UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

School of Telecommunications Engineering

Analysis of performance of actual implementation of QKD systems

End of Degree Project

Bachelor's Degree in Telecommunication Technologies and Services Engineering

AUTHOR: Schroedt-Girard Maestre, Yohan-Eder

Tutor: Diego Antón, María de

External cotutor: Martelli, Paolo

ACADEMIC YEAR: 2023/2024

Resumen

En los sistemas de telecomunicaciones modernos, es necesario cifrar la información para evitar que agentes externos accedan, alteren o almacenen el mensaje. La distribución de claves necesaria para ambas partes comunicantes, tradicionalmente referidas como Alice y Bob, presenta un cambio de paradigma debido a los avances significativos en las aplicaciones de Información Cuántica. Este proyecto es un estudio de la Distribución de Claves Cuánticas (QKD) como solución a la inminente falta de seguridad en la distribución de claves, definiendo sus fundamentos teóricos, problemas de implementación y evaluando su rendimiento a través de simulaciones en MATLAB. El trabajo considera dos casos para comparar: el caso de un protocolo BB84 ideal que utiliza fuentes de fotones únicos, y un caso práctico de estado señuelo que utiliza láseres atenuados, ambos teniendo en cuenta dos tipos diferentes de detectores, un diodo de avalancha de fotón único (SPAD) y un detector de fotones individuales de nanocables superconductores (SSPD).

Resum

En els sistemes de telecomunicacions moderns, és necessari xifrar la informació per a evitar que agents externs accedisquen, alteren o emmagatzemen el missatge. La distribució de claus necessària per a ambdues parts comunicants, tradicionalment referides com Alice i Bob, presenta un canvi de paradigma degut als avanços significatius en les aplicacions d'Informació Quàntica. Aquest projecte és un estudi de la Distribució de Claus Quàntiques (QKD) com a solució a la imminent falta de seguretat en la distribució de claus, definint els seus fonaments teòrics, problemes d'implementació i avaluant el seu rendiment a través de simulacions en MATLAB. El treball considera dos casos per a comparació: el cas d'un protocol BB84 ideal que utilitza fonts de fotons únics, i un cas pràctic d'estat senyal que utilitza làsers atenuats, ambdós tenint en compte dos tipus diferents de detectors, un díode d'allau de fotó únic (SPAD) i un detector de fotons individuals de nanofils superconductors (SSPD).

Abstract

In modern telecommunications systems, it is necessary to encrypt information to prevent external agents from accessing, altering, or storing the message. The distribution of keys required by both communicating parties, traditionally referred to as Alice and Bob, needed to encrypt and decrypt the message, presents a paradigm shift due to significant advances in Quantum Information applications. This project is a study of Quantum Key Distribution as a solution to the imminent lack of security in key distribution, defining its theoretical foundations, implementation issues, and evaluating its performance through MATLAB simulations. The work considers two cases for comparison: the case of an ideal BB84 protocol that exploits single-photon sources, and a practical decoy state case, using attenuated lasers, both taking into account two different detectors, a single-photon avalanche diode (SPAD) and a superconducting nanowire single-photon detector (SSPD).

EXECUTIVE SUMMARY

The degree thesis must develop in the text the following concepts, appropriately justified and discussed, focusing on the telecommunication engineering

CONCEPT (ABET)	**Done? (Y/N)**	**Where? (page numbers)**
1. IDENTIFY:	**Y**	**39-44**
1.1. Problem statement and opportunity	Y	39
1.2. Constraints (standards, codes, needs, requirements & specifications)	Y	40-44
1.3. Setting of goals	Y	39-40
2. FORMULATE:	**Y**	**45-55**
2.1. Creative solution generation (analysis)	Y	45
2.2. Evaluation of multiple solutions and decision-making (synthesis)	Y	45-55
3. SOLVE:	**Y**	**56-57**
3.1. Fulfilment of goals	Y	56
3.2. Overall impact and significance (contributions and practical recommendations)	Y	56-57

Table of contents

Objectives

This work aims to introduce Quantum Key Distribution (QKD) and provide a comprehensive overview of the challenges in its experimental implementation. It compares, through simulations, the most studied QKD protocol, the BB84, with ideal single-photon sources with respect to the decoy-state method applied in attenuated lasers in two primary scenarios: for Single Photon Avalanche Diode (SPAD) and Superconducting nanowire Single Photon detector (SSPD).

The work is organized in four chapters as follows:

Chapter 1 - In the opening chapter, classical cryptography is introduced and placed into context. Then the OTP scheme is explained, and the viability of this solutions is discussed. Finally, the foundational principles of quantum mechanics are introduced to help readers better grasp the concepts discussed in this work

Chapter 2 – The following section is a journey from the definition of the qubit and the definition of quantum gates to the need to implement these concepts in current telecommunications systems. The issue of current key distribution in the face of the threat posed by quantum computers is discussed, along with the two possible solutions to secure key distribution: PQC and QKD. Finally, possible attacks on a QKD system are introduced, along with the challenges of physically implementing these protocols, introducing decoy states as a solution.

Chapter 3 – Introduction to the problem that single-photon sources are not realistic today, with the solution considered through the decoy-state method. The setup of the simulations is reported, the characterization of the devices is justified, and the performance of an ideal single-photon laser and an attenuated laser is simulated for two different situations: for a SPAD and a a SSPD. The objectives is to compare theses two scenarios and evaluate whether the solution provided by the decoy state for non-ideal single-photon sources has a similar performance in terms of key rate and an optimization rule for the decoy state levels is established.

Chapter 4 – An analysis of the results is seen as a review of the objective, improving the performance of the BB84 protocol. Conclusion regarding the results and optimizations made in the simulations. Outlook on the future of these technologies, different initiatives, main drawback of SSPDs and final discussion of the work regarding the United States Sustainable Development Goals.

Work Packages

To enhance the efficiency of structuring this project, the decision has been made to divide the project into several work packages based on the specific objectives. Each package will focus on a particular area, enabling more detailed management and monitoring in each phase. The defined work packages, their descriptions, and the associated deliverables are described below.

1. **Scope Definition**

    - Task 1.1: Investigation of the historical and technological context of the art of cryptography.
    - Task 1.2: Problem statement and opportunity of the actual cryptographic systems.
    - Task 1.3: Research on the issue of sources and the technology behind detectors.
    - Task 1.4: Setting of goals and originality of the project's contributions.

2. **Quantum Information research**

    - Task 2.1: Research on the theoretical objects used in the project (qubits) and its operations from a physical perspective.
    - Task 2.2: Contextualization of PQC and research on QKD as long-term solution.
    - Task 2.3: In-depth research on the BB84 protocol, attacks, security, and definition of concepts.

3. **Simulation Description**

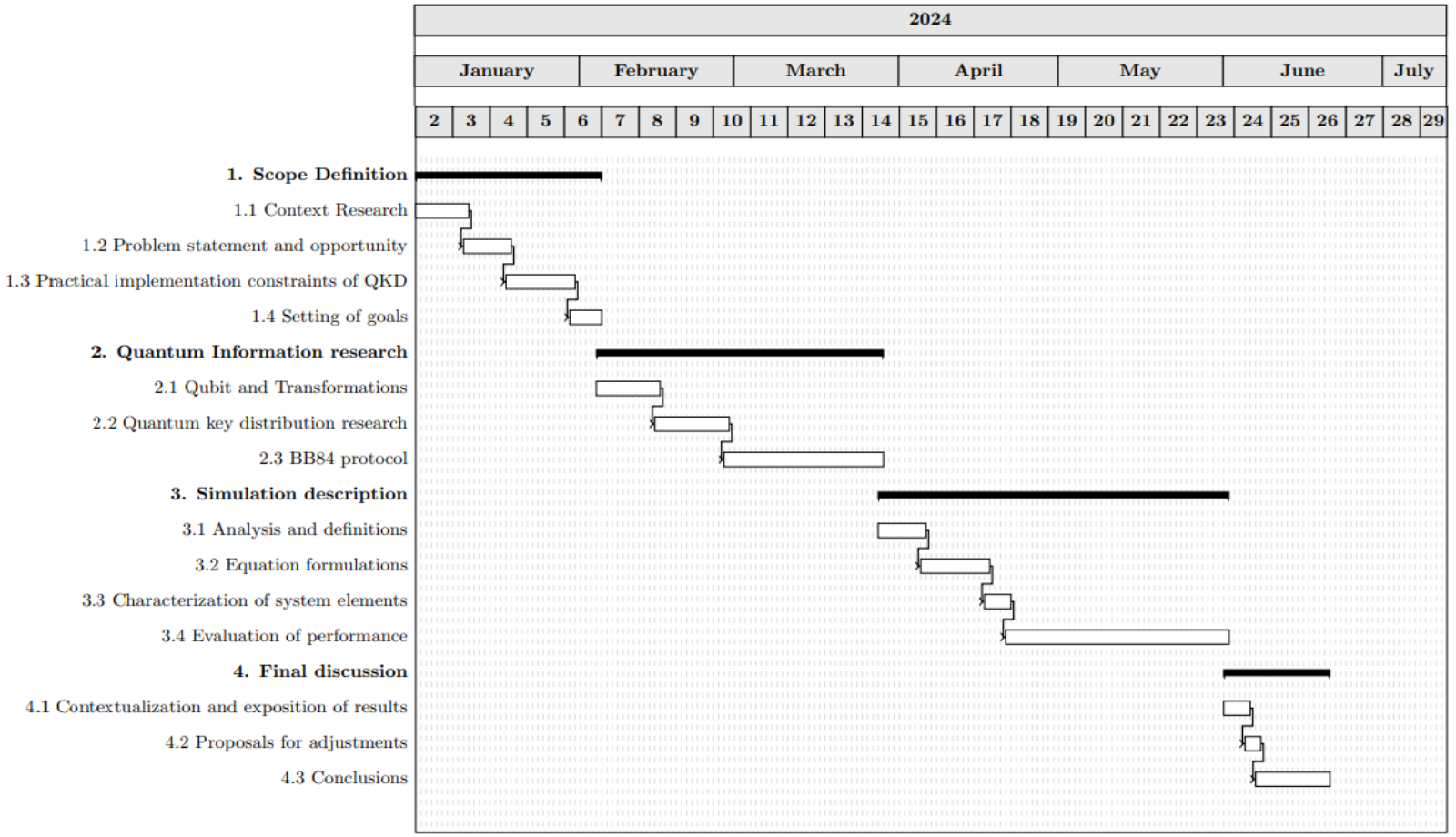
    - Task 3.1: Analysis of the proposed system and definition of concepts used in the simulation
    - Task 3.2: Equation formulations
    - Task 3.3: Obtaining the fundamental elements that characterize the QKD system and further discussion with the tutor.
    - Task 3.4: Evaluation of the performance of the multiple cases described in the Bachelor's Thesis.

4. **Final Discussion**

    - Task 4.1: Presentation of the results, interpretation, and comparison with respect to the main objective
    - Task 4.2: Proposal of adjustments, correction, and clarification of the contents of the Bachelor's Thesis.
    - Task 4.3: Final conclusions.

The **Simulation Description** holds the most weight, as coding in MATLAB involves a deep study of theory and practical applications of the BB84 protocol.

The detailed schedule information for task assignment for this Bachelor's Thesis with weekly time allocations is presented in the following **Gantt Diagram.**



Chapter 1. Introduction

Cryptography, derived from the Greek words "crypto" meaning secret and "graphy" meaning writting, has roots extending over centuries. Its development is typically dated to the Ancient Romans. This field has a long history of milestones and failures; as new encoding methods emerged, corresponding cryptanalysis techniques evolved to break them. However, it was not until World War II that cryptography experienced its most significant development, driven by the exponential increase in information traffic. Alongside advancements in channel capacity with new modulation systems and developments in multiplexing and materials engineering, there arose an urgent need to secure information in telecommunications networks consistent with current technological advancements.

Most classical protocols used today no longer rely on the secrecy of the methods but instead depend directly on the hardness of mathematical problems, such as factoring large prime numbers. Consequently, they offer only computational security, meaning they are secure with our current technology. These systems take advantage of the absence of known efficient classical algorithms to solve the problems that lead to obtaining the original plaintext.

This situation is changing radically with the development of Quantum Information and the advent of applications like quantum computers. These computers can solve problems much more efficiently, achieving in hours what would be impossible for a classical computer, such as factoring large prime numbers, as the algorithm designed by Peter Shor in 1994. The application of the extensive theoretical physics developed throughout the 19th century is beginning to have direct implications for the technologies being developed today. In recent years, several theoretical and experimental trials have been conducted, and today, small functional quantum computers are already available and working, such as the publicly accessible one from IBM.

As quantum computers continue to advance, there is a growing urgency to prepare for the potential breach of classical encryption systems. When these quantum computers become capable of executing Shor's Algorithm for large prime numbers, the security of classical encryption systems could be compromised, so cryptography must evolve in a manner that is compatible and consistent with theoretical developments to maintain the security of telecommunications systems. The most promising solution is Quantum Key Distribution (QKD), which provides information-theoretic security by harnessing the fundamental laws of quantum physics and the one-time pad encryption technique. The BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984, is one of the most well-known QKD protocols.

1.1 Context

In 1896, Wilhelm Wien derived an empirical approach to accurately describe the radiation emitted by a Blackbody, described as a collection of oscillators [1] in a thermal bath in equilibrium with the radiation emitted by the oscillators themselves. Electromagnetic radiation excites/relaxes the oscillators, leading to the thermal equilibrium characterized by a stable amount of electromagnetic energy and an average number of excited oscillators.

In 1900, Max Plank introduced that electromagnetic radiation can be quantized as a result of formulating the solution to the Blackbody problem; Plank would receive the 1918 Nobel Prize in Physics for his discovery of energy quanta. This quantization of the energy would become the beginning of great discoveries such as the Photoelectric effect (1921 Einstein's Nobel Prize), the Schroedinger wave Equation (1926), the experimental demonstration of diffraction of electrons and the Dirac theoretical formulation of quantum mechanics (bra-ket notation) yielding the so-called Quantum Physics. Alongside advancements in Theoretical Physics, advancements in Information Theory began in the mid-20th century.

Information Theory was established through Claude Shannon's pioneering work, "A Mathematical Theory of Communication", published in 1948 [2]. He introduces the concepts of entropy and channel capacity and suggests modelling information sources as a random process, where entropy quantifies the amount of information. Consequently, this model facilitated the development of efficient coding schemes for data compression and reliable transmission over noisy channels. These developments marked the foundation of modern information theory as we know it today, so much so, that its impact still has significant impact across various fields, most notably in cryptography, which is of particular interest in this Bachelor's Thesis (BT).

The relationship between information theory and cryptography is foundational as Shannon's contributions to Information Theory also influenced the field of cryptography, especially through his 1949 paper "Communication Theory of Secrecy Systems" [3]. Furthermore, Shannon defined a "perfect cypher" as one where the ciphertext reveals no information about the plaintext, meaning perfect secrecy. To achieve this perfect secrecy, a mandatory requirement is that the key must be at least as long as the message encrypted. The algorithm that fulfils the requirements is the so-called One-Time-Pad used by Special Operations teams during WW2; further considerations will be discussed.

Quantum Physics and Information Theory converge in Quantum Key Distribution (QKD), which uses the fundamental laws of quantum physics to provide theoretically unbreakable encryption.

1.2 Classical Cryptography

Cryptography is the study (and the art) of rendering a message unintelligible to any unauthorized party, and it is a part of the broader field of cryptology. To achieve this, an algorithm combines the message with some additional information – known as the key – and produces a cryptogram.

One of the earliest and most well-known methods of classical cryptography is Caesar's cypher, a type of substitution cypher where each letter in the plaintext is shifted a fixed number of positions down the alphabet. Although cryptography studies existed throughout various eras, it was not until World War II that its use grew exponentially, with the development of mechanical cyphers, such as the Enigma machine used extensively by Nazi Germany during World War II, which allowed Nazis to hide their military communications from the Allied Powers. However, the German strategy did not consider that the Allied cryptanalysts had developed the Bombe, a device that could decrypt Enigma's messages, crucially influencing the outcome of the world conflict.

From a theoretical point of view, defined by [4], two parties can establish communication, aiming to ensure that neither party knows the message of the other party, maintaining the assumed confidentiality of each message. A way to convert conventional text into encrypted text is through a key.

Let us consider Alice and Bob as the two parties sharing a message through an assumed safe link.

Alice wants to send the message using an encryption algorithm that transforms her plaintext message into a ciphertext.

A way to do this is through a cryptographic hash function.

$$\boldsymbol{h_A = H(k_A || m)}. \tag{1.1}$$

Where *H* is the hash function defined as

$$\boldsymbol{H}: \{\mathbf{0},\mathbf{1}\}^* \rightarrow \{\mathbf{0},\mathbf{1}\}\boldsymbol{n}. \tag{1.2}$$

Where, $\{0,1\}^*$ represents a set of all binary strings of arbitrary length, including the empty string. On the other hand, $\{0,1\}n$ refers to a ser of binary elements with length n. Thus, it means that a hash function maps an input of arbitrary length to an output of fixed length.

From **(1.1)** $\boldsymbol{h_A}$ is the ciphertext, $\boldsymbol{k_A}$ is a random value, also called the key, chosen by Alice and concatened with $\boldsymbol{m}$, the sent message. The expression could be rewritten.

$$\boldsymbol{C = e_k \cdot m}. \tag{1.3}$$

In which C is the ciphertext, e_k is the cryptographic key, and $\boldsymbol{m}$ is the message sent.

Now that Bob has the ciphertext, to retrieve the original message, he must reapply the same cryptographic hash function to the concatenation of the key and the message.

$$\boldsymbol{h_B = H(k_A||m)}\,. \tag{1.4}$$

Finally, Bob compares the new hash value $\boldsymbol{h_B}$ with the original value sent by Alice, $\boldsymbol{h_A}$, verifying if both values match, if they do, Bob can confirm that the message m is authentic and has not been altered.

In the realm of contemporary cryptographic systems, two principal types predominate: *symmetric* and *asymmetric.* The former employs a single key for both encryption and decryption. The only provably information-theoretic secure cryptosystem is the One-Time Pad, proposed by Vernam in 1926 [5-6]. On the other hand, asymmetric cryptography uses different keys for encryption and decryption. The fundamentals of this approach were proposed by Diffie and Hellman in 1976 [7] and were later implemented in 1978 by Rivest, Shamir and Adleman in the well-known RSA algorithm, which is extensively used in internet communications and digital signatures [8].

1.2.1 One-Time Pad

Classical cryptographic methods, such as the Caesar cypher [9], played a very important role in protecting information throughout history. However, these methods, despite being ingenious and effective for their time, have become mere literature due to significant advancements in cryptanalysis (the art of breaking cryptographic algorithms). This brings us to one of the greatest advancements in the field of cryptographic security: the One-Time Pad (OTP).

The One-Time Pad, also called the perfect cypher, is an encryption algorithm that belongs to the *symmetrical* cryptography group and combines the key with the plaintext. It is the only provably secure cryptosystem demonstrated to date.

This security is rooted in its design. The encryption key has to be unique and random for every message. Hence, some considerations must be made:

- Alice and Bob possess a common secret key, at least as long as the message itself.
- XOR operation between the message and the secret key

$$\boldsymbol{s = m_1 \oplus k}. \tag{1.5}$$

Where s is the ciphertext, m_1 is the plaintext message, and k is the secret key.

The XOR's truth table is shown in Table 1.

Input A	Input B	Output (A $\oplus$ B)
0	0	0
0	1	1
1	0	1
1	1	0

Table 1. XOR truth table

- Key used just for a single encryption, otherwise an Eavesdropper (Eve) could obtain information about the encoded plain texts and the key.

$$\boldsymbol{s_1 \oplus s_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2}. \quad \textbf{(1.6)}$$

Here, $\boldsymbol{s_1}$ and s_2 are two ciphertexts encrypted with the same key, so the XOR of the two ciphertexts ($\boldsymbol{s_1 \oplus s_2}$) reveals the XOR of the two plaintexts ($\boldsymbol{m_1 \oplus m_2}$)

- Key has to be transmitted by some trusted means.

Both parties must receive the key through a trusted channel to ensure it is not intercepted by Eve; this is particularly important because, as we will see later, the goal is to establish a secure parallel link through which to send the key.

Currently, the OTP cryptosystem is used only for the most critical applications; this is because, for high-volume communications, the volume associated with key generation makes OTP impractical. Additionally, the distribution of keys must be secure; otherwise, the security of the message will be compromised [10]. Hence, they are mainly used in diplomatic communications and by intelligence and defence agencies [11-13]

With the growing development of new advanced computing technologies, such as quantum computers, the advent of quantum physics has also become related to cryptography, particularly in key distribution.

The classical model for symmetric cryptosystems is shown in Figure 1, and a short overview of the increasing number of publications in quantum cryptography is exposed in Figure 2.

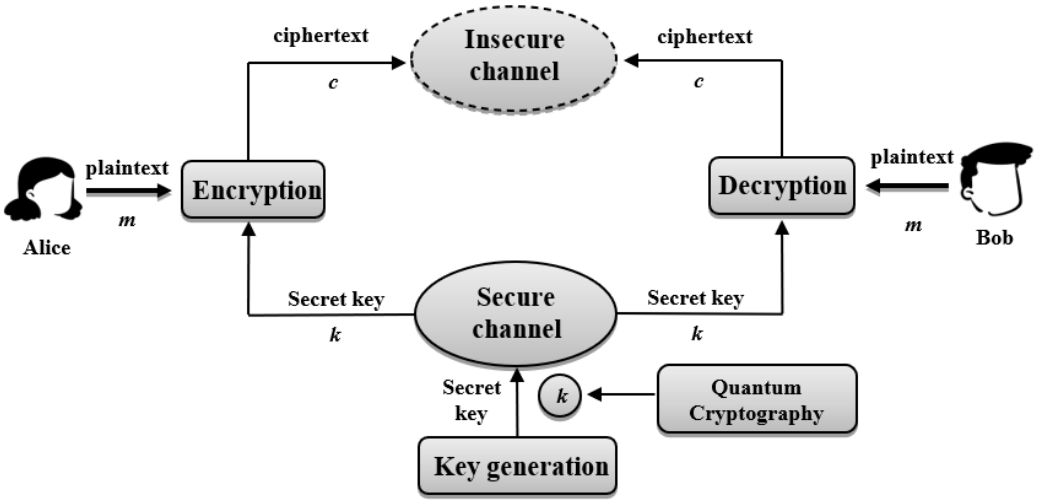


Figure 1. Channel model for symmetric cryptosystems. Quantum Cryptography consideration

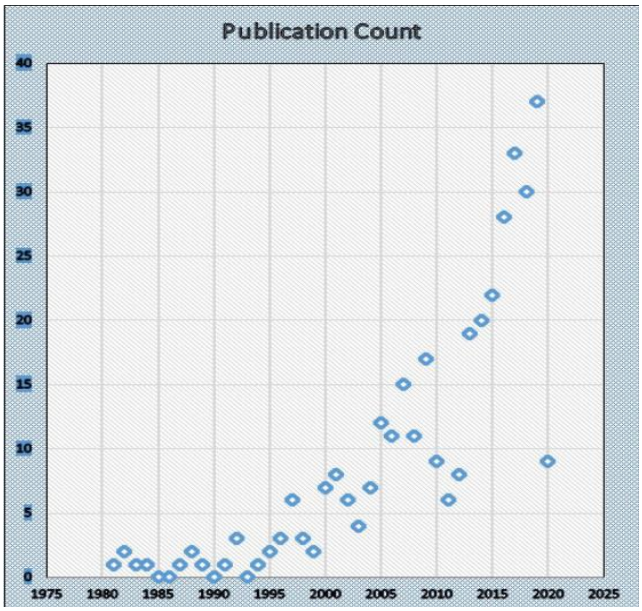


Figure 2. Number of publications from 1980 onward in the area of quantum cryptography [14].

1.3 Preliminaries

Einstein applied the energy quantization rule of Plank to explain the photoelectric effect.

From the Blackbody problem, Plank derived the quantization of the energy level that the oscillators can reach, which is given by:

$$\boldsymbol{E_{ph} = \hbar \cdot \omega.} \tag{1.7}$$

Being $\hbar$ the reduced Plank constant and ω the angular frequency.

The emission of an electron is induced by the absorption of a single photon with energy at least equal to the work function W of the metal:

$$\boldsymbol{E_{ph} = \hbar \cdot \omega \geq W \Rightarrow \nu \geq \frac{W}{h}} \tag{1.8}$$

Where ν is the minimum frequency for extracting the electron.

De Broglie extended the particle-wave dualism. Formulating the hypothesis that each microscopic particle is associated with a matter wave of wavelength:

$$\boldsymbol{\lambda = \frac{h}{p} = \frac{h}{m \cdot v}} \tag{1.9}$$

Where p is the linear momentum of the particle.

To describe the phenomena in the microscopic world, we have two complementary pictures, either the *wave* or the *particle* picture, for both the radiation and matter.

For the wave-particle relation for radiation, we have:

$$\mathbf{E} = \hbar \cdot \boldsymbol{\omega}. \tag{1.10}$$

$$\mathbf{p} = \frac{\boldsymbol{E}}{\boldsymbol{c}} = \hbar \cdot \boldsymbol{k}. \tag{1.11}$$

And for the wave-particle relation for matter (non-relativistic theory):

$$\boldsymbol{E_{kin} = \frac{1}{2} \cdot m \cdot v^2 = \frac{p^2}{2m}} \tag{1.12}$$

$$\mathbf{p} = \boldsymbol{h \cdot \nu}\,. \tag{1.13}$$

This treatment of particles, which until then had been approached deterministically, now received a new perspective.

While in classical mechanics, it is possible to determine simultaneously with arbitrary accuracy both the position and velocity of a macroscopic object. Due to the appreciable value of the mass of a macroscopic object, the perturbation induced on the object by the light scattering is negligibly small.

The situation is completely different in the microscopic objects due to their extremely small mass. So, the scattering of light by electrons produces a relevant perturbation as an effect of the measurement process. It is no more possible to consider the results of measurements on microscopic entities as independent from the measurement nor as mere registration of the "objective" values of the physical quantities. They are not deterministic physical quantities anymore.

In 1927, Heisenberg proposed an experiment for measuring the position of an electron by observing with a microscope the light scattered by the electron, which yielded the so-called Principle of Indetermination [15], which mathematically can be described as:

$$\boldsymbol{\Delta x \cdot \Delta p_x \approx h}. \tag{1.14}$$

Where Δx is the spread of the precision in the measurement of the position coordinate x, Δp_x is the spread of precision in the measurement of the momentum p_x . The increase in precision in measuring one quantity is related to the decrease in the precision in measuring the other complementary quantity.

Hence, in Quantum Physics, it is not possible to simultaneously measure with arbitrary precision the position and momentum of a microscopic particle.

From this point, a quantum quantity is well-defined when its measurement is deterministic, as in the classical case.

We can identify a quantum state according to the quantum principle of superposition described by a vector in a so-called complex Hilbert-Space [16].

The preparation of a quantum state with a well-defined position makes a completely undetermined momentum, it is also true for the complementary case. The quantum measurement of an observable $\boldsymbol{A}$ is a random and discontinuous irreversible process described as an orthogonal projection into a quantum state with a well-defined value for the observable $\boldsymbol{A}$, also called random quantum collapse. Therefore, two consecutive quantum measurements of the same physical quantity (the main observable) are equivalent to a single one.

This principle is crucial in quantum cryptography, where the security of a quantum key distribution (QKD) protocol relies on the fact that Eve's attempt will perturb the quantum states and be detectable. Once an observable is measured, its value will remain the same no matter how many times we measure it again.

The interplay between the theory of quantum collapse and the Heisenberg Indetermination Principle establishes a foundation for quantum cryptography.

Chapter 2. Quantum Technology

Over the past few decades, Quantum Technologies have made tremendous progress, with increasing investment from both governments and private companies [17]. The technologies that have been developed allow us to directly address individual quantum states to exploit their properties. These advancements frame the quantum technology study in two domains: computing and communications. [18]

Both technologies use the qubit as the fundamental unit of information, which is in some way analogous to the bit in the classical case.

2.1 Qubit

A classical bit is the fundamental entity of classical computing and digital communications. It represents a state in a binary system, which can assume one of two possible values: 0 or 1.

Its importance extends across all technological aspects of our modern life, from how the television in the living room works to our mobile phones guiding us. Every piece of information, whether text, video, or image, is represented as a sequence of bits. Voltage differences with a well-defined threshold act as a bit across transmission links. There are countless practical examples of the importance of the bit in our daily lives; I particularly like this analogy: t*he bit is the atom of a technological world*.

On the other hand, a quantum bit is the fundamental entity of quantum information, computation, and communication theory.

Qubits are described as abstract vectors of a two-dimensional Hilbert Space ($\boldsymbol{\mathcal{H}_2}$), it also could be described as a ray of ($\boldsymbol{\mathcal{H}_2}$), a collection of non-zero vectors linearly dependent to a given non-zero vector $\overrightarrow{v}$. The qubits are the quantum states of a two-state quantum system described by a ($\mathcal{H}_2$).

A general quantum state of a n-dimensional Hilbert Space is described by:

$$\boldsymbol{\psi = \Sigma_n \lambda_n \varphi_n \in \mathcal{H}: \forall n = \mathbb{N}} . \qquad \textbf{(2.1)}$$

Being $\boldsymbol{\lambda_n}$ the expansion coefficient and $\boldsymbol{\varphi_n}$ a vector of the orthonormal basis.

For the case of qubit, the general quantum state is particularized for n=2. Let us consider the following representation in the context of linear algebra in the Figure 3.

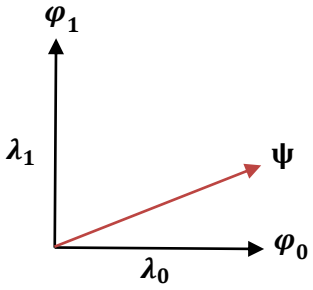


Figure 3. Representation of two-orthonormal basis $\{\varphi_0, \varphi_1\}$ along with an abstract vector ψ.

For this two-dimensional orthonormal basis $\{\varphi_0, \varphi_1\}$

$$\psi = \sum_{n=0}^{1} \lambda_n \varphi_n = \lambda_0\varphi_0 + \lambda_1\varphi_1. \tag{2.2}$$

Depending on the scalar coefficients of the expansion, we get different combinations of quantum states, also described as qubits.

The norm of the quantum state is introduced in (2.3), which is a measure of the length of the state vector in the Hilbert Space.

Let us see the relation between the scalar coefficients and the final norm of the quantum state.

$$||\psi||^2 = \langle\psi|\psi\rangle = \sum_n |\lambda_n|^2 = 1. \tag{2.3}$$

Applied to qubits:

$$||\psi|| = \sqrt{|\lambda_0|^2 + |\lambda_1|^2} = 1. \tag{2.4}$$

The norm must be equal to one to preserve the orthonormality of the base, so the scalar coefficients can be considered as the probability of obtaining the quantum state with a well-defined value, this reveals that deterministic results are not presented anymore but probabilistic ones instead.

In (2.3), the so-called Bra-ket notation or Dirac notation is used to define the scalar product. This notation emerged in the late 1920s, during the early development of quantum mechanics, and has become a fundamental tool due to its versatility and simplicity. The notation unlocks the ability to precisely represent states, inner products, and operators, among other utilities.

Now it is considered the representation of the two well-defined values of the qubit using the ket notation:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.5}$$

$$|\mathbf{1}\rangle = \begin{bmatrix}\mathbf{0}\\ \mathbf{1}\end{bmatrix} \tag{2.6}$$

Hence:

$$|\boldsymbol{\psi}\rangle = \boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle = \begin{bmatrix}\boldsymbol{\alpha}\\ \mathbf{0}\end{bmatrix} + \begin{bmatrix}\mathbf{0}\\ \boldsymbol{\beta}\end{bmatrix} = \begin{bmatrix}\boldsymbol{\alpha}\\ \boldsymbol{\beta}\end{bmatrix} \tag{2.7}$$

Being $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ the expansion coefficients.

Quantum states with well-defined values can take on various physical meanings as long as the basis formed between them is orthonormal. For example, they can take the values of 0 and 1, as we have seen, collapsing into the classical bits we know. However, the qubit can also represent the polarization state of a single photon, for instance, a plane wave between vertical and horizontal polarization.

The main difference with respect to the classical case is that the value 0 or 1 of the classical bit, in the quantum case, is no more than two states but infinite as a superposition of the two classical ones. The quantum measurement described is now a discontinuous irreversible process that recovers the classical bit 0 or 1, which means that after the detection phase, we still have 0 or 1 as the output of the qubit.

2.1.1 Quantum Gates

Before introducing the quantum gates, it is important to determine the main bases and their importance in QKD systems.

The representation has been seen $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ is known as the computational orthonormal basis for $\mathcal{H}_2^{(KET)}$, and it is represented by the ket $|\mathbf{0}\rangle$ and the ket $|\mathbf{1}\rangle$ where:

$$|\mathbf{0}\rangle = \mathbf{1}\cdot|\mathbf{0}\rangle + \mathbf{0}\cdot|\mathbf{1}\rangle \tag{2.8}$$

$$|\mathbf{1}\rangle = \mathbf{0}\cdot|\mathbf{0}\rangle + \mathbf{1}\cdot|\mathbf{1}\rangle\,. \tag{2.9}$$

The following basis is known as the Diagonal basis, from the diagonal state of polarization and is defined by $\{|+\rangle, |-\rangle\}$, represented by the ket $|+\rangle$ and the ket $|-\rangle$ where:

$$|+\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle) \tag{2.10}$$

$$|-\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle - |\mathbf{1}\rangle) \tag{2.11}$$

Finally, the last one is known as circular polarization and is defined by $\{|\boldsymbol{i}\rangle, |-\boldsymbol{i}\rangle\}$, represented by the ket $|\boldsymbol{i}\rangle$ and the ket $|-\boldsymbol{i}\rangle$ where:

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \tag{2.12}$$

$$|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \tag{2.13}$$

It can be verified that the three bases are orthonormal with this quick check using the inner product of the states:

$$\langle 1|0\rangle = \langle +|-\rangle = \langle i|-i\rangle = 0 \tag{2.14}$$

Where is used the bra and ket notation, where there is a dependency between bra and ket as follows:

$$\langle 1| = |1\rangle^{\dagger}. \tag{2.15}$$

For the BB84 protocol, the most and best-known protocol in QKD, which is considered in further chapters, the computational and diagonal bases are used by Alice and Bob and for a first exchange of bits, the bases chosen by them two may not match, introducing a degree of randomness in the communication.

Using as reference the computational basis, in order to implement qubits physically, a bi-stable quantum system must be managed, in which two orthogonal quantum states $|0\rangle$, $|1\rangle$ have to be controlled in order to adjust the superposition (the coefficients α, β) generating any possible qubit. The superposition is called coherent superposition (ideal), which means that α, β are stable coefficients (not changing in time) apart when they are changed in a controlled way through quantum gates.

Logic gates are the most basic building blocks in digital electronics. They are used to perform logical operations on the input bits and thus obtain output bits. The same idea applies to qubits; analogously, there is a set of operators or quantum gates capable of manipulating the value of qubits.

The quantum gates are unitary operators $\hat{U}$:

$$\hat{U} \cdot \hat{U}^{\dagger} = \hat{U}^{\dagger} \cdot \hat{U} = \hat{I}. \tag{2.16}$$

This condition means that unitary operators can be seen as linear operators with inverse equal to the adjoint.

$$\hat{U}^{\dagger} = \hat{U}^{-1}. \tag{2.17}$$

The unitary operator is considered as a representation in the orthonormal basis by a square unitary matrix.

For an initial quantum state, the quantum gate acts as:

$$\hat{\mathbf{U}} \cdot |\boldsymbol{\psi}_{in}\rangle = |\boldsymbol{\psi}_{out}\rangle \tag{2.18}$$

Considering this property:

$$(\mathbf{A} \cdot \mathbf{B})^{\dagger} = \boldsymbol{B}^{\dagger} \cdot \boldsymbol{A}^{\dagger} \tag{2.19}$$

The scalar product is preserved, yielding to this conclusion:

$$||\boldsymbol{\psi}_{out}||^2 = \langle \boldsymbol{\psi}_{out} | \boldsymbol{\psi}_{out} \rangle = \langle \boldsymbol{\psi}_{in} | \boldsymbol{\psi}_{in} \rangle = ||\boldsymbol{\psi}_{in}||^2 = \mathbf{1}. \tag{2.20}$$

This result shows that the norm is preserved, so also, for the final quantum state, the sum of the probabilities must be normalized so it is equal to 1.

This is useful because now a quantum gate could be defined as an operator which applies deterministic, reversible, linear operations and preserves scalar products on qubits.

$$\hat{\boldsymbol{U}} = \begin{bmatrix} \boldsymbol{a_{00}} & \boldsymbol{a_{01}} \\ \boldsymbol{a_{10}} & \boldsymbol{a_{11}} \end{bmatrix} \tag{2.21}$$

Let us consider the Quantum NOT gate, also called the X-Pauli gate, $\hat{X}$ is represented in computational basis $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ by the matrix:

$$\hat{\boldsymbol{X}} = \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix} \tag{2.22}$$

The quantum NOT gate flips the input qubit from a $|0\rangle \rightarrow |1\rangle$ and vice versa. A more visual example is shown in Figure 4.

$$\begin{cases} \hat{\boldsymbol{X}}|\mathbf{0}\rangle = |\mathbf{1}\rangle \\ \hat{\boldsymbol{X}}|\mathbf{1}\rangle = |\mathbf{0}\rangle \end{cases} \tag{2.23}$$

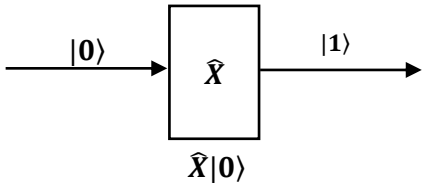


Figure 4. Quantum NOT gate applying to a $|0\rangle$ qubit.

The following one is also a Pauli operator, the Y-Pauli gate, represented as $\hat{Y}$ by the matrix, defined in Figure 5.

$$\begin{cases} \hat{Y}|0\rangle = i|1\rangle \\ \hat{Y}|1\rangle = -i|0\rangle \end{cases} \tag{2.24}$$

$$\hat{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{2.25}$$

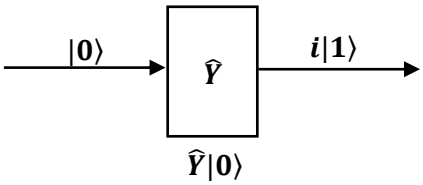


Figure 5. Pauli Y-gate applying to a $|0\rangle$ qubit.

The Phase-Shift quantum gate $\hat{R}_\phi$, also represented in the computational basis by the matrix:

$$\hat{R}_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \tag{2.26}$$

$\hat{R}_\phi$ is a diagonal matrix, the basis in computational basis is formed by eigenstates of the operators. A representantion is shown in Figure 6.

$$\begin{cases} \hat{R}_\phi|0\rangle = |0\rangle \\ \hat{R}_\phi|1\rangle = e^{i\phi}|1\rangle \end{cases} \tag{2.27}$$

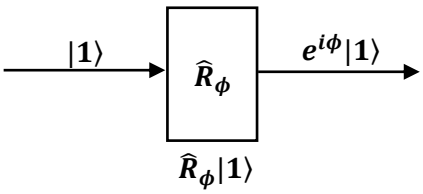


Figure 6. Phase-Shift quantum gate applying to a $|1\rangle$ qubit.

The eigenstates for (2.26) are $|0\rangle$ and $|1\rangle$ and for (2.27) the eigenvalues are 1 and $e^{i\phi}$.

It is considered the follow unitary matrix (gates) derived from the Phase-Shift quantum gate.

For $\phi = \boldsymbol{\pi}$ we have the $\widehat{\boldsymbol{Z}}$-Pauli operator $\widehat{\boldsymbol{R}}_{\boldsymbol{\pi}} = \widehat{\boldsymbol{Z}}$, which is a gate that acts as the general Phase-Shift quantum gate, but with eigenvalues **1** and **-1**.

$$\widehat{\boldsymbol{R}}_{\boldsymbol{\pi}} = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{-1} \end{bmatrix} \tag{2.28}$$

For $\phi = \frac{\boldsymbol{\pi}}{\mathbf{2}}$ we have the $\widehat{\boldsymbol{S}} = \widehat{\boldsymbol{R}}_{\frac{\boldsymbol{\pi}}{\mathbf{2}}}$:

$$\widehat{\boldsymbol{R}}_{\frac{\boldsymbol{\pi}}{\mathbf{2}}} = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{i} \end{bmatrix} \tag{2.29}$$

With eigenvalues **1** and $\boldsymbol{e}^{\boldsymbol{i}\frac{\boldsymbol{\pi}}{\mathbf{2}}}$.

For $\phi = \frac{\boldsymbol{\pi}}{\mathbf{4}}$ we have the $\widehat{\boldsymbol{T}} = \widehat{\boldsymbol{R}}_{\frac{\boldsymbol{\pi}}{\mathbf{4}}}$:

$$\widehat{\boldsymbol{R}}_{\frac{\boldsymbol{\pi}}{\mathbf{4}}} = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{e}^{\frac{\boldsymbol{\pi}}{\mathbf{4}}} \end{bmatrix} \tag{2.30}$$

With eigenvalues **1** and $\boldsymbol{e}^{\boldsymbol{i}\frac{\boldsymbol{\pi}}{\mathbf{4}}}$.

Finally, we describe one of the most important quantum gates, the so-called Hadamard gate, illustrated in Figure 7, which flips the basis as follows:

$$\widehat{\boldsymbol{H}} = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}} \cdot \begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} \end{bmatrix} \tag{2.31}$$

$$\begin{cases} \widehat{\boldsymbol{H}}|\mathbf{0}\rangle = |+\rangle \\ \widehat{\boldsymbol{H}}|\mathbf{1}\rangle = |-\rangle \end{cases} \tag{2.32}$$

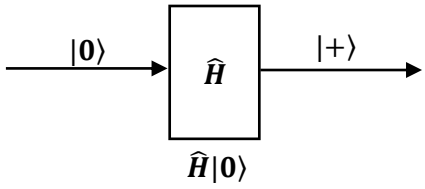


Figure 7. Hadamard quantum gate applying to a $|\mathbf{0}\rangle$ qubit.

The Hadamard gate is a subclass of the Pauli operator. It is used to generate a superposition state from the ket $|0\rangle$, which is a well-defined quantum state we obtain after the Hadamard gate transformation $|+\rangle$, which we remember is $|+\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle)$. The superposition of the well-defined states ket $|\mathbf{0}\rangle$ and ket $|\mathbf{1}\rangle$ now exists with equal probability $\frac{1}{2}$.

There is a more visual way to refer to the quantum transformations that the operators perform on qubits, and this way is through the Bloch Sphere (Figure 8), a geometrical representation of the state of a single qubit.

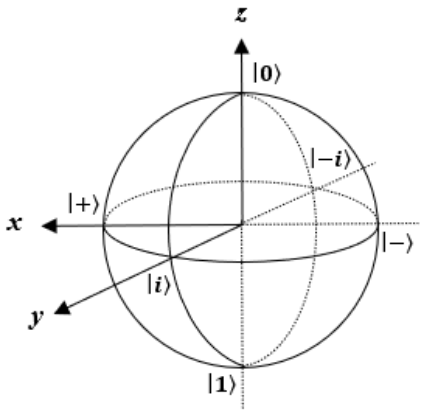


Figure 8. Geometric representation of a qubit Bloch Sphere

There is a one-to-one correspondence between points and rays of the ($\mathcal{H}_2$), being the rays no more than equivalent classes of non-zero vectors. The point is given by two coordinates ϑ, ϕ:

$$\rho: \begin{cases} 0 \leq \vartheta \leq \pi \\ 0 \leq \phi \leq 2\pi \end{cases} \tag{2.33}$$

The action of a quantum gate on a state of the qubit, seen on the Bloch Sphere, is the rotation of the sphere around an axis joining two points (P_0, P_1) representing the eigenstates of $\hat{U}$ of the two eigenvalues (coefficients) λ_0, λ_1 with the angle of rotation equal to the difference of the phases:

$$\lambda_0 = e^{i\gamma_0}, \lambda_1 = e^{i\gamma_1}\ ;\ \phi = \measuredangle\lambda_1 - \measuredangle\lambda_0 = \gamma_1 - \gamma_0. \tag{2.34}$$

The sign of ϕ, known as longitude, shows clock or anti-clock rotation. Negative sign for the former case.

The colatitude ϑ is given by:

$$\vartheta = 2\tan^{-1}\frac{\lambda_1}{\lambda_0}. \tag{2.35}$$

The coordinates ϑ, θ are now well defined. In order to plot the state in the Bloch Sphere the relation shown in (2.36) must be followed:

$$\begin{bmatrix} \cos(\frac{\vartheta}{2}) \\ \sin(\frac{\vartheta}{2}) \cdot e^{i\phi} \end{bmatrix} \tag{2.36}$$

Let us now show the advantages of this representation of the qubit with respect to the Dirac Notation. The Pauli operators, such as the quantum NOT gate ($\hat{X}$-Pauli operator) and the $\hat{Z}$-Pauli operator that we have already seen, are binary π – rotations. Also, from the Hadamard gate, what is happening with the qubit can intuitively be seen in Figure 9. Since Pauli gates are unitary and hermitian operators, if we apply a Hadamard gate to another, we recover the identity, meaning it's as if no transformation is applied to the state (Involution properties).

This can be verified analytically (2.37).

$$\hat{H} \cdot \hat{H}|0\rangle = \hat{H} \cdot |+\rangle = \hat{H}^{-1}|+\rangle = |0\rangle \Rightarrow \hat{H} = \hat{H}^{-1} \Rightarrow \hat{H}^2 = \hat{I}. \tag{2.37}$$

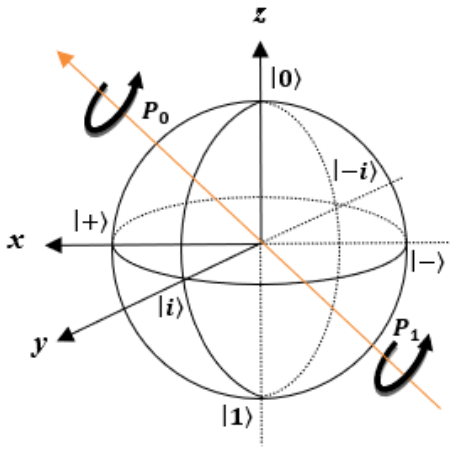


Figure 9. Geometric representation of a qubit Bloch Sphere applying a Hadamard gate

From the first application of the Hadamart to the ket $|0\rangle$, the rotation taking the axis of rotation P_0, P_1 transforms the ket $|0\rangle$ into the ket $|+\rangle$, a change of basis. If we apply this same gate again, we recover the initial quantum state, analytically, it is like applying the identity matrix.

The definition of the qubit and how it can be modified or transformed in a controlled manner are the building blocks for constructing technology that takes advantage of these properties. Now, the theoretical framework of the BT will be introduced.

2.2 Quantum Cryptology

To address the problem, let us introduce a very simple scheme that takes the classical cryptography point of view.

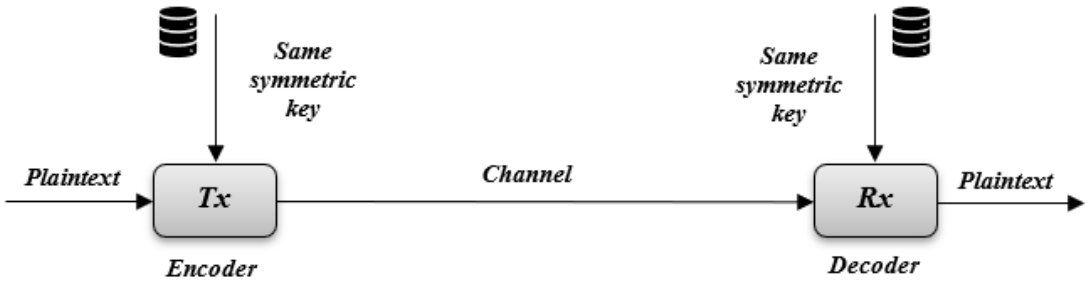


Figure 10. Simple telecommunication scheme.

In the scheme presented in Figure 10, the message is encoded and decoded using the same key, so using symmetric keys. As its discussed in previous chapters, the only scheme of cryptography that is unconditionally secure, which means it is secure against any possible attack with unlimited computational resources, is the OTP scheme.
In very limited cases in which we have very secret communication between two parties, these parties share a common database with a sequence of keys that can be used for the transmission. When the transmission uses all the keys, the two parties must build a new database and find some way to generate the keys in order to restore new keys for new messages.
In modern practical systems, the refresh of the key is performed using asymmetric cryptographic schemes, which are pretty easy to implement, like RSA. However, it is not secure against quantum computers. Nowadays, this is the usual situation because, in any case also, AES [19], OTP and other schemes require the key in the transmitter and receiver, so at the moment, it is secure against attacks using classical computers but, when a quantum computer with a capacity of managing estimated one million of qubit, that will arrive probably within ten years [20], then using the Shor's Algorithm [21], implemented in a quantum computer, it will be possible to break RSA and extract the key exchanged. Once the key is known, the message ciphered using OTP or AES will be completely exposed. This is a very dangerous situation. On one side, this is the motivation for addressing a great investment in order to build an effective quantum computer. On the other side, it is also the motivation for finding new technologies for key distribution.
The fundamental problem is the exchange of the key in order then to implement, for instance, the OTP or a practical (meaning no more information-theoretically secure but considered with an acceptable level of security) cryptographic symmetric scheme (AES with 256-bit length), which is considered secure also for the classified exchange of information even though the key must be refreshing in one way or another.
There are two possibilities nowadays for solving the problem: *Post-Quantum cryptography* and *Quantum Key Distribution.* The former is dedicated to searching for new algorithms, but at the present moment, no quantum algorithm is known to break them. It is also based on computational complexity, and again, the problem here is that "at the moment" works, but it does not provide unconditional security. The latter provides unconditional security and is based on the fundamental laws of quantum physics.

2.2.1 PQC

Once a large Quantum Computer is developed, the existing classical security algorithms will become insecure. Post-quantum cryptography is classical cryptography under the assumption that the attacker is using scalar Quantum Computers. In the end, it deals with a cryptosystem that runs on a conventional computer but is secure against attacks by quantum computers [22].

The main schemes are classified into Lattice-Based Cryptography, Code-Based Cryptography, Hash-Based Cryptography, Multivariate Quadratic Equations. A brief explanation for these schemes is given:

- Lattice-Based Cryptography

Lattice-based cryptography relies on the hardness of mathematical problems involving lattice structures in high-dimensional spaces. The concept of lattice comes from a regular grid of points extending infinitely in all directions, defined by a basis of linearly independent vectors. More research is needed to be carried out to gain confidence against quantum attacks [23].

- Code-Based Cryptography

Code-Based cryptosystems use error-correcting codes, relying on the computational difficulty of decoding a randomly chosen linear code. The primary challenge with code-based cryptography is the substantial key size, often reaching megabytes to ensure robust security. Despite various proposed code-based cryptography schemes, many have been susceptible to specific attacks. Nevertheless, the original McEliece [24] cryptosystem remains unbroken, although its practicality is limited by the large key sizes required.

- Hash-Based Cryptography

The Hash-Based Cryptography depends on the properties of Hash functions and necessitates minimal security assumptions. Their main applications are in the Digital signature framework [25]

- Multivariate Quadratic Equations

This approach is based on the difficulty of solving systems of multivariate quadratic equations. These systems involve finding solutions to equations where each term is a product of at most two variables, and they are known to be NP-hard. This means that, as the number of variables increases, the problem's complexity grows exponentially, making it infeasible to solve using any known polynomial-time algorithm.

According to Chen et al., "It seems improbable that any of the currently known algorithms can serve as a drop-in replacement for what is in use today. One challenge that will likely need to be overcome is that most of the quantum-resistant algorithms have larger key sizes than the algorithms they will replace. This may result in needing to change various Internet protocols,

such as the Transport Layer Security (TLS) protocol, or the Internet Key Exchange (IKE). The ways in which this should be done must be carefully considered". None of these proposals have been shown to guarantee security against all quantum attacks [26].

PQC gives us a temporary solution for the scaling problem of Quantum computers. However, another possibility exists to secure the key distribution.

2.2.2 Quantum Key Distribution (QKD)

Quantum Key Distribution provides information-theoretically secure using the concept of quantum mechanics properties to share the key between Alice and Bob. If an eavesdropper, commonly called Eve, attempts to intercept the key, she will introduce errors in the detection of the quantum signal so Alice and Bob can detect her presence. Upon detecting an eavesdropper, they can abort the key generation process and initiate a new one, ensuring the security of their communication.

There are two types of QKD protocols, classified into *Discrete variable QKD* (DV-QKD) and *Continuous variable QKD* (CV-QKD).

The former refers to the use of the spin of electrons or the polarization of single photons to transmit information, for instance, the BB84 that is the object of study in this BT, or others such as B92 [27].

For CV-QKD, the information is no longer contained in discrete parameters anymore but in continuous properties of quantum states, like its amplitude and phase. Instead of single photons, it uses light waves and special detection methods to measure these phases and amplitudes.

DV-QKD usage is both a classical and a quantum channel, the quantum channel is a completely untrusted channel, which means that an eavesdropper can read and also write, used to transmit qubits, and the classical channel is used to discuss and compare some of the qubits they received, must be trusted in the sense that any third party could read the information, authenticated in some way using for example the OTP.

A detailed explanation of how the BB84 protocol of QKD works is provided.

2.2.2.1 BB84

In 1984, Bennet and Brassard developed the BB84 protocol, the first QKD protocol and the core of all the news protocols, such as B92 or MDI-QKD [28], and it's still widely used nowadays, for example, in the Tokyo QKD network [29].

BB84 is considered in the simulation part of the BT as an implementation of a single-photon source, which means that the key cannot be cloned by Eve due to the non-cloning theorem [30], but we are considering instead not a perfect communication system. In this part, we will present a theoretical treatment of the protocol.

The basis of this protocol and for the security of Quantum Key Distribution are related to the following statements.

Let us consider a completely completely unknown state of the qubit in the Bloch Sphere, illustrated by Figure 11.

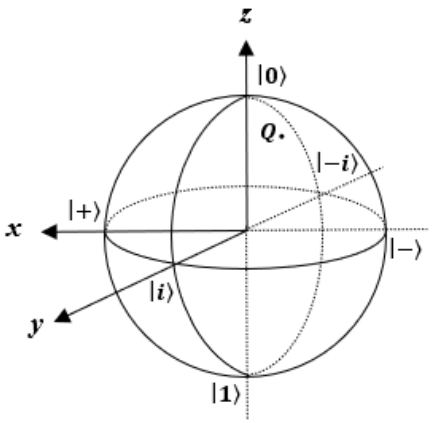


Figure 11. Geometric representation of a qubit Bloch Sphere

Where the point Q represents the unknown state of the qubit on the Bloch Sphere.

The fundamental fact in quantum mechanics is that it is not possible (from a theoretical point of view, with probability $P = 0$) to exactly reconstruct the state of a completely unknown qubit, this is related to the theory of measurement of the qubit [31].

It is supposed that Alice is transmitting a qubit that can be implemented as a single photon in some state of polarization, related to the Bloch Sphere, which means that the generic point Q is in some position of the Bloch Sphere.

We now consider that Eve interrupts the communication system, and she performs some operations, such as applying quantum gates and measuring this qubit. To reconstruct the qubit, Eve must perform a measurement on one of the three Pauli operators in order to collapse the qubit in the x, y and z coordinates of the Bloch Sphere.

Let us imagine that Eve performs a measurement of the X-Pauli operator, it is known that the qubit will collapse in either the $|+\rangle$ or $|-\rangle$ state shown in Figure 12.

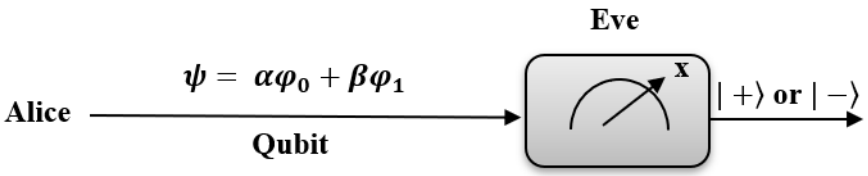


Figure 12. Measurement of a random qubit ψ in the X-basis

Also presented in the Figure 13 in the Bloch Sphere:

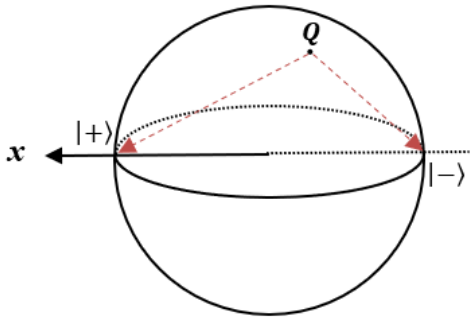


Figure 13. Geometric representation of a qubit in the Bloch Sphere. Measurement of the qubit in Diagonal basis

The action of Eve in order to find the precise position of the state of the qubit will produce a random result and a random perturbation of the qubit as a consequence of the measurement. So, it is no more possible, after this measurement, for Eve to restore the original position of the point Q , because this is intrinsically forbidden by the rule of quantum measurement. It is no longer possible for Eve to intercept or reconstruct the qubit sent by Alice.

But also, for Bob, who is the original receiver of the qubit, it is not possible to reconstruct the qubit in this situation.

The manoeuvre is the following one:

A completely unknown qubit means that a priori all the points of the Bloch sphere are equiprobable, but there is another situation if the qubit is one between two orthogonal states.

For instance, Alice now chooses either P' or P'' points but orthogonal ones that belong to a given orthonormal basis. The Bloch sphere is represented in Figure 14.

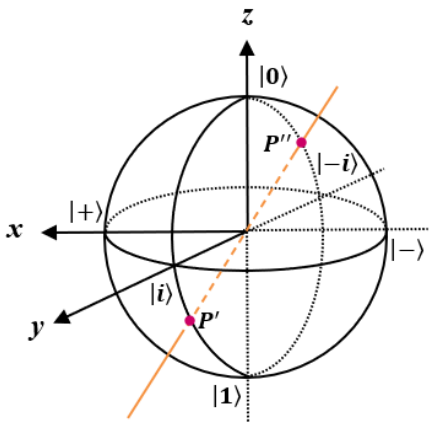


Figure 14 Geometric representation of a qubit Bloch Sphere using a random orthonormal basis with eigenstates P' and P''

In order to measure, the generic basis must be reconducted to the computational basis, applying a quantum gate to modify these two possible transmitting qubits. The measurement scheme is described in Figure 15.

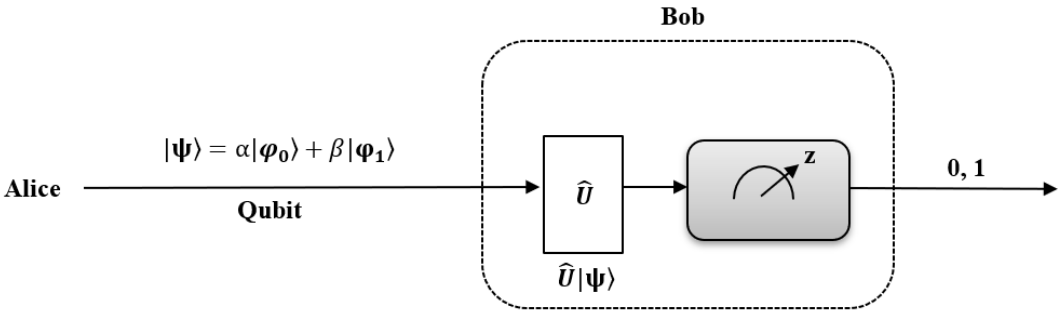


Figure 15. Measurement of a random qubit ψ using an unitary operator which applies a rotation in terms of Bloch sphere, the measurement in Z-basis yields whether 0 or 1.

Performing these unitary transformations, represented also in Figure 16 as just the inverse of a quantum gate, followed by the measurement on a computational basis, makes it possible to restore the initial position of the qubit, so it recovers exactly the qubit transmitted from Alice.

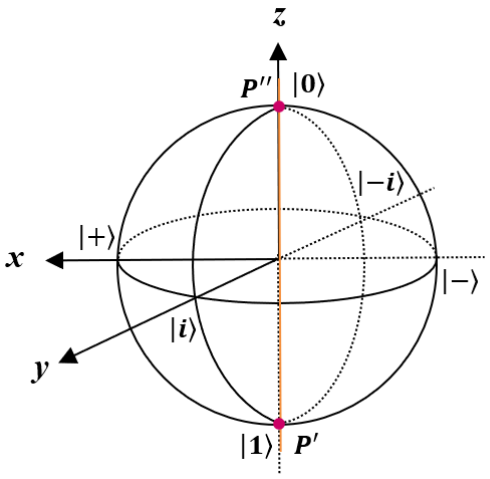


Figure 16 Geometric representation of a qubit Bloch Sphere using a random orthonormal basis with eigenstates P' and P'' projected, due tothe Unitary gate, in the Computational basis

Alice is choosing to transmit two possible qubits, which is the same as choosing between transmitting bit 0 or bit 1; this choice can be reconstructed by any receiver knowing the basis on which the measurement has been made. It means knowing the pair of orthogonal states $\boldsymbol{P'}, \boldsymbol{P''}$ in which Alice performs the choice.

Merging the two facts: It is not possible to reconstruct the state of a completely unknown qubit exactly, and if the qubit is one between two orthogonal states, it's possible to reconstruct the qubit exactly. It's possible to build a system unconditionally secure against any attack.

Let us now show how the QKD BB84 protocol works from a communication between Alice and Bob.

For a practical example, in order to understand how the protocol works, Alice will transmit a sequence of qubits chosen among the four qubits belonging to two complementary bases, which means the orthogonal axis of the Bloch sphere.

The Z-Basis $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ and the X-Basis $\{|+\rangle, |-\rangle\}$ are chosen and sent following the sequence shown in (2.38).

$$\{|\mathbf{0}\rangle, |+\rangle, |+\rangle, |\mathbf{1}\rangle, |-\rangle, |\mathbf{1}\rangle, |-\rangle, |\mathbf{0}\rangle\} \quad \textbf{(2.38)}$$

To generate this random sequence, Alice must first generate a sequence of two random sequences of bits and communicate the basis chosen to Bob. The generation of these random sequences is non-trivial and cannot go unnoticed. The number generation for a computer by some numerical algorithms can not be considered as truly random number generation, and this

is why it must be generated through Quantum random numbers generator (QRNGs), which uses quantum mechanics to generate completely random numbers.

Initially, Alice just has:

$$\begin{cases} \textbf{Random "state" bit sequence } \{a_k\}_{k=7} \\ \textbf{Random "basis" bit sequence } \{b_k\}_{k=7} \end{cases} \tag{2.39}$$

For the case proposed in equation (2.38), $k = 7$, a random sequence of up to eight qubits is generated.

According to these random sequences, it is possible to build the actual quantum circuit, as illustrated in Figure 16.

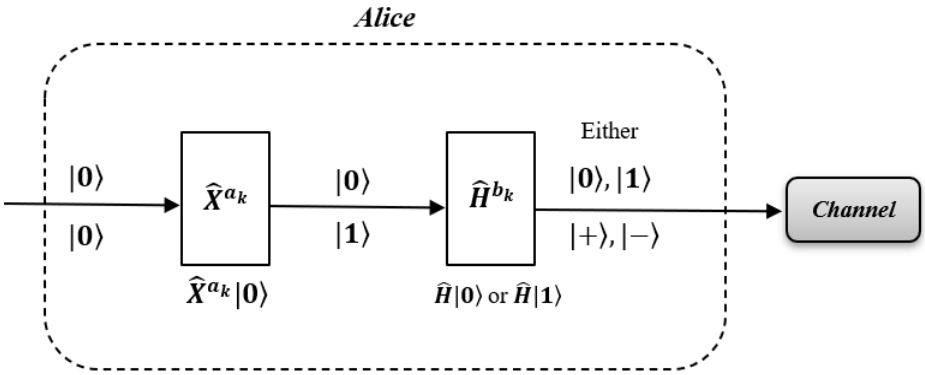


Figure 16. Scheme of Alice, generation $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ states

This Quantum Circuit is the generator of each one of the four quantum states that we are sending to Bob.

At first, Alice starts generating a sequence of $|0\rangle$ qubits, and at each k, she will apply two quantum gates. The first one is a quantum NOT-Gate, but to the power of $\{a_k\}$, the actual motivation for the exponent is:

$$\begin{cases} \hat{X}^0 = \hat{I}, & a_k = 0 \\ \hat{X}^1 = \hat{X}, & a_k = 1 \end{cases} \tag{2.40}$$

If the bit related to $a_k = 0$, the qubit $|0\rangle$ remains equal, but $a_k = 1$, there is a flip from the qubit $|0\rangle$ to the qubit $|1\rangle$.

The second operator is a Hadamard Gate with the exponent b_k, which behaves similarly:

$$\begin{cases} \hat{H}^0 = \hat{I}, & b_k = 0 \\ \hat{H}^1 = \hat{H}, & b_k = 1 \end{cases} \tag{2.41}$$

In this case for $\boldsymbol{b_k} = \mathbf{0}$, there is no change of the basis, so the qubit remains as before, it means either $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$, so the basis is the Computational basis or Z-basis.

For the other case $\boldsymbol{b_k} = \mathbf{1}$, the effect of the Hadamard gate is relevant and so we flip the base from Z-Basis to X-Basis, the result will be either $|+\rangle$ or $|-\rangle$. The combination of the two random sequences of bits determines the quantum state Alice will send to Bob.

The quantum states or qubits emitted by Alice are represented in the Mapping table defined in Table 2.

a_k	b_k	**Alice qubit**
0	0	$\|\mathbf{0}\rangle$
0	1	$\|+\rangle$
1	0	$\|\mathbf{1}\rangle$
1	1	$\|-\rangle$

Table 2. Quantum Mapping table

Recovering the initial qubits that we wanted to transmit from (2.38).

The two sequences, one from the states $\boldsymbol{a_k}$ and the other for the bases $\boldsymbol{b_k}$ are the following ones:

$$\{\boldsymbol{a_k}\} = \{\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{0}\} \tag{2.42}$$

$$\{\boldsymbol{b_k}\} = \{\mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}\}. \tag{2.43}$$

The qubits travel through the quantum channel (for now, we are supposing no Eve's detection) and finally reach Bob. He performs the measurement, considering that Bob chooses the basis for the measurement in a random way. When he chooses the Z-Basis, the received qubit is just measured using the Z-Basis, just assuming that the unitary operator is a simple $\hat{I}$, obtaining a value of Bob's "state" bit sequence $\boldsymbol{a_k}'$, but it also has to be considered the implementation of the possibility of making the measurement of the X-Basis.

From a physical point of view if we treat the qubit as a single polarized photon, we have mentioned in **Chapter 2.1** that the eigenstates of the orthonormal basis of a qubit could be the horizontal and vertical polarization, the implementation of the Z-basis meter is just a polarizing beam splitter [32], a mirror and two SPADs [33] as shown in Figure 17.

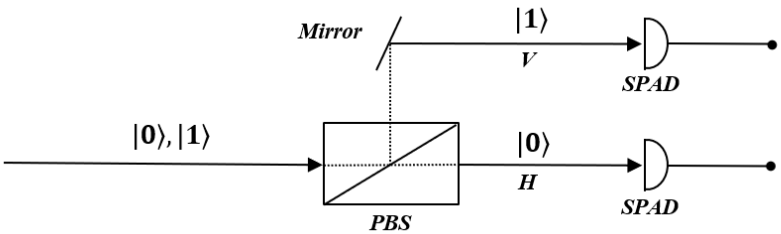


Figure 17. Real receiver with one Polarizing Beam Splitter and two SPAD detectors. The polarization state of the PBS match with the polarization state of the incident photon

If the photon goes up, it means it is vertical, which it's associated with $|1\rangle$ and we will have a click in the upper SPAD, so $a_k' = 1$, for the horizontal case, we will have $a_k' = 0$. This situation is easy to understand because the PBS is polarized according to the horizontal and vertical polarization, so the projection of the measurement is precise because we are projecting on the Z-basis, so there is a precise measurement. The problem is that when Bob chooses the wrong basis, it lies in a true quantum undetermination situation because the input $|+\rangle$ or $|-\rangle$ will collapse at 50% in one SPAD or the other, so the result becomes random, as illustrated in Figure 18.

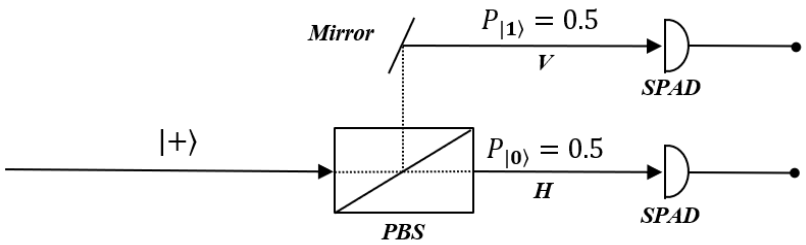


Figure 18. Real receiver with one Polarizing Beam Splitter and two SPAD detectors. The polarization state of the PBS does not match with the polarization state of the incident photon

So here, the problem is the measurement of the X-Basis.

For solving this problem, it is sufficient to put, before the measurement in the computational basis, a gate that transforms the Z-Basis in the X-Basis, but it also applies to any orthonormal basis $\{|\varphi_0\rangle, |\varphi_1\rangle\}$.

$$\hat{U}|0\rangle = |\varphi_0\rangle \, , \hat{U}|1\rangle = |\varphi_1\rangle \tag{2.44}$$

Beeing $\hat{U}$ unitary, implies that the inverse is also the adjoint:

$$\hat{U}^{-1}|\varphi_0\rangle = |0\rangle \, , \hat{U}^{-1}|\varphi_1\rangle = |1\rangle \tag{2.45}$$

For the work case:

$$\hat{U}|0\rangle = |+\rangle \, , \hat{U}|1\rangle = |-\rangle \tag{2.46}$$

$$\hat{U}^{-1}|+\rangle = |0\rangle \, , \hat{U}^{-1}|-\rangle = |1\rangle. \tag{2.47}$$

Applying the inverse gate and the Z-measurement is equivalent to the measurement in the $\{|+\rangle,|-\rangle\}$.

The gate that transform from the Computational Basis to the X-Basis is the Hadamard Gate, and the inverse, in this case is the same as the original gate because it's also hermitian, as we have seen (2.37). The Hadamard operator will be raised to the exponent b'_k which is the "basis" bit sequence that Bob has chosen randomly and independently from Alice.

The receiver diagram is presented in Figure 19.

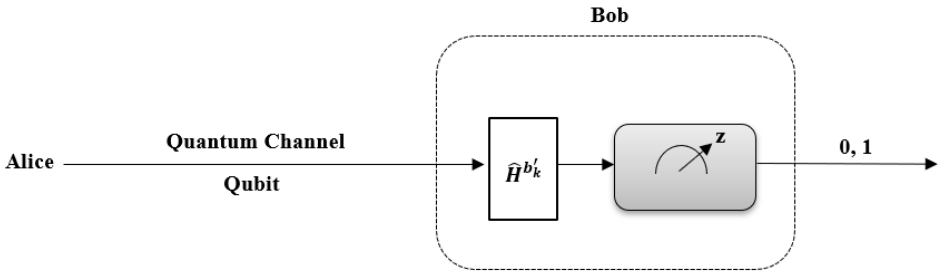


Figure 19. Scheme of Bob. The unitary operator is a Hadamard gate. Measurement in Z-basis

Where:

$$\begin{cases} \hat{\boldsymbol{H}}^{\mathbf{0}} = \hat{\boldsymbol{I}}, & \boldsymbol{b'_k = 0} \\ \hat{\boldsymbol{H}}^{\mathbf{1}} = \hat{\boldsymbol{H}}, & \boldsymbol{b'_k = 1} \end{cases} \tag{2.48}$$

When $b'_k = \mathbf{0}$ the Hadamard acts as a $\hat{I}$ operator so Bob is performing the measurement in the Z-Basis. In the other case, when $b'_k = \mathbf{1}$ Bob is applying a a Hadamard gate, which flips the basis, so Bob begins to measure in the X-Basis.

For the Bob random basis:

$$\{\boldsymbol{Z}, \boldsymbol{Z}, \boldsymbol{X}, \boldsymbol{Z}, \boldsymbol{Z}, \boldsymbol{X}, \boldsymbol{X}, \boldsymbol{X}\} \tag{2.49}$$

$$\boldsymbol{b'_k} = \{\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{1}\}. \tag{2.50}$$

Alice and Bob, at the end of the transmission of the qubits, communicate in a public classical channel the choices of the bases they used. Alice transmits to Bob the sequence $\{\boldsymbol{b_k}\}$ and Bob compares its sequence $\{b'_k\}$, and also Bob shares their bases choice with Alice, at the end, there is a mutual bases exchange between them both.

In the absence of errors (No Eve intervention):

$$\boldsymbol{b_k = b'_k \Rightarrow a_k = a'_k}\,. \tag{2.51}$$

This means that if all the bases of Alice and Bob are the same, the "state" bit sequence must also be the same.

But for the case that the basis does not match:

$$b_k \neq b'_k \Rightarrow a'_k \; at \; random \; . \tag{2.52}$$

This can be quickly checked in Figure 20 if we consider, for instance a 0 bit in Z-Basis measuring with X-Basis (Applying the Hadamard gate at Bob's side):

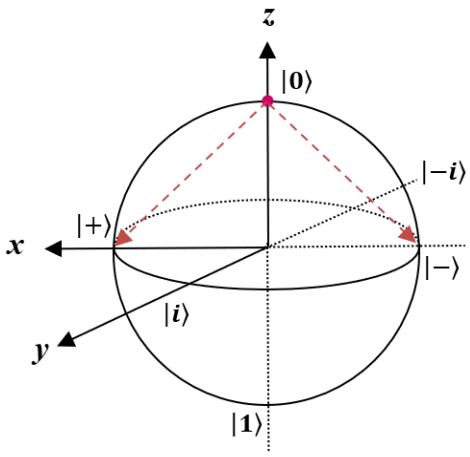


Figure 20. Geometric representation of a qubit Bloch Sphere. Projection of $|0\rangle$ due to the measurement in X-basis

The probability to get $|+\rangle$ or $|-\rangle$, in this case, is completely random. On Bob's side, it could happen that the final bit appears correct, but once Bob checks that the basis for this qubit does not match, he will discard the bit because it is uncorrelated to the original bit sequence that Alice sent.

In our case, the bases only match in terms of subindex $\boldsymbol{k}$ for $\boldsymbol{k} = \mathbf{0}, \mathbf{2}, \mathbf{3}, \mathbf{6}$. From these indexes, they recover the classical bits transmitted, yielding this new key:

$$a'_k = \{\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{1}\} \tag{2.53}$$

This is the so-called shifted key, composed only of the bits generated and measured in the time interval (the time interval within the pulses of the laser emitting single photons) with the same basis. It is called shifted because it is extracted from Bob's measurement but only in the case that Bob's and Alice's bases match.

The final BB84 scheme is described in Figure 21

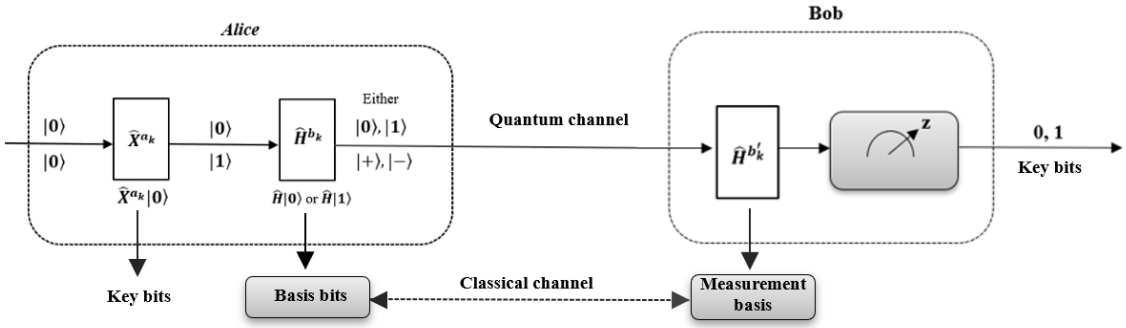


Figure 21. BB84 protocol scheme

Even not considering losses associated with the link attenuation, the shifted key is reduced in length by half of the original or raw key.

Quantum communications based on single photons are much slower than classical ones. It is not possible to use Optical Amplifiers because the generation of additional photons could be intercepted by Eve and extract some information [34].

Furthermore, real implementations of BB84 could make differ the two sequences in some bits, due to the non-ideality of the experimental realization, the dark count rate in the single-photon detection and also, if we transmit in optical fiber, the birefringence of the fiber could change the polarization of the photon [35]. All these imperfection realizations of the protocol and the possibility of Eve's intervention are reflected in the number of errors in the key.

To detect the presence of Eve, Alice and Bob select in a random way, a portion of the shifted key bits and compare them to calculate the quantum bit error rate (QBER). The QBER is determined by dividing the number of incorrect bits in the shifted key by the total number of shifted key bits. If the QBER exceeds a certain threshold (Typically set at 11% [36]), it is assumed that Eve could have acquired too much information about the key, so the QKD process is insecure, Alice and Bob discard the shifted key and a new key exchange is started on a different quantum channel. If the QBER does not exceed the threshold, the protocol proceeds with some standard error correction strategy [37].

After error correction, Alice and Bob share identical copies of the key, but Eve may still have some information about it, they need to reduce Eve's information to an arbitrarily low value using a classical privacy amplification procedure. The privacy amplification shortens the key while maintaining it error-free, reducing Eve's information [38]. From here on, it can be used as an OTP scheme for successive communication over the public channel.

2.2.3 Quantum Attacks and actual device imperfections

The QKD procedure is thus based on a quantum process (the qubit exchange) together with the application of some classical protocols for error correction and privacy amplification. The protocol permits first obtaining identical data and then making it completely secret.

The problem of eavesdropping is to find protocols that, given a specific measure of the QBER only, provide Alice and Bob with a verifiably secure key or stop the protocol and inform the users that the key distribution has failed.

Eve is only limited by the laws of quantum mechanics; the following considerations must be taken into account:

- Eve has no limits in terms of computational power.
- Eve cannot clone, but she can use any unitary interaction between one or several qubits and an auxiliary system of her choice.
- After the interaction, Eve can leave the auxiliary system unperturbed and in complete isolation from the environment for an arbitrarily long time.
- After listening to all the public discussions between Alice and Bob, Eve can perform the measurement of her choice on her system.
- All the errors present in the transmission are assumed due to Eve.

There are several types of attacks that Eve can adopt: *Individual attacks*, *Coherent attacks*, *Collective attacks,* and *Side-channel attacks.* More details on these types can be found in [39] and [40].

For the Individual type attack, Eve probes each qubit independently, one after the other, for the technology available today, only Individual attacks [41] and Side-channel attacks are applicable. Coherent attacks occur when Eve processes several qubits coherently, then we consider Collective attacks as an intermediate class between the two, individual and coherent attacks. In this Collective attack Eve probes each qubit individually but then performs a coherent measure on several of them. The last class of attack is the Side-channel attack where Eve exploits the technical imperfections of the realistic implementation of the protocol.

A review of the *intercept and resend* attack, which belongs to the Individual attack type, will be made, so the implementation problems related to the source and the *Photon Number Splitting* attack, which belongs to the Side-Channel attack category, will be introduced.

Let us consider the case seen in Figure 21. Now, Eve attacks a BB84 protocol with an *intercept and resend* strategy, which is one of the most important types of Individual attacks. The scheme of the new system considering Eve is described in Figure 22.

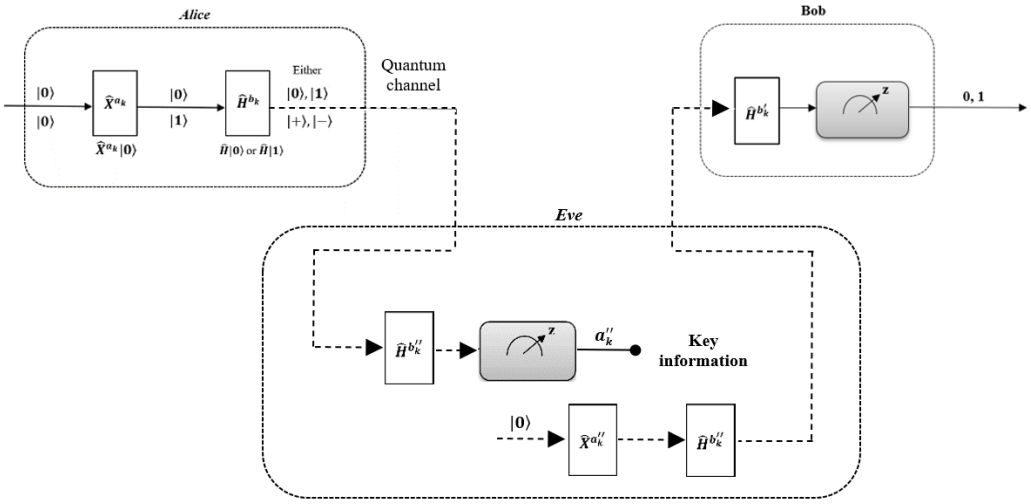


Figure 22. BB84 protocol scheme under the attack of the *intercept and resend* strategy

For this scheme, Eve mimics the behaviour of a Bob-like receiver, for Eve it is possible to know that the transmission between Alice and Bob uses just an X and Z basis, because of that, she uses a Hadamard gate in order to recover either the X or the Z basis.

Eve doesn't know the Alice and Bob basis bit sequence because they maintain the secret at the start of the procedure, just at the end of the measurement, they share through a public channel the basis they had used. So, Eve must choose random sequences between Z and X bases. With this choice of bases, Eve's measurement becomes $\boldsymbol{a_k''}$.

This new information must be used to "regenerate" another qubit, so Eve will use the same scheme as Alice but replace the old sequences with the new ones.

$$\boldsymbol{a_k \rightarrow a_k''}\,, \boldsymbol{b_k \rightarrow b_k''}\,. \tag{2.54}$$

Finally, the procedure is as follows: Eve takes a qubit from the main system, measures it, "regenerates" it and resends a copy to Bob.

There are two possibilities of the Eve's performance:

Because the probability of error is just related to the shifted key, the exchange of information about the errors is in the shifted key.

$$\boldsymbol{b_k = b_k'}. \tag{2.55}$$

- For our first case, the bases chosen by Eve is equal to Alice and Bob bases.

$$\boldsymbol{b_k = b_k' = b_k''}. \tag{2.56}$$

In this case, Eve measures the qubit with precision without introducing any perturbation.

$$a_k = a'_k = a''_k. \tag{2.57}$$

Eve also measures the shifted key precisely, but its action is not revealed to Bob.

With a 50% probability, Eve can guess the correct basis and thereby extract the bit's information and replace it without revealing its action.

- The second case is a wrong choice of the Eve's basis.

$$b''_k \neq b_k. \tag{2.58}$$

It means a''_k will be completely random in terms of bit, then a''_k is not correlated to a'_k , so in this second case, we have a 50% probability that Eve's basis is wrong with respect to Alice. However, even if Eve guesses incorrectly, 50% of the times the collapse in Bob's measurement will make the final bit correct.

When Eve tries to intercept and resend all the qubits, she introduces errors, which are measured in the QBER.

$$QBER = P_{Eve\ wrong\ basis} \cdot P_{Bob\ random\ wrong\ bit\ measurement} = 0.5 \cdot 0.5 = 25\% \tag{2.59}$$

The security of BB84 is given by the fact that intercepting a wrong bit 25% of the time means that also Eve will generate a wrong bit in Bob with the same probability, so at the end of this process, in case of intervention of Eve, Alice and Bob will share the keys (We are considering the errors in the shifted key) and they could understand that the rate of error is very high, in that case the communication will be discarded.

However, Eve can apply this attack scheme to just a fraction of the qubits to decrease the distubance. Therefore, Alice and Bob must use procedures to correct the errors, as we have seen, classical error correction and privacy amplification.

The complications arise when it is wanted to project this abstract strategy in practical implementations. For the BB84 scheme, it is considered that the source must be a single-photon laser source, but this first statement is difficult to achieve because single-photon source is not available for QKD nowadays [42].

Attenuated lasers using weak coherent pulses offer a practical and cost-effective method for probabilistically generating single-photon pulses. However, because the number of photons in each time interval obeys Poisson statistics, it is impossible to guarantee the creation of a single-photon pulse. Therefore, the probabilities of emitting both multi-photon and vacuum pulses (no emission) must be carefully managed because of possible Eve's attacks. For the quantum optics literature [43], the weak coherent pulses are highly attenuated so that the average number of photons per pulse, μ decreases below 1. They can be realized using only standard lasers and calibrated attenuators. Also derived from the Mandel Expression (1958) for the limit laser case, the probability of finding n photons in such a coherent state follows the Poisson statistics [44].

$$P(n, \mu) = \frac{\mu^n}{n!}\, e^{-\mu}. \tag{2.60}$$

The probability that a nonempty weak coherent pulse contains more than one photon is given by:

$$P(n > 1 | n > 0, \mu) = \frac{1 - P(0,\mu) - P(1,\mu)}{1 - P(0,\mu)} = \frac{1 - e^{-\mu}(1+\mu)}{1 - e^{-\mu}} \cong \frac{\mu}{2}. \quad \textbf{(2.61)}$$

However, when μ is small, most pulses are empty.

$$P(n = 0) \approx 1 - \mu. \quad \textbf{(2.62)}$$

The problem arises at the detector part, when these *vacuum* states produce a really low signal-to-noise ratio because the detector must receive all the pulses and the dark count noise is high (i.e, click in the absence of photons arriving). The typical value of $\mu = 0.1$, meaning that the probablity of a nonempty weak coherent pulse containing multiple photons is around 0.05, showing that one of twenty weak coherent pulses contains more than one photon. However, it is important to point out that there is an optimal μ depending on the transmission losses [45]. The consideration of weak coherent pulses as a source for the BB84 protocol introduces the possibility for Eve to exploit multiple photon pulses to extract information.

The next attack we are considering is the *Photon Number Splitting Attack* (PNS attack), which belongs to the Side-Channel attack category.

Alice is now using weak coherent pulses; Eve can, therefore, measure the number of photons in a given pulse, when the pulse contains just one photon, she just blocks it because if she tries to measure the photon, we recover a kind of *intercept and resend* strategy where Eve risks to disturb the system so increasing the QBER and also increasing the probability to be detected by Alice and Bob, blocking that photon can be disguised as losses in the channel, that could be associated to the typical attenuation values of the optical fiber. When the pulse contains more than one photon, she can split the photons using a classical beam splitter (BM), then Eve picks out one or more photons from these pulses and stores them in quantum memory while letting the others reach Bob. Eve waits for the bases to be revealed. Thereafter, Eve reveals the state, comparing the bases with the stolen photon state. Being n the number of photons, P_A the probability that a nonempty pulse has more than one photon as Alice's output, P_B the probability of detecting a nonempty pulse by Bob:

$$P_A(n > 1) > P_B(n \neq 0). \quad \textbf{(2.63)}$$

When the inequation (2.63) is satisfied, Eve can get a kind of eavesdropping called quantum non-demolition attacks, which is a generalization of the PNS attack. Eve's presence remains undetected as the photon rate received by Bob remains unchanged and the losses of the process are masked by the channel losses. Hence, without an appropriate countermeasure, completely renders QKD systems unusable.

2.2.4 Decoy-State

It is clear after the last chapter that implementation using ideal single photon sources is not possible. As we have seen, the most recommended solution exposed in the literature [46] is to use sources that employ weak coherent pulses. The problem with these sources is that they seem to enable a new type of attack (non-demolition attacks) that allows information to be extracted without disturbing the system. This is extremely dangerous, so a countermeasure is now introduced to restore security using attenuated sources.

The idea behind the decoy-state method is as follows, The Photon Number Splitting (PNS) attack takes advantage of the fact that the source sends pulses with an undetermined number of photons in each of them, and as we have seen from 2.2.3, extracts photons only in cases where the pulse is a nonempty multi-photon pulse. This means that Bob will receive more multi-photon pulses than 'ideal' pulses with only one photon. The latter, when measured by Eve, are blocked and disguised to Bob as simple attenuation attributed to the channel. In this context, the parameter *yield* (**Y**) is introduced, which indicates the conditional probability that Bob receives the signal having been sent a multi-photon pulse by Alice.

Here lies the trick of the decoy state: Alice adopts two photon sources, one associated with the average signal with a high single-photon pulse probability, and the other source associated with the decoy with a high multi-photon pulse probability. Now, intentionally alternates between the signal source and the decoy source with a certain probability. Once the qubit transmission ends, through a classical channel (so for the bases discussion), Alice announces the source they had used for each pulse, so they estimate the total yield for the signal and decoy source. Eve cannot differentiate whether the pulses are decoy or belong to the original signal, so the yield of the pulses will be similar. Hence, if equation (2.64)

$$\boldsymbol{Y_d \gg Y_s} \tag{2.64}$$

Is satisfied, they abort the whole process, allowing Alice and Bob to now detect if Eve is trying to extract information from the system. This idea was introduced and designed by Won-Young Hwang [47].

Introduced by [48], nowadays, the most used decoy state is the *vacuum + weak decoy* state. By using the *vacuum* as a decoy state, Alice and Bob can measure the dark count rates of their detectors, so it is also a tool for characterizing the detector, and by using weak decoy states, they can lower bound the yield of single-photon sources. Therefore, the relation between the average photon number for pulse in the signal, weak decoy state and *vacuum* state is:

$$\boldsymbol{0 < \nu < \mu} \tag{2.65}$$

Chapter 3. Simulation Description

As we have pointed out throughout the theoretical framework of this BT, QKD systems emerge as a solution to the imminent development of quantum technologies capable of breaking the security of current key distribution methods. Therefore, ensuring that the implementation of QKD is secure is necessary.

Since ideal sources do not exist, the alternative of using weak coherent pulses with attenuated lasers opens the door to a new category of attacks called PNS (photon number splitting) attacks, which belong to the so-called side-channel attack. A new method called the decoy state has been designed to address this emerging issue. This method is relatively recent, so the characterization of its performance presents a research opportunity.

As we have seen for the BB84 protocol, the system uses a quantum channel to transmit the qubits. The so-called dark fiber is generally used for this channel, an unused optical fiber available in fiber optical systems. Since the system naturally integrates with pre-existing installations, it does not require significant investment in installation [49-50].

This work considers the link between Alice and Bob as the emitter and receiver on a channel completely separate from conventional data channels, so only the QKD signal will be considered. The scheme of the system considered is presented in Figure 23.

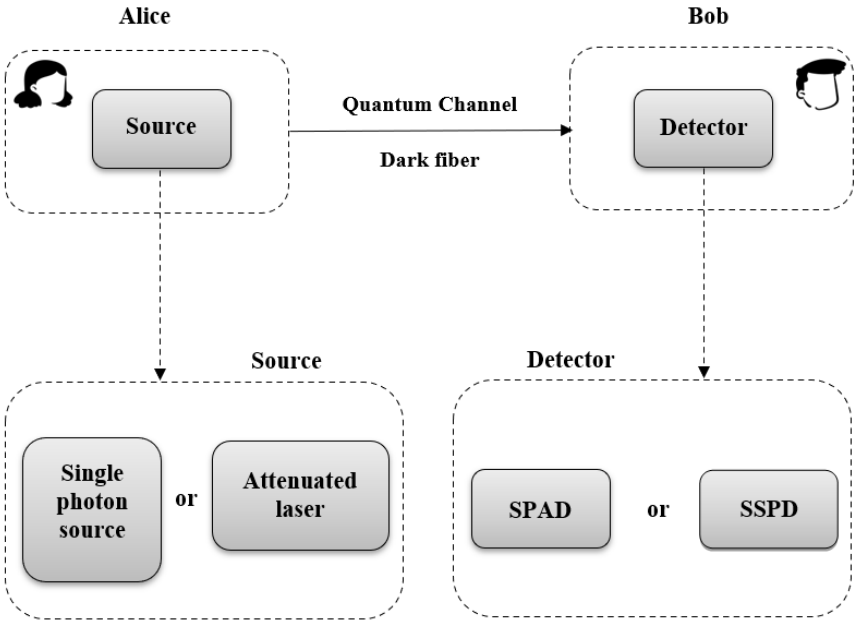


Figure 23. Simulation scheme description. Sources: Ideal Single-Photon source and Attenuated laser sources. Receivers: SPAD detector and SSPD

The objective of the BT is to compare the performance of two links using the BB84 protocol with an ideal single-photon source versus one using an attenuated laser that employs weak coherent pulses, in the case of using a SPAD detector and a SSPD.

SPADs are the most used detectors [51]. They can click when the current is equivalent to that induced by a single photon. On the other hand, SSPDs are the fastest detectors for counting individual photons, the choice of both detectors is based on the interest in comparing the state-of-the-art detectors with those that have been used for several years and applying these technologies in the context of quantum communications [52]. The characterization of the detectors will be based on the detector's efficiency and the dark count rate, the latter being an average value of clicks the detector makes in the absence of incident photons, those clicks usually are caused by thermal noise.

The simulations will be carried out in MATLAB, a GitHub repository has been created to store and share all the simulation codes [53]. For the system characterization, the following parameters have been used: the attenuation that the fiber has on the signal, the internal losses of the detector, the detector efficiency, the dark count rate, and the misalignment from which a photon hits the wrong detector. As shown in Figure 17 and Figure 18, depending on the polarization of the qubit or small physical errors of the PBS, the incorrect detector may click.

The initial numerical data is provided by the Polytechnic University of Milan, which collaborates with POLIQI, a project arising from the collaboration of the Polytechnic University of Milan, the Lombardy Region, ARIA, Intesa Sanpaolo, and the 1st Army Transmission Regiment, whose goal is to create an ultra-secure post-quantum network in Milan for the first time.

3.1 System Configuration

To describe the system model that implements the BB84 protocol, the source, channel, and detector must be described and characterized.

The laser source will be modelled according to a Poisson distribution introduced in (2.60), where $\boldsymbol{\mu}$ indicates the average photon number set by Alice. As will be seen later, the choice of $\boldsymbol{\mu}$ will not be random, and we will need to find an optimization rule.

For the channel modelling, we consider an optical fiber that operates in the 3rd window (1550nm) due to its low attenuation and dispersion. The attenuation that the signal receives is described by:

$$\boldsymbol{l_{AB} = 10^{-\alpha \cdot L/10}.} \tag{3.1}$$

Being **L** the total distance between Alice and Bob and $\boldsymbol{\alpha = 0,2\,\frac{db}{km}}$ the attenuation coefficient for an optical fiber operating in 3rd window.

For the detector, we consider the overall efficiency of the system that determines how many photons sent by Alice are correctly detected by Bob after accounting for all losses:

$$\boldsymbol{\eta = l_{AB} \cdot l_{BOB} \cdot \eta_D.} \tag{3.2}$$

Where $\boldsymbol{l_{BOB}}$ is the intern detector losses and $\boldsymbol{\eta_D}$ is the detector efficiency.

The overall detection efficiency is related to to the transmittance of the *i*-photon signal as:

$$\eta_i = 1 - (1 - \eta)^i \,. \tag{3.3}$$

So, for the case of a Single-Photon source:

$$\eta_1 = \eta \,. \tag{3.4}$$

It is necessary to consider a threshold in Bob's side. The detector is able to differentiate between a nonvacuum state and a vacuum state, but it can not recognize how many photons is detecting, At the end, the detector will click if at least there is one photon.

The conditional probability that Bob receives a signal when Alice sends a *vacuum* pulse, it means that Alice sends non-photon pulse, it is the detection of background noise:

$$Y_0 = 2p_{dc} - {p_{dc}}^2 \,. \tag{3.5}$$

Where p_{dc} is the dark count rate.

The same conditional probability could be generalized for i-photons. The probability that Bob receives a signal when Alice sends a i-photon pulse is:

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \approx Y_0 + \eta_i \,. \tag{3.6}$$

In the case of a Single-Photon source:

$$Y_1 \approx Y_0 + \eta_1 \,. \tag{3.7}$$

The next parameter we are going to introduce is the gain, which is defined as the product of the Poissonian probability for emmitting a *i*-photon pulse and the yield for a *i*-photon pulse.

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu} \,. \tag{3.8}$$

Since for a Single-Photon source the probability $P_1 = \delta_1 = 1$ and $P_i = \delta_i = 0 : \; i \neq 1$:

$$Q_1 \approx Y_1 \,. \tag{3.9}$$

The overall gain of the signal is given by:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = \sum_{i=0}^{\infty} Q_i \,. \tag{3.10}$$

The error rate of the *i*-photon pulse is defined by:

$$e_i = \frac{e_0 Y_0 + e_{mis}\eta_i}{Y_i}. \tag{3.11}$$

Where e_{mis} is the missalignment and e_0 is the error rate of the background $e_0 = \frac{1}{2}$.

The overall QBER is expressed as:

$$E_\mu = \frac{1}{Q_\mu}\sum_0^\infty e_i Q_i = \frac{1}{Q_\mu}\sum_0^\infty e_i Y_i \frac{\mu^i}{i!}\, e^{-\mu} \tag{3.12}$$

The final formulas for E_μ and for Q_μ are given by:

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu}. \tag{3.13}$$

$$E_\mu = \frac{1}{Q_\mu}[e_0 Y_0 + e_{mis}(1 - e^{-\eta\mu})] \tag{3.14}$$

In the standard BB84 protocol the secure key generation rate [bit/pulse] can be shown to be given by:

$$R = q\{Q_1[1 - H_2(e_1)] - f_e Q_\mu H_2(E_\mu)\} \tag{3.15}$$

Where $q = \frac{1}{2}$ since Alice and Bob choose the righ basis half of the time, Q_1 and e_1 is te gain of single-photon pulse and the error rate of single-photon pulse respectively, the possitive term of the equation is related to the single-photon contribution in the final key.

Delving into the second part of the equation, $f_e \geq 1$ is the error correction efficiency, for us $f_e = 1$ because we assume no error correction, so this procedure does not introduce noise, Q_μ and E_μ are the overall gain and QBER respectively. This second term is related to the contributions of multi-photon pulses to the final key. Both terms are related to the binary Shannon entropy H_2 calculated as:

$$H_2(x) = -x log_2(x) - (1 - x) log_2(1 - x). \tag{3.16}$$

For the ideal case where single-photon sources are considered, we can stablish a lower bound for the secure key rate (SKR) deriving the formula of (3.15).

$$R \geq q Q_\mu\{\Omega[1 - H_2(e_1)] - H_2(E_\mu)\} \tag{3.17}$$

Where:

$$\Omega = \frac{Q_1}{Q_\mu} \tag{3.18}$$

For the first ideal case, where $Q_\mu = Q_1$ and $E_\mu = e_1$ because the gain and the error bit just depend on the contribution of Single-Photon pulses, so $\Omega = 1$.

The final lower bound for the secure key rate is shown:

$$R \geq qQ_1\{1 - 2H_2(e_1)\} \tag{3.19}$$

Considering now attenuated sources, the distribution of photons in the pulses is not deterministic but probabilistic shown in equation (2.60); therefore, the probability of obtaining multi-photons in the pulses is non-zero. The parameter μ defines this probability. By choosing an appropriate value of μ, we can significantly improve the lower bound of the secret key rate. Next, we will consider an optimization rule for the parameter μ.

Following the disccusion from [54]. For increase **R**, we need to maximize the gain Q_1 and minimize the overall gain Q_μ, it means, remain (3.18) as higher as possible. Intuitively we have a constrain of μ as:

$$\mu \in (0, 1] \tag{3.20}$$

For the SPAD and the SSPD we can assume that the background rate is low ($Y_0 \ll \eta$) so the secure key rate is given by:

$$R \approx -\eta\mu f(e_{mis})H_2(e_{mis}) + \eta\mu e^{-\mu}[1 - H_2(e_{mis})] \tag{3.21}$$

Where can be optimized $\frac{dR}{d\mu} = 0$, considering $f(e_{mis}) = 1$ from where we obtain the following optimization relation:

$$(1 - \mu)e^{-\mu} = \frac{H_2(e_{mis})}{1 - H_2(e_{mis})}. \tag{3.22}$$

The optimizated value μ depends only on the Shannon Entropy and the missalignment of the detector.

Now, we introduce the model of the decoy-state method applying the *Vacuum + Weak decoy* state, which is the optimal case for the decoy-state since, as it has been seen, there is no notable improvement between the two-decoy-state and a divergence number of decoy states.

The *Vacuum + Weak decoy state* is already introduced in **(2.2.4) Decoy-State**. The authors of [55] provide the final formulas of Y_1, Q_1, e_1.

$$Y_1 = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2}Y_0\right). \tag{3.23}$$

$$Q_1 = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \quad \textbf{(3.24)}$$

$$e_1 = \frac{E_\mu Q_\mu e^\mu}{Y_1 \mu}. \quad \textbf{(3.25)}$$

Where ν is the average photon number for the non-vacuum decoy state $\nu < \mu$. According to the consensus within the community, ν is small (~0.1), and Q_ν is expressed as:

$$Q_\nu = Y_0 + 1 - e^{-\eta\nu}. \quad \textbf{(3.26)}$$

3.2 Performance Analysis and Results

To characterize the implementation of QKD systems, a comparison is proposed:

The original contribution lies in integrating an SSPD as an additional element that provides information and paves the way for new QKD systems. Specifically, the use of the BB84 protocol takes advantage of the characteristics of this new type of detector, which in this work are characterized by two essential parameters in optical communications: detector efficiency ($\boldsymbol{\eta_D}$) and dark count rate ($\boldsymbol{p_{dc}}$). The potential solution for implementing a QKD system based on an SSPD will be compared to the SPAD detector. It is expected that the performance in terms of secret key rate will be significantly higher in the case of the SSPD, given its superior characteristics, which will be discussed below.

In this section, the QKD performanced is evaluated in terms of secret key rate (**SKR**) in different scenarios.

- Ideal Single-Photon source with SPAD and SSPD.

The parameters used in the following simulation are listed in Table 3 and Table 4.

l_{BOB}	-3dB
p_{dc}	10^{-5}
e_{mis}	10^{-2}
η_D	0.2
f_e	1
e_0	0.5

Table 3. System parameters used in simulations for SPAD

l_{BOB}	-3dB
p_{dc}	10^{-9}
e_{mis}	10^{-2}
η_D	0.9
f_e	1
e_0	0.5

Table 4. System parameters used in simulations for SSPD

A comparison of the SKR for a single-photon source propagating in an optical fiber with detectors varying between the two types used is performed and exposed in Figure 24. The slopes are, therefore, related to the difference in detector efficiency rate between the SPAD and the SSPD and also to the dark count rate, which is much lower in the case of the SSPD.

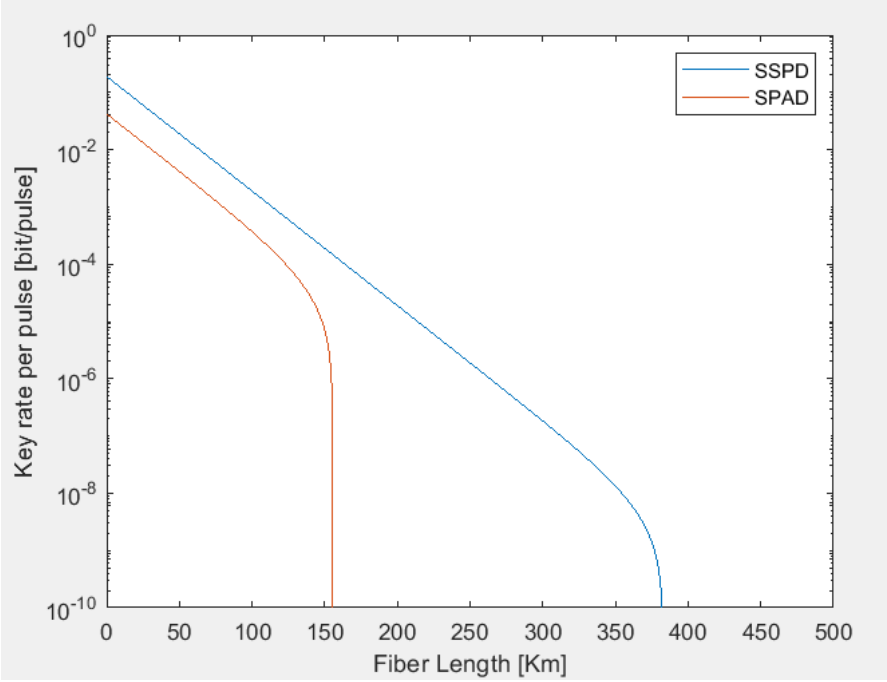


Figure 24. Secure Key Rate [bit/pulse] vs Fiber Length [km], SPAD and SSPD, performance of ideal Single-photon source in BB84

From Figure 25, the very-high detector efficiency and low dark count rate of the SSPD provide an increase in distance of the SKR of more than double compared to what the SPAD offers. The distance at which the 3dB drop occurs, where the signal associated with the SPAD begins to collapse, is 148.4 km. For the SSPD, this distance is 375.6 km.

For every 5 km, the variation in SKR is calculated, thus establishing the 3dB drop.

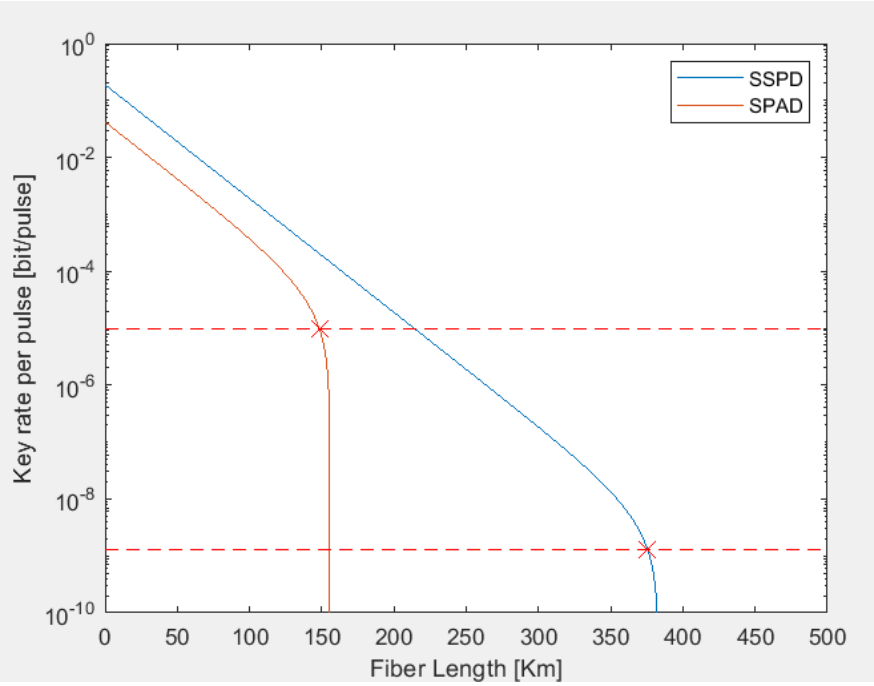


Figure 25. Secure Key Rate [bit/pulse] vs Fiber Length [km], SPAD and SSPD, performance of ideal Single-photon source in BB84 protocol. The dashed red line indicates the SKR at which the signal drops by 3dB

Now, to further characterize the performance of the BB84 protocol, the dark count rate and the misalignment of the detectors will be parameterized. Assuming it is an ideal device, Bob's internal losses will not be considered. The rest of parameters are indicated in Table 5. The dependency between the SKR and the total detection efficiency the link can withstand before collapsing is shown in Figures 26 and 27.

l_{BOB}	-0dB
p_{dc}	Parametrized
e_{mis}	Parametrized
f_e	1
e_0	0.5

Table 5. System parameters used in follow simulations, misalignment and dark count rate are parametrized

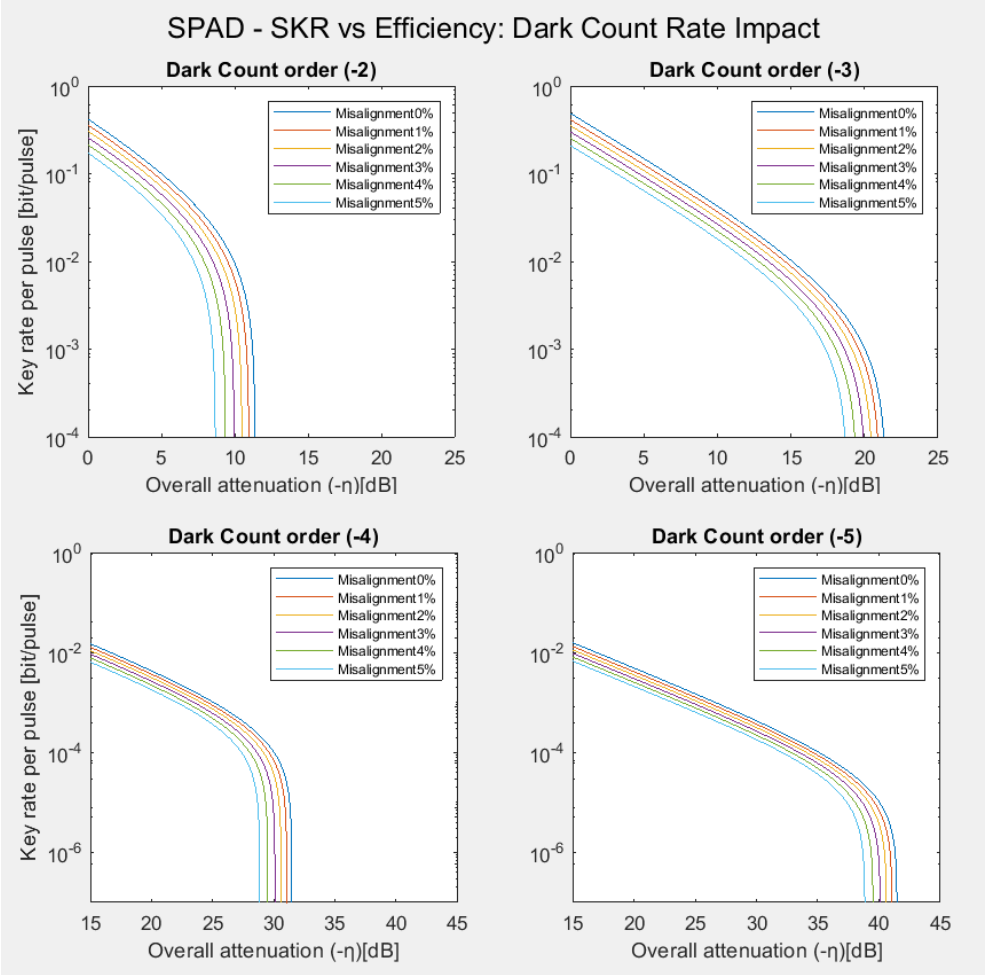


Figure 26. Secure Key Rate[bit/pulse] vs Overall detection efficiency[dB], e_{mis} from 0% to 5% and p_{dc} from 10^{-2} to 10^{-5} parametrized.

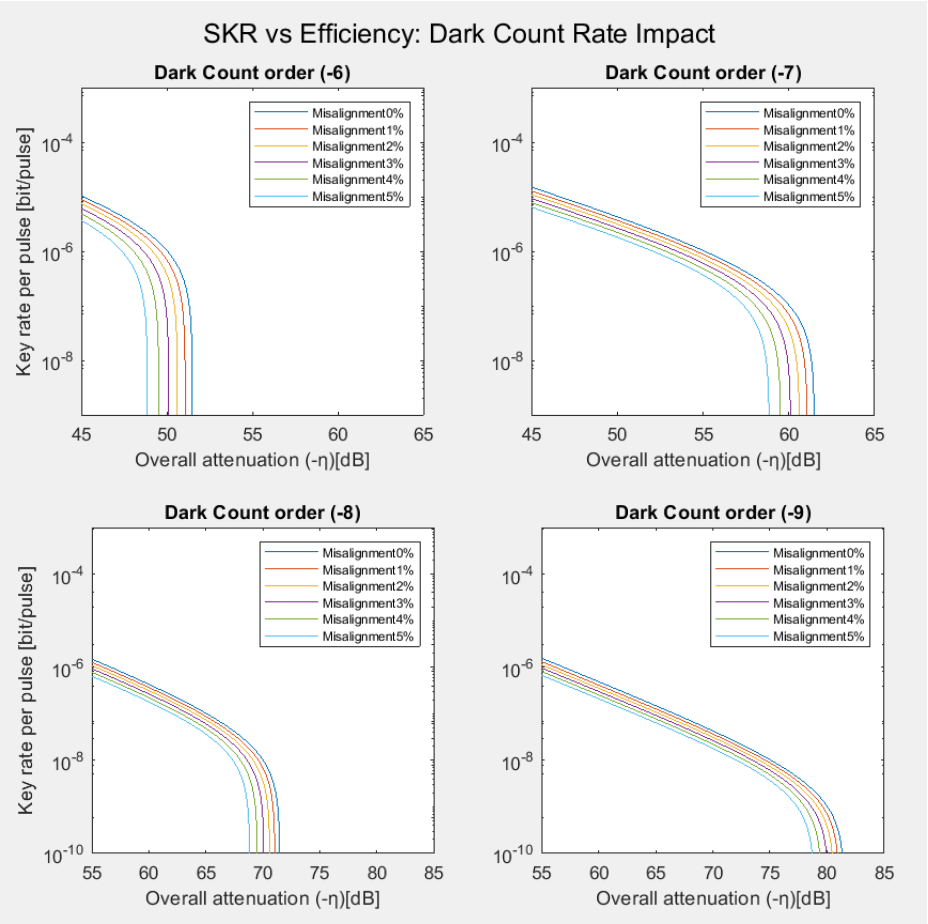


Figure 27. Secure Key Rate [bit/pulse] vs Overall detection efficiency [dB], e_{mis} from 0% to 5% from 10^{-6} to 10^{-9} parametrized.

From Figure 26 and Figure 27, the dependence between the overall attenuation in the link and the **SKR** is observed. The overall detection efficiency is described in (3.2). As it's normalized to one, the best scenario considering that no attenuation is involved $\boldsymbol{l_{AB} = 1}$. The efficiency of the detector $\boldsymbol{\eta_D}$ is 100%, and the internal losses of Bob $\boldsymbol{l_{BOB}}$ are 0dB, means $\boldsymbol{\eta = 0dB}$. Since the optical fiber remains invariant and the internal losses of Bob are neglected, the total attenuation depends only on the detector efficiency $\boldsymbol{\eta_D}$ and is exactly equal a $\boldsymbol{-\eta}$.

Varying for each order of the dark count with the misalignment ranging from perfect alignment to a 5% misalignment. The variation of the overall attenuation is $2.7\text{dB} \pm 0.3\text{dB}$, thus, misalignment plays a crucial role in designing the system, and a 5% variation can decrease the SKR by up to 50%.

Regarding the variation of $\boldsymbol{p_{dc}}$, the change in order is meaningful. For a dark count rate of 1 erroneous click per 100 clicks, 10^{-2}, the SKR collapses for an overall detector efficiency centred at $10\text{dB} \pm (\sim 3\text{dB})$ due to the variation of the misalignment. The trend remains the same, for each order of magnitude by which the dark count $\boldsymbol{p_{dc}}$ decreases, the maximum attenuation that the system can support consequently increases by 10dB.

For the case of the SPAD detector, if we set $\boldsymbol{p_{dc} = 10^{-5}}$ and $\boldsymbol{e_{mis} = 10^{-2} = 1\%}$ in Figure 26. The maximum attenuation is (~40dB). Therefore, we can deduce the maximum distance the signal will achieve.

$$(\sim \mathbf{40}[\boldsymbol{dB}]) + \boldsymbol{l_{BOB}}[\boldsymbol{dB}] + \boldsymbol{\eta_D}[\boldsymbol{dB}] = \mathbf{30}[\boldsymbol{dB}] \quad \textbf{(3.27)}$$

We use the attenuation coefficient $\boldsymbol{\alpha}$ exposed in **System Configuration** (**3.1**); The total distance is given by $\frac{\mathbf{30}\boldsymbol{dB}}{\mathbf{0.2}\frac{\boldsymbol{dB}}{\boldsymbol{Km}}} = \mathbf{150}\boldsymbol{km}$ which is consistent with the results.

The maximum distance the link must have in order to assure the SKR can be derived from Figure 26 and 27 using (3.27).

- Attenuated laser source with SPAD and SSPD.

Finally, the simulations of the real implementation of the BB84 systems with decoy state will be shown. The parameters used in the following simulation are listed in Table 6.

l_{BOB}	-3dB
p_{dc}	10^{-5}
e_{mis}	parametrized
η_D	0.2
μ	$\mu_{optimal}$
ν	0.05
f_e	1
e_0	0.5

Table 6. System parameters used in follow simulations, variation of the misalignment and $\mu_{optimal}$ parameter

In Figure 28, the dependency between the SKR and the distance is established. In this case, a comparison between three situations is evaluated:

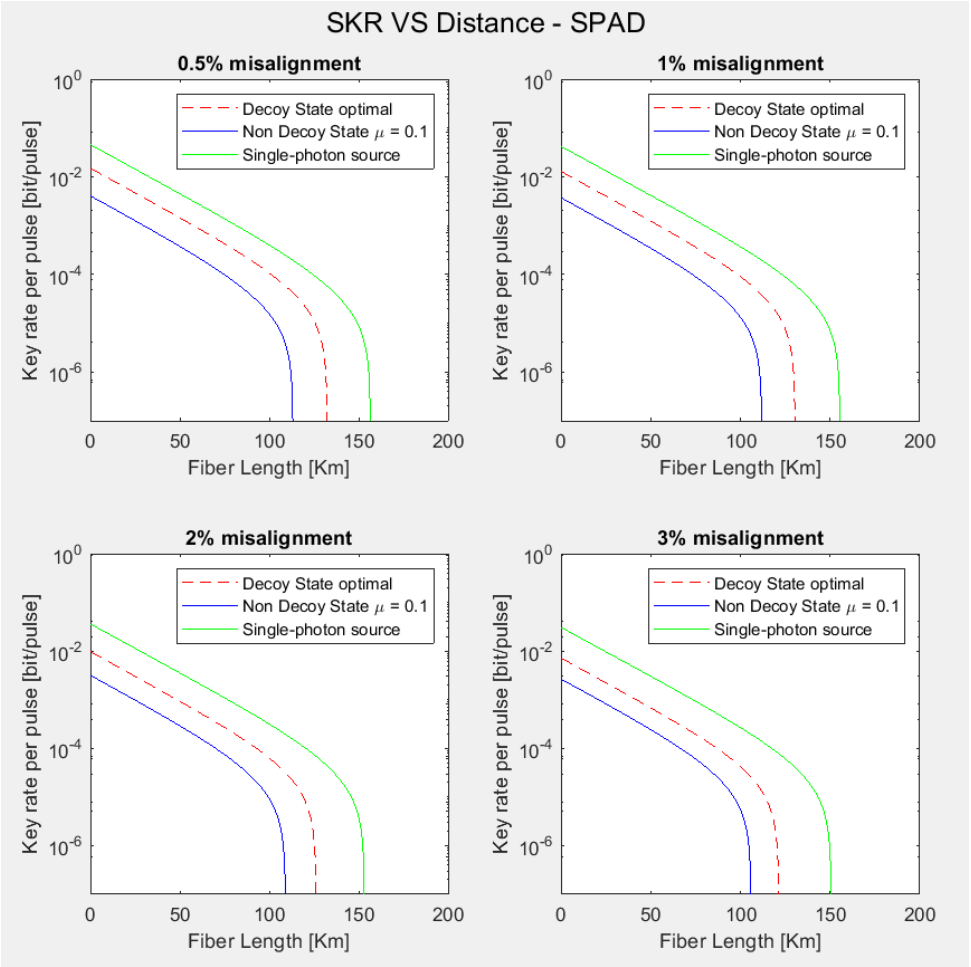


Figure 28. SPAD – SKR [bit/pulse] vs Distance [km]. Considering the following situations: Green line: ideal single-photon source. Blue line: attenuated laser with a nonzero probability of multiple-photon pulses with non-decoy state. Dashed red line: attenuated laser with nonzero probability of multiple-photon pulses using *vacuum + weak* decoy state with $\mu_{optimal}$

For the single-photon source, we recover the same data we used in Table 3.

For the non-decoy State, we are still facing a situation of possible multi-photon pulses because we are using an attenuated laser as the source. However, in this case, we do not alternate between different values of the mean number of photons per pulse; we only have one value, **μ**. This value has been set to 0.1, which implies that 5% of the pulses are multi-photon. This can be seen in Figure 29. This value makes sense to be set so low because if we do not use a decoy state, we want most pulses to be single photon to prevent Eve from extracting information using the PNS attack.

Lastly, we use the equation (3.22) for obtain $\boldsymbol{\mu_{optimal}}$ and then apply (3.23), (3.24), (3.25) using the *vacuum + weak decoy* state formula.

The performance of the Decoy state is much better than the non-decoy state one, the difference is in the order of $20Km$. The performance of the decoy state using $\boldsymbol{\mu_{optimal}}$ is a $80\% \pm 5\%$ with respect to the ideal source case. This value can be obtained comparing the distance achieved for an equal value of the secure key rate.

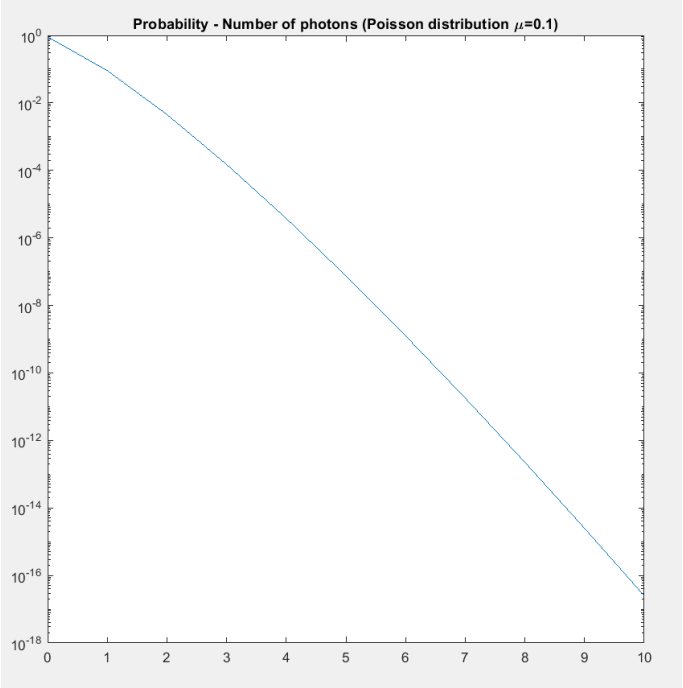


Figure 29. Poisson distribution for $\mu = 0.1$. The conditional probability that a nonempty weak coherent pulse contains more than one photon is given by: $\frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)} = 0,046 \approx 5\%$

To better explain the dependence of the performance of the decoy state using $\boldsymbol{\mu_{optimal}}$ concerning the $\boldsymbol{e_{mis}}$, Figure 30 offers a graphical comparison:

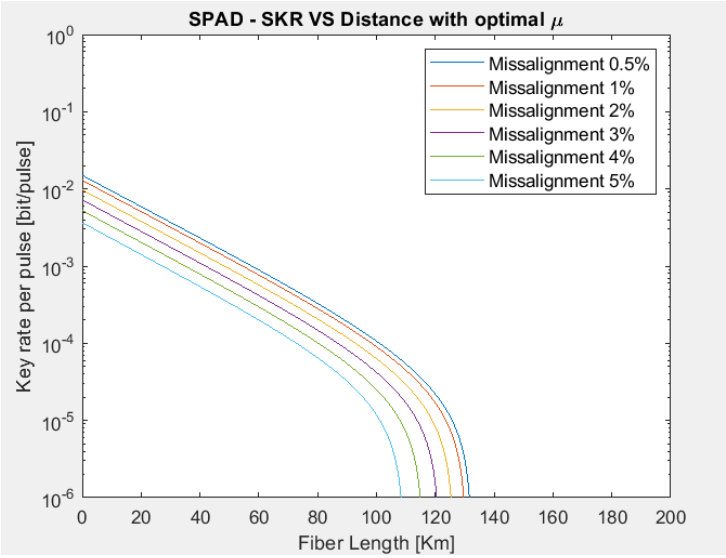


Figure 30. SPAD – SKR [bit/pulse] vs Distance [km]. Comparation between *Vacuum+Weak decoy* state using $\mu_{optimal}$ with e_{mis} parametrized

A difference of 20km in range arises as a result of the difference between a lower misalignment of 0.5% compared to 5%.

The values of $\mu_{optimal}$ for each misalignment showed in Figure 30 are represented in Table 7.

e_{mis}	$\mu_{optimal}$
0.5%	0.8848
1%	0.8037
2%	0.6761
3%	0.5723
4%	0.4821
5%	0.4008

Table 7. Related values of $\mu_{optimal}$ for each e_{mis} for SPAD and SSPD

Since the values of e_{mis} remains the same in both cases, the values of $\mu_{optimal}$ are equal in the SPAD and SSPD cases.

Considering now this data for the SSPD detector Table 8.

l_{BOB}	-3dB
p_{dc}	10^{-9}
e_{mis}	parametrized
η_D	0.9
μ	$\mu_{optimal}$
ν	0.05
f_e	1
e_0	0.5

Table 8. System parameters used in follow simulations, variation of the misalignment and $\mu_{optimal}$ parameter

Now the dependence for SKR with respect to the distance for the SSPD case is seen in Figure 31.

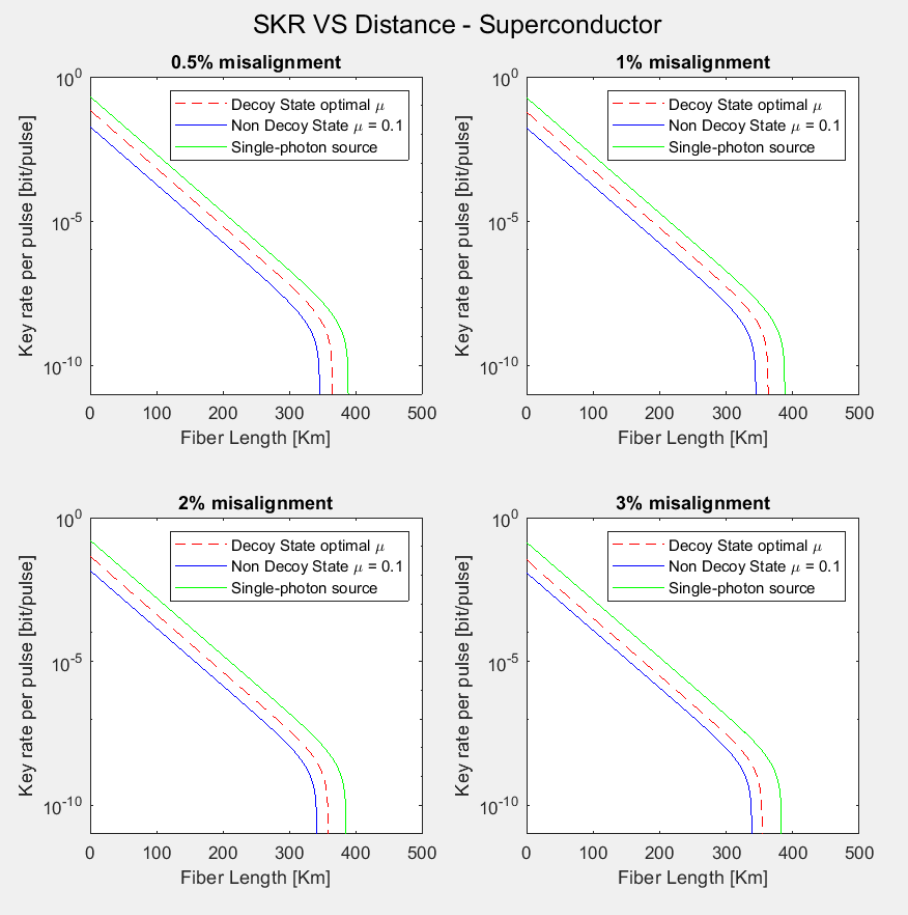


Figure 31. SSPD – SKR [bit/pulse] vs Distance [km]. Considering the following situations: Green line: ideal single-photon source. Blue line: attenuated laser with a nonzero probability of multiple-photon pulses with non-decoy state. Dashed red line: attenuated laser with nonzero probability of multiple-photon pulses using *vacuum + weak* decoy state with $\mu_{optimal}$

The relation between the different $\mu_{optimal}$ with respect to the values of misalignment is also shown in Figure 32. The performance of the Decoy state using $\mu_{optimal}$ is a $90\% \pm 5\%$ with respect to the ideal single-photon source case.

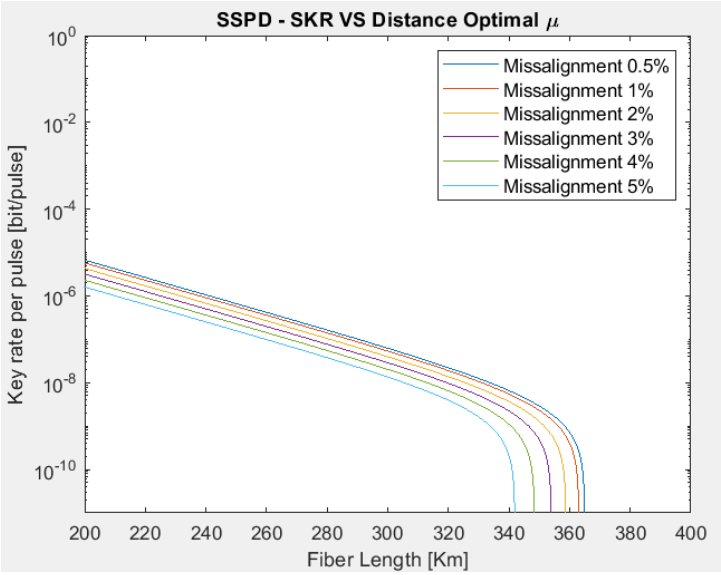


Figure 32. SSPD – SKR [bit/pulse] vs Distance [km]. Comparation between *Vacuum+Weak decoy* state using $\mu_{optimal}$ with e_{mis} parametrized

The overall performance is much better for the SSPD detector for the ideal single-photon source and the attenuated laser source. Regarding distance, using an SSPD instead of SPAD, is translated as an increase of ~200km. For the decoy state case using $\boldsymbol{\mu_{optimal}}$, the distance increment is $\sim 20km$ with respect to a non-decoy source with $\boldsymbol{\mu = 0.1}$.

Chapter 4. Simulation Discussion and Conclusions

The frequencies at which the SPAD and the SSPD operate are typically 1 MHz and 1 GHz [56], respectively. Considering that for the case of an ideal single-photon source at 100 km, the secure key rate is around 3×10^{-4} for the SPAD and 1×10^{-3} for the SSPD. The final rates are on the order of Kb/s and Mb/s. It should be noted that these rates are for the distribution of the keys. Using these keys, an OTP scheme, or a suboptimal encryption scheme (in terms of information security), such as AES-256, encrypts the message. The final rate will depend on the encryption scheme we use and its dependency on key refresh. In the case of the OTP scheme, the key must be refreshed for each message sent, these rates are still small compared to those commonly seen in classical optical communications but are sufficient, for example, for video transmission. However, for the AES-256 encryption scheme, the refresh of the key is around minutes, which is a frequently reported order of magnitude value in the bibliography [57], this condition makes the final rates in the order of Gb/s, which means that it is achievable the speeds of classical optical communications.

Regarding the performance of BB84 using attenuated laser sources, the performance in terms of SKR is very similar to that offered by an ideal single-photon source. Therefore, the implementation of two Decoy States using the *vacuum + Weak* state method allows attenuated lasers to protect communication against the PNS attack, and at the same time, the performance of the SPAD and the SSPD relative to the ideal source case reflects about ($\sim$80%) and ($\sim$90%), respectively, so a better performance for the SSPD compared to the SPAD one, as we exposed in the **Performance Analysis and Results** (3.2).

In this work a comparison has been studied, presenting as reference model of the BB84 protocol using a single-photon source. The system's performance is evaluated by considering two different detectors, an SPAD and an SSPD. Since the ideal single-photon source has yet to be created, real implementations of the BB84 protocol use highly attenuated lasers where the photon distribution in each pulse follows a Poisson distribution. In this dramatic scenario, the PNS attack is fatal to key distribution security. As a solution to this problem, the decoy-state method emerges. The classic BB84 protocol has been modified by adding the decoy-state method, and an $\boldsymbol{\mu_{optimal}}$ has been evaluated for a specific application of the decoy state, the *vacuum+weak decoy* state. The gain performance is analyzed in detail by substituting the SPAD detector with the SSPD in both cases for a Single-Photon source and an Attenuated source.

In conclusion, for the system and parameters considered in this BT, the method to obtain the best performance of actual QKD systems based on the BB84 protocol is using a *vacuum+weak* decoy state with $\boldsymbol{\mu_{optimal}}$, with the lowest misalignment possible and introducing an SSPD at the receiver. The BT's original contribution relies on integrating this new SSPD and evaluating the performance using an $\boldsymbol{\mu_{optimal}}$ for the concrete application of the *vacuum+weak* decoy state in the BB84 protocol.

Despite the excellent performance of SSPDs, the more significant problem is the cost. While SPAD detectors can be purchased for around 10,000 Euros, the implementation cost of an SSPD typically is about 100,000 Euros. The higher cost of SSPDs is attributed to the cryogenic system and maintenance requirement. Nevertheless, SSPDs offer scalability as multiple SSPD detectors can be placed within the same cryogenic system, if the costs were reduced, they could be a competitive product widely used in the industry, significantly increasing the link range of QKD systems. With future investments, this technology could be developed to become economically viable.

Various initiatives are employing these technologies, such as the Beijing-Shanghai Backbone Network, a quantum communication link connecting Beijing and Shanghai.

Currently, the BB84 protocol with the decoy-state method is considered, in terms of cost, robustness, and reliability of the devices, the best solution for real implementation. Other protocols have emerged as an evolution of the BB84 protocol, such as what is known as Device-independent QKD, another theoretical model that ensures complete protection from Eve. From this scheme, other feasible models arise, such as Measurement Device Independent-QKD, which is being studied as a possible resolution to the endless war between Eve and the pair, Alice and Bob.

Trust in institutions has been diminishing in recent decades. Overexposure to any type of information is increasing scepticism in society, discrediting highly demanding and rigorous professional work. According to the Secretary-General of the United Nations (UN), António Guterres [58-59], the world is suffering from a "trust deficit disorder", leading people to lose faith in political insitutions. Not only that but the generalization of this diagnosis is reflected in the wave of denialist movements in all areas and senses.

This new chaos, which is becoming more noticeable, has particularly corrupted Information Systems, where constant news about hacks [60-61] generates doubt about the ability of organizations and institutions to protect information.

With the advancement of quantum computers and the issue of losing security in key distribution, the security of institutions, banks, government agencies, and the most critical infrastructure will be at risk. The potential breakdown of the fabric of this technological society will lead to insecurity that could result in violent conflicts caused by fear. The comparison made in this BT highlights the importance of developing this technology, which will protect institutions and justice through security, integrity, and transparency, matching with Objective 16 of the United Nations Sustainable Developing Goals (UN-SDGs) [62].

Regarding Objective 17 of the United Nations SDGs [63], in a European collaborative effort, the implementation of QKD in an international network is being investigated in the European project EURO QCI. The European Commission will work with the 27 EU member states and ESA (European Space Agency) to develop a large and secure quantum communications infrastructure covering the entire European Union, reinforcing the protection of European government institutions, their data centres, hospitals, and other critical facilities, becoming the cornerstone of the EU's Cybersecurity Strategy for the years ahead.

Bibliography

[1] Boyer, Timothy H. Thermodynamics of the harmonic oscillator: derivation of the Planck blackbody spectrum from pure thermodynamics. *European Journal of Physics*, 2019, vol. 40, no 2, p. 025101.

[2] Verdu, Sergio. Fifty years of Shannon theory. *IEEE Transactions on information theory*, 1998, vol. 44, no 6, p. 2057-2078.

[3] Shannon, Claude E. Communication theory of secrecy systems. *The Bell system technical journal*, 1949, vol. 28, no 4, p. 656-715.

[4] Smart, Nigel Paul, et al. Cryptography: an introduction. New York: McGraw-Hill, 2003.

[5] Vernam, Gilbert S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 1926, vol. 45, no 2, p. 109-115.

[6] Rijmenants, Dirk. One-time pad. p. 04-13.

[7] Diffie, Whitfield; Hellman, Martin E. New directions in cryptography. En *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*. 2022. p. 365-390.

[8] Adeniyi, Emmanuel A., et al. Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. *Information*, 2022, vol. 13, no 10, p. 442.

[9] Gaines, Helen F. *Cryptanalysis: A study of ciphers and their solution*. Courier Corporation, 2014.

[10] Sun, Li, et al. Approaching Shannon's One-Time Pad: Metrics, Architectures, and Enabling Technologies. *arXiv preprint arXiv:2303.06359*, 2023.

[11] Kahn, David. *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster, 1996.

[12] Borowski, Mariusz; Leśniewicz, Marek. Modern usage of "old" one-time pad. En *2012 Military Communications and Information Systems Conference (MCC)*. IEEE, 2012. p. 1-5.

[13] Aid, Matthew M. *The secret sentry: The untold history of the National Security Agency*. Bloomsbury Publishing USA, 2009.

[14] Griffiths, David J.; Schroeter, Darrell F. *Introduction to quantum mechanics*. Cambridge university press, 2018.

[15] Kumar, Ajay; Garhwal, Sunita. State-of-the-art survey of quantum cryptography. *Archives of Computational Methods in Engineering*, 2021, vol. 28, p. 3835.

[16] Young, Nicholas. *An introduction to Hilbert space*. Cambridge university press, 1988.

[17] The Quantum Insider, "Quantum Technology Investment Update, 2022 Review". https://thequantuminsider.com/2023/02/17/quantum-technology-2022-investment-update-key-trends-and-players. [Online]

[18] Acín, Antonio, et al. The European quantum technologies roadmap. *arXiv preprint arXiv:1712.03773*, 2017.

[19] Marqas, Ridwan B.; Almufti, Saman M.; Ihsan, Rasheed Rebar. Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. *Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture & Technology*, 2020, vol. 12, no 3, p. 3110-3116.

[20] Gibney, Elizabeth. Hello quantum world! Google publishes landmark quantum supremacy claim. *Nature*, 2019, vol. 574, no 7779, p. 461-463.

[21] Bhatia, Vaishali; RAMKUMAR, K. R. An efficient quantum computing technique for cracking RSA using Shor's algorithm. En *2020 IEEE 5th international conference on computing communication and automation (ICCCA)*. IEEE, 2020. p. 89-94.

[22] Bernstein, Daniel J.; Lange, Tanja. Post-quantum cryptography. *Nature*, 2017, vol. 549, no 7671, p. 188-194.

[23] Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. NTRU: A ring-based public key cryptosystem. En *International algorithmic number theory symposium*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998. p. 267-288.

[24] Mceliece, Robert J. A public-key cryptosystem based on algebraic. *Coding Thv*, 1978, vol. 4244, p. 114-116.

[25] Preneel, Bart. Cryptographic hash functions. *European Transactions on Telecommunications*, 1994, vol. 5, no 4, p. 431-448.

[26] Chen, Lily, et al. *Report on post-quantum cryptography*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.

[27] Yang, Ching-Nung; Kuo, Chen-Chin. Enhanced quantum key distribution protocols using BB84 and B92. 2002.

[28] Xu, Feihu, et al. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, 2014, vol. 21, no 3, p. 148-158.

[29] Sasaki, Masahide, et al. Field test of quantum key distribution in the Tokyo QKD Network. *Optics express*, 2011, vol. 19, no 11, p. 10387-10409.

[30] Bužek, Vladimir; Hillery, Mark. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 1996, vol. 54, no 3, p. 1844.

[31] Clerk, Aashish A., et al. Introduction to quantum noise, measurement, and amplification. *Reviews of Modern Physics*, 2010, vol. 82, no 2, p. 1155.

[32] Flórez, Jefferson, et al. A variable partially polarizing beam splitter. *Review of Scientific Instruments*, 2018, vol. 89, no 2.

[33] Jiang, Shuangfeng; SAFARI, Majid. High-speed free-space QKD in the presence of SPAD dead time. En *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2022. p. 457-462.

[34] Orange, "Orange and the quantum technologies for the security of data exchange", The Quantum Insider, Quantum Technology Investment Update, 2022 Review. https://thequantuminsider.com/2023/02/17/quantum-technology-2022-investment-update-key-trends-and-players. [Online]

[35] Moeller, Lothar. Nonlinear depolarization of light in optical communication fiber. *APL photonics*, 2020, vol. 5, no 5.

[36] Shor, Peter W.; Preskill, John. Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, 2000, vol. 85, no 2, p. 441.

[37] Marøy, Øystein, et al. Error estimation, error correction and verification in quantum key distribution. *IET Information Security*, 2014, vol. 8, no 5, p. 277-282.

[38] Bennett, Charles H.; BRASSARD, Gilles; ROBERT, Jean-Marc. Privacy amplification by public discussion. *SIAM journal on Computing*, 1988, vol. 17, no 2, p. 210-229.

[39] Garcia-Patron Sanchez, Raul. Quantum information with optical continuous variables: from Bell tests to key distribution. 2007, p.159-186.

[40] Lo, Hoi-Kwong; Curty, Marcos; Qi, Bing. Measurement-device-independent quantum key distribution. *Physical review letters*, 2012, vol. 108, no 13, p. 130503

[41] Kumar, Ajay; Garhwal, Sunita. State-of-the-art survey of quantum cryptography. *Archives of Computational Methods in Engineering*, 2021, vol. 28, p. 3834-3837.

[42] Liu, Wei-Tao, et al. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution. *Physical Review A*, 2011, vol. 83, no 4, p. 042326.

[43] Gisin, Nicolas, et al. Quantum cryptography. *Reviews of modern physics*, 2002, vol. 74, no 1, p. 156-158.

[44] Agarwal, G., Ou, Z. Leonard Mandel (1927–2001). *Nature* **410**, 538 (2001).

[45] Lütkenhaus, Norbert. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 2000, vol. 61, no 5, p. 052304.

[46] Huttner, Bruno, et al. Quantum cryptography with coherent states. *Physical Review A*, 1995, vol. 51, no 3, p. 1863.

[47] Hwang, Won-Young. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 2003, vol. 91, no 5, p. 057901.

[48] Lo, Hoi-Kwong. Quantum key distribution with vacua or dim pulses as decoy states. En *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* IEEE, 2004. p. 137.

[49] Ma, Lijun; Mink, Alan; Tang, Xiao. High speed quantum key distribution over optical fiber network system. *Journal of research of the National Institute of Standards and Technology*, 2009, vol. 114, no 3, p. 149.

[50] Gagliano, Alessandro. Impact of Raman effect on integrated quantum-classical communication systems. 2020.

[51] Jiang, Shuangfeng; Safari, Majid. High-speed free-space QKD in the presence of SPAD dead time. En *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2022. p. 457-462.

[52] European Commission, "Single-Photon detector for secure and superfast quantum communications". https://cordis.europa.eu/article/id/254146-singlephoton-detector-for-secure-and-superfast-quantum-communications [Online].

[53] GitHub Repository, "ThesisYohanQKD". https://github.com/YESGM/ThesisYohanQKD.

[54] Ma, Xiongfeng, et al. Practical decoy state for quantum key distribution. *Physical Review A*, 2005, vol. 72, no 1, p. 012326-(3-4)

[55] MA, Xiongfeng, et al. Practical decoy state for quantum key distribution. *Physical Review A*, 2005, vol. 72, no 1, p. (012326-(6-7)

[56] Diamanti, Eleni, et al. Practical challenges in quantum key distribution. *npj Quantum Information*, 2016, vol. 2, no 1, p. 1-12.

[57] Zavitsanos, Dimitris, et al. On the QKD integration in converged fiber/wireless topologies for secured, low-latency 5G/B5G fronthaul. *Applied Sciences*, 2020, vol. 10, no 15, p. 5193.

[58] Naciones Unidas, Noticias ONU." Mirada global historias humanas". https://news.un.org/es/story/2018/09/1442282

[59] Naciones Unidas, Noticias ONU," Mirada global historias humanas". https://news.un.org/es/story/2020/11/1484242

[60] The New York Times, "How the Global Spyware Industry Spiraled Out of Control". https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html

[61] Interpol, "aumento alarmante de los ciberataques durante la epidemia de COVID-19. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

[62] United Nations, "Goal 16: Promote just, peaceful and inclusive societies". https://www.un.org/sustainabledevelopment/peace-justice. [Online].

[63] United Nations, "Goal 17: Revitalize the global partnership for sustainable development". https://www.un.org/sustainabledevelopment/globalpartnerships. [Online].

Acronyms

QKD	Quantum Key Distribution
BB84	Bennett and Brassard 1984 protocol
BT	Bachelor's Thesis
SPAD	Single-Photon Avalanche Diode
SSPD	Superconducting Nanowire Single-Photon Detector
PQC	Post-Quantum Cryptography
OTP	One-Time Pad
RSA	Rivest-Shamir-Adleman
AES	Advanced Encryption Standard
PBS	Polarizing Beam Splitter
QBER	Quantum Bit Error Rate
PNS	Photon Number Splitting attack
SKR	Secure Key Rate
UN-SDG	United Nations Sustainable Development Goals
EURO-QCI	European Quantum Communication Infrastructure
ESA	European Space Agency