Alma Mater Studiorum · Università di Bologna

Scuola di Scienze
Dipartimento di Fisica e Astronomia
Corso di Laurea in Fisica

Advancements in Quantum Key Distribution: Achieving Secure Communication.

Relatore:
Prof.ssa Elisa Ercolessi

Presentata da:
Andrea Turci

Anno Accademico 2022/2023

Abstract

Questa tesi fornisce una panoramica sul funzionamento del sistema di Quantum Key Distribution, nel contesto della crittografia quantistica, come una delle prime implementazioni della meccanica quantistica attraverso protocolli specifici. In particolare, viene esaminato il modello BB84 che, tanto semplice quanto efficace, fornisce sicurezza incondizionata al problema della crittografia in condizioni tecnologiche ideali, grazie alle leggi infrangibili della meccanica quantistica - tra cui il Principio di Indeterminazione e il Teorema di No-Cloning quantistico. Queste premesse teoriche - come la creazione di singoli fotoni perfetti, rivelatori con un'efficienza del 100%, canali senza perdite - si traducono tutte in ostacoli nell'implementazione sperimentale del protocollo BB84 con le tecnologie attuali: vengono analizzati i problemi e le limitazioni che ne derivano, esaminando le potenziali vulnerabilitá di sicurezza, come gli attacchi PNS. Di conseguenza, con l'obiettivo di fornire una prova di sicurezza definitiva, la seguente tesi si propone di analizzare una possibile soluzione, il Decoy State Method, che fornisce simultaneamente sicurezza incondizionata ed elevate prestazioni. Per concludere, allo scopo di evidenziare la praticitá del modello, i concetti introdotti vengono applicati al caso Weak and Vacuum Decoy State, per il quale si ottiene una distanza massima per una comunicazione sicura di 140.55 km, leggermente inferiore a quella dell'Asymptotic Case del Decoy State.

Abstract

This thesis provides an overview of the workings of the Quantum Key Distribution system, in the context of quantum cryptography, as one of the first implementations of quantum mechanics through specific protocols. In particular, the BB84 model is explored, which, as simple as it is effective, provides the ultimate security to the encryption problem under ideal technological conditions, thanks to the unbreakable laws of quantum mechanics - including the Uncertainty Principle and the No-Cloning Theorem. These ideal assumptions - such as the la creation of perfect single-photons, 100% efficiency detector, channels without loss - all translate into obstacles in the experimental implementation of the BB84 protocol with current technologies: the problems and limitations involved are analyzed, examining the potential security vulnerabilities, like the PNS attacks. Consequently, with the goal of providing an ultimate security proof, the following thesis aims to analyze a possible solution, the Decoy State Method, which simultaneously provides unconditional security and strong performances. To conclude, with the purpose of highlighting the practicality of the model, the introduced concepts are applied to the Weak and Vacuum Decoy State case, for which a maximum distance for secure communication of 140.55km is obtained, slightly lower than the Asymptotic Case of the Decoy State.

Contents

Introduction

Cryptography, from ancient Greek κρυπτός "hidden, secret" and γραφειν "to write" is the scientific discipline of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it.
Historically, the *Caesar Cipher* encryption method is mentioned among the earliest attempts at cryptography. From simple and breakable models, over the centuries encryption protocols have become more sophisticated; one of the most notorious examples of cryptographic algorithms was developed by the Germans in World War II, and broken by Alan Turing's Enigma machine.
The role of cryptography as a point of contact between scientific, social and political disciplines began to emerge. With the advent of computers and communication networks in the 20th century, this synergy was strengthened, and attempts to create effective encryption methods that corresponded to the new requirements led to the development of the RSA model in the 1970s (named after the inventors: Rivest, Shamir and Adleman). Basing its safety on the problem of factoring large prime numbers, the RSA algorithm is a mathematically asymmetric protocol that has ensured security in modern cryptography for the past 50 years. Due to the computationally challenging mathematical issue, the safety of this method is strictly bond both with the calculation power of the eavesdropper computer and with the conviction that a more efficient and fast algorithm to solve the problem won't be developed. Hence, the RSA algorithm possesses points of weakness since it is breakable, in principle.
Quantum computing has recently been paid a lot of attention following the rapid development of new disruptive technologies based on the most powerful features and resources of quantum mechanics - such as quantum entanglement, teleportation, and the No-Cloning

Theorem. The forthcoming development of quantum computers constitutes a real threat to classical cryptography techniques, and the institutions are already aware of it: citing the U.S. National Security Agency "If realizable, a cryptographically relevant quantum computer would be capable of undermining the widely deployed public key algorithms". More specifically, the greatest threat comes from the Shor's algorithm. Based upon a classical algorithm with a quantum subprocedure, it would employ the quantum Fourier transform to factorize keys in a few minutes instead of billions of years with the present technology.

In 2012 it was estimated that a billion physical qubits would be needed to break RSA encryption, but in 2019 after further technological breakthroughs the estimate plummeted to only 20 million physical qubits. Looking at the state of IBM's quantum computers, only thousands of qubits are available nowadays but the trend appears to be exponential: as a consequence, this reduces the issue to a matter of when these two trends will intersect, involving the disruption of cryptographic systems in telecommunications networks, financial and health care systems as well as government and military ones.

The threats of quantum computers are not just limited to the near future, but are already relevant because of the *Store Now Decrypt Later* principle that makes the transition to quantum-resistant cryptography necessary.

One possible approach can be offered by the post-quantum cryptography, that would offer systems that are robust against already known quantum algorithm, thus creating only temporary solutions.

Therefore, the best currently known technique for executing quantum cryptography operations is the Quantum Key Distribution (QKD), performed through appropriate protocols, which is the main topic of the following study. By restoring security based on the basic principles of quantum mechanics and resulting from unbreakable laws of nature, such as the Uncertainty Principle and the No-Cloning Theorem, it provides the ultimate solution to the encryption issue.

In particular, this thesis focuses its analysis on the BB84 protocol, which, as simple as it is effective, was proposed in 1984 by Charles Bennett of IBM and Gilles Brassard of The University of Montréal, with particular emphasis on the technological issues and the in-field implementations. Taking into account the vulnerabilities that arise from the

practical implementations, such as PNS attacks, the Decoy State Method is analyzed as a possible solution to the above-mentioned problems, both from a security and performance perspective.
In particular, this thesis aims to examine the special case of the Weak and Vacuum Decoy State, comparing its key generation rate with that of the Asymptotic Case. The goal is to argue the reasons why the Decoy State is an excellent candidate to become the international standard in Quantum Cryptography.

The thesis is structured as follows. In Chapter 1 the profound principles that underlie quantum mechanics and information theory are explored, laying a solid foundation for the subsequent analysis. In Chapter 2, the functioning and classification of QKD protocols are examined. Chapter 3 is assigned to an analytical description of the workings of the BB84 protocol, while the classification of the eavesdropper strategies to hack the communication channel are analyzed in Chapter 4. Chapter 5 focuses on the practical implementations of the BB84 protocol leading to the limitations of its security, and the PNS attack is examined. To conclude, Chapter 6 examines the Decoy State Method applied to the BB84 protocol as a possible solution to the aforementioned problems, with special attention to its safety and its performances.

Chapter 1

Introduction to Quantum Mechanics and Information Theory

In this chapter, the profound principles that underlie quantum mechanics and information theory are explored, laying a solid foundation for the subsequent investigation into quantum cryptography and, in particular, the BB84 protocol.
Quantum mechanics, conceived in the early 20th century, revolutionized the comprehension of the microscopic world, defying classical intuitions and revealing a plethora of new phenomena.
Central to this framework are quantum bits, or qubits, which possess exceptional attributes, including superposition and entanglement. By delving into the nature of qubits, we aim to gain a deeper understanding of their behavior when subjected to measurements and the inherent uncertainty that Heisenberg's Uncertainty Principle captures. Moreover, the powerful framework of density matrices is explored, which provides a comprehensive formalism for characterizing the probabilistic nature and interrelationships of quantum states. Furthermore, the profound implications of the No-Cloning Theorem is investigated, a fundamental principle that prohibits the exact replication of arbitrary quantum states. This theorem assumes a pivotal role in establishing the security foundations of quantum cryptographic protocols.
After unveiling these concepts in a methodical manner, a detailed analysis of the BB84 protocol will be provided in the following chapters.

1.1 Qubit States

The concept of qubit is crucial to describe and explain quantum cryptography, since it represents the quantum extension of the basic unit to store and transmit information. It is described as a vector in the two-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$, superposition of a binary system made of two vectors, written in the Dirac notation

$$\begin{aligned} |0\rangle &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ |1\rangle &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{aligned} \tag{1.1}$$

which represent the orthonormal basis of $\mathcal{H}$, also called computational basis.
The qubit can exist in either a pure state or a mixed state.
A pure qubit is represented by a precise wave function in probabilistic sense as a superposition of the basis elements:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.2}$$

where α and β are two complex coefficients, called probability amplitudes. They satisfy the normalization condition $|\alpha|^2+|\beta|^2 = 1$, with $|\alpha|^2$ and $|\beta|^2$ representing the probability that a measure of ψ yields the value $|0\rangle$ and $|1\rangle$ respectively, according to the Born rule. Thanks to that, it is possible to write α and β using the Hopf coordinates:

$$\alpha = e^{i\delta}\cos\left(\frac{\theta}{2}\right) \tag{1.3}$$

$$\beta = e^{i(\delta+\varphi)}\sin\left(\frac{\theta}{2}\right) \tag{1.4}$$

where $\theta \in]0;\pi[$ and $\varphi \in]0;2\pi[$. In addition, since the factor $e^{i\delta}$ is shared, it does not affect measures of observables; thus the probability amplitudes become:

$$\alpha = \cos\left(\frac{\theta}{2}\right), \quad \beta = e^{i\varphi}\sin\left(\frac{\theta}{2}\right) \tag{1.5}$$

Therefore, $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ [1]. Then, each qubit is depicted as a point on the two-dimensional surface of the so-called Bloch sphere, or Poincaré sphere, shown

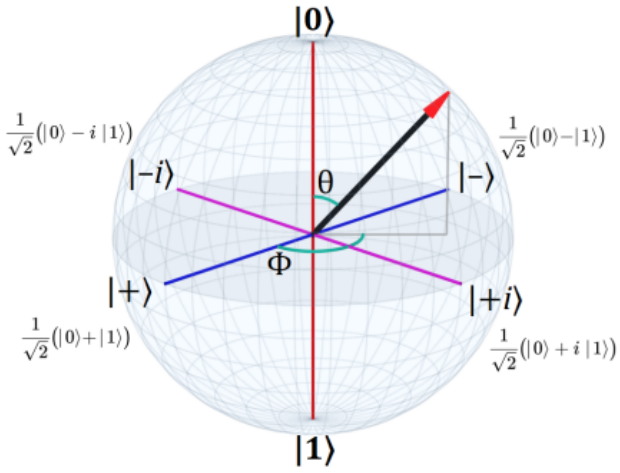

Figure 1.1: *Visual representation of the Bloch sphere with the qubit states* $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|+i\rangle$ *and* $|-i\rangle$. [2]

in Figure 1.1.

In particular, if the value $\theta = \pi/2$ is chosen, the vectors lying on the equatorial plane of the above-mentioned sphere are obtained; among those, four are of particular importance for many protocols of quantum cryptography, like the BB84 protocol which will be analysed in the following sections, that are achievable for appropriate choices of the θ angle [3]:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{if} \quad \varphi = 0 \tag{1.6}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \text{if} \quad \varphi = \pi \tag{1.7}$$

$$|+i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix} = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} \quad \text{if} \quad \varphi = \frac{\pi}{2} \tag{1.8}$$

$$|-i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix} = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \quad \text{if} \quad \varphi = \frac{3\pi}{2} \tag{1.9}$$

Using the Pauli formalism, it is necessary to introduce the following matrices:

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad , \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad , \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad , \tag{1.10}$$

and the two-dimensional identity matrix:

$$\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{1.11}$$

Thus, we have that $M_1 = \{|0\rangle, |1\rangle\}$ contains eigenstates of σ_z and it is called $\mathbb{Z}$ basis, or computational basis, $M_2 = \{|+\rangle, |-\rangle\}$ contains eigenstates σ_x and it is called $\mathbb{X}$ basis, or Hadamard basis, $M_3 = \{|+i\rangle, |-i\rangle\}$ contains eigenstates of σ_y and it is called $\mathbb{Y}$ basis. M_1, M_2 and M_3 are called mutually unbiased bases (MUB), because if a state is prepared in one of the bases M_i and it is later measured in a basis M_j with $i \neq j$, both the possible outcomes are predicted with the same probability [3].
Formally, given two MUB belonging to a $p-$dimensional Hilbert space $\{\varphi_1, \varphi_2, ..., \varphi_p\}$ and $\{\phi_1, \phi_2, ..., \phi_p\}$, the following result comes after [4, 5]:

$$|\langle \varphi_i | \phi_j \rangle|^2 = \frac{1}{p} \qquad \forall i, j \tag{1.12}$$

Our case of interest treats the easier situation of a two-dimensional Hilbert space with $p = 2$.
In the relevant case here treated, the photons constitute the physical support of quantum cryptography, in which information is carried by means of polarization of light that is represented by the qubit ψ of the physical system taken into consideration. In particular, the polarization of photons is described by two independent polarization states. For the linear vertical and horizontal states, the $\mathbb{Z}$ basis is used, with $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$, where H and V refer to the directions of the electromagnetic field oscillation. Vice versa, the vectors belonging to the $\mathbb{X}$ basis describe linear diagonal states, perpendicular to each other, $|+\rangle = |D\rangle$ and $|-\rangle = |A\rangle$. Finally, the vectors of the $\mathbb{Y}$ basis $|i\rangle$ and $|-i\rangle$ describe circular states, clockwise and anti-clockwise respectively: $|i\rangle = |R\rangle$ and $|-i\rangle = |L\rangle$ [3].
As previously stated, the security yielded from quantum cryptography is not guaranteed by the inability of the current computational power to break an algorithm, instead it is insured by physical principles which act at a quantum-mechanical level, given its

probabilistic and non-deterministic nature. Among those, the Heisenberg Uncertainty Principle and the No-Cloning Theorem, which will be analyzed in the following sections.

1.2 Measurements and Density Matrices

In a quantum cryptography protocol, the act of measurement is essential to exchange information between legitimate parties. It turns out that it is necessary to formalize the concept of measurement [1, 6].

Definition 1.2.1. Given $M_x : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, the measurement is defined as a set $\{M_x\}$ of operators, where the possible results are indexed by the variable $x \in \mathcal{X}$. These operators respect the so-called completeness relation:

$$\sum_{x \in \mathcal{X}} M_x^\dagger M_x = \mathbb{I} \tag{1.13}$$

Applying the measurement act to a system that lies in the pure state $|\psi\rangle$, the outcome $x \in \mathcal{X}$ is yielded with probability [1]

$$P^\psi(x) = \langle\psi|M_x^\dagger M_x|\psi\rangle\,. \tag{1.14}$$

Therefore, resulting from the measurement, the state is [7]:

$$|\psi_f\rangle = \frac{M_x\,|\psi\rangle}{\sqrt{\langle\psi|M_x^\dagger M_x|\psi\rangle}} \tag{1.15}$$

In quantum cryptography protocols, a useful example is considering the measurements operators standing for the measurement of a qubit in the $\mathbb{Z}$ basis, which has two possible results, 0 and 1:

$$M_0 = |0\rangle\langle 0| \qquad M_1 = |1\rangle\langle 1| \tag{1.16}$$

Considering the density matrix formalism, the explanation of measurements is straightforward to broaden.
Overall, we could not possess full understanding of the actual physical state but rather a collection of states, each of which has a particular likelihood of occurring. Let's take a quantum system that is defined by a statistical combination of state vectors

$|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_p\rangle \in \mathcal{H}$ that have probability to occur respectively of $p_1, p_2, ..., p_p$ satisfying the condition of $\sum_{i=1}^{p} p_i = 1$ with $p_i \geqslant 0 \quad \forall i \in \{1, ..., p\}$.
The whole ensemble $\{p_i; |\psi_i\rangle\}_{1,...,p}$ therefore describes the system's state, and the expectation value of $|\psi_i\rangle$ with probability p_i is interpreted as the equivalent density matrix of the system, which is:

$$\rho = \sum_{i=1}^{p} p_i |\psi_i\rangle \langle\psi_i| \tag{1.17}$$

Formally, the density matrix is defined as follows.

