frac{TOL\sqrt{n}}{s_x}\right)\right] < \delta \tag{3.35}$$

  being s_x the sample standard deviation and $\phi\left(\cdot\right)$ the standard normal of the cumulative distribution function.

6 Results

6.1 Verification and Validation of the code

The results yielded by the code have been verified in the following manner:

- The probabilities of selecting each bit and each basis tend to 1/2 as the number of trials increases.
- Taking into account the Poissonian probability distribution of the number of photons, the number of non-empty pulses received by Bob is at most the number of photons reaching their destination.
- The trends concerning the quantum transmission are captured. For instance, the higher the repetition frequency is, the higher the raw (or sifted) key rate is; or the higher the losses are, the lower the raw (or sifted) key rate is.
- In general conditions, the reconciliation methods work and their performances have been satisfactorily compared with the results published in their respective papers. The confirmation and the privacy amplification protocol work as well.

Alhough the implementation has been quite simplified and finding experiments whose results could be compared was not always possible, the simulation of the quantum transmission has been validated by the mean sifted key rate obtained in [46]. Under the same conditions of repetition rate, dead time, mean photon number and losses, the sifted key rate in the experiment was 145bps after 10min, whereas the simulation yields 134.6bps after the same time interval. The differences could be due to the distinct pseudo-random number generators that were employed as well as to all those phenomena which, despite not being implemented here, happen in reality, such as the dark counts, after pulses, etc.

6.2 Sifted key rate vs losses and imperfections

In this section, the effect that the losses and the imperfections have on the length of the sifted key is remarked. Before that, a scenario is simulated as an example to give an idea of the statistical fluctuations. Such scenario has been simulated until $\delta < 1\%$ for $TOL \approx 5\%$ of the average rates in accordance with Eq. (3.35), and the results can be found in Figure 6.1.

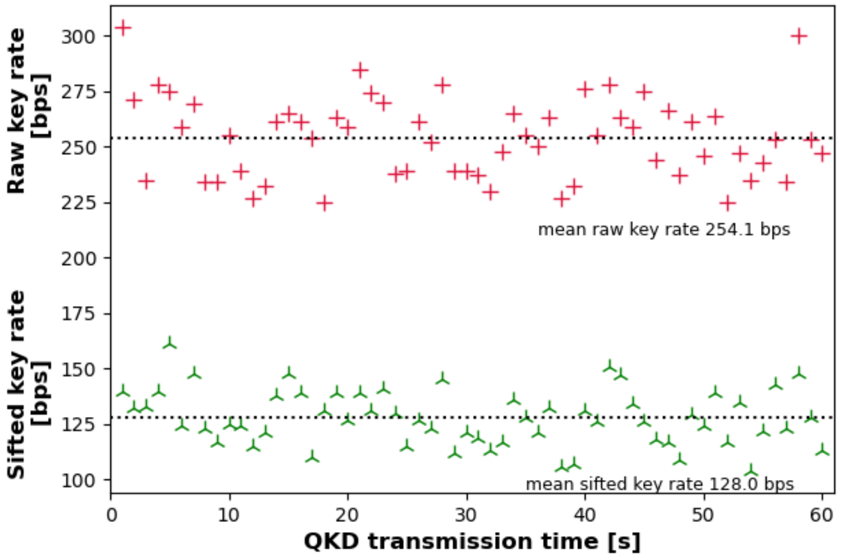

Figure 6.1 – Sample of the raw key rate (in crimson) and the sifted key rate (in green) during one minute of QKD transmission. Each point represents the average rate for one second. The simulation has been performed with f_{rep} = 1MHz, μ = 0.1, 20dB of losses through the quantum channel, 3dB of losses inside the receiver, η = 0.5 and τ = 50ns.

The following analysis that is carried out relates the mean sifted key rate to the losses through the quantum channel, with the repetition frequency as a parameter. Figure 6.2 shows the results.

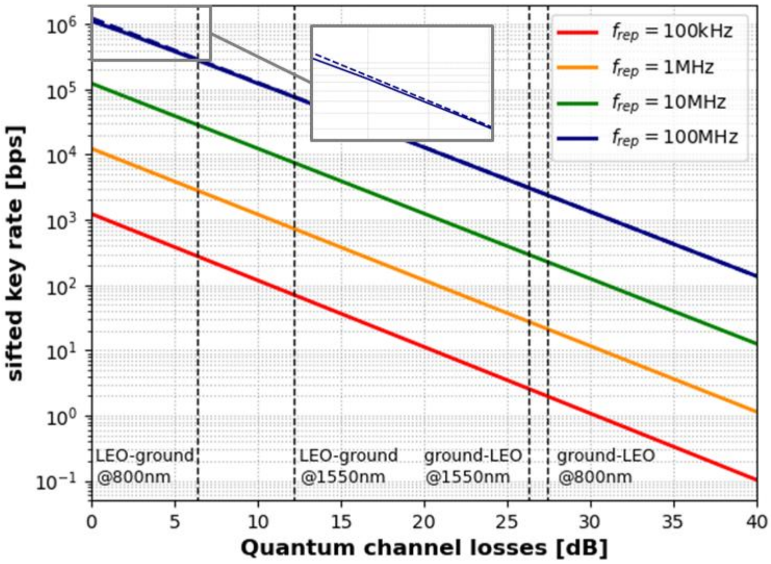

Figure 6.2 – Sifted key rate depending on the losses through the quantum channel. The simulation has been performed with different repetition frequencies, μ = 0.1, 3dB of losses inside the receiver, η = 0.5 and τ = 50ns. In addition, characteristic losses for satellite QKD have been marked. Such values have been extracted from Table 1 of [18].

Notice in Figure 6.2 how the effect of the dead time starts limiting the sifted key rate as the frequency increases. In the simulated scenario, with dead time 50ns, the limitation appears for high repetition frequencies in the order of 100MHz.

Another interesting analysis consists in seeing what happens with the sifted key rate as the mean photon number increases. The results bring to light the losses due to the attenuation of the laser pulses.

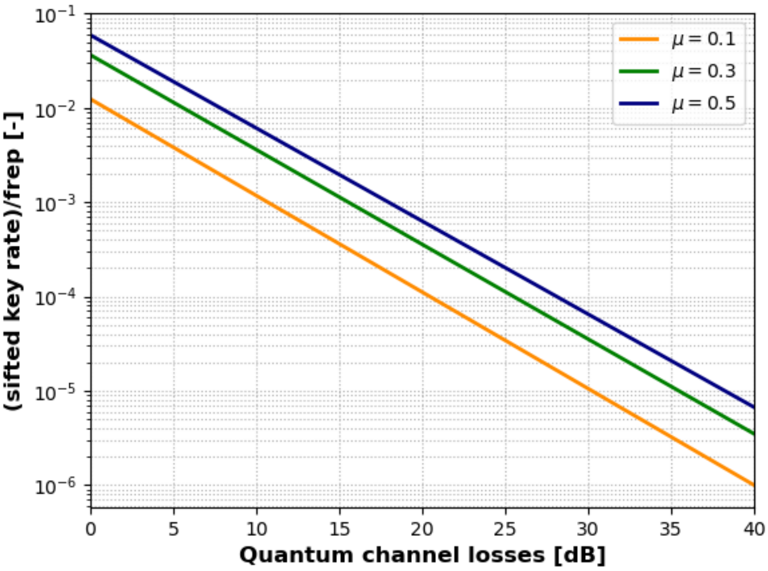

Figure 6.3 – Sifted key rate divided by the repetition frequency depending on the losses through the quantum channel. The simulation has been performed with different values of mean photon number, μ, 3dB of losses inside the receiver, $\eta = 0.5$ and $\tau = 50$ns.

Next, the impact of the quantum efficiency is stressed, taking it as a parameter in the simulations. See Figure 6.4.

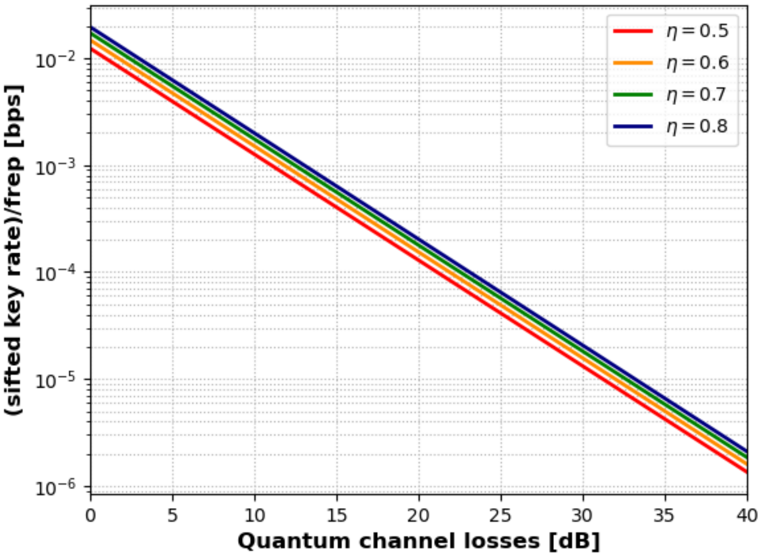

Figure 6.4 – Sifted key rate divided by the repetition frequency depending on the losses through the quantum channel. The simulation has been performed with $\mu = 0.1$, 3dB of losses inside the receiver, different values of quantum efficiency η and $\tau = 100$ns.

6.3 Comparison of the information reconciliation methods

In order to highlight the strengths and the weaknesses of the LDPC code, the reconciliation efficiency given by Eq. (3.7) and the CPU time are calculated for the former method as well as for the Cascade protocol varying two parameters: size (with QBER being approximately constant and perfect estimation of it) and imperfect estimation of QBER (with fixed QBER and size). Again, it is necessary to average the results. The first case is shown in Figure 6.5.

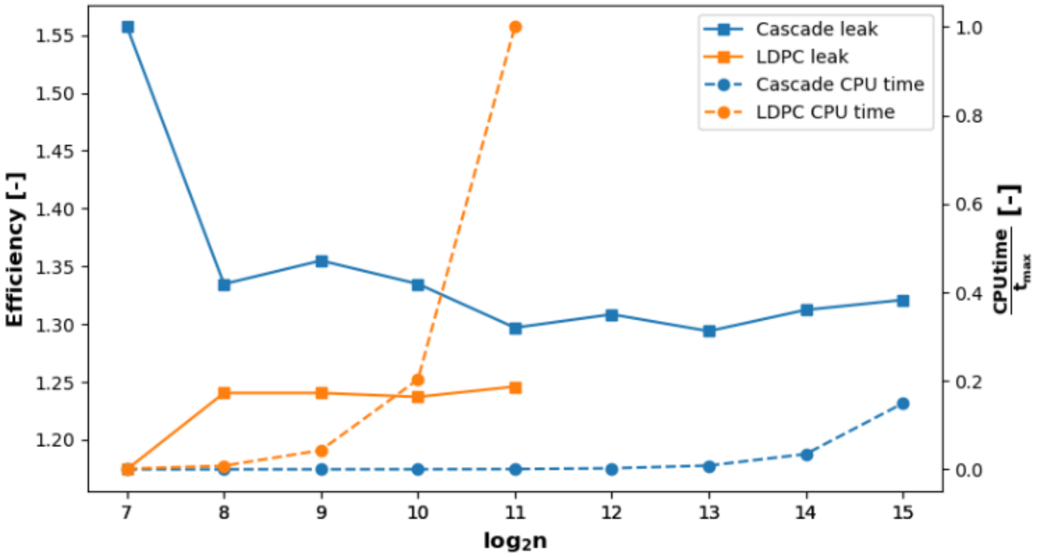

Figure 6.5 – Efficiency and CPU time against size with QBER = 5%.

As illustrated in Figure 6.5, the LDPC code seems to be better than the Cascade protocol from the leak perspective for the case of perfect error estimation, despite being much more time-consuming. The latter might be disconcerting at first sight. However, the reason lies in the construction of the matrix *H* (see Figure 6.6). The solution to this problem which is typically adopted is the construction in advance of the matrix.

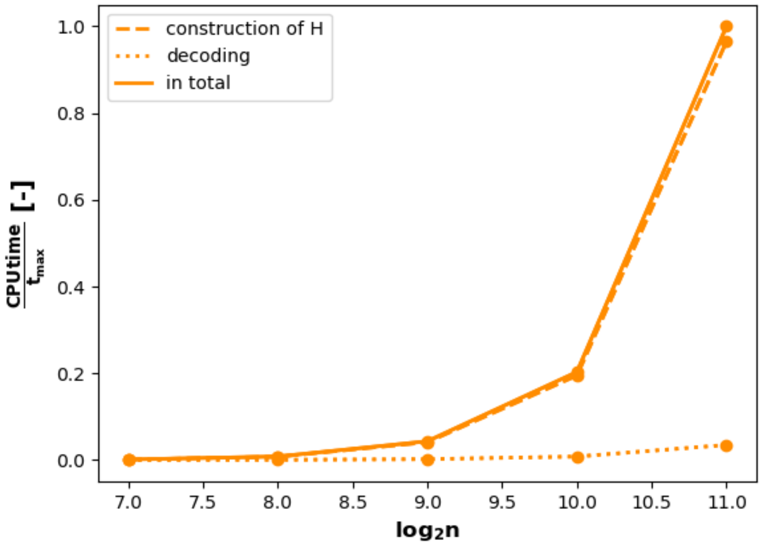

Figure 6.6 – CPU time against size for the LDPC code separating the construction of the matrix and the decoding.

Second, how the estimation of the QBER affects the performance of the reconciliation methods is simulated. In terms of efficiency, the result is that the LDPC code seems to be more efficient when the QBER is underestimated, whereas the contrary happens when it is overestimated. In terms of time, it is found that the LDPC code always takes a longer time to resolve. See Figure 6.7 below.

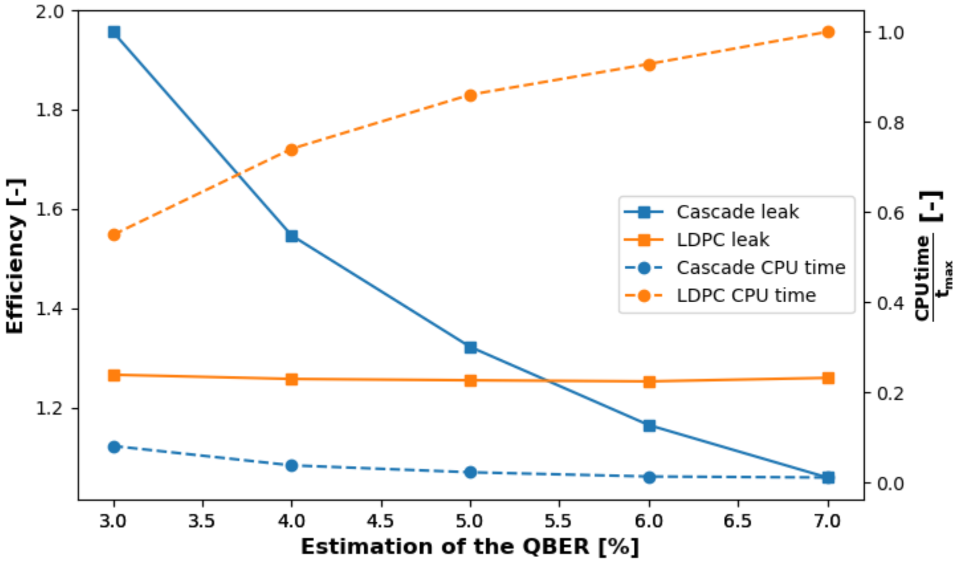

Figure 6.7 - Efficiency and CPU time against the estimation of the QBER, with QBER = 5%.

It is clear that the probability that the error-correcting methods fail gets bigger as the estimation becomes poorer. In the interval plotted in Figure 6.7, while this probability is in the order of 10^{-2} for the Cascade protocol, it is below 10^{-3} for the case of the LDPC code. However, it has been checked that this probability increases when the difference between the real QBER and the estimation grows, being higher when the QBER is underestimated.

6.4 Detection of Eve

In this section, the effect of Eve's interaction with the qubits sent by Alice is remarked. In the first place, the QBER is calculated during the QKD transmission assuming that any additional error sources do not exist. Moreover, the IR attack is simulated during different time intervals to see if the length of the sifted key allows to detect the presence of the eavesdropper. See Figure 6.8.

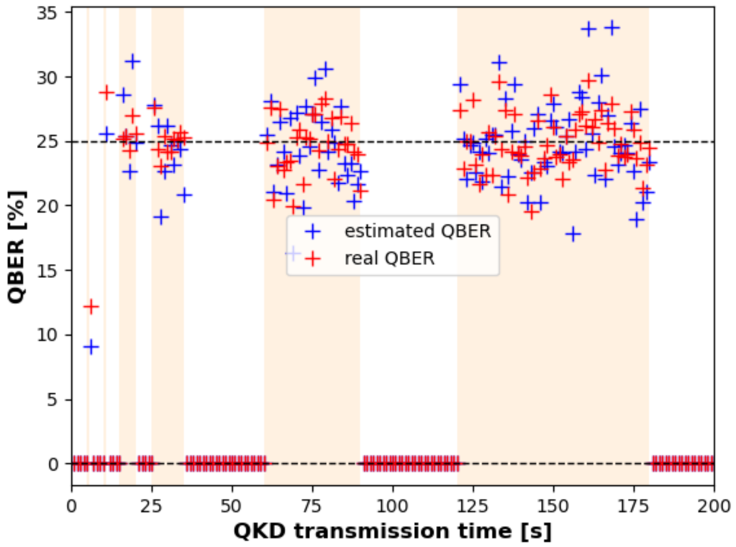

Figure 6.8 – QBER during more than three minutes of QKD transmission. Each point represents the average rate for one second. The IR attacks start being simulated at $t = 5$, 10, 15, 25, 60 and 120s, with duration 0.5, 1, 5, 10, 30 and 60s, respectively. The simulation has been performed with f_{rep} = 1MHz, $\mu = 0.1$, 15dB of losses through the quantum channel, 3dB of losses inside the receiver, η = 0.5 and τ = 50ns.

In Figure 6.8, despite the fluctuations, it is observed how the presence of the eavesdropper is easily detected. In the case of a fast attack, the estimation of the QBER might be below 25%. However, a sudden rise is visible. Now, let us see in Figure 6.9 what happens when there exists some noise independently of the IR attack.

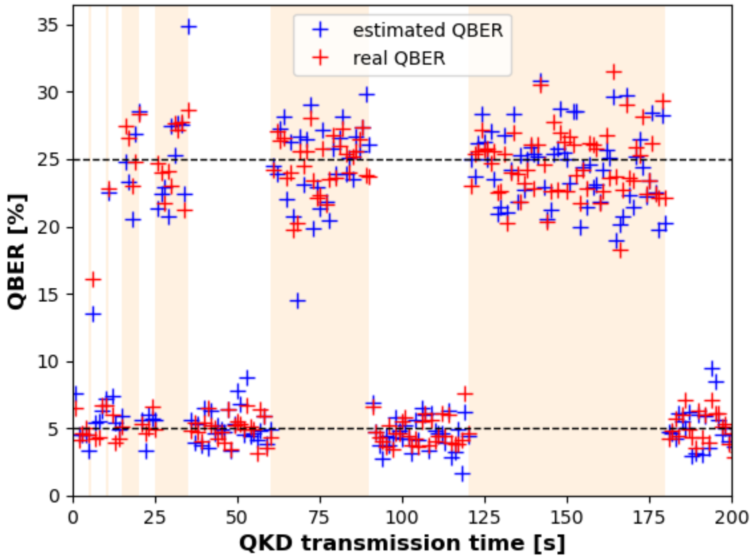

Figure 6.9 - QBER during more than three minutes of QKD transmission. Each point represents the average rate for one second. The IR attacks start being simulated at $t = 5$, 10, 15, 25, 60 and 120s, with duration 0.5, 1, 5, 10, 30 and 60s, respectively. The simulation has been performed with f_{rep} = 1MHz, $\mu = 0.1$, 15dB of losses through the quantum channel, 3dB of losses inside the receiver, η = 0.5, τ = 50ns and approximately 5% of QBER.

Again, the presence of the eavesdropper is immediately detected in spite of the fact that some additional noise exists.

6.5 Parametric study of the secret-key generation

In order to produce a valid secret key, it is important to know the length of the corrected key which is required so that the privacy amplification algorithm returns the desired length. Since the check performed with Eq. (3.22) contains various parameters, it is thus interesting to include their variations in this study. This is precisely what is made in the current section. The first parameter sweep affects the number of parity checks during the information reconciliation, or equivalently, the QBER. The results are illustrated in Figure 6.10.

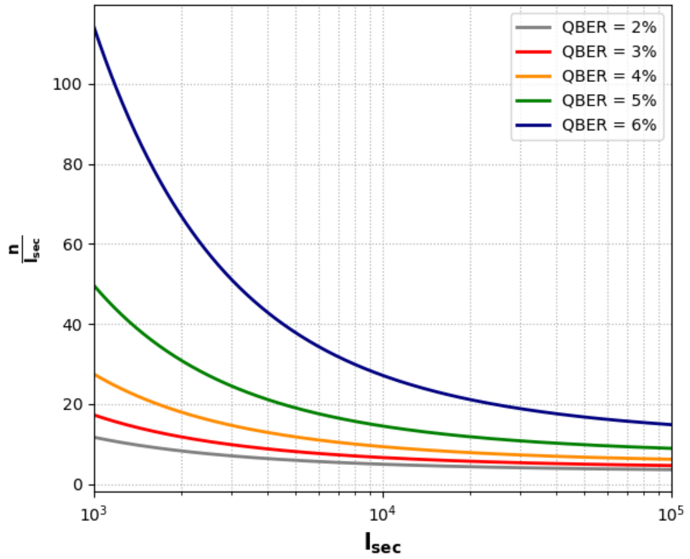

Figure 6.10 – Ratio between the lengths of the corrected key and the secret key against the desired number of bits for the secret key. This simulation considers QBER$_{max}$ = 11% and $\varepsilon_{pa} = 10^{-10}$.

Notice that the length of the corrected key needs to be at least one order of magnitude larger. This proportion increases when the QBER grows, exceeding the two orders of magnitude for shorter secret keys.

Next, the effect of the variation of the QBER threshold is shown in Figure 6.11. From it, two ideas can be extracted. First, the necessary lengh of the corrected key increases as the chosen threshold grows. Second, the effect is not negligible, therefore the choice must be carefully made in practice.

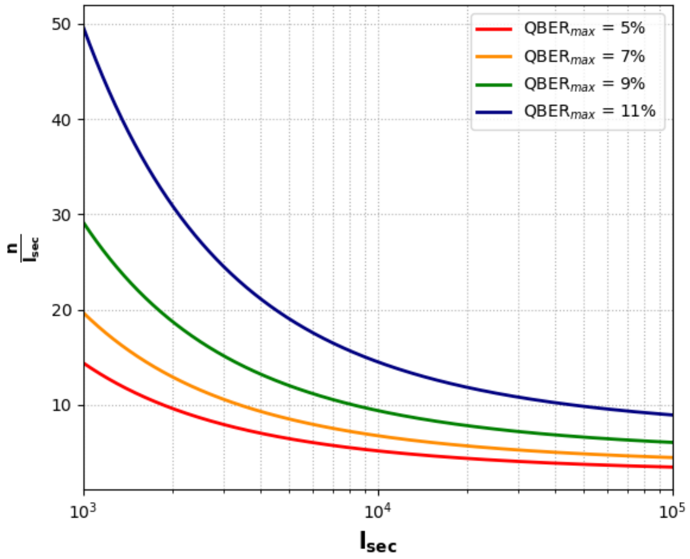

Figure 6.11 - Ratio between the lengths of the corrected key and the secret key against the desired number of bits for the secret key. This simulation considers QBER = 5% and $\varepsilon_{pa} = 10^{-10}$.

The third parameter sweep that is performed affects the security parameter of the privacy amplification (recall that this not the only contribution to the total security parameter). Figure 6.12 presents such study, showing that the effect of this parameter becomes more significant when the length of the secret key is shorter.

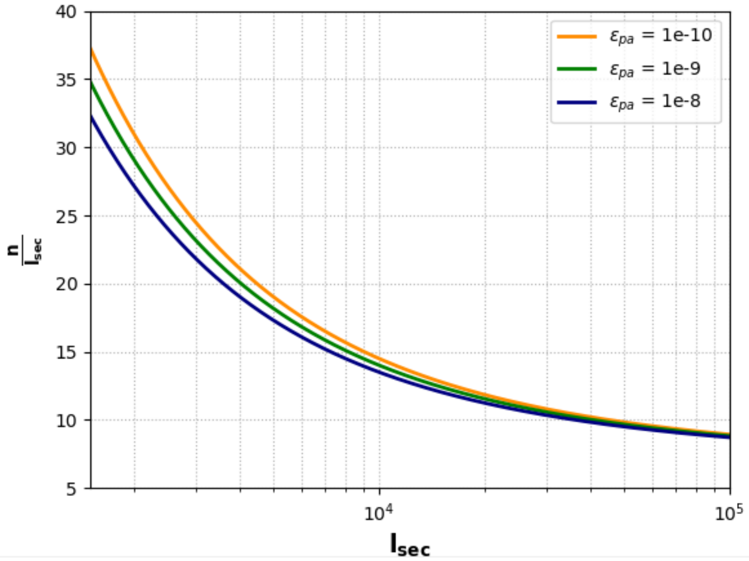

Figure 6.12 - Ratio between the lengths of the corrected key and the secret key against the desired number of bits for the secret key. This simulation considers QBER = 5% and QBER$_{max}$ = 11%.

7 Discussion

7.1 Conclusions

Throughout this document, the contents required to understand and simulate a practical QKD have been built up. First, among all the QKD protocols, the BB84 has been chosen after a conscientious study of what has been and is being made in the context of satellite QKD. The entanglement-based counterpart BBM92 could have been another interesting option, but it is left as future work. Taking into account the quantum coding of the BB84 protocol, some fundamentals about quantum states, how they can evolve with time and the importance of performing a measurement in the correct basis have been introduced. Subsequently, the protocol is described in detail, stressing the motivation behind each step. In spite of not being possible to address a deep analysis of some parts, specific methods have been justifiably selected from the set of existing solutions in the literature.

On the other hand, the code created in this project is able to run a practical BB84 protocol, including some of the imperfections of the QKD components that are typically used to implemente it, the losses and noise through the quantum channel and in the receiver, as well as the IR attack. Once again, information about the experimental QKD missions in space and state-of-the-art technology has been gathered to make the results more interesting.

In order to get an insight into a real implementation of the BB84 protocol, the results of the simulation have been collected in four sections.

Starting from the end, the eventual use of the secret key establishes a clear requirement for its length. Therefore, it is of interest to know the size of the corrected key that must reach the privacy amplification in order to satisfy this requirement. In this sense, the demand of corrected-key bits seems to be quite stringent. Additionally, it is observed that the minimum length of the corrected key increases when the QBER and the error threshold grow, whereas it decreases for higher security parameter of the privacy amplification.

Once the minimum size of the key after the reconciliation is obtained, one can estimate the duration of the QKD transmission. This is vital in the case of satellite QKD since the visibility window may be a matter of a few minutes for a LEO. To do so, it is assumed an error estimation which consists in discarding half of the bits, the minimum sifted-key length is the double. In turn, the minimum length of the raw key is approximately the double of the former as well. This quantity together with the raw key rate allows to estimate the time. Obviously, the higher the raw key rate is, the shorter the QKD transmission needs to be. To make it higher, the repetition frequency should be as high as possible to overcome the effects of the mean photon number after the attenuator, the losses and the quantum efficiency of the detector. One of the limitations of the repetition rate is the dead time, which starts being visible at high frequencies and when the losses are low.

Finally, the importance of the error estimation has been stressed for two reasons: first, because of the reduction in the performance of the information reconciliation method; and second, because it allows the detection of an IR attack.

7.2 Future work

Even though this document covers the foundations of QKD and, particularly, of the BB84 protocol from a practical viewpoint, a lot of work remains to be done. In order to fill the gap between the limited simulations performed in this work and a practicable and competitive QKD system, it is necessary to make a further study of certain areas.

From the theoretical viewpoint, understanding how the security of QKD systems can be proved is mandatory. More precisely, it is vital to become familiar with the kind of assumptions that are typically made and how to build up a QKD system in a consistent manner. On this matter, the security implications of more flexible and sophisticated attacks also need to be understood.

Additionally, it would be useful to learn more about those QKD protocols which are awaking interest; in particular, the decoy-state BB84, entanglement-based protocols and superdense coding.

On the other hand, a practical implementation faces more issues than the ones that have been considered here. Therefore, having full awareness of them is important. Some examples are how to deal with the effects of the dark counts, how to ensure an adequate synchronization between the users or how to give a solution to the time jitter.

With respect to the post-processing, it has been stressed its impact on the success of the whole protocol. For this reason, refining the different steps as much as possible is always beneficial. More concretely, it is interesting: to learn more efficient ways of estimating the QBER; to seek more efficient and robust reconciliation methods; and to adapt the confirmation step in such a way that, although the error correction fails, it is able to extract the bits that are right, discarding the ones that are not coincident.

Appendix A: Operator-sum representation

At first sight, to model the interaction between a quantum system *Q* and the environment *E*, it is tempting to take the composite system formed by both systems. As viewed in Subsection 2.1.2, using the density operator representation,

$$\rho^{QE} = \rho^{Q} \otimes \rho^{E} \tag{3.36}$$

Now, similarly to Eq. (2.28), a general evolution of the total system is given by

$$\rho^{QE'} = U^{QE} \rho^{QE} \left(U^{QE}\right)^{\dagger} = U^{QE} \left(\rho^{Q} \otimes \rho^{E}\right)\left(U^{QE}\right)^{\dagger} \tag{3.37}$$

Denoting the state of the sytem *Q* after the unitary transformation with $\varepsilon\left(\rho^{Q}\right)$, it is possible to have access to it by way of the partial trace over the environment *E*. In other words, the reduced density operator for system *Q* is

$$\varepsilon\left(\rho^{Q}\right) = \mathrm{tr}_{E}\left(\rho^{QE'}\right) = \mathrm{tr}_{E}\left(U^{QE}\left(\rho^{Q} \otimes \rho^{E}\right)\left(U^{QE}\right)^{\dagger}\right) \tag{3.38}$$

In order to transform Eq. (3.38) into something more tangible, pay attention to the following assumptions. From this point forward, the mathematical formulation becomes more abstract. Suppose the system *Q* has dimension *d* and the environment *E* has dimension *m*. In addition, suppose that $\{\left|q_i\right\rangle\}_{i=0,\ldots,d-1}$ *and* $\{\left|e_k\right\rangle\}_{k=0,\ldots,m-1}$ are two orthonormal bases for the state spaces of *Q* and *E*, respectively, being $\rho^{E} = \left|e_0\right\rangle\left\langle e_0\right|$ the initial state of the environment [14 p. 360]. Notice that this is a pure state. However, there is no loss of generality because if the real environment finds itself in a mixed state, a fictitius system *R* such that $\rho^{E} = \mathrm{tr}_{R}\left(\left|ER\right\rangle\left\langle ER\right|\right)$ can be introduced to accomplish a purification [14 p. 110]. Moreover, if the initial state of the environment is a superposition of states, it is enough to change the basis.

On the other hand, the unitary matrix (or operator) U^{QE} cannot always be directly expressed in terms of $U^{QE} = U^{Q} \otimes U^{E}$. However, the decomposition of U^{QE} into a sum of tensor products is feasible. To do so, consider the following general unitary matrix U^{QE} with *dm* rows and *dm* columns:

$$U^{QE} = \begin{bmatrix} u_{1,1} & \cdots & u_{1,dm} \\ \vdots & \ddots & \vdots \\ u_{dm,1} & \cdots & u_{dm,dm} \end{bmatrix}_{dm \times dm} \tag{3.39}$$

Note that the same matrix U^{QE} can be expressed in blocks $U_{i,j}$ of size $m \times m$ and that this fact permits to start with the decomposition (recall that $\left|q_i\right\rangle$ is but a vector with all entries zero except for the entry *i*, which is one):

$$U^{QE}=\begin{bmatrix}[U_{1,1}] & \cdots & [U_{1,d}]\\ \vdots & \ddots & \vdots\\ [U_{d,1}] & \cdots & [U_{d,d}]\end{bmatrix}_{dm\times dm}=\sum_{i,j}|q_i\rangle\langle q_j|\otimes U_{i,j} \tag{3.40}$$

Substituting the initial state of the environment $|e_0\rangle\langle e_0|$ and the decomposition given by Eq. (3.40) into Eq. (3.38), and manipulating a bit the result, it turns out that

$$\varepsilon\left(\rho^Q\right)=\mathrm{tr}_E\left(\sum_{i,j}|q_i\rangle\langle q_j|\otimes U_{i,j}\left(\rho^Q\otimes|e_0\rangle\langle e_0|\right)\left(\sum_{i,j}|q_i\rangle\langle q_j|\otimes U_{i,j}\right)^\dagger\right)= \tag{3.41}$$

$$=\mathrm{tr}_E\left(\sum_{i,j}|q_i\rangle\langle q_j|\otimes U_{i,j}\left(\rho^Q\otimes|e_0\rangle\langle e_0|\right)\sum_{i,j}|q_j\rangle\langle q_i|\otimes\left(U_{i,j}\right)^\dagger\right)= \tag{3.42}$$

$$=\mathrm{tr}_E\left(\sum_{i,j,r,s}|q_i\rangle\langle q_j|\otimes U_{i,j}\left(\rho^Q\otimes|e_0\rangle\langle e_0|\right)|q_s\rangle\langle q_r|\otimes\left(U_{r,s}\right)^\dagger\right)= \tag{3.43}$$

$$=\sum_{i,j,r,s}\mathrm{tr}_E\left(|q_i\rangle\langle q_j|\otimes U_{i,j}\left(\rho^Q\otimes|e_0\rangle\langle e_0|\right)|q_s\rangle\langle q_r|\otimes\left(U_{r,s}\right)^\dagger\right) \tag{3.44}$$

Now, making use of $\sum_k|e_k\rangle\langle e_k|=I^E$ (identity matrix in the state space of *E*) and the Eq. (2.28),

$$|q_i\rangle\langle q_j|\otimes U_{i,j}\left(\rho^Q\otimes|e_0\rangle\langle e_0|\right)|q_s\rangle\langle q_r|\otimes\left(U_{r,s}\right)^\dagger= \tag{3.45}$$

$$=|q_i\rangle\langle q_j|\otimes\sum_k|e_k\rangle\langle e_k|U_{i,j}\left(\rho^Q\otimes|e_0\rangle\langle e_0|\right)|q_s\rangle\langle q_r|\otimes\left(U_{r,s}\right)^\dagger\sum_k|e_k\rangle\langle e_k|= \tag{3.46}$$

$$=|q_i\rangle\langle q_j|\rho^Q|q_s\rangle\langle q_r|\otimes\sum_k|e_k\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger\sum_k|e_k\rangle\langle e_k|= \tag{3.47}$$

$$=|q_i\rangle\langle q_j|\rho^Q|q_s\rangle\langle q_r|\otimes\sum_{k,l}|e_k\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_l\rangle\langle e_l|= \tag{3.48}$$

$$\begin{aligned}&=|q_i\rangle\langle q_j|\rho^Q|q_s\rangle\langle q_r|\otimes\sum_k|e_k\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_k\rangle\langle e_k|+\\&+|q_i\rangle\langle q_j|\rho^Q|q_s\rangle\langle q_r|\otimes\sum_{k\neq l}|e_k\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_l\rangle\langle e_l|\end{aligned} \tag{3.49}$$

Next, introducing Eq. (3.49) into Eq. (3.44) and realizing that the part of *E* in the last addend is a non-diagonal matrix (i.e. the partial trace over *E* is zero), it results that

$$\varepsilon\left(\rho^Q\right)=\sum_{i,j,r,s}\mathrm{tr}_E\left(|q_i\rangle\langle q_j|\rho^Q|q_s\rangle\langle q_r|\otimes\sum_k|e_k\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_k\rangle\langle e_k|\right) \tag{3.50}$$

If the notation is carefully used, it is possible to rearrange the expression $|q_i\rangle\langle q_j|\rho^Q|q_s\rangle\langle q_r|$ to obtain $\langle q_j|\rho^Q|q_s\rangle|q_i\rangle\langle q_r|$, and the expression $|e_k\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_k\rangle\langle e_k|$ to obtain $\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_k\rangle|e_k\rangle\langle e_k|$, where $\langle q_j|\rho^Q|q_s\rangle$, $\langle e_k|U_{i,j}|e_0\rangle$ and $\langle e_0|\left(U_{r,s}\right)^\dagger|e_k\rangle$ are scalars. Therefore, taking out all the scalars and the summation over *k* from the partial trace,

$$\varepsilon\left(\rho^Q\right)=\sum_k\sum_{i,j,r,s}\langle q_j|\rho^Q|q_s\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^\dagger|e_k\rangle\,\mathrm{tr}_E\left(|q_i\rangle\langle q_r|\otimes|e_k\rangle\langle e_k|\right) \tag{3.51}$$

The former together with the definition of the partial trace over any system presented in Eq. (2.14), leads to

$$\varepsilon\left(\rho^{Q}\right)=\sum_{k}\sum_{i,j,r,s}\langle q_j|\rho^{Q}|q_s\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^{\dagger}|e_k\rangle|q_i\rangle\langle q_r|\operatorname{tr}\left(|e_k\rangle\langle e_k|\right)= \tag{3.52}$$

$$=\sum_{k}\sum_{i,j,r,s}\langle q_j|\rho^{Q}|q_s\rangle\langle e_k|U_{i,j}|e_0\rangle\langle e_0|\left(U_{r,s}\right)^{\dagger}|e_k\rangle|q_i\rangle\langle q_r| \tag{3.53}$$

Finally, to obtain the desired expression, rearrange the scalars and the vectors $|q_i\rangle$ and $|q_r\rangle$, extend the transpose operation on the right and divide the summation over *i*, *j*, *r*, *s* into the two original summations.

$$\varepsilon\left(\rho^{Q}\right)=\sum_{k}\sum_{i,j,r,s}\langle e_k|U_{i,j}|e_0\rangle|q_i\rangle\langle q_j|\rho^{Q}|q_s\rangle\langle q_r|\langle e_0|\left(U_{r,s}\right)^{\dagger}|e_k\rangle= \tag{3.54}$$

$$=\sum_{k}\sum_{i,j,r,s}\langle e_k|U_{i,j}|e_0\rangle|q_i\rangle\langle q_j|\rho^{Q}\left(\langle e_0|U_{r,s}|e_k\rangle|q_r\rangle\langle q_s|\right)^{\dagger}= \tag{3.55}$$

$$=\sum_{k}\left(\sum_{i,j}\langle e_k|U_{i,j}|e_0\rangle|q_i\rangle\langle q_j|\rho^{Q}\sum_{i,j}\left(\langle e_0|U_{i,j}|e_k\rangle|q_i\rangle\langle q_j|\right)^{\dagger}\right)= \tag{3.56}$$

$$=\sum_{k}E_k\rho^{Q}\left(E_k\right)^{\dagger} \tag{3.57}$$

The operators E_k are known as Kraus operators or operation elements for the quantum operation ε and the approach is called operator-sum representation. The matrix representation of E_k is

$$E_k=\sum_{i,j}\langle e_k|U_{i,j}|e_0\rangle|q_i\rangle\langle q_j|=\begin{bmatrix}\langle e_k|U_{1,1}|e_0\rangle & \cdots & \langle e_k|U_{1,d}|e_0\rangle\\ \vdots & \ddots & \vdots\\ \langle e_k|U_{d,1}|e_0\rangle & \cdots & \langle e_k|U_{d,d}|e_0\rangle\end{bmatrix}_{d\times d} \tag{3.58}$$

The procedure narrated between Eq. (3.39) and Eq. (3.58) is not taken from anywhere. In [14 p. 360], the operator-sum representation is presented, but it is difficult to believe for a beginner at dealing with tensor products and partial traces. For this reason, although it is rather longer, the detailed deduction used in this appendix seems to be more convenient.

Finally, there are two assumptions made at the beginning that remain to be clarified. First, the fact that the joint state ρ^{QE} can be expressed as a tensor product between the individual states. This is allowable providing that there is no correlation (entanglement) between the system *Q* and the environment *E* [14 p. 358]. Although this condition is not always fulfilled, the experimentalist has some control mechanisms. For example, it is difficult to imagine a situation with entanglement for a system *Q* consisting of a newly released photon. Second, even though the dimension of the environment *m* needs to be sufficiently large, it is not necessary the whole universe. It is enough to consider an environment of dimension d^2 at the most [14 p. 358].

Appendix B: Binary symmetric channel

The conditional entropy $H\left(X_A \mid X_B\right)$ can be expressed in terms of the joint probability distribution and the conditional probability distribution as follows

$$H\left(X_A \mid X_B\right) \equiv H\left(X_A, X_B\right) - H\left(X_B\right) = \tag{3.59}$$

$$= -\sum_{x_A,\, x_B} p\left(x_A, x_B\right) \log_2 p\left(x_A, x_B\right) + \sum_{x_B} p\left(x_B\right) \log_2 p\left(x_B\right) \tag{3.60}$$

The joint probability is related to the conditional probability through

$$p\left(x_A, x_B\right) = p\left(x_A \mid x_B\right) p\left(x_B\right) \tag{3.61}$$

Moreover,

$$p\left(x_B\right) = \sum_{x_A} p\left(x_A, x_B\right) \tag{3.62}$$

Substituting Eq. (3.61) and Eq. (3.62) into Eq. (3.59) and using the product rule for logarithms, it results

$$\begin{aligned} H\left(X_A \mid X_B\right) &= -\sum_{x_A, x_B} p\left(x_A, x_B\right) \left[\log_2 p\left(x_A \mid x_B\right) + \cancel{\log_2 p\left(x_B\right)} \right] + \\ &+ \cancel{\sum_{x_A, x_B} p\left(x_A, x_B\right) \log_2 p\left(x_B\right)} = \end{aligned} \tag{3.63}$$

$$= -\sum_{x_A, x_B} p\left(x_A, x_B\right) \log_2 p\left(x_A \mid x_B\right) \tag{3.64}$$

Now, to make Eq. (3.63) start looking like the binary entropy with parameter QBER, express $p\left(x_A \mid x_B\right)$ in terms of $p\left(x_B \mid x_A\right)$

$$p\left(x_A \mid x_B\right) = \frac{p\left(x_A, x_B\right)}{p\left(x_B\right)} = \frac{p\left(x_B \mid x_A\right) p\left(x_A\right)}{p\left(x_B\right)} \tag{3.65}$$

and begin to use the binary *symmetric* channel properties

$$p\left(x_B\right) = p\left(x_A\right) \tag{3.66}$$

$$p\left(x_B \mid x_A\right) = \begin{cases} QBER & \text{if } x_B \neq x_A \\ 1 - QBER & \text{if } x_B = x_A \end{cases} \tag{3.67}$$

To get the binary entropy expression, it is enough to use Eqs. (3.65) through (3.67) and separate $H\left(X_A \mid X_B\right)$ into two terms

$$H\left(X_A \mid X_B\right) = -\sum_{x_A, x_B} p\left(x_A, x_B\right) \log_2 p\left(x_B \mid x_A\right) = \tag{3.68}$$

$$= -\sum_{x_A \neq x_B} p\left(x_A, x_B\right) \log_2 \mathrm{QBER} - \sum_{x_A = x_B} p\left(x_A, x_B\right) \log_2 \left(1 - \mathrm{QBER}\right) = \tag{3.69}$$

$$= -\left[\sum_{x_A \neq x_B} p\left(x_A, x_B\right)\right] \log_2 \mathrm{QBER} - \left[\sum_{x_A = x_B} p\left(x_A, x_B\right)\right] \log_2 \left(1 - \mathrm{QBER}\right) = \tag{3.70}$$

$$= -p\left(x_A \neq x_B\right) \log_2 \mathrm{QBER} - p\left(x_A = x_B\right) \log_2 \left(1 - \mathrm{QBER}\right) = \tag{3.71}$$

$$= -\mathrm{QBER} \log_2 \mathrm{QBER} - \left(1 - \mathrm{QBER}\right) \log_2 \left(1 - \mathrm{QBER}\right) = h\left(\mathrm{QBER}\right) \tag{3.72}$$

References

[1] STYER, D. Appendix A – A Brief History of Quantum Mechanics. In: *The Strange World of Quantum Mechanics.* Ohio: Cambridge University Press, 2008, pp. 119-132. ISBN 978-0521667807.

[2] HEISENBERG, W. The Physical Content of Quantum Kinematics and Mechanics. In: WHEELER, J. and ZUREK, W., Eds. *Quantum Theory and Measurement*. Princeton: Princeton University Press, 1983, pp. 62-66.

[3] DIRAC, P. *The Principles of Quantum Mechanics.* Fourth edition.Oxford: Oxford University Press, 1958. ISBN 9333605502.

[4] ZWIEBACH, B. Chapter 1 – Key Features of Quantum Mechanics. In: *Lecture notes of Quantum Physics I.* Mass.: MIT Press, 2016, pp.12-14.

[5] COUTEAU, C. Spontaneous Parametric Down-Conversion. *Journal of Contemporary Physics.* Springer. August 2018, vol. 59(3), 291-304. doi: 10.1080/00107514.2018.1488463.

[6] JAEGER, L. *The Second Quantum Revolution.* Baar: Springer, 2018. ISBN 978-3319988238.

[7] QUANTUM FLAGSHIP IQCLOCK CONSORTIUM.iqClock [online]. 2018 [Cited: 13 August 2020]. Available at: https://www.iqclock.eu/.

[8] KEESEY, L. Industry Team Creates and Demonstrates First Quantum Sensor for Satellite Gravimetry. NASA Goddard Space Flight Center News [online]. December 2018 [Cited: 13 August 2020]. Available at: https://www.nasa.gov/feature/goddard/2018/nasa-industry-team-creates-and-demonstrates-first-quantum-sensor-for-satellite-gravimetry.

[9] QUANTUM SPACESHIP. Quantum Technologies in Space. s.l.: 2019, pp.14-15. Policy White Paper. Available at: http://www.qtspace.eu/?q=whitepaper.

[10] EUROPEAN COMMISSION. *Quantum Technologies and the advent of the Quantum Interne*t. Luxembourg: Publications Office of the European Union, 2019. ISBN 978-92-76-08960-5, doi:10.2759/458430.

[11] QUANTUM FLAGSHIP COMMUNITY. Supporting Quantum Technologies beyond H2020. Oberkochen: 2018 p.5. Quantum Support Action, v1.1. Available at: http://www.qtspace.eu/?q=whitepaper.

[12] JONES, N. Google and NASA snap up quantum computer. *Nature* [online]. May 2013 [Cited: 13 August 2020]. Available at: https://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999.

[13] QUROPE. *Quantum Manifiesto. A New Era of Technology*. [Online]. May 2016 [Cited: 13 August 2020]. Available at: http://qurope.eu/manifesto.

[14] NIELSEN, M. and CHUANG, I. *Quantum Computation and Quantum Information*. Tenth edition. Cambridge: Cambridge University Press, 2010.ISBN 978-1-107-00217-3.

[15] GIDNEY, C. and EKERA, M. *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. arXiv e-print. December 2019. arXiv:1905.09749.

[16] FANG, X, *et al*. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nature Photon*, vol. 14, 2020, 422-425. doi:10.1038/s41566-020-0599-8.

[17] SCHEIDL, T, *et al*. Feasibility of 300 km Quantum Key Distribution with Entangled States. *New J. Phys*. IOP Publishing. August 2009, vol. 11(8). doi: 10.1088/1367-2630/11/8/085002.

[18] ASPELMEYER, M., *et al*. Long-Distance Quantum Communication with Entangled Photons using Satellites. *IEEE Journal of Selected Topics in Quantum Electronics*. IEEE. 2003, vol. 9(3), 1541-1551. doi: 10.1109/JSTQE.2003.820918.

[19] KHAN, I., *et al*. Satellite-based QKD. *Optics & Photonics News.* OSA. February 2018, vol. 29, 26-33.

[20] SHANNON, C. A Mathematical Theory of Communication. *Bell System Technical Journal*. July 1948, vol. 27(3), 379-423. doi: 10.1002/j.1538-7305.1948.tb01338.x.

[21] SLEPIAN, D. and WOLF, J. Noiseless coding of correlated information sources. In: *IEEE Transactions on Information Theory*. IEEE. s.l.: July 1973, vol. 19(4), 471-480. doi: 10.1109/TIT.1973.1055037.

[22] SCARANI, V., *et al*. The Security of Practical Quantum Key Distribution. *Rev. Mod. Phys.* APS. September 2019, vol. 81(3), 1301-1350. doi: 10.1103/RevModPhys.81.1301.

[23] HIRANO, T., *et al*. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Sci. Technol.* IOP Publishing. June 2017, vol. 2(2). doi: 10.1088/2058-9565/aa7230.

[24] DIAMANTI, E., *et al*. Practical challenges in quantum key distribution. *Quantum Inf.* Nature Publishing Group. November 2016, vol. 2(16025). doi:10.1038/npjqi.2016.25

[25] PASCHOTTA, R. Optical heterodyne detection. In: *Encyclopedia of Laser Physics and Technology*. s.l.: Wiley-VCH, 2008. ISBN 978-3-527-40828-3.

[26] ASIF, R. and BUCHANAN, W. Seamless Cryptographic Key Generation via Off-the-Shelf Telecommunication Components for End-to-End. In: *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE. Exeter: 2017, 910-916. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.140.

[27] LAUDENBACH, F. Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations. *Adv. Quantum Technol.* Wiley-VCH. June 2018, vol. 1(1). doi: 10.1002/qute.201800011.

[28] ZHANG, Y., *et al*. Long-Distance Continuous-Variable Quantum Key Ditribution over 202.81 km of Fiber. *Phys. Rev. Lett.* American Physical Soiciety. June 2020, vol. 125(1), 010502. doi: 10.1103/PhysRevLett.125.010502.

[29] HUANG, D., *et al*. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* Nature Publishing Group. January 2016, vol. 6(19201). doi: 10.1038/srep19201.

[30] LI, C., QIAN, L. and LO, H. *Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources*. arXiv e-print. August 2019, 1. arXiv:1908.11423.

[31] DJORDJEVIC, I. *Physical-Layer Security and Quantum Key Distribution.* Gewerbestrasse: Springer, 2019. ISBN 978-3-030-27564-8.

[32] BENNETT, C. and BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. IEEE. Bangalore: 1984, 175-179. doi: 10.1016/j.tcs.2014.05.025.

[33] EKERT, A. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* APS. 1991, vol. 67(6), 661-663. doi: 10.1103/PhysRevLett.67.661.

[34] BENNETT, C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* APS. 1992, vol. 68(21), 3121-3124. doi: 10.1103/PhysRevLett.68.3121.

[35] BENNETT, C., BRASSARD, G. and MERMIN, N. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* APS. 1992, vol.68(5), 557-559. doi: 10.1103/PhysRevLett.68.557.

[36] ISLAM, N., *et al*. Provably-Secure and High Rate Quantum Key Distribution with Time-Bin Qudits. *Science Advances*. Nov 2017, vol. 3(11). doi: 10.1126/sciadv.1701491.

[37] SPEDALIERI, F. *Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum*. arXiv e-print. Sep 2004. arXiv:quant-ph/0409057.

[38] HWANG, W. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* APS. August 2003, vol. 91(5), 057901. doi: 10.1103/PhysRevLett.91.057901.

[39] PASCHOTTA, R. Coherent states. In: *Encyclopedia of Laser Physics and Technology*. s.l.: Wiley-VCH, 2008. ISBN 978-3-527-40828-3.

[40] GHALAII, M., *et al*. Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. *IEEE Journal on Selected Areas in Communications.* IEEE. March 2020, vol. 38(3), 507. doi: 10.1109/JSAC.2020.2969058.

[41] GROSSHANS, F. and GRANGIER, P. Continuous Variable Quantum Cryptography Using Coherent States. Phys. Rev. Lett. APS. 2002, vol. 88(5), 057902. doi: 10.1103/PhysRevLett.88.057902.

[42] BEDINGTON, R., ARRAZOLA, J. and LING, A. Progress in satellite quantum key distribution. *Quantum Information*. Nature Publishing Group. August 2017, vol. 3(30). doi: 10.1038/s41534-017-0031-5.

[43] KHAN, I., *et al*. Satellite-based QKD. *Optics & Photonics News.* OSA. February 2018, vol. 29, 26-33.

[44] VALLONE, G., *et al*. Experimentl Satellite Quantum Communications. *Phys. Rev. Lett.* APS. July 2015, vol. 115(4). doi: 10.1103/PhysRevLett.115.040502.

[45] WANG, J., *et al*. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photon*. Nature Publishing Group April 2013, vol. 7, 387-393. doi: 10.1038/nphoton.2013.89.

[46] NAUERTH, S. *Air to Ground Quantum Key Distribution*. Munich: Universität München, 2013. Dissertation.

[47] GUNTHNER, K., *et al*. *Quantum-limited measurements of optical signals from a geostationary satellite.* arXiv e-print. February 2017. arXiv:1608.03511.

[48] LIAO, S., *et al*. Space-to-Ground Quantum Key Distritbution Using a Small-Sized Payload on

Tiangong-2 Space Lab. *Chin. Phys. Lett.* Chinese Physical Society and IOP Publishing Ltd. 2017, vol. 34(9), 090302. doi: 10.1088/0256-307X/34/9/090302.

[49] LIAO, S., *et al*. Satellite-to-ground quantum key distribution. *Nature.* August 2017, vol. 549, 43-47. doi:10.1038/nature23655.

[50] YIN, J., *et al*. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*. June 2020, vol. 582, 501-505. doi: 10.1038/s41586-020-2401-y.

[51] PUGH, C., *et al*. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Sci. Technol.* IOP Publishing. June 2017, vol. 2(2), 024009. doi: 10.1088/2058-9565/aa701f.

[52] TAKENAKA, H., *et al*. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nature Photon.* Nature Publishing Group. July 2017, vol. 11, 502-508. doi: 10.1038/nphoton.2017.107.

[53] GRIEVE, J., *et al*. SpooQySats: cubesats to demonstrate quantum key distribution technologies. *Acta Astronautica*. ElSevier. Adelaide: October 2018, vol. 151, 103-106. doi: 10.1016/j.actaastro.2018.06.005.

[54] HABER, R., *et al*. QUBE – A CubeSat for Quanqum Key Distribution Experiments. In: *32nd Annual AIAA/USU Conference on Small Satellites.* 2018. Available at: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4081&context=smallsat

[55] SCIENCE AND TECHNOLOGY FACILITIES COUNCIL. *UK and Singapore Collaborate on £10m satellite project to develop next generation communications networks* [online]. September 2018 [Cited: 28 August 2020]. Available at: https://stfc.ukri.org/news/uk-and-singapore-collaborate-on-10m-satellite-project/.

[56] JENNEWEIN, T., *et al*. The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. In: *Proceedings SPIE Security and Defense*. Amsterdam: 2014, vol. 9254, 925402. doi: 10.1117/12.2067548.

[57] KERSTEL, E., *et al*. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technol.* Springer. June 2018, vol. 5(6). doi: 10.1140/epjqt/s40507-018-0070-7.

[58] PODMORE, H. *et al*. Optical Terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat). In: *2019 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*. IEEE. Portland: 2019, 1-5. doi: 10.1109/ICSOS45490.2019.8978993.

[59] ALEX LING GROUP. Quantum Tech demos on CubeSat nanosatellites. 2015. Presentation. Available at: http://www.qtspace.eu/sites/testqtspace.eu/files/presentations/Bedington%20-%20CQT%20Singapore%20-%20Quantum%20CubeSats_1.pdf.

[60] PAYER, M. *SES Announces 10 Project Partners in QUARTZ Satellite Cybersecurity Consortium* [online]. June 2018 [Cited: 28 August 2020]. Available at: https://www.ses.com/press-release/ses-announces-10-project-partners-quartz-satellite-cybersecurity-consortium.

[61] PULTAROVA, T. *Unleashing quantum into the world* [online]. April 2018 [Cited: 28 August 2020]. Available at: https://https://eandt.theiet.org/content/articles/2019/04/unleashing-quantum-into-the-world/eandt.theiet.org/content/articles/2019/04/unleashing-quantum-into-the-world/.

[62] EUROPEAN COMMISSION. European Industry White Paper on the European Quantum Communication Infraestructure. 2019. White Paper. Available at: http://www.qtspace.eu/sites/testqtspace.eu/files/other_files/IndustryWhitePaper_V3.pdf.

[63] GRAHAM, T., *et al*. Superdense teleportation using hyperentangled photons. *Nat Commun.* Nature Publishing Group. May 2015, vol. 6, 7185. doi: 10.1038/ncomms8185.

[64] CHAPMAN, J., *et al*. Time-Bin and Polarization Superdense Teleportation for Space Applications. *Phys. Rev. Applied*. APS. July 2020, vol. 14(1), 014044. doi: 10.1103/PhysRevApplied.14.014044.

[65] ERA LEARN. Project: Quantum-safe Communications for High Altitude Platforms [online]. 2018 [Cited: 28 August 2020]. Available at: https://www.era-learn.eu/network-information/networks/eurostars-2/eurostars-cut-off-3/quantum-safe-communications-for-high-altitude-platforms.

[66] OI, D., *et al*. CubeSat quantum communications mission. *EPJ Quantum Technol.* Springer. April 2017, vol. 4, 6. doi: 10.1140/epjqt/s40507-017-0060-1.

[67] KRAWCSYK, H. LFSR-based Hashing and Authentication. In: *Desmedt Y.G. (eds) Advances in Cryptology (CRYPTO 1994).* Lecture Notes in Computer Science. Springer. 1994, vol 839. doi: 10.1007/3-540-48658-5_15.

[68] SHOR, P. and PRESKILL, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* APS. July 2000, vol. 85, 441-444. doi: 10.1103/PhysRevLett.85.441.

[69] KIKTENKO, E., *et al*. Error estimation at the information reconciliation stage of the quantum key distribution. *J. Russ. Laser Res.* Springer. November 2018, vol. 39, 558-567. doi: 10.1007/s10946-018-9752-y.

[70] MARTINEZ-MATEO, J., *et al*. Demystifying the Information Reconciliation Protocol Cascade. *Quantum Information & Computation*. April 2015, vol. 15(5&6), 453-477. doi: 10.5555/2871401.2871407.

[71] PEARSON, D., *et al.* High-speed QKD Reconciliation using Forward Error Correction. *AIP Conference Proceedings*. AIP. November 2015, vol. 734(1), 299-302. doi: 10.1063/1.1834439.

[72] ETSI. Quantum Key Distribution (QKD); Security Proofs. 2010-2012. Available at: https://www.etsi.org/deliver/etsi_gs/qkd/001_099/005/01.01.01_60/gs_qkd005v010101p.pdf.

[73] BRASSARD, G. and SALVAIL, L. Secret-Key Reconciliation by Pulbic Discussion. In: *Advances in Cryptology –EUROCRYPT '93.* Springer Berlin Heidelberg. 1994, LNCS vol. 765, 410-423. doi: 10.1007/3-540-48285-7_35.

[74] MARTINEZ-MATEO, J., ELKOUSS, D. and MARTIN, V. Blind Reconciliation. *Quantum Information and Computation*. 2012, vol. 12(9), 0791. Also available at: arXiv:1205.5729.

[75] MACKAY, D. and NEAL, R. Near Shannon limit performance of low density parity check codes. *Electronics Letters*. August 1996, vol. 32(18), 1645-1646. doi: 10.1049/el:19961141.

[76] KIKTENKO, E., *et al.* Post-processing procedure for industrial quantum key distribution systems. *J. Phys. Conf. Ser.* IOP Publishing. March 2016, vol. 741, 012081. doi: 10.1088/1742-6596/741/1/012081.

[77] FEDOROV, A., KIKTENKO, E. and TRUSHECHKIN, A. Symmetric blind information reconciliation and hash-function-based verification for quantum key distribution. *Lobachevskii J. Math*. Springer. September 2018, vol. 39, 992. doi: 10.1134/S1995080218070107.

[78] KROVETZ, T. and ROGAWAY, P. Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction. In: *Won D. (eds.) Information Security and Cryptology (ICISC 2000).* Springer, Berlin, Heidelberg. 2001, LNCS vol. 2015. doi: 10.1007/3-540-45247-8_7.

[79] ETSI. Latest publications [online]. 2020 [Cited: 15 September 2020]. Available at: https://www.etsi.org/committee/1430-qkd.

[80] SHI, H. An introduction of ISO/IEC 23837. In: QKD Standardization in ISO/IEC JTC 1/SC 27 ISO. June 2019. Presentation. Available at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Presentation_Hongsong%20Shi_QKD_in_ISO-V5.pdf.

[81] TOMAMICHEL, M. and LEVERRIER, A. A largely self-contained and complete security proof for quantum key distribution. *Quantum*. July 2017, vol. 1, 14. doi: 10.22331/q-2017-07-14-14.

[82] FOX, M. *Quantum Optics – An Introduction.* New York: Oxford University Press, 2006. ISBN: 978-0198566731.

[83] REIMER, M. and CHER, C. The quest for a perfect single-photon source. *Nat. Photonics*. Nature Publishing Group. October 2019, vol. 13, 734-736. doi: 10.1038/s41566-019-0544-x.

[84] ETSI. Quantum Key Distribution (QKD); Component characterization: characterization optical components for QKD systems. 2016. Available at:
https://www.etsi.org/deliver/etsi_gs/QKD/001_099/011/01.01.01_60/gs_QKD011v010101p.pdf.

[85] HUGHESM R. and NORDHOLT, J. Quantum space race heats up. *Nat. Photonics*. Springer Nature. August 2017, vol. 11, 458.

[86] PASCHOTTA, R. Avalanche Photodiodes. In: *Encyclopedia of Laser Physics and Technology*. s.l.: Wiley-VCH, 2008. ISBN 978-3-527-40828-3.

[87] LASER COMPONENTS. Pulsed Laser Diodes and Avalanche Photodiodes [online]. 2018 [Cited: 20 September 2020]. Supply catalog, p. 48. Available at:
https://www.lasercomponents.com/fileadmin/user_upload/home/Datasheets/lc/kataloge/pld-apd.pdf.

[88] LASER COMPONENTS. Silicon Geiger Mode Avalanche Photodiodes [online]. 2020 [Cited: 20 September 2020]. Supply catalog, pp. 4-5. Available at:
https://www.lasercomponents.com/fileadmin/user_upload/home/Datasheets/lc-apd/sap-series.pdf

[89] CIRQ DEVELOPERS. Cirq documentation [online]. 2018 [Cited: 20 September 2020]. Available at: https://cirq.readthedocs.io/en/stable/.