Definition 1.2.2. A density matrix ρ, also known as a density operator, is an operator on the Hilbert space $\mathcal{H}$ that meets the requirements listed below:

1. $Tr(\rho) = 1$, that means it is normalized;

2. $\rho^\dagger = \rho$, that means it is Hermitian;

3. $\langle\psi|\rho|\psi\rangle \geqslant 0, \ \forall |\psi\rangle \in \mathcal{H}$, that means it is positive semi-definite.

Each system is associated with one and only one density matrix, but each density matrix is not associated with one and only one quantum system.
Using the Pauli representation, it is possible to write the density operator as:

$$\rho = \frac{1}{2}\mathbb{I} + \bar{n} \cdot \bar{\sigma} \tag{1.18}$$

where $\bar{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}$ and $\bar{n}$ is a Bloch vector of unitary modulus for a pure qubit state. If the state taken into consideration is a pure state, then it's possible to claim to know the system exactly. In this case the summation of equation (1.17) collapses to a single term; in the case where $p_1 = 1$ and $p_i = 0 \quad \forall i \neq 1$, the density matrix is:

$$\rho = |\psi_1\rangle \langle\psi_1| \tag{1.19}$$

The ensemble is considered to exist in a mixed state if the summation contains many terms. In addition, the following theorem holds true as a necessary and sufficient condition for ρ to be a pure state.

Theorem 1.2.1. A density matrix represents a pure state if and only if

$$\rho^2 = \rho \tag{1.20}$$

which means it is idempotent.

Similarly, it is possible to differentiate between pure and mixed states using the definition of purity.

Definition 1.2.3. Given a density matrix ρ, the purity $\mathcal{P}(\rho)$ is defined as:

$$\mathcal{P}(\rho) = Tr\left(\rho^\dagger \rho\right) = Tr\left(\rho^2\right) \tag{1.21}$$

In this way, the purity of a pure state is $\mathcal{P}(\rho) = 1$, and the purity of a mixed state is $\mathcal{P}(\rho) \leqslant 1$.

Provided the set of operators $\{M_x\}$, we require to execute a measurement. Starting with an initial state $|\psi_i\rangle$, the outcome $x \in \mathcal{X}$ is yielded with probability

$$P^{\psi_i}(x) = \langle\psi_i|M_x^\dagger M_x|\psi_i\rangle = Tr\left(M_x^\dagger M_x |\psi_i\rangle \langle\psi_i|\right) = Tr\left(M_x^\dagger M_x \rho_{\psi_i}\right) \tag{1.22}$$

while examining the complete ensemble, the probability is

$$P^\rho(x) = \sum_i p_i P^{\psi_i}(x) = \sum_i p_i Tr\left(M_x^\dagger M_x |\psi_i\rangle \langle\psi_i|\right) = Tr\left(M_x^\dagger M_x \rho\right) \tag{1.23}$$

and the final state after the act of measurement is

$$\rho_f = \frac{M_x \rho M_x^\dagger}{Tr\left(M_x^\dagger M_x \rho\right)} \tag{1.24}$$

Making a distinction between quantum states through measurements is a significant issue in quantum information theory. It is always possible to design a projected measurement that permits us to differentiate between each state given a collection of orthogonal quantum states. Given a collection of orthonormal quantum states $\{|\psi_i\rangle\}$, the measurement operator M_i is defined to be

$$M_i = |\psi_i\rangle \langle\psi_i| \qquad \forall i \tag{1.25}$$

and one additional measurement operator

$$M_0 = \mathbb{I} - \sum_{i \neq 0} |\psi_i\rangle \langle\psi_i| \tag{1.26}$$

As well as the completeness relation, these operators follow the following property:

$$P^{\psi_i}(i) = \langle\psi_i|M_i|\psi_i\rangle = 1 \tag{1.27}$$

There is no quantum measurement that is capable of accurately determining the states in the case that they are not orthonormal. Therefore, treating a general case, the mathematical formalism of a positive operator-valued measure (POVM) turns out to be useful, including the fact that measurement outcomes are frequently what are of interest rather than the system's final state after the measurement [1]. A POVM is formally defined as follows [7, 8]:

Definition 1.2.4. Given a finite outcome collection $\mathcal{X}$, a positive operator-valued measure (POVM) is a set E of operators E_x, with $x \in \mathcal{X}$, which follow the relations

$$\forall x \in \mathcal{X} : E_x \geqslant 0, \quad \sum_{x \in \mathcal{X}} E_x = \mathbb{I} \tag{1.28}$$

Using a density-operator system ρ it is possible to recover the previous relations using the POVM definition:

$$P^{\rho}(x) = Tr(\rho E_x) \tag{1.29}$$

As an example, let's consider the case where the sender of the information, called Alice, can select between $|\psi_0\rangle = |0\rangle$ and $|\psi_1\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.
The POVM components are [1]:

$$E_0 = \frac{\sqrt{2}}{\sqrt{2}+1} |1\rangle \langle 1| \tag{1.30}$$

$$E_1 = \frac{\sqrt{2}}{\sqrt{2}+1} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \tag{1.31}$$

$$E_2 = \mathbb{I} - E_0 - E_1 \tag{1.32}$$

Thus, with three measures, we can create a POVM that sometimes differentiates the two states without ever incorrectly identifying either one. Indeed, if the measurement outcome is 0, the only possible measured state is $|\psi_1\rangle$, because $\langle\psi_0|E_0|\psi_0\rangle = 0$. Analogously, if the measurement outcome is 1, the only possible measured state is $|\psi_0\rangle$ because $\langle\psi_1|E_1|\psi_1\rangle = 0$. However, if the outcome is 2, it is not possible to gain information about the state since $\langle\psi_0|E_2|\psi_0\rangle = \langle\psi_1|E_2|\psi_1\rangle = \frac{1}{2}$.

1.3 Uncertainty Principle

Quantum cryptography is supported by the generalized Uncertainty Principle, for which the measurement of a quantum system leads the wave function that describes it to collapse, and disturbs the system, implying the impossibility to gain total information about how the system before the measurement was.
In its broadest sense, Heisenberg's Uncertainty Principle refers to the measurement error (or variance) of so-called non-commuting variables [9].
It asserts that, given two observables represented by Hermitian operators $\hat{A}$ and $\hat{B}$,

$$\sigma_A^2 \sigma_B^2 \geqslant \left(\frac{1}{2i}\langle\left[\hat{A};\hat{B}\right]\rangle\right)^2 \tag{1.33}$$

where

$$\begin{cases} \langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle = Tr\left[\rho_\psi \hat{A}\right] \\ \sigma_A^2 = \langle(\hat{A} - \langle\hat{A}\rangle)\psi|(\hat{A} - \langle\hat{A}\rangle)\psi\rangle \\ \left[\hat{A};\hat{B}\right] = \hat{A}\hat{B} - \hat{B}\hat{A} \end{cases} \tag{1.34}$$

correspond respectively to the expectation value of the observable $\hat{A}$, the standard deviation of observable $\hat{A}$ and to the commutator between operators $\hat{A}$ and $\hat{B}$.
The importance in the subject matter of quantum cryptography is the following: the measurement of the photons polarization according to the M_i basis and according to the M_j basis with $i \neq j$ correspond to two non-commuting operators. This implies that measuring in M_i basis and later in M_j basis yields a different outcome, instead of executing the measurement in M_j basis only, since uncertainty on the "M_i basis polarization" is added.

Formally, the operators which correspond to the measurement of polarization in $\mathbb{Z}$ and $\mathbb{X}$ bases are respectively:

$$\hat{P}_{\mathbb{Z}} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{1.35}$$

$$\hat{P}_{\mathbb{X}} = |+\rangle\langle +| - |-\rangle\langle -| \tag{1.36}$$

In this way, $|0\rangle$ and $|1\rangle$ are eigenstates of the $\hat{P}_{\mathbb{Z}}$ operator, with eigenvalues $\lambda_{|0\rangle} = +1$ and $\lambda_{|1\rangle} = -1$, representing respectively the case of transmission and reflection of the photon. Analogously, $|+\rangle$ and $|-\rangle$ are eigenstates of the $\hat{P}_{\mathbb{X}}$ operator, with $\lambda_{|+\rangle} = +1$ and $\lambda_{|-\rangle} = -1$. If the $|1\rangle$ state were measured in the $\mathbb{X}$ basis, one would obtain:

$$\begin{aligned}\hat{P}_{\mathbb{X}} = &|+\rangle\langle +|1\rangle - |-\rangle\langle -|1\rangle = \frac{1}{\sqrt{2}}|+\rangle\langle +|+\rangle - \frac{1}{\sqrt{2}}|+\rangle\langle +|-\rangle \\ &-\frac{1}{\sqrt{2}}|-\rangle\langle -|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\langle -|-\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\end{aligned} \tag{1.37}$$

This shows the importance for the legitimate parties to use the same basis in the communication procedure in order to transmit a qubit deterministically.
As will be analysed later, coherent states are crucial in the analysis of practical real-life quantum key protocols. They are defined as particular quantum states of the harmonic oscillator that exhibit classical motion [10], and are given by the following expression:

$$|z\rangle = \sum_{n=0}^{\infty} |n\rangle \frac{z^n}{\sqrt{n!}} e^{-\frac{|z|^2}{2}} \qquad z \in \mathbb{C} \tag{1.38}$$

They saturate the levels of the Uncertainty Principle for the particle's measure of position and momentum, making the inequality in (1.33) an equality: $\Delta p_z \Delta q_z = \frac{\hbar}{2}$.

1.4 No-Cloning Theorem

Because of the "destructive" nature of quantum mechanics, the No-Cloning Theorem is of paramount importance in ensuring security of principle for quantum encryption protocols, as it guarantees the eavesdropper failure.
It asserts that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. Indeed, it is wanted a machine that takes as input a state $|\psi\rangle_A$ in the so-called *data* slot A, and copy it in the *target* slot B, where the initial pure state

$|X\rangle_B$ is prepared. The systems A and B share the same Hilbert space: $\mathcal{H} = \mathcal{H}_\mathcal{A} = \mathcal{H}_\mathcal{B}$. Hence, the copying machine starts out with the state

$$|\psi\rangle_A \otimes |X\rangle_B \tag{1.39}$$

and wants to end up with the state

$$|\psi\rangle_A \otimes |\psi\rangle_B \tag{1.40}$$

The quantum operator that acts on the composite system belonging to $\mathcal{H}\otimes\mathcal{H}$ is a unitary operator U; it affects the evolution of the system in the following way:

$$|\psi\rangle_A \otimes |X\rangle_B \xrightarrow{U} U\left(|\psi\rangle_A \otimes |X\rangle_B\right) = |\psi\rangle_A \otimes |\psi\rangle_B \tag{1.41}$$

Let's suppose that the states ψ_1 and ψ_2 are successfully cloned:

$$U\left(|\psi_1\rangle_A \otimes |X\rangle_B\right) = |\psi_1\rangle_A \otimes |\psi_1\rangle_B \tag{1.42}$$

$$U\left(|\psi_2\rangle_A \otimes |X\rangle_B\right) = |\psi_2\rangle_A \otimes |\psi_2\rangle_B \tag{1.43}$$

Given that unitary transformations preserve inner products, from the previous relations one gets:

$$\langle\psi_1|\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|^2 \tag{1.44}$$

that yields either $|\langle\psi_1|\psi_2\rangle| = 0$ or $|\langle\psi_1|\psi_2\rangle| = 1$, which means that either $|\psi_1\rangle$ and $|\psi_2\rangle$ are equal (just a phase difference) or they are orthonormal. We conclude that the machine is able to copy only orthonormal states and not general ones.
Thus, it is possible to clone eigenstates with the respect to a certain basis, such as $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = |1\rangle$ for $\mathbb{Z}$, but it is not possible to do so with nontrivial linear combinations. For example, in the physical case of our interest, it results in the impossibility of cloning $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ because they are not orthogonal to each other.
Moreover, this is the reason why the sender and receiver of the information must use the same basis to communicate, while an eavesdropper who does not know the bases used fails to clone the information.

1.5 Theory of Information Related Quantities

A fundamental concept for information theory, and thus for quantum cryptography, is the Shannon entropy.

Definition 1.5.1. Given a random variable X, which can have outcomes $X_1, X_2, ..., X_n$, with probabilities $p_1, p_2, ..., p_n$ respectively, the Shannon entropy for variable X is defined as [7]:

$$H(X) = X(p_1, p_2, ..., p_n) = -\sum_i p_i \log p_i \tag{1.45}$$

It can be seen that the Shannon entropy does not depend on the type of outcomes that the variable X can take, but on their output probabilities, and thus ultimately on the probability distribution $p_1, ..., p_n$. To better understand its meaning, the Shannon entropy measures the amount of information we typically learn when we discover the outcome value X_i of the variable X. The greater the probability p_i of obtaining the outcome X_i, without any other prior information about it, the less the information gained after the outcome occurs will be. Indeed, given a set of possible outcomes X_i, $i \in \{1, ..., n\}$ with probability p_i the definition of the corresponding information is $Q_i = -\log p_i$, measured in bits, and the Shannon entropy corresponds to the expectation value of Q [11]:

$$S = \langle Q \rangle = \sum_i Q_i p_i = -\sum_i p_i \log p_i \tag{1.46}$$

The Shannon entropy also quantifies the degree of uncertainty around X before we find its value, thanks to the knowledge of the probability distribution. The greater the probability p_i the less will be the uncertainty of the outcome X_i and vice versa.
These two ways of viewing entropy as mean information obtained and as uncertainty associated with an outcome overlap.
In cryptography, the random variable X to be considered often has only two possible outcomes, i.e. the 0 and 1 classical bits, or the $|0\rangle$ and $|1\rangle$ qubits. In this case it is possible to define the binary Shannon Entropy [1]:

Definition 1.5.2. The binary Shannon Entropy is defined as follows

$$H^{bin}(p) = -p \log p - (1-p) \log (1-p) \tag{1.47}$$

where p is the probability of the first outcome and $1-p$ of the second one.

The graph of $H^{bin}(p)$ is shown in Figure 1.2 where it can be seen that it has the maximum value for $p = 1/2$.

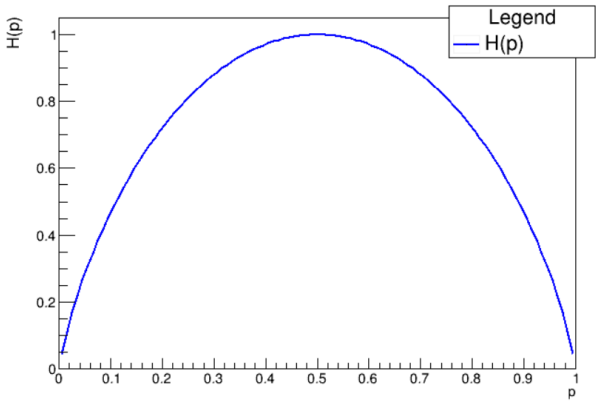

Figure 1.2: *Representation of the binary Shannon Entropy as a function of p.*

Definition 1.5.3. Given two random variables X and Y, the conditional entropy $H(X|Y)$ is defined as follows:

$$H(X|Y) = \sum_{x\in X}\sum_{y\in Y} P(x,y)\log\frac{1}{P(x|y)} = H(X,Y) - H(Y) \tag{1.48}$$

that is the entropy of a source X given the information of source Y.
$P(x,y)$ is the joint probability of X and Y while $P(x|y)$ the conditional probability of X given Y.

Definition 1.5.4. Given two random variables X and Y, the mutual information $I(X,Y)$ is defined as follows:

$$I(X,Y) = \sum_{x\in X}\sum_{y\in Y} P(x,y)\log\frac{P(x,y)}{P_1(y)P_2(y)} = H(X) - H(X|Y) \tag{1.49}$$

and it is a measure of the correlation between the two variables X and Y that follow the joint probability distribution $P(x,y)$.

1.6 Entanglement

At the heart of the differences between classical and quantum physics lies the concept of quantum entanglement. Concept existing only in quantum mechanics, it asserts that an entangled system is such that it cannot be expressed as a factorization of its elements: there are no individual separate components but an inseparable ensemble, causing what Einstein referred to as "spooky action at distance."
There are additional conceivable states in the composite Hilbert space besides product states, in particular states with interesting features that do not display such a product shape. Quantum correlations can be seen when two (or more) parties that are separated in space share the same quantum state. Entanglement is the term given to this phenomena.
Formally, the following definition of entanglement is provided:

Definition 1.6.1. If a pure bipartite state $|\psi\rangle_{AB}$ cannot be expressed as a product state $|\phi\rangle_A \otimes |\eta\rangle_B$ for every combination of states $|\phi\rangle_A$ and $|\eta\rangle_B$, it is said to be entangled. Otherwise, it is said to be separable.

In addition, we can give the definition of *maximally entangled states* as follows:

Definition 1.6.2. Given a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $dim(\mathcal{H}_A) = dim(\mathcal{H}_B) = d$ with orthonormal basis respectively $\{|j\rangle_A\}$ and $\{|j\rangle_B\}$, the maximally entangled system is

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |jj\rangle \tag{1.50}$$

To conclude, a useful theorem is provided in order to examine pure bipartite states.

Theorem 1.6.1 (Schmidt Decomposition)**.** Given $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, thus

$$|\psi\rangle = \sum_{j=1}^{d} \lambda_j |j\rangle_A |j\rangle_B \tag{1.51}$$

with $\{|j\rangle_A\}$ and $\{|j\rangle_B\}$ the orthonormal basis for the system A and B respectively. The amplitudes λ_j, that are strictly positive, real, satisfying $\sum_j \lambda_j^2 = 1$, are called Schmidt

coefficients. The Schmidt rank d corresponds to the number of λ_j and the following relation holds:

$$d \leqslant \min\{dim(\mathcal{H}_A), dim(\mathcal{H}_B)\} \tag{1.52}$$

An example of entangled state is given by the *Bell states*, that are four maximally entangled two-qubits Bell states, which create a maximally entangled basis (Bell basis) of the four-dimensional Hilbert space (two qubits). They are defined as follows:

$$\begin{aligned}
\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_A \otimes \left|0\right\rangle_B + \left|1\right\rangle_A \otimes \left|1\right\rangle_B\Big) \\
\left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_A \otimes \left|0\right\rangle_B - \left|1\right\rangle_A \otimes \left|1\right\rangle_B\Big) \\
\left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_A \otimes \left|1\right\rangle_B + \left|1\right\rangle_A \otimes \left|0\right\rangle_B\Big) \\
\left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_A \otimes \left|1\right\rangle_B - \left|1\right\rangle_A \otimes \left|0\right\rangle_B\Big)
\end{aligned} \tag{1.53}$$

The concept of quantum entanglement plays a crucial role in quantum cryptography, particularly in the implementation of entanglement-based protocols in quantum key distribution (QKD), enabling secure key distribution between two distant parties, as will be examined in further sections.

Chapter 2

Quantum Key Distribution

The quantum key distribution (QKD) process is the best currently known method for performing quantum cryptography operations, which is implemented through suitable protocols. The QKD offers the ultimate solution to the cryptography problem, in contrast to post-quantum cryptography that would offer systems that are robust against already known quantum algorithm. Indeed, since the latter would expose the information to undiscovered quantum algorithms, the QKD restores the security basing on fundamental laws of quantum mechanics and resulting from unbreakable principles of nature, like the above-mentioned Uncertainty Principle and No-Cloning Theorem [3].
Therefore, unlike classical cryptography, this key generating mechanism is demonstrably secure from every attack that an eavesdropper might launch.
Each QKD protocol aims to provide a shared secret key that can be used to encrypt and decrypt messages between two authorized parties which is known only to them by means of a public communication channel.
A quantum key distribution technique may generally be split into two distinct sections: the quantum transmission stage taking up the first section, in which Alice and Bob send and/or measure quantum states. The second stage is the classical post-processing phase, where two sets of safe keys are created from the bit strings produced in the quantum stage [1, 12].
The transmission of information by qubits according to QKD can take place in two different types of protocols, which differ in the properties they use. They are prepare-and-

measure protocols that require a quantum channel to transmit the information, which is then measured, and entanglement-based protocols, in which the legitimate parties obtain a pair of entangled qubits and extract the key by measuring their subsystems. It is possible to demonstrate [7] that each prepare-and-measure procedure corresponds to an entanglement-based method. Since entanglement-based protocols tend to be simpler to evaluate because they do not include quantum channels, this equivalence is very beneficial for security demonstrations.

2.1 Prepare-and-Measure Protocols

The legitimate parties, the sender (Alice) and the receiver (Bob), possess two communication channels available. The first is a quantum channel, in which the sender sends qubits (often polarized photons), after *preparing* them, to Bob, who then *measures* them. This quantum transmission is one-way, and there is no restriction whatsoever on the possibility that a third party (Eve) is performing eavesdropping of any kind.
The second communication channel is a classical authenticated channel [13, 14, 15], i.e. the internet or the telephone, in which classical information is exchanged. Authenticated means that the legitimate parties are sure that they are communicating with each other and not sending the information to a third party. In this channel Eve is only able to read the information, but not to retain or modify it in any way. This is a two-way channel, and information can flow from Alice to Bob and vice versa.

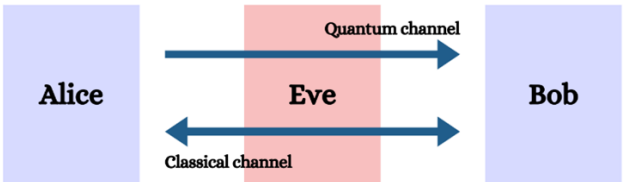

Figure 2.1: *Schematic of the operating principle in the Prepare-and-Measure protocols.*

Examples of prepare-and-measure protocols are the BB84 protocol, which will be analysed in more detail in the next sections, the Six-State protocol, a variant of BB84, and the SARG04 protocol.

2.2 Entanglement-Based Protocols

In this type of protocol, Alice and Bob receive qubits from an external source, which distributes a pair of entangled states between them. There are no limitations on where the source can be located: it can be at Alice's lab, or at Bob's lab, it can be a third party (Charlie), or even Eve. As a result, it is usual to designate the source as untrusted, taking the worst case in which Eve controls the source. Again, the legitimate parties share a classical authenticated channel in which to perform post-processing operations on the raw keys [7].

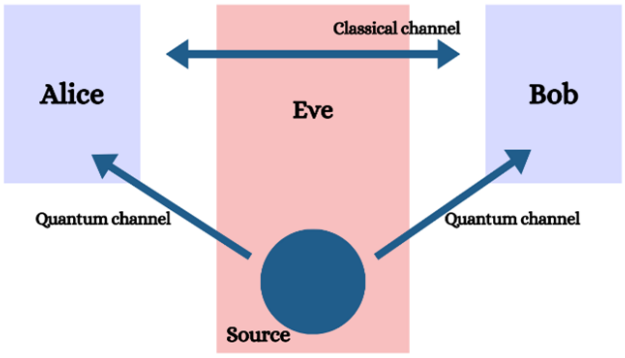

Figure 2.2: *Schematic of the operating principle in the Entanglement-Based protocols.*

It is possible to note that in this case Alice and Bob do not communicate via a quantum channel. This implies significant simplifications in that it makes entanglement-based protocols easier to analyse from a security perspective; it also makes attacks by Eve much more difficult to accomplish.
However, they possess significant practical limitations, such as the ability to realize

sources that prepare perfect entangled qubits with a sufficiently high rate, which prevent implementation in current quantum cryptosystems.
An example of entanglement-based protocols is the Ekert91 protocol.

2.3 Quantum Channel

The dynamics in a quantum cryptosystem take place within the so-called quantum channel, as introduced earlier. Mathematically we denote the quantum channel as $\mathcal{E}$, and it is an operator that maps states belonging to a Hilbert space $\mathcal{H}_\mathcal{A}$ to states belonging to a Hilbert space $\mathcal{H}_\mathcal{B}$. First, it is necessary to introduce some definitions to describe the quantum channel [7, 16]:

Definition 2.3.1 (Convex - Linearity)**.** A map $\mathcal{E} : \mathcal{B}(\mathcal{H}_\mathcal{A}) \to \mathcal{B}(\mathcal{H}_\mathcal{B})$ is convex-linear if the following condition is satisfied:

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i), \tag{2.1}$$

with $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$ Hilbert spaces, $\{\rho_i\} \in \mathcal{B}(\mathcal{H}_\mathcal{A})$ density operators.

Definition 2.3.2 (Complete Positivity)**.** A linear map $\mathcal{E} : \mathcal{B}(\mathcal{H}_\mathcal{A}) \to \mathcal{B}(\mathcal{H}_\mathcal{B})$ is said to be completely positive if the map

$$\mathcal{E} \otimes id_n : \mathcal{B}(\mathcal{H}_\mathcal{A}) \otimes \mathcal{B}(\mathbb{C}^n) \to \mathcal{B}(\mathcal{H}_\mathcal{B}) \otimes \mathcal{B}(\mathbb{C}^n) \tag{2.2}$$

is positive $\forall n \in \mathbb{N}$, where id_n represents the identity map in $\mathbb{C}^n$.

Definition 2.3.3 (Trace Preserving)**.** During the transmission in the quantum channel, the trace of the state must not change:

$$Tr\left(\rho_A\right) = Tr\left(\mathcal{E}(\rho_A)\right), \quad \rho_A \in \mathcal{B}(\mathcal{H}_\mathcal{A}) \tag{2.3}$$

This is a necessary condition in order to ensure that the quantum channel transforms density operators into density operators.

Given the three above-mentioned definitions, the quantum channel is defined as follows:

Definition 2.3.4 (Quantum Channel)**.** The quantum channel is defined as a map $\mathcal{E} : \mathcal{B}(\mathcal{H}_\mathcal{A}) \to \mathcal{B}(\mathcal{H}_\mathcal{B})$ that it is convex-linear, completely positive and trace-preserving.

It is important that the map is completely positive, and not simply positive. Taking as an example the following map applying the transpose operation on a single qubit state

$$\begin{aligned} \mathcal{T} : \rho \to & \rho^T \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \to & \begin{bmatrix} a & c \\ b & d \end{bmatrix} \end{aligned} \tag{2.4}$$

and considering as qubit the state

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.5}$$

the density operator is $\rho_{\Phi^+} = |\Phi^+\rangle \langle\Phi^+|$, and it yields:

$$\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{\mathcal{T}\otimes id} \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.6}$$

The eigenvalues of the final matrix include $\lambda = -1/2$, which implies that the matrix is not positive and therefore is not a good density operator [7].
Below the Choi-Kraus Theorem is stated, which allows the quantum channel to be described in terms of its Kraus decompositions. For a proof see [17].

Theorem 2.3.1. The Kraus decomposition of a map $\mathcal{E} : \mathcal{H}_\mathcal{A} \to \mathcal{H}_\mathcal{B}$ is

$$\mathcal{E}(\rho_A) = \sum_{j=1}^{d} K_j \rho_A K_j^\dagger \tag{2.7}$$

if and only if the map is linear, completely positive and trace preserving, where $\rho_A \in \mathcal{B}(\mathcal{H}_\mathcal{A})$, $K_j : \mathcal{H}_\mathcal{A} \to \mathcal{H}_\mathcal{B} \quad \forall j \in \{1, ..., d\}$ and

$$\sum_{j=1}^{d} K_j^\dagger K_j = \mathbb{I}_A \tag{2.8}$$

with $d < dim(\mathcal{H}_\mathcal{A}) \cdot dim(\mathcal{H}_\mathcal{B})$

If the system is closed, the quantum channel is defined by a unitary operator $U : \mathcal{H} \to \mathcal{H}$ with the property that:

$$\rho_f = U\rho_i U^\dagger = \mathcal{U}(\rho_i) \tag{2.9}$$

where ρ_f and ρ_i are respectively the final and initial state.
In this case, it is also possible to perform the reverse procedure by creating the reversed channel, via the adjoint map $\mathcal{U}^\dagger$:

$$(\mathcal{U}^\dagger \circ \mathcal{U})(\rho) = U^\dagger U \rho U^\dagger U = \rho \tag{2.10}$$

Chapter 3

BB84 Protocol

In this chapter the workings of the BB84 protocol are analysed, a pioneering method for secure key distribution in the realm of quantum cryptography. Proposed by Charles H. Bennett and Gilles Brassard in 1984, the BB84 protocol represents one of the most widely used protocols in QKD because it is easy to implement and guarantees security against eavesdropping proven on many occasions [18].
Through a meticulous exploration, it is provided a comprehensive understanding of the key components and operational principles of the protocol. By elucidating the steps involved in key generation, transmission, and reconciliation, the mechanisms that ensure secure communication between two parties is explored.
This opens the way to the insights of its strengths, limitations, and potential avenues for future advancements, that will be examined in later chapters in the thesis.

3.1 Description

Like any QKD protocol, the BB84 protocol can be divided into two stages; in the first "quantum" stage the sender (called Alice) and the receiver (Bob) use a quantum channel to exchange quantum states and thus create the raw encryption key, while in the second "classical" stage, through already existing information channels, they perform a classical post-processing operation on the sifted key and the actual exchange of information.

The BB84 protocol bases its working principle on the polarization of photons to com-

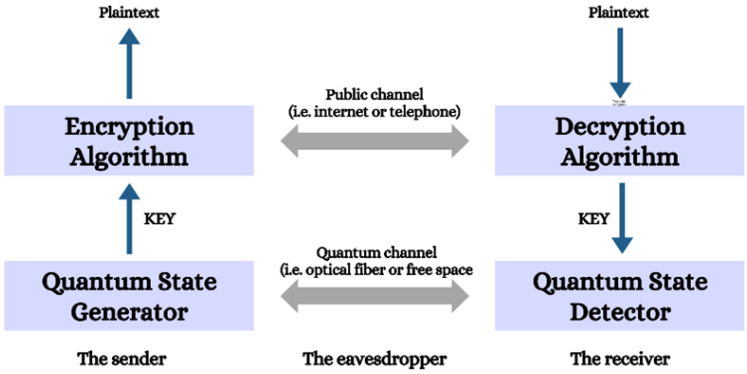

Figure 3.1: *Schematic of the operating principle in Quantum Key Distribution protocols.*

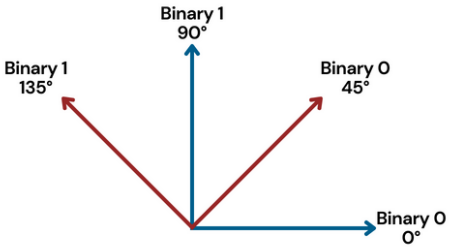

Figure 3.2: *Correspondence between the polarization of photons and binary meaning in the BB84 protocol.*

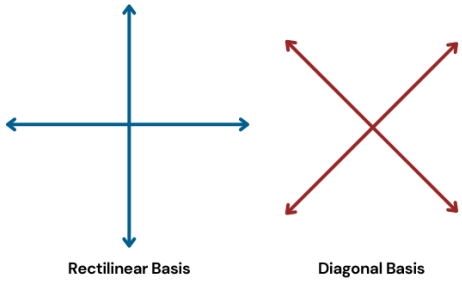

Figure 3.3: *Rectilinear and Diagonal bases used in the BB84 protocol.*

municate information, assuming that the emitted signal is composed of single photons; this is an assumption difficult to implement in practice, and in the next sections it will be analysed how to take into account the practical impossibility of obtaining single photon sources, arriving at the description of the Decoy State Method.
The quantum states used here are the qubits (1.1)(1.6)(1.7) of the $\mathbb{Z}$ and $\mathbb{X}$ bases [12], which in this case are denoted by rectilinear and diagonal bases, respectively. A graphical representation of the qubits is given in Figures 3.2 3.3 [19].

The classical bits 0 and 1 can be represented either in the rectilinear (+) or diagonal ($\times$) basis, according to the following convention:

	Basis +	**Basis ×**
Bit 0	0°	45°
Bit 1	90°	−45°

Table 3.1: *Convention used in order to communicate the binary message.*

3.2 Quantum Stage

The first "quantum" stage can be schematized as follows [12]:

Bit Generation. Alice randomly generates a series of bases (rectilinear or diagonal) and pairs it with equally long series of randomly generated classical bits (0 and 1).

Bit Preparation and Communication. Alice then prepares a series of photons, i.e. a string of qubits based on Table 3.1 and sends them to Bob through the quantum channel.

Bit Measurement. Similarly, Bob randomly extracts a similar string of × and + bases, and reads the qubits received in the selected basis. Since × and + are mutually unbiased bases, if the sender and the receiver used the same basis, and this happens statistically half the time, the qubit Bob receives is the same as the one Alice sent, assuming perfect calibration of the experimental apparatus. Therefore, Bob has 1/2 chance of reading the same bit sent by Alice and 1/2 chance of reading the opposite bit.
At this point the legitimate parties both have a string of bits k_A^{raw} and k_B^{raw} called raw quantum keys and which do not coincide in general.

The protocol is based on a fundamental principle: Alice and Bob's choice of bases is completely autonomous and unknown to any third party, such as a possible eavesdropper Eve, who tries to obtain the bit without being discovered using the most basic intercept-resend strategy in which she receives the information from Alice and sends it to Bob.

Indeed, an eavesdropper cannot perfectly replicate or measure the prepared states thanks to the non-orthogonality criterion. This is accurate because, according to the No-Cloning Theorem, she is unable to duplicate a particle with an unknown state. She cannot properly decode the information encoded by Alice since the $\times$ and $+$ bases are mutually unbiased, and her activity disturbs the quantum states in a way that can be seen by authorized users. Without knowing the basis used, statistically, half the time Eve chooses a different basis than Alice, and among those half of the time she measures the incorrect bit [20, 21].

3.3 Classical Stage

At this point the second "classical" stage begins, in which Alice and Bob communicate through a classical channel, and so Eve can only read the information, but not modify it or send her own to the sender. It can be schematized in the following way [12]:

Announcement. Alice and Bob communicate to each other the strings of $\times$ and $+$ bases used. It is important to emphasize that there is no exchange regarding the corresponding bits, sent by Alice or received by Bob. This occurs for the reasons mentioned above, being that only in the case where the legitimate parties have the same basis they are able to transmit bits to each other deterministically.

Key Extraction. At this point, from the strings k_A^{raw} and k_B^{raw} the sender and the receiver retain only those bits for which they have the same basis, eliminating the remainders. This process, called extraction, leads to the creation of two new bit strings k_A^{sifted} and k_B^{sifted}. They constitute the extracted keys, which should be identical in principle. However, there are two cases in which they may differ. The first concerns the presence of noise in the quantum transmission channel, which must be taken into account, and secondly, the presence of an eavesdropper, which, measuring in a different basis than Alice's can lead, for the reasons mentioned above, to changes in the bits measured by Bob. These are the two main sources of errors that lead to $k_A^{sifted} \neq k_B^{sifted}$, while we go on to neglect the presence of

absorption in the communication channel.

In a noiseless situation, the presence of an error would unequivocally indicate the presence of an observer. In this situation, clients have the option to terminate all ongoing communications, throw away the key, and start new ones. However, given the flaws in physical implementations, noise is always present in real-world situations. It is tempting to think that one can describe the problems in the physical channel and assume that any "extra" errors are caused by Eve. Alice and Bob would not be able to discern between legitimate errors (i.e. not attributable to Eve) and errors caused by her interference, assuming that Eve can actually replace the channel with one free of noise.

If the protocol were to be interrupted every time an error is detected, Alice and Bob would never be able to create a secure key. Therefore, the challenge is less about identifying an eavesdropper and more about determining how to derive a private key in the presence of an eavesdropper.

Using current technology, errors in sifted keys are about a few percent of the key length, realistically, as opposed to about 10^{-9} error rate in the current classical key distribution mechanism [15].

As a result, legitimate parties need to perform the processes of error correction and then privacy amplification on the keys, that will be described below.

Error Rate Estimation and Creation of Secret Keys. Let's consider $P(X, Y, Z)$ the joint probability distribution of three discrete random variables X, Y, Z of Alice, Bob and Eve respectively. The sender and the receiver only have access to $P(X, Y)$ and with this they want to place constraints on the information Eve possesses by going to place constraints on $P(X, Y, Z)$.

Knowing $P(X, Y, Z)$, there is no necessary and sufficient condition to have a secret-key rate $S(X : Y||Z) > 0$. However, it is possible to provide a lower bound on $S(X : Y||Z)$ in the following way, taking into account that if Eve knows about one random variable of the legitimate parties, then the secret-key rate must be higher [15, 22]:

$$S(X : Y||Z) \geqslant \max\Big\{I(X, Y) - I(X, Z); I(X, Y) - I(Y, Z)\Big\} \tag{3.1}$$

where $I(X, Y)$ is the mutual information between the variables X and Y. The limit of equality is reached when it comes to one-way communication, for example, from Alice to Bob. In two-way communication, a secret-key agreement can be reached even when the condition (3.1) is not satisfied, which means that Eve possesses more information than Bob. Verifying this condition is therefore necessary.
In order to establish a secret-key, Alice selects a subset of bits from the sifted key, and compare them with Bob using the public channel in order to get the error rate estimation. Then they discard those bits from the sifted key and verify whether the condition (3.1) is satisfied or not. In the first case they proceed to the next step, otherwise they abort the protocol.

Error Correction. To see the presence of errors, they usually take k_A^{sifted} as the reference. To detect and, consequently, correct errors present in k_B^{sifted} they apply error correction codes, which end with a procedure called "verification." Among the most commonly used error correction codes, worth mentioning are linear error correction codes, and in particular low-density parity-check codes (LDPC)[12]. At the end of this procedure legitimate parties obtain $k_A^{ver} = k_B^{ver}$ with a high level of probability.
A simple error correction protocol can be executed in the following way [15]; Alice and Bob choose same pairs of bits from the sifted keys and both announce their XOR value, i.e., their exclusive disjunction, which is an operator that is false if and only if its arguments are the same: see Table 3.2.

Bit 1	**Bit 2**	**XOR value Bit 1 $\oplus$ Bit 2**
1	1	0
1	0	1
0	1	1
0	0	0

Table 3.2: *Exclusive disjunction operation between two bits values.*

If Bob's XOR value matches Alice's XOR value, he announces "accepted," and they both keep the first bit of the pair and discard the second. If Bob's value does

not match Alice's one, he announces "rejected" and both bits are discarded. Eventually the legitimate parties keep sharing the same keys.

Recognition of the Eavesdropper Presence and Level of Eavesdropping. In error analysis, if the error rate obtained through the study of the communication channel exceeds a certain threshold level established a priori, the key extraction protocol is aborted, as errors are attributed not to the noise or channel loss but to the presence of an eavesdropper.

Privacy Amplification. Subsequent to error correction, Alice and Bob obtained an identical copy of the key. However, Eve may possess fractional information about them, and to avoid this scenario the privacy amplification technique is applied, so as to reduce the information gained by Eve by an arbitrary level.

To do this, the legitimate parties use functions that allow the mapping of data with arbitrary size to values with defined size, the so-called hash functions [12, 23], and they do this in the following way: Alice chooses a given hash function, and sends it to Bob via the classical channel. They both apply it to their extracted keys k_A^{ver} and k_B^{ver}, and obtain two keys of smaller but identical length, $k_A^{fin} = k_B^{fin}$, called final keys. With this procedure the eavesdropper has a lower level of gained information about the keys than before; in particular, this level can be made as small as desired. If Eve has a large amount of information about the sifted keys, the required privacy amplification process should make the final keys very short, so that Eve's level of gained information about the keys is greatly diminished, and vice versa.

Users calculate the required amount of Privacy Amplification based on the percentage of errors found in their experiment, or "quantum bit error rate" (QBER) which will be formally described in the later sections. Therefore, the hunt for the ultimate security proof simply entails finding the optimal plan of action Eve may use to obtain the maximum information gain, given the level of QBER observed.

Picking up on the use of XOR value seen earlier, a simple privacy amplification protocol might be the following: Alice chooses a pair of bits and computes their XOR value. Unlike before, Alice does not tell Bob the XOR value, but the position

of the bits on which she performed the procedure. Both of them, at this point, replace the pair of bits with their XOR value. In this way, the length of the key is decreased without the possibility of introducing errors, and consequently, Eve's knowledge about the key is decreased. In fact, if it has partial information about the bits, the information about their XOR values is even less. For example, if she knows the first bit but not the second one, she has no information about the XOR value. Otherwise, if Eve knows the value of both bits with 70% probability, she knows the XOR value with $0.7^2 + 0.3^2 = 58\%$ probability.

This last point ends the "classical" stage, and thus the BB84 protocol with the production of the encryption key.

3.4 Intercept-Resend Technique

Let us see how the eavesdropper is able to obtain information through the intercept-resend technique by introducing noise, and how the ideal situation in which the maximum possible information is obtained is Bob's.
Suppose that in the first quantum stage Alice sends a $|\psi\rangle$ state. Eve intercepts it and projects it along the state $|\theta\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ and onto the state orthogonal to it $\left|\theta^{\perp}\right\rangle$. At this point it is her intention to deduce the state $|\psi\rangle$ after the classical stage announcement, using Bayes' theorem [1, 24]:

$$P\big(|\psi\rangle \,|\, |\theta\rangle\big) = \frac{P\big(|\theta\rangle \,|\, |\psi\rangle\big) \cdot P\big(|\psi\rangle\big)}{\sum_j P\big(|\theta\rangle \,|\, |\psi_j\rangle\big) \cdot P\big(|\psi_j\rangle\big)} \tag{3.2}$$

However, after the announcement phase the possible values of $|\psi_j\rangle$ can be either $|\psi\rangle$ or $\left|\psi^{\perp}\right\rangle$, hence:

$$P\big(|\psi\rangle \,|\, |\theta\rangle\big) = \frac{P\big(|\theta\rangle \,|\, |\psi\rangle\big) \cdot P\big(|\psi\rangle\big)}{P\big(|\theta\rangle \,|\, |\psi\rangle\big) \cdot P\big(|\psi\rangle\big) + P\big(|\theta\rangle \,|\, |\psi^{\perp}\rangle\big) \cdot P\big(|\psi^{\perp}\rangle\big)} \tag{3.3}$$

For the reasons mentioned above, $P\big(|\psi\rangle\big) = P\big(\left|\psi^{\perp}\right\rangle\big) = 1/2$, and the expression becomes $P\big(|\psi\rangle \,|\, |\theta\rangle\big) = P\big(|\theta\rangle \,|\, |\psi\rangle\big)$.

In the special case where $|\psi\rangle = |1\rangle$, when Alice uses the $\mathbb{Z}$ basis,

$$\begin{aligned} P\big(|1\rangle \,|\, |\theta\rangle\big) = |\langle 1|\theta\rangle|^2 &= \left|\cos\left(\frac{\theta}{2}\right)\langle 1|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)\langle 1|1\rangle\right|^2 \\ &= \sin^2\left(\frac{\theta}{2}\right) \end{aligned} \tag{3.4}$$

On the other hand, if Alice uses the $\mathbb{X}$ basis, in the case where $|\psi\rangle = |+\rangle$, we have:

$$\begin{aligned} P\big(|+\rangle \,|\, |\theta\rangle\big) = |\langle +|\theta\rangle|^2 &= \left|\cos\left(\frac{\theta}{2}\right)\frac{1}{\sqrt{2}}\langle 0|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)\frac{1}{\sqrt{2}}\langle 1|1\rangle\right|^2 \\ &= \frac{1}{2} + \frac{\sin\theta\cos\phi}{2} \end{aligned} \tag{3.5}$$

Eve's uncertainty on Alice's encoding is measured by Shannon's entropy, depending on the basis used; thus, we have [3]:

$$H_{Eve}^{\mathbb{Z}} = -\cos^2\left(\frac{\theta}{2}\right)\cdot\log_2\left(\cos^2\left(\frac{\theta}{2}\right)\right) - \sin^2\left(\frac{\theta}{2}\right)\cdot\log_2\left(\sin^2\left(\frac{\theta}{2}\right)\right) \tag{3.6}$$

$$\begin{aligned} H_{Eve}^{\mathbb{X}} = &-\frac{1+\sin\theta\cos\phi}{2}\cdot\log_2\left(\frac{1+\sin\theta\cos\phi}{2}\right) \\ &-\frac{1-\sin\theta\cos\phi}{2}\cdot\log_2\left(\frac{1-\sin\theta\cos\phi}{2}\right) \end{aligned} \tag{3.7}$$

It is possible to see that if the eavesdropper uses $\theta = 0$ then $H_{Eve}^{\mathbb{Z}} = 0$, and the uncertainty in the measurement is minimized in the case where the sender uses $\mathbb{Z}$ basis; however, this induces a maximum value of $H_{Eve}^{\mathbb{X}}$, i.e. the case where Alice uses $\mathbb{X}$ basis. Decreasing the uncertainty for $H_{Eve}^{\mathbb{Z}}$ increases the uncertainty for $H_{Eve}^{\mathbb{X}}$, and vice versa. This agrees with the fact that $\mathbb{X}$ and $\mathbb{Z}$ are two mutually unbiased bases, in which, measuring in one basis, maximizing information gain maximizes the uncertainty for the complementary basis.

The only way to minimize both uncertainties for $H_{Eve}^{\mathbb{Z}}$ and $H_{Eve}^{\mathbb{X}}$ is to use two different bases for measuring the polarization of photons, which should match Alice's choices; one solution might be to randomly choose the bases and discard the events for which they do not match: this is exactly Bob's situation.

The legitimate parties exchange maximal information, while Eve has a gain information of 1/2. If the eavesdropper makes a measurement using $\mathbb{Z}$ basis, while Alice and Bob

use $\mathbb{X}$ basis, the probability that Eve records the same bit sent by Alice is 50%, and the probability that Bob receives the same bit as Eve is 50%. Consequently, the legitimate parties detect a 25% error in their keys. However, Eve can apply her strategy to a small number of bits sent by Alice, such as 10%. In this way Eve gets information of about 5%, but the error rate will be approximately 2.5% [3].
In addition, it is possible to consider the case where $\theta = \pi/4$, since we have $H^{\mathbb{Z}}_{Eve} = H^{\mathbb{X}}_{Eve}$. Assuming that the sender and the receiver use $\mathbb{Z}$ basis, then Eve projects Alice's qubit to $|\theta\rangle$ with probability $\cos^2(\pi/8)$ and to $\left|\theta^{\perp}\right\rangle$ with probability $\sin^2(\pi/8)$. In the former case Bob measures the erroneous qubit with probability $\sin^2(\pi/8)$, in the latter with probability $\cos^2(\pi/8)$. To conclude, the error rate is $2\cos^2(\pi/8)\sin^2(\pi/8) = 0.25$, as in the previous case.

In summary, from the physical point of view the BB84 protocol is based on 4 principles and ideal assumptions:

- The sources create perfect single photons;
- The channel has no loss, but there is noise present that disrupts the signal, and on which the eavesdropper relies to leak the information without being detected;
- Bob's (and therefore Eve's) detector has a detection efficiency of 100%.
- The alignment between the sender and the receiver is perfect. This implies that the rectilinear and diagonal bases are perfectly rotated at 45° to each other.

With these starting assumptions, several security proofs of the BB84 method have been formulated that ensure safety against eavesdropping. Among these, worth mentioning are the security proofs of Mayers, Biham et al., Ben-Or and Shor-Preskill.
However, these are unrealistic assumptions, and we will see how to account for a weakening of some of the starting assumptions by taking into account the state of current technology, so as to see how to arrive at a secure model of quantum cryptography that is at the same time also practical for the means at hand.

Chapter 4

Eavesdropping Strategies and Attacks Classification

Regarding certain quantum cryptosystems, the main goal of eavesdropping evaluation is to discover the most thorough and useful proofs of security. Since the eavesdropper employs not just the most advanced technology currently available, but also any hypothetical future technology, "ultimate proofs" ensure safety from all kinds of eavesdropping assaults.

After seeing the working principle of the intercept-and-resend technique performed by the eavesdropper to obtain information, we proceed by analyzing the more general case of an attack launched by Eve on the BB84 protocol. Similarly, it shows the close correlation between the level of information obtained from the attack and the disturbance of the physical system involved in the measurement.

In this section [7] is used as the main reference.

Formally, let's denote the qubit states (1.1)(1.6)(1.7) as follows:

$$\begin{aligned} |\psi_{00}\rangle &= |0\rangle \\ |\psi_{10}\rangle &= |1\rangle \\ |\psi_{01}\rangle = |+\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |\psi_{11}\rangle = |-\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{4.1}$$

An eavesdropper might evaluate about connecting an ancilla, $\mathcal{E}$, to Alice's qubit and causing them to interact in an effort to gather information. $\mathcal{E}$ represents a quantum system that could be bigger than a qubit in size. As this interaction is qubit state independent and abides by the laws of quantum mechanics, it may be characterized by applying a unitary operator U to the composite system.

Considering for hypothesis the case in which the eavesdropper performs the measurement of Alice's and Bob's states without introducing disturbance, we want to analyse which is the level of information possessed by Eve. To do this, let's consider the attack on two states that are not orthogonal, like $|\psi_{10}\rangle$ and $|\psi_{01}\rangle$; it yields [7]:

$$\begin{aligned} U\,|\psi_{10}\rangle\,|\mathcal{E}\rangle &= |\psi_{10}\rangle\,|\mathcal{E}_{\psi_{\mathbf{10}}}\rangle \\ U\,|\psi_{01}\rangle\,|\mathcal{E}\rangle &= |\psi_{01}\rangle\,|\mathcal{E}_{\psi_{\mathbf{01}}}\rangle \end{aligned} \tag{4.2}$$

where $|\mathcal{E}_{\psi_{\mathbf{10}}}\rangle$ and $|\mathcal{E}_{\psi_{\mathbf{01}}}\rangle$ represent the ancilla's state after the unitary operation on $|\psi_{10}\rangle$ and $|\psi_{01}\rangle$ respectively.

Since the unitary operator preserves the scalar product, multiplying the two relationships in (4.2) gives:

$$\langle\psi_{10}|\psi_{01}\rangle\,\langle\mathcal{E}|\mathcal{E}\rangle = \langle\psi_{10}|\psi_{01}\rangle\,\langle\mathcal{E}_{\mathbf{10}}|\mathcal{E}_{\mathbf{01}}\rangle \tag{4.3}$$

and since $\langle\mathcal{E}|\mathcal{E}\rangle = 1$, then $\langle\mathcal{E}_{\mathbf{10}}|\mathcal{E}_{\mathbf{01}}\rangle = 1$. This implies that $|\mathcal{E}_{\mathbf{10}}\rangle$ and $|\mathcal{E}_{\mathbf{01}}\rangle$ represent the same state, and consequently the eavesdropper did not get any information from Alice's states. In conclusion, if Eve does not disturb the system, she does not get any information.

Therefore, let's consider the case in which a disturbance is introduced into Alice's states after the eavesdropper attaches the ancilla:

$$\begin{aligned} U\,|\psi_{10}\rangle\,|\mathcal{E}\rangle &= |\psi'_{10}\rangle\,|\mathcal{E}_{\psi_{\mathbf{10}}}\rangle \\ U\,|\psi_{01}\rangle\,|\mathcal{E}\rangle &= |\psi'_{01}\rangle\,|\mathcal{E}_{\psi_{\mathbf{01}}}\rangle \end{aligned} \tag{4.4}$$

Hence:

$$\langle \psi_{10}|\psi_{01}\rangle = \langle \psi'_{10}|\psi'_{01}\rangle \langle \mathcal{E}_{\psi_{\mathbf{10}}}|\mathcal{E}_{\psi_{\mathbf{01}}}\rangle \tag{4.5}$$

Given a fixed value of $\langle \psi_{10}|\psi_{01}\rangle$, the smaller $\langle \mathcal{E}_{\psi_{\mathbf{10}}}|\mathcal{E}_{\psi_{\mathbf{01}}}\rangle$ is, the bigger $\langle \psi'_{10}|\psi'_{01}\rangle$ is, meaning that the states are more distinguishable, and vice versa. It implies that the more the eavesdropper gather information the bigger the disturbance will be, resulting to Eve's detection.

4.1 Attacks Classification

The types of attacks that the eavesdropper can perform are divided into three categories, in order of their power: individual attacks, collective attacks, and coherent attacks [15]. The first two categories include attacks in which Eve has a limited ability to act on qubits, conversely, it is assumed that in coherent attacks she has unlimited computational capacity, resources and technology, and thus is constrained only by the laws of quantum mechanics. Considering only the first two attacks can often be sufficient to give a simple security proof of the quantum cryptography protocol, however, coherent attacks must also be analyzed to outline a complete security proof. The eavesdropper possesses ideal technology; she is just constrained by the limitations of quantum mechanics and not in any way by existing technology. Eve is specifically prohibited from cloning qubits because doing so would violate the principles of quantum mechanics but she is allowed to employ a unitary interaction among qubits and an ancillary system she choices. Additionally, after the interaction, Eve can maintain her auxiliary system in total isolation from the outside world for an indefinite amount of time without being disturbed. She is able to make the measurement she chooses on her system after hearing the entire public exchange involving Alice and Bob, again being constrained solely by the principles of quantum physics.

In order to gain information, the eavesdropper generally execute the following steps: she attaches an ancillary system in the initial state $|\mathcal{E}\rangle_E \langle\mathcal{E}|$ to the state that the sender forwards, which is ρ_A. After performing the unitary operation on the composite system via the unitary operator U, the ancillary system is in the state:

$$\rho_E = Tr_A \left(U^\dagger \rho_A |\mathcal{E}\rangle_E \langle\mathcal{E}| U \right) \tag{4.6}$$

After that, the eavesdropper measures the ancillary system, which is given by a POMV $M = \{M_i\}$ where the outcome M_i of measuring a generic state ρ comes out with probability $P_i = Tr(M_i\rho)$.
Let's consider the case of individual attacks, in which Eve attaches individual probes to each qubit and performs a measurement to her probes one at the time. Alice sends n states, labelled $\rho_A^1, \rho_A^2, ..., \rho_A^n$ and Eve attaches the ancillary system $|\mathcal{E}\rangle_E \langle\mathcal{E}|$ to each ρ_A^i, $i \in \{1, ..., n\}$. She then performs the unitary operation via the unitary operator U, and after that, the ancillary state in this case is expressed as:

$$\rho_E^i = Tr_A \left(U^\dagger \rho_A^i \otimes |\mathcal{E}\rangle_E \langle\mathcal{E}| U\right) \tag{4.7}$$

for each state the sender forwards.
In collective attacks, the operating principle is similar, except that the eavesdropper collectively measures the states from Alice; however, she is only able to attach individual ancillary systems to the states. Even though the same unitary is utilized in each state, a global POVM provides the measurement, therefore ρ_E^i follows equation (4.7).
Regarding the coherent attacks, Eve attaches a single ancilla to the tensor product of Alice's states $\rho_A^1 \otimes \rho_A^2 \otimes ... \otimes \rho_A^n$. After that she applies a single unitary operator U_{tot} to the total system. Therefore, after this step, before the measurement, the ancilla is described by:

$$\rho_E = Tr_A \left[U_{tot}^\dagger \left(\rho_A^1 \otimes ... \otimes \rho_A^n\right) \otimes |\mathcal{E}\rangle_E \langle\mathcal{E}| U_{tot}\right] \tag{4.8}$$

Joint attacks, which are the most common coherent attacks, are based on the assumption that Eve attaches a single probe to each qubit, like in individual attacks, yet is capable of measuring multiple probes coherently, like in coherent attacks.

4.2 Individual Attacks

During individual attacks, or incoherent attacks, the eavesdropper attaches single qubit states individually in the same manner. The purpose is to describe analytically the amount of information obtained in this way, using the concepts of mutual information, introduced earlier, particularly between Alice and Eve.

With this type of strategy, the only degree of freedom is the unit operation via the U operator that is applied on the composite system. Considering the computational basis $M_1 = \{|0\rangle ; |1\rangle\}$ for Alice, then we have:

$$\begin{aligned} U|0\rangle|\mathcal{E}\rangle &= \sqrt{F}|0\rangle|\mathcal{E}_{\mathbf{00}}\rangle + \sqrt{1-F}|1\rangle|\mathcal{E}_{\mathbf{01}}\rangle \\ U|1\rangle|\mathcal{E}\rangle &= \sqrt{F}|1\rangle|\mathcal{E}_{\mathbf{11}}\rangle + \sqrt{1-F}|0\rangle|\mathcal{E}_{\mathbf{10}}\rangle \end{aligned} \tag{4.9}$$

where $|\mathcal{E}\rangle$ represents the initial state of the ancilla, and $|\mathcal{E}_{\mathbf{10}}\rangle$ $|\mathcal{E}_{\mathbf{00}}\rangle$ $|\mathcal{E}_{\mathbf{01}}\rangle$ $|\mathcal{E}_{\mathbf{11}}\rangle$ its possible final states. F is a coefficient, called *fidelity* that represents the probability that Bob, working in the same M_1 basis as Alice, will get the correct qubit, that is, the one actually sent to him; $1-F$ thus represents the probability of measuring the wrong qubit. Also, in this case, F coincides with the definition of fidelity between Alice's initial state, $|\psi_{in}\rangle$, and the final state that Bob obtains, ρ_B:

Definition 4.2.1. Given two quantum states $\sigma, \rho \in \mathcal{B}(\mathcal{H})$ the fidelity is defined as follows:

$$F(\sigma,\rho) = \left[Tr\left(\sqrt{\sigma^{\frac{1}{2}}\rho\sigma^{\frac{1}{2}}}\right)\right]^2 \tag{4.10}$$

In this case, the sender's state is a pure state, thus $\sigma = |\psi_{in}\rangle\langle\psi_{in}|$, and consequently the definition is simplified to:

$$\begin{aligned} F\left(|\psi_{in}\rangle, \rho\right) &= \left[Tr\left(\sqrt{|\psi_{in}\rangle\langle\psi_{in}|\rho|\psi_{in}\rangle\langle\psi_{in}|}\right)\right]^2 \\ &= \langle\psi_{in}|\rho|\psi_{in}\rangle\left(Tr\sqrt{|\psi_{in}\rangle\langle\psi_{in}|}\right)^2 \\ &= \langle\psi_{in}|\rho|\psi_{in}\rangle \end{aligned} \tag{4.11}$$

and if ρ is a pure state too, with $\rho = |\phi\rangle\langle\phi|$, hence $F(\sigma,\rho) = |\langle\phi|\psi_{in}\rangle|^2$.

For the BB84 protocol, it was shown [25] that the mutual information between Alice and Eve and between Alice and Bob is expressed in terms of the so-called *disturbance* $\mathcal{D} = 1 - F$, which is a measure of the unwanted changes or alterations that occur to a quantum system during its transmission in cryptographic protocols. Since the fidelity quantifies the similarity between the input state and the output state of a cryptographic operation, hence representing the probability of successfully transmitting or receiving the information without any undesired alterations, the disturbance represents the probability

of alterations occurring: a disturbance value of 1 implies that the quantum system has been completely disturbed or altered, while a disturbance value of 0 indicates no unwanted changes have occurred.
Studying the disturbance caused by an eavesdropper who attempts to gain information, it has been demonstrated in [25] that the mutual information between Alice and Eve and between Alice and Bob can be expressed in the following way:

$$I(A,E) = \frac{1}{2}\Big(1 + f\left(\mathcal{D}\right)\Big)\log\Big(1 + f\left(\mathcal{D}\right)\Big) + \frac{1}{2}\Big(1 - f\left(\mathcal{D}\right)\Big)\log\Big(1 - f\left(\mathcal{D}\right)\Big) \tag{4.12}$$

$$I(A,B) = 1 + \mathcal{D}\log\mathcal{D} + \Big(1 - \mathcal{D}\Big)\log\Big(1 - \mathcal{D}\Big) \tag{4.13}$$

where $f(\mathcal{D}) = 2\sqrt{\mathcal{D}(1-\mathcal{D})}$.
$I(A,E)$ and $I(A,B)$ are depicted in Figure 4.1. The sender and the receiver are able to extract information if and only if $I(A,B) > I(A,E)$, according to the Csiszar-Korner analysis [22] which asserts that when the legitimate parties have an edge against Eve with regard to of the shared information, they can derive the secret key. Hence, the quantity $I(A,B) - I(A,E)$ is expressed in function of $\mathcal{D}$ as shown in Figure 4.2, and when it becomes negative it is not possible for the legitimate parties to exchange information.
As a result, the mutual information functions from equations (4.12)(4.13) intersect at a particular error rate $\mathcal{D}_0$ [15]:

$$I(A,E) = I(A,B) \iff \mathcal{D} = \mathcal{D}_0 \simeq 14.6\% \tag{4.14}$$

Therefore, the BB84 protocol's safety requirement against individual attacks becomes:

$$\text{BB84 secure} \iff \mathcal{D} < \mathcal{D}_0 \simeq 14.6\% \tag{4.15}$$

4.3 Collective and Coherent Attacks

In the case of collective and coherent attacks, the proof on the conditions for the security of quantum cryptography protocols is much more complicated. This is especially true for coherent attacks in which the Hilbert space to be considered has a much larger dimension, since the eavesdropper interacts with the tensor product of the states sent

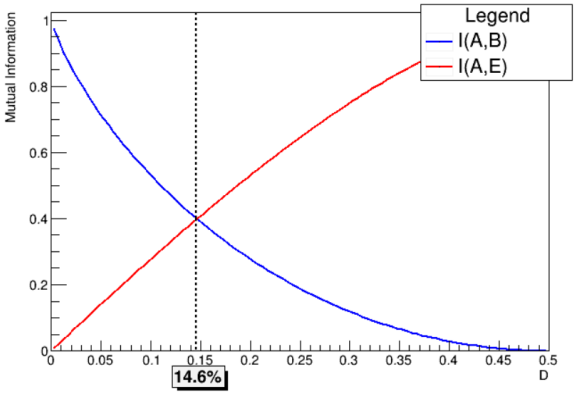

Figure 4.1: *Representation of the mutual information between Alice and Bob, and Alice and Eve. The threshold value is* $\mathcal{D} = 14.6\%$.

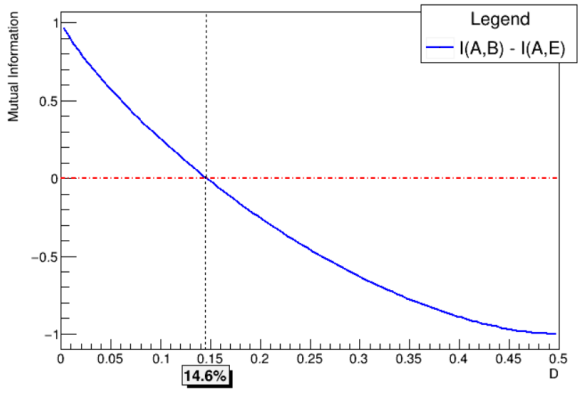

Figure 4.2: *Representation of the difference in mutual information* $I(A,B) - I(A,E)$. *It becomes negative when* $\mathcal{D} = 14.6\%$

by Alice: $\rho_A^1 \otimes \rho_A^2 \otimes ... \otimes \rho_A^n$.

Theorems delineating upper bounds on safe conditions, such as the quantum De Finetti theorem [26], are often used. For the BB84 protocol, the analysis against this kind of attack is provided in [27].

It was seen earlier that, considering *individual attacks*, the limit value for the disturbance corresponds to $\mathcal{D} = \mathcal{D}_0 \simeq 14.6\%$. However, reporting the analysis in [15] Eve might potentially handle numerous qubits coherently, thus we now consider *coherent attacks*. Dominic Mayers (1996b) provided the key concepts for demonstrating security in 1996. Afterwards, two significant publications were made available (Mayers, 1998; Lo and Chau, 1999). Due to the studies of Shor and Preskill (2000), Inamori et al. (2001), and Biham et al. (1999), these proofs are now widely recognized as correct.

The necessary requirement for the disturbance $\mathcal{D}$ is obtained as follows [15]:

$$\mathcal{D} \log \mathcal{D} + \Big(1 - \mathcal{D}\Big) \log\Big(1 - \mathcal{D}\Big) \leqslant \frac{1}{2} \tag{4.16}$$

that is satisfied for $\mathcal{D} = \mathcal{D}_0 \leqslant 11\%$.

After Shor and Preskill improved the demonstration for coherent attacks in 2000, the found threshold of $\mathcal{D}_0 \leqslant 11\%$ is exactly the one that Mayers' demonstration yielded in 1996, thus reinforcing the result obtained.

The aforementioned demonstration is only legitimate and appropriate if the key is significantly longer than the total amount of coherently attacked qubits, therefore the Shannon information employed constitutes averages over a large number of independent realizations of classical random variables [15]. This means that the legitimate parties are able to use the aforementioned demonstration to protect keys considerably longer than n_0 bits, providing Eve can coherently attack a huge yet finite number n_0 of qubits.

Chapter 5

Practical Implementations and Limitations

In this section, practical implementations of the BB84 model are analyzed. As previously seen, the analysis so far has been based on ideal assumptions, such as transmission of perfect single photons, no loss in the communication channel, 100% efficiency in the detectors, and perfect alignment of the experimental apparatus.
In the practice of the experiment, however, with a view to extending quantum communication to the commercial level, it is necessary to analyze the security of protocols with these limitations. It will be seen in the following paragraphs that in order to avoid security problems, the BB84 protocol can be implemented in the Decoy State Method, which provides in-principle security of communication.

5.1 Source: Coherent States

Despite the BB84 as described in the previous sections might be used with single photons, it has several practical drawbacks and limitations. Current systems rely on weak pulses of coherent states, with an average of much less than one photon per pulse, because they are difficult to obtain by experiments. This shows that the light generator uses a mixture of the so-called Fock states to emit photons exactly in the polarization required by the legitimate parties. Coherent states are defined as follows:

Definition 5.1.1. A coherent state, emitted by a practical source of light in a given polarization, is defined as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{j=0}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle \tag{5.1}$$

where $|j\rangle$, with $j \in \mathbb{N}$, is the so called *Fock-state* or number state, representing the state with a number of j photons, and $\alpha = |\alpha|e^{i\varphi}$ with $|\alpha|$ and φ called respectively *amplitude* and *phase* of the coherent pulse.

The parameter of the coherent state is $\alpha \in \mathbb{C}$, while the pulse *intensity* is defined to be $\mu = |\alpha|^2$, thus $\alpha = \sqrt{\mu}e^{i\varphi}$.
The method asks for a random phase shift of the coherent state for every pulse. This is done by either attaching an additional component to the sender's optical device that is connected to a generator of random numbers and modifies the phase (active randomization) or by using a laser mode of operation (passive randomization)[12]. Since the phase gets uniformly distributed, a pulse state is therefore described by the density matrix:

$$\begin{aligned} \rho_{Source} =& \frac{1}{2\pi} \int_0^{2\pi} \left||\alpha|e^{i\varphi}\right\rangle \left\langle|\alpha|e^{i\varphi}\right| d\varphi \\ =& \frac{1}{2\pi} \int_0^{2\pi} e^{-|\alpha|^2} \sum_{j,j'=0}^{\infty} \frac{|\alpha|^{j+j'}}{\sqrt{j!j'!}} e^{i\varphi(j-j')} |j\rangle \langle j'| \, d\varphi \\ =& \sum_{j=0}^{\infty} e^{-|\alpha|^2} \frac{|\alpha|^{2j}}{j!} |j\rangle \langle j| = \sum_{j=0}^{\infty} e^{-\mu} \frac{\mu^j}{j!} |j\rangle \langle j| \end{aligned} \tag{5.2}$$

As a result, the eavesdropper and the receiver measure a superposition of coherent states defined in equation (5.1).
Therefore, the state containing j photons is transmitted with a probability of [3]:

$$p_j = e^{-\mu} \frac{\mu^j}{j!} \tag{5.3}$$

Because of this, the variable μ that is the average photon number of the pulse follows the Poisson distribution. These pulses are known as weak coherent pulses since $\mu \ll 1$ is usually selected.
Considering that the laser closely follows the Poisson photon statistic, a weak laser pulse with $\mu \ll 1$ nevertheless possesses a probability of producing more than one photon in a

single pulse [28].
Usually, the average photon number of the Poisson distribution in a weak laser pulse is $\mu = 0.1$ [15]. The vast majority of the pulses in this scenario are vacuum signals. $P(0) = e^{-\mu} \simeq 90.5\%$ indicates the probability that zero photons will be transmitted. In addition, the probability that a single photon will be delivered is precisely $P(1) = \mu e^{-\mu} \simeq 9\%$, and the scenario in which multiple photons will be transmitted has a probability of $P(n > 1) = 1 - (1 + \mu)e^{-\mu} \simeq 0.5\%$ [7].
Thus, using a low value of μ to lower the probability of two or more photons being sent implies the drawback of having a high probability that the signal contains no photons.

5.2 Channel

Earlier it has been stated that the channel does not possess loss and that noise remains the only factor that can disturb the signal, allowing Eve to quietly leak data. It is important to remember that this is an ideal assumption and channel loss needs to be considered while using any QKD protocol.
The variable α, represented in dB/km, and the fiber characteristic length l, can be employed to determine the loss rate of the quantum channel in QKD protocols based on optical-fiber. The channel's transmittance, t_{AB}, is defined as follows [29]:

$$t_{AB} = 10^{-\frac{\alpha l}{10}} \tag{5.4}$$

In signal transmission, the choice of wavelength is crucial, and in general there are two possibilities. The first choice is a wavelength of about 800nm, which is the wavelength for which commercially available photon detectors are efficient; in this case the medium for communication must be either free-space or a special type of optical fiber, which, however, is not the one used in today's telecommunications optical fibers.
The second choice is a wavelength between 1300nm and 1550nm, as it is compatible with existing and already used optical fibers. However, in this case there would be a need to develop new detectors sensitive to this type of wavelength, as silicon semiconductors are transparent to signals above 1000nm.

Taking the above into account, let's analyze the absorption of the fibers in the two cases. With wavelengths of 1300nm and 1550nm, the attenuation is 0.35dB/km and 0.20dB/km, respectively, so there is a 50% loss of signal after 9km and 15km; on the other hand, with wavelengths of 800nm, the channel loss is 2 dB/km, so 50% attenuation after just 1.5 km.
In optical fibers, channel loss as a function of signal wavelength is depicted in Figure 5.1, [15].

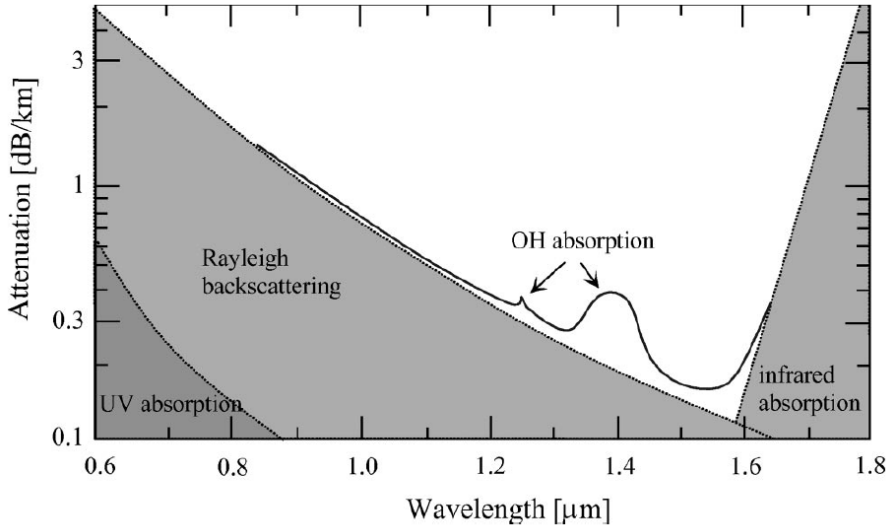

Figure 5.1: *Representation of the channel loss expressed in dB/km as a function of the signal wavelength, for optical fibers (Gisin et al., 2002, pp. 158).*

Choosing free-space as a communication channel implies the use of 800nm wavelength, which coincides with the region of the spectrum where absorption is low; however, it must be taken into account that in free-space it is necessary to always have air-line connections.

5.3 Detector

The detector, which is the final element in the transmission process, is flawed as well. It demonstrates that the detection efficiency of Bob's (and consequently Eve's) detector

is below 100%.
Taking the variable η_B denoting the transmittance in Bob's side, considering the transmittance of the optical components t_B and the efficiency of the detector η_D [29],

$$\eta_B = t_B \eta_D \tag{5.5}$$

Therefore, the overall transmission and detection efficiency η between Alice and Bob is determined by

$$\eta = t_{AB} \eta_B \tag{5.6}$$

The idea of a threshold detector in the receiver's component is quite common. Bob's sensor is consequently assumed to be able to tell the difference between a vacuum and a non-vacuum scenario. It is hard to figure out the specific number of photons in the pulse in the case it contains more than one photon.
It is plausible to suppose that the actions of the i photons in $i-$photon states are independent of one another. In regard to a threshold detector, the transmittance associated with the $i-$photon state η_i thus gets provided by [30]

$$\eta_i = 1 - (1 - \eta)^i, \quad \text{for} \quad i = 0, 1, 2... \tag{5.7}$$

In addition, detector efficiency induces the possibility of so-called dark-counts: Bob detects photons in the signal even though it does not contain them. It has been seen above how with $\mu = 0.1$ the probability that the signal does not contain photons is $P(0) \simeq 90.5\%$; therefore, the effect of an efficiency $\eta \neq 1$ has a great impact on the key production and signal transmission, and must be taken into account in the discussion.

5.4 Photon-Number-Splitting Attack (PNS)

Let's consider the BB84 protocol with weak coherent pulses source instead of perfect single-photons signals. The case in which single photons are transmitted in the communication channel is brought back to the case of the ideal BB84 protocol, and thus does not lead to any problems; on the other hand, the case of no photons being sent only

results in a decrease in the signal rate, since Eve cannot obviously obtain useful information if no photons are sent. The problematic situation arises in the case where multiple photons are transmitted, and, if there is loss in the transmission channel as in practical implementations, Eve is capable of performing the so-called Photons-Number-Splitting (PNS) attacks against the BB84 protocol under those realistic conditions.
If the sender sends weak coherent state with Poisson distribution parameter μ and the communication channel possesses a transmittance η, then the receiver will observe signals with photons distributed according to the Poisson statistic with parameter $\mu \cdot \eta$, under the assumption that both μ and η are known. Thus, the probability of observing a non-vacuum signal with at least one photon inside is equal to $P_{non-vac} = 1 - e^{-\mu \cdot \eta}$.
The eavesdropper must extract information from the signal sent by Alice, but at the same time it must ensure that Bob receives coherent states with the same expectation value of getting non-vacuum signals: if Bob receives non-vacuum signals with a fraction different from the expected one, Eve will be detected.
In order to provide an ultimate security proof for cryptographic protocols, highlighting all possible future critical issues arising from technological advancement, let's consider the case where the eavesdropper has unlimited technological capabilities (such as the ability to perform quantum non-demolition measurements or store photons in a quantum memory) and is limited only by the laws of quantum mechanics.
After establishing Eve's inability to copy photons received from Alice due to the No-Cloning Theorem, Eve can only retain photons, with the consequence that Bob will observe signals with decreased parameter μ. If $\mu \cdot \eta$ needs to remain constant, Eve replaces the communication channel with an ideal one with zero loss, or at least with a more efficient one.
Afterwards it performs the so-called quantum non-demolition measurements on the signals coming from Alice, so it is able to count the number of photons within a signal without disturbing their polarization. At this point, Eve acts differently depending on the number of photons present within each signal [7]:

- The vacuum states are transmitted to Bob without being retained, since Eve is unable to extract information from them.

- If she receives multi-photon signals, she retains one photon and transmits the

remaining ones to Bob through the channel without altering their polarization. However, Eve does not immediately measure the polarization of the photon she kept, but waits for the moment in the protocol in which Alice reveals to Bob the bases used through the public channel. In this way she is able to perform the correct measurement and extract information. In this step, it is assumed that the eavesdropper has such a technology that it can store photons in a quantum memory.

- From the signals that contain a single photon, Eve blocks a portion of them so as to ensure that Bob gets detection events with the probability he expects: $P_{non-vac} = 1 - e^{-\mu \cdot \eta}$. Instead, the remaining ones are retained by Eve, on which she performs any kind of attack to extract information.

  The quantity of losses rises as a consequence of the eavesdropper stopping certain pulses, which may be seen by the rightful parties. In order to replicate the amount of loss that occurs naturally, it is thus assumed that the eavesdropper is able to substitute the communication channel and the sensors with ideal ones in order to stop the maximum number of single-photon signals as feasible. The greater number of single-photon pulses Eve can block, the greater the degree of intrinsic losses will be. The eavesdropper would acquire complete knowledge of the information without adding noise in the event the channel's intrinsic losses were so great that she could stop all single-photon states from occurring [12]. This is because all the pulses that arrive to Bob would be multi-photon pulses.

A schematic representation of this attack is depicted in Figure 5.2.

Thus, under the assumptions of realistic implementation of the BB84 protocol, the eavesdropper is able to obtain information without introducing perturbation and satisfying the expectation values of the sender, which instead attributes the channel loss effect to the transmittance.

Recent years have seen an increase in interest in quantum nondemolition attacks. The issue is still open to debate. It is a common idea to believe that assuming an eavesdropper capacity of performing optimal quantum nondemolition attacks may be unreasonable or perhaps unphysical. She actually has to be able to measure the photon numbers in quantum nondemolition first. This is a valid hypothesis even if it is unattainable with

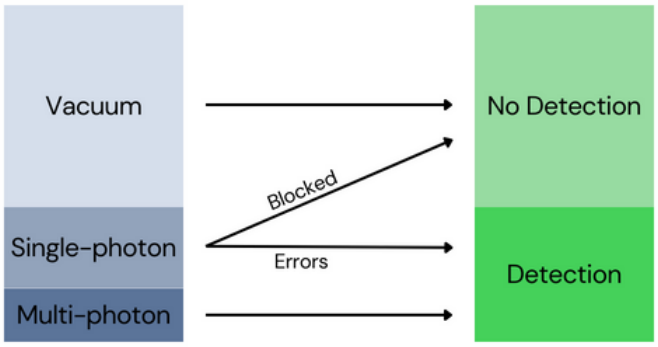

Figure 5.2: *Schematic of Eve's behaviour according to the number of photons present within each signal coming from Alice.*

current techniques [31]. Afterward, she has to hold the photon as long as the legitimate parties declare the basis used in the communication. In theory, a loop with an ideal and lossless channel might accomplish this [15]. The eavesdropper might also be able to associate the photon with a quantum memory.

Although a quantum memory doesn't exist at the moment, it may well be available at a later time. Knowing that the legitimate parties might potentially wait for minutes before revealing the bases, it should be noted that the quantum memory requires basically infinite decoherence time. Furthermore, the eavesdropper has to connect to a channel that is lossless, or with smaller losses than the channel employed by the legitimate parties. The most difficult part could be that.

The technical capabilities of communications fibers have already been reached. Rayleigh scattering, that is inevitable when the Schrödinger equation is solved in an inhomogeneous material, is the primary cause of the loss [15].

Ideal lossless fibers are challenging to envision if the discrepancies are brought on by the medium's molecular structure. The minimum value of 0.18 dB/km in silica fibers with a wavelenght of 1550 nm is determined more by physics than by technology. The attenuation at telecommunications wavelengths is fairly significant, therefore using air is not a practical approach. Because of diffraction, another necessary physical phenomenon, vac-

uum, the only environment in which Rayleigh scattering cannot occur, has constraints as well. The eavesdropper appears to have just two options remaining at this point. She can either employ teleport or change the photons' wavelength without disturbing the qubit. These two approaches seem unlikely to be implemented in the near future.
However, in an ultimate security proof the realistic implementation of the BB84 method is not secure since vulnerable to PNS attacks; a possible solution to that problem could be found in the Decoy State Method, described in the following section.

Chapter 6

Decoy State Method

Since it is necessary to take into account the vulnerabilities that arise from practical implementations of Quantum Key Distribution protocols such as BB84, arising from the use of coherent source of light and loss in the communication channels, it is required to ask whether they can be remedied by effective countermeasures to counter possible actions of eavesdroppers.
The solution to the weaknesses brought by Photon-Number-Splitting attacks performed by Eve, for the BB84 protocol, is provided by the Decoy State Method, which is analyzed in this section.
As will be pointed out later, implementing the Decoy State Method on a protocol such as the BB84 with coherent source of light is easy in terms of technology [7, 30]; moreover, the Decoy State Method guarantees excellent performances from the point of view of the communication transmission, obtaining estimates on the maximal secure distance for communication that exceeds the best values reported in the literature for protocols, such as BB84, *without* the Decoy State.
Consequently, since the Decoy State BB84 QKD protocol has been examined in detail both from a theoretical [32, 33, 34] and a practical [35, 36] point of view, including Russian internal systems [37], considering its high level of security and the possibility of having a very high key generation rate at large distances, it is an excellent candidate to become the protocol implemented in commercial applications as an international standard.

The references [30] and [29] are used in this section.

6.1 Model Description and Security

The main idea behind the Decoy State Method is that Alice does not send coherent states of light with the same parameter μ of the Poissonian distribution, but instead sends pulses in two different coherent states: the signal states, which are the conventional BB84 protocol states, and the decoy states.
These two types of states must necessarily have the same spatial and temporal characteristics, such as wavelength and time information, so that they are indistinguishable to a hypothetical eavesdropper. Their difference lies in the corresponding parameters of the Poisson statistic: denoted by μ_S and μ_D the average number of photons per pulse of the signal state and decoy state respectively, they are chosen so that $\mu_S \ll \mu_D$.
The signal states are used for the unique purpose of creating the encryption key in the QKD, while the decoy states are used for the unique purpose of detecting eavesdropping attacks.
Alice randomly sends decoy states to Bob among signal states with a probability α. The eavesdropper is only able to distinguish pulses based on the number of photons they contain; therefore, since it is unable to differentiate decoys from signal states, it performs the attack strategy described in the previous paragraph (PNS attack) by treating the signals it receives equally, and in particular by treating signal and decoy states that possess the same number of photons equally.
However, only after Bob has received the signals Alice declare the position of the decoy and signal states in the announcement phase in the classical stage of the BB84 protocol. At this point, legitimate parties are able to evaluate the variables that characterize the communication channel, such as the signal gain and quantum bit error rate (QBER), which will be better defined in the next section. In the case of an attack from an eavesdropper, the values of these quantities deviate from their expectation value; in particular, since $\mu_S \ll \mu_D$, in the case of a PNS attack Bob would discover a significantly bigger loss than expected in the signal states, as a result of Eve's attempt to preserve the incorrect

percentage of detection and no detection events.
With the intent of providing a better mathematical description of the Decoy State Method, it is necessary to introduce some variables to describe the signals and the communication channel in the absence of an eavesdropper [30, 29].

Yield. The yield Y_n of the $n-$photon state is defined as the conditional probability that Bob's detector has a detection event if Alice sends an $n-$photon state.
Consider the yield Y_n for a realistic setup, differentiating the cases according to the value of n.

$n = 0$. In this case, the probability that Bob has a detection event with 0 photons sent by Alice is denoted by Y_0, and is given by the probability p_{dark}, i.e. the background rate due to background contribution and background noise: $Y_0 = p_{dark}$, and therefore it is such that $Y_0 \geqslant 0$.

$n \geqslant 1$. The probability of having a detection event for an $n-$photon state can be caused either by a background event p_{dark} or by an actual reception of the $n-$photon state signal, the rate of which is provided by η_n, defined in equation (5.7).
Thus, we have:

$$Y_n = \eta_n + p_{dark} - \eta_n \cdot p_{dark} \simeq \eta_n + p_{dark} \tag{6.1}$$

where the last approximation is justified by the fact that $\eta_n \cdot p_{dark}$ is an infinitesimal of lower order, being η_n on the order of 10^{-3}, and p_{dark} on the order of 10^{-5} [29].
Moreover, it allows us to perform another approximation: taking the definition of the overall transmission efficiency from equation (5.7), we have that $\eta_n \simeq n \cdot \eta$, and consequently, since $\eta_n \gg p_{dark}$ we have

$$Y_n \simeq \eta_n \simeq n \cdot \eta \tag{6.2}$$

Gain. The gain is a variable that quantifies the transmission efficiency of coherent states used in quantum key distribution protocols, and it plays a key role in determining the quality of the encryption key that is generated: high values of the gain

correspond to high communication efficiency, thus high key quality that allows information to be transmitted over large distances.

The gain of an $n-$photon coherent state is defined as the product of Alice's probability of sending an $n-$photon coherent state and the conditional probability that Bob will have a detection event if Alice sends an $n-$photon state:

$$Q_n = Y_n p_n = Y_n e^{-\mu} \frac{\mu^n}{n!} \tag{6.3}$$

The total gain is the sum over n, number of possible photons in the coherent states, of the Q_n's:

$$Q_\mu = \sum_{n=0}^{\infty} Q_n = \sum_{n=0}^{\infty} Y_n e^{-\mu} \frac{\mu^n}{n!} = Y_0 + 1 - e^{-\eta\mu} \tag{6.4}$$

where $1-e^{-\eta\mu}$ corresponds to the probability $P_{non-vac}$ of receiving a detection event.

Quantum Bit Error Rate (QBER). The Quantum Bit Error Rate is a variable that quantifies the errors that happen in the transfer of qubits in a QKD protocol, and it represents an important factor that establishes the level of quality of the encryption key that is created.

Some of those qubits might get damaged or lost in the communication as a consequence of the noisy channel, leading to mistakes. As a result, the QBER is expressed as the percentage of mistakes to all qubits sent during transmission.

Therefore, the QBER must be maintained as low as feasible to guarantee the integrity of the key.

Let the QBER relative to an $n-$photon state be defined as follows [29]:

$$e_n = \frac{e_0 Y_0 + e_{detector}\eta_n}{Y_n} \tag{6.5}$$

where e_0 and Y_0 are, respectively, the QBER and the yield of the $0-$photon state, Y_n the yield of the $n-$photon state, and $e_{detector}$ is a constant value, independent of n that indicates the probability of the signal hitting an erroneous detector . With this definition, contributions to e_n of both erroneous detections and background contributions are taken into account.

Supposing that the background event rates of the two detectors are equal, the result

is completely random and the error rate is 50% [30]. In other words, $e_0 = 1/2$ is the QBER value for the vacuum state.

The total QBER for a coherent state is E_μ and the following relationship holds:

$$Q_\mu E_\mu = \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu} = e_0 Y_0 + e_{detector}(1 - e^{-\eta\mu}) \tag{6.6}$$

As mentioned above, the eavesdropper cannot distinguish decoy states from signal states, since they possess the same characteristics (such as wavelength and timing information) and is only capable of counting the number of photons per pulse. From the definitions above, it can be seen that the yield Y_n and the QBER e_n do not depend on the signal intensity μ, and thus on the distribution of the number of photons, but only on the number of photons in the signal state. We thus arrive at the essence of the Decoy State Method, which can be set forth in the following two equations [30]:

$$\begin{aligned} Y_n(decoy) =& Y_n(signal) = Y_n \\ e_n(decoy) =& e_n(signal) = e_n \end{aligned} \tag{6.7}$$

In a general and ideal situation Alice can vary the intensity of the pulses μ by creating, as a result, an infinite number of decoy states with different Poissonian parameter than the signal state. In the next sections it will be shown how few decoy states are actually sufficient. When these signals arrive to Bob, the legitimate parties are able to experimentally determine the specifications of the communication channel, then to determine the overall QBER E_μ and gain Q_μ.

From the equations (6.4) and (6.6) it is possible to see how the relationships between Q_μ's and Y_n's and between E_μ's and e_n's, respectively, are linear.

Consequently, given the set of variables Q_μ's and E_μ's that the legitimate parties obtain experimentally, Alice and Bob are able to determine with a high level of confidence the range within which the solution sets $\{Y_0, Y_1, ..., Y_n\}$ and $\{e_0, e_1, ..., e_n\}$ lie, then to find a range of acceptance of Y_n's and e_n's, simultaneously and for each n.

As mentioned earlier, if Alice and Bob use the Decoy State BB84 Method, any attempt by Eve to perform a PNS attack would involve a change in the values of Y_n's and e_n's that would necessarily be detected by Alice and Bob, implying Eve being detected and

the protocol to abort. For Y_n's and e_n's to fall within the expectation range of the legitimate parties following a PNS attack, Eve has very little power to act, which is useless for the purpose of decrypting the information.
This shows how the Decoy State Method may represent a solution to the problem of PNS attacks in the case of real implementations of the BB84 protocol.

6.2 Advantages in Key Rate Generation

The Decoy State is a method that can also provide excellent performances in the amount of information transmitted per unit time, thus making it an excellent candidate for future implementations.
In this regard, a fundamental variable analyzing the security proof is the *Key Rate*. In quantum cryptography, the key rate refers to the rate at which secret key bits can be generated and securely shared between two parties over a quantum communication channel. It represents the speed at which the parties can establish a secure cryptographic key that can be used for encrypting and decrypting their communication.
The key rate is influenced by various factors, including the properties of the quantum channel, the efficiency of the quantum cryptographic protocol being used, and the presence of any potential eavesdroppers. The goal is to achieve a high key rate while ensuring the security of the key against any potential attacks.
In practical terms, the key rate is typically measured in bits per second (bps) and represents the number of secure key bits that can be generated and exchanged in a given time period. Higher key rates are desirable as they allow for faster establishment of secure communication channels, enabling real-time secure communication between parties.
Regarding the Decoy State Method, a detailed analysis of the key generation rate has been provided by Gottesman, Lo, Lutkenhaus and Preskill, commonly known as GLLP result [38], that gives the following formula for the key generation rate R:

$$R \geqslant q\Big\{-Q_\mu f(E_\mu)H(E_\mu) + Q_1\big[1 - H(e_1)\big]\Big\} \tag{6.8}$$

where q is a constant that depends on the protocol used (for the BB84 protocol it is $1/2$ since in half of the cases Alice and Bob generate discordant bases in the first phase);

E_μ and Q_μ are respectively the overall QBER and gain of the signal state that has μ as its relative intensity; Q_1 and e_1 are respectively the gain and QBER for single photon states; $H(p)$ is the binary Shannon Entropy defined in equation (1.47) and, finally, $f(x)$ is the efficiency of bi-direction error correction (for an example, see [39]) as a function of E_μ: normally $f(x) \geqslant 1$ with Shannon limit $f(x) = 1$ [29].

6.2.1 Optimal Intensity Value

In this section we are interested in finding the optimal value μ of the signal intensity, in order to maximize the value of the key generation rate R of the Decoy State Method. Therefore, on one hand it is necessary to maximize the value Q_1, that is the gain of single photon states, which is associated with the probability of Alice emitting single photons; in particular, since the probability follows the Poissonian statistic, we obtain a maximum value for Q_1 when $\mu = 1$.
However, the overall gain Q_μ is also a function of μ: increasing μ also Q_μ increases. Since Q_μ is associated with multi-photon states, it must be kept low.
Consequently, the ratio Q_1/Q_μ must be high. Thus it is reasonable to assume that

$$\mu \in \left]0; 1\right[\tag{6.9}$$

Let's consider a realistic situation in which $Y_0 \ll \eta$ and $\eta \ll 1$, being the realistic values $Y_0 \simeq 10^{-5}$ and $\eta \simeq 10^{-3}$.
In this situation we have

$$\begin{cases} \eta_1 = \eta \\ Y_1 = \eta \\ Q_\mu = \eta\mu \\ E_\mu = e_1 = e_{detector} \\ Q_1 = \eta\mu e^{-\mu} \end{cases} \tag{6.10}$$

Then the key generation rate, with $q \simeq 1$ for a generic QKD protocol, becomes:

$$R \simeq q\Big\{-\eta\mu f(e_{detector}) H(e_{detector}) + \eta\mu e^{-\mu}\big[1 - H(e_{detector})\big]\Big\} \tag{6.11}$$

Therefore:

$$\left.\frac{\partial R}{\partial \mu}\right|_{\mu=\mu_{opt}} = 0 \quad \Rightarrow \quad e^{-\mu_{opt}}\big(1-\mu_{opt}\big) = \frac{f(e_{detector})H(e_{detector})}{1-H(e_{detector})} \tag{6.12}$$

Afterwards, considering the parameters taken from some recent experiments [40, 41] provided in Table 6.1, we may solve this equation and determine that $\mu_{opt}^{GYS} \simeq 0.54$ for $f(e) = 1$ and $\mu_{opt}^{GYS} \simeq 0.48$ for $f(e) = 1.22$ [29].

Experiment	$\lambda[nm]$	$\alpha[dB/km]$	$e_{detector}[\%]$	Y_0	η_{Bob}	f
GYS[40]	1550	0.21	3.3	$1.7 \cdot 10^{-6}$	0.045	$2MHz$
KTH[41]	1550	0.2	1	$4 \cdot 10^{-4}$	0.143	$0.1MHz$

Table 6.1: *Parameters of decoy state experiments.*

6.2.2 Two Decoy States and One Signal State

After finding the optimal values for the intensity μ of the signal state, we proceed to maximize the value of the key rate R with the decoy states. Looking at the equation (6.8), one realizes that the only term that depends on $\{Y_i\}$ and $\{e_i\}$ is $Q_1\big[1-H(e_1)\big]$, the term one must work on in order to maximize R.
Accordingly, we must proceed to find the lower bound for Y_1, and the upper bound for e_1.
As is shown in [30, 42] a few decoy states are sufficient to obtain good results for R, and here the case with two decoy states is analyzed.
Let us consider two decoy states with intensities ν_1 and ν_2 such that

$$0 \leqslant \nu_2 < \nu_1 \quad \text{and} \quad \nu_1 + \nu_2 < \mu \tag{6.13}$$

with μ intensity of the signal state.

Lower Bound for Y_1

The overall gains for the decoy states are defined as

$$Q_{\nu_1} = \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!} e^{-\nu_1} \quad \text{and} \quad Q_{\nu_2} = \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!} e^{-\nu_2} \tag{6.14}$$

Consequently, by taking $\nu_1 Q_{\nu_2} - \nu_2 Q_{\nu_1}$ we are able to obtain the lower bound for the background rate Y_0 :

$$\begin{aligned} \nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1} &= (\nu_1 - \nu_2) Y_0 - \nu_1 \nu_2 \left[\frac{Y_2}{2!}(\nu_1 - \nu_2) + \frac{Y_3}{3!}(\nu_1^2 - \nu_2^2) + ... \right] \\ &\leqslant (\nu_1 - \nu_2) Y_0 \end{aligned} \tag{6.15}$$

Therefore

$$Y_0 \geqslant Y_0^L = \max \left\{ \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}; 0 \right\} \tag{6.16}$$

where the equality holds when $\nu_2 = 0$, that is when one decoy state is a vacuum state. We now proceed to calculate the lower bound for Y_1. For contributions from multi-photon states of signal states, the following relation holds:

$$\sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} = Q_\mu e^\mu - Y_0 - Y_1 \mu \tag{6.17}$$

As a result we get:

$$\begin{aligned} Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} &= \sum_{i=0}^{\infty} \frac{Y_i}{i!}(\nu_1^i - \nu_2^i) = Y_1(\nu_1 - \nu_2) + \sum_{i=2}^{\infty} \frac{Y_i}{i!}(\nu_1^i - \nu_2^i) \\ &= Y_1(\nu_1 - \nu_2) + \sum_{i=2}^{\infty} \frac{Y_i}{i!}\left(\frac{\nu_1^i}{\mu^i} - \frac{\nu_2^i}{\mu^i}\right)\mu^i \end{aligned} \tag{6.18}$$

At this point we use the property for which $a^i - b^i \leqslant a^2 - b^2$ if $0 < a + b < 1$ and $i \geqslant 2$, where in this case $a = \frac{\nu_1}{\mu}$, $b = \frac{\nu_2}{\mu}$, and $a^i = \frac{\nu_1^i}{\mu^i}$, $b^i = \frac{\nu_2^i}{\mu^i}$. Thus

$$\begin{aligned} Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} &\leqslant Y_1(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} \\ &= Y_1(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \Big[Q_\mu e^\mu - Y_0 - Y_1 \mu \Big] \\ &\leqslant Y_1(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \Big[Q_\mu e^\mu - Y_0^L - Y_1 \mu \Big] \end{aligned} \tag{6.19}$$

Therefore the lower bound for Y_1 is given by

$$Y_1 \geqslant Y_1^{L,\nu_1,\nu_2} = \frac{\mu}{\mu(\nu_1-\nu_2)-\nu_1^2+\nu_2^2}\left[Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - \frac{\nu_1^2-\nu_2^2}{\mu^2}\left(Q_\mu e^\mu - Y_0^L\right)\right] \quad (6.20)$$

and the lower bound for the gain of the single-photon $Q_1 = Y_1\mu e^{-\mu}$ is given by

$$Q_1 \geqslant Q_1^{L,\nu_1,\nu_2} = \frac{\mu^2 e^{-\mu}}{\mu(\nu_1-\nu_2)-\nu_1^2+\nu_2^2}\left[Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - \frac{\nu_1^2-\nu_2^2}{\mu^2}\left(Q_\mu e^\mu - Y_0^L\right)\right] \quad (6.21)$$

where Y_0^L is given by the equation (6.16).

Upper Bound for e_1

The following relationships hold for QBERs

$$E_{\nu_1}Q_{\nu_1}e^{\nu_1} = e_0Y_0 + e_1\nu_1Y_1 + \sum_{i=2}^{\infty} e_iY_i\frac{\nu_1^i}{i!} \quad (6.22)$$

$$E_{\nu_2}Q_{\nu_2}e^{\nu_2} = e_0Y_0 + e_1\nu_2Y_1 + \sum_{i=2}^{\infty} e_iY_i\frac{\nu_2^i}{i!} \quad (6.23)$$

Consequently, with calculations similar to those mentioned above, we obtain the upper bound for e_1:

$$e_1 \leqslant e_1^{U,\nu_1,\nu_2} = \frac{E_{\nu_1}Q_{\nu_1}e^{\nu_1} - E_{\nu_2}Q_{\nu_2}e^{\nu_2}}{(\nu_1-\nu_2)Y_1^{L,\nu_1,\nu_2}} \quad (6.24)$$

In this way the legitimate parties are able to obtain a lower bound for Y_1 and an upper bound for e_1 and consequently they are able to compute the key generation rate by substituting their values:

$$R \geqslant q\left\{-Q_\mu f(E_\mu)H(E_\mu) + Q_1^{L,\nu_1,\nu_2}\left[1 - H(e_1^{U,\nu_1,\nu_2})\right]\right\} \quad (6.25)$$

Once this result is obtained, it is possible to proceed analyzing the quality of the bounds found, and consequently the performance of the model with two decoy states.
It is possible to examine the special case, called the *Asymptotic Case*, in which $\nu_1 \to 0$ and $\nu_2 \to 0$, with $\nu_2 < \nu_1 \ll \mu = O(1)$. Taking the above limits yields the following results [29]:

$$Y_1^{L,\nu_1,\nu_2}\Big|_{\nu_1,\nu_2\to 0} = Y_0 + \eta \quad \text{and} \quad e_1^{U,\nu_1,\nu_2}\Big|_{\nu_1,\nu_2\to 0} = \frac{e_0Y_0 + e_{detector}\eta}{Y_1} \quad (6.26)$$

Since in this limit the formulas (6.1)(6.5) are obtained again, the Asymptotic Case of the model with two decoy states is as good as the most general possible protocol, analyzed above, with an infinite number of decoy states. However, the Asymptotic Case has the disadvantage that in practice it is necessary to have at least one between ν_1 and ν_2 with a finite value. Moreover [29] shows how, fixing a finite value of ν_1, the key generation rate is maximized when $\nu_2 = 0$, that is, when the second decoy state is a vacuum state. Consequently, we come to establish the fundamental importance in practical developments held by the model *Weak and Vacuum Decoy State*, proposed in [30].

Weak and Vacuum Decoy State

The *Weak and Vacuum Decoy State* is a special case of the Two Decoy State with $\nu_2 \to 0$. Presented in [30] and analyzed in [43], it provides excellent values for the performances in communication, achieving high values of key generation rate for long-distance communication.
Alice is able to generate the vacuum state by simply turning off its photon source. For the vacuum state the legitimate parties are able to estimate:

$$Q_{vac} = Y_0 \quad \text{and} \quad E_{vac} = e_0 = \frac{1}{2} \tag{6.27}$$

The second decoy state that Alice realizes has a small but finite intensity value ν. For the weak decoy state the legitimate parties are able to compute the lower bound for Y_1 and gain Q_1, and the upper bound for e_1 by taking the limit with $\nu_2 \to 0$ respectively of the formulas (6.20) (6.21) (6.24):

$$Y_1 \geqslant Y_1^{L,\nu,0} = Y_1^{L,\nu,\nu_2}\Big|_{\nu_2\to 0} = \frac{\mu}{\mu\nu - \nu^2 +} \left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2}\left(Q_\mu e^\mu - Y_0^L\right)\right] \tag{6.28}$$

$$Q_1 \geqslant Q_1^{L,\nu,0} = Q_1^{L,\nu,\nu_2}\Big|_{\nu_2\to 0} = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2 +} \left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2}\left(Q_\mu e^\mu - Y_0^L\right)\right] \tag{6.29}$$

$$e_1 \leqslant e_1^{U,\nu,0} = e_1^{U,\nu,\nu_2}\Big|_{\nu_2\to 0} = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{\nu Y_1^{L,\nu,0}} \tag{6.30}$$

This gives the lower bound for the key generation rate R:

$$R^L = q\left\{-Q_\mu f(E_\mu) H(E_\mu) + Q_1^{L,\nu,0}\left[1 - H\left(e_1^{U,\nu,0}\right)\right]\right\} \tag{6.31}$$

Taking into consideration the data from the GYS experiment given in Table 6.1, the optimal value of the signal state intensity $\mu = 0.48$ for $f(e) = 1.22$, $\nu = 0.05$, and looking at the BB84 model for which $q = 1/2$, we obtain the lower bound of the key generation rate as a function of distance, the graph of which is depicted in Figure 6.1.

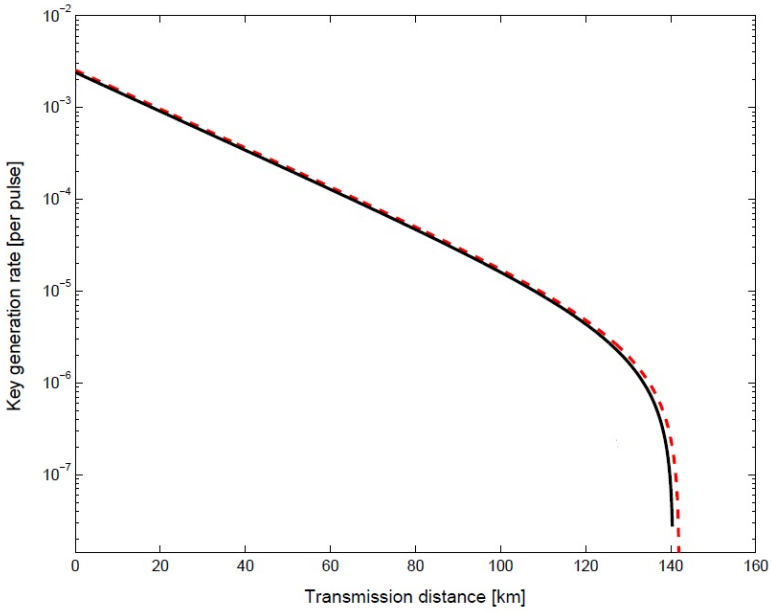

Figure 6.1: *The red dashed line represents the lower bound of R in the Asymptotic Case situation, following equation (6.8) for which the maximum safety distance is 142.05km. The black continuous line represents the Weak and Vacuum Decoy State situation, following equation (6.31) with* $\mu = 0.48$, $f(e) = 1.22$, $\nu_1 = 0.05$ *and* $\nu_2 = 0$. The other variables are taken from the GYS experiment reported in Table 6.1. ([29])

As can be seen, this yields a maximum distance for which communication is secure of $140.55km$ [29], a value slightly lower than the Asymptotic Case, which concerns the most generic case with an infinite number of decoy states (hence with the best performances), for which a maximum distance of $142.05km$ is obtained.

Conclusions

The present study set itself the goal to present an analysis in the field of quantum cryptography, and in particular an analytical description of the implications to consider when technological limitations arise in the application of quantum key distribution (QKD) protocols.

The QKD process is the best currently known method for performing quantum cryptography operations, which is implemented through suitable protocols. Indeed, it offers the ultimate solution to the cryptography problem, in contrast to post-quantum cryptography that would offer systems that are robust against already known quantum algorithm, thus creating only temporary solutions. While the latter would expose the information to undiscovered quantum algorithms, the QKD restores the security basing on fundamental laws of quantum mechanics and resulting from unbreakable principles of nature, like the Uncertainty Principle and No-Cloning Theorem.

The BB84 model is the protocol taken as a reference, which, as simple as effective, is demonstrably secure from every attack that an eavesdropper might launch. Proposed in 1984 by Charles Bennett of IBM and Gilles Brassard of The University of Montréal, it bases its security in the exchange of communication between the legitimate parties on the laws of quantum mechanics mentioned above; however, the procedures for the creation of the encryption key require ideal assumptions that are difficult to implement in practice: the creation of perfect single-photon source, channel without loss, 100% detector efficiency. These assumptions all translate into obstacles in the experimental implementation of the BB84 protocol with current technologies, especially if the goal is to realize secure communication networks, commercial and financial applications and the protection of sensitive infrastructures, where both security and communication perfor-

mances are essential.

The Photon-Number-Splitting attack was examined as a possible vulnerability to the BB84 protocol that arises from the coexistence of weak coherent states and noise in the quantum channel. Although the eavesdropper must possess advanced and currently inaccessible technologies to implement it, such as quantum memories or the ability to perform non-demolition measurements, they may be available in the future.

To mitigate the consequences resulting from realistic experimental apparatus, the Decoy State Method can provide a solution to possible future critical issues arising from technological advancement, such as PNS attacks. It is a method implementable on any type of quantum key distribution protocol: in this review it has been applied on the BB84 model.

As a result to this analysis, the Decoy State guarantees excellent performances from both a qualitative, concerning its security, and a quantitative point of view, concerning the amount of information and distance that can be achieved in communication; however, at the same time it is a straightforward model for experimental implementation, since the sender of the information only needs to modulate the intensity μ of the Poisson statistic between the signal and decoy states values.

Consequently, it has been seen that using even only two decoy states is sufficient to ensure a high level of security, and in particular the key generation rate is maximized when one of the two decoy states is a vacuum state: to produce a vacuum state, it is sufficient to turn off the photon source.

Examining the lower bound of the key generation rate in detail, it has been analysed that, in the Weak and Vacuum Decoy State case, the maximum distance for a secure communication is 140.55km, a value slightly lower than the Asymptotic Case, which concerns the most generic case with an infinite number of decoy states, for which a maximum distance of 142.05km is obtained. Thus, if an eavesdropper attempted to hack the communication channel, the legitimate parties would notice both different values of the quantities characterizing the quantum channel and a value of the key generation rate lower than the lower bound.

Because of these considerations, the Decoy State Method, applied to a model such as the BB84 protocol, is an excellent candidate for being used in commercial implementations

of quantum cryptography protocols. In fact, in recent years it has been examined in detail from both a theoretical and practical point of view, and has been given attention as a possible international standard.
In addition to the reasons mentioned above, the Decoy State is of particular utility in today's situation in which technologies such as quantum networks based on quantum repeaters or perfectly entangled particles, which would enable long-distance communication, or quantum digital signatures, which would ensure that the authenticity and integrity of the message, are inaccessible.
Despite the Decoy State approach and QKD protocols seem to be the most advanced quantum technologies now accessible, both theoretical and practical research meet a number of challenges and open questions. There is still a big need for more dependable QKD techniques that can go farther and faster.
Theoretically, one of the main challenges concerns providing more rigorous security proofs in the Decoy State Method. While it has been shown to be secure in specific scenarios, developing a comprehensive security analysis that accounts for various potential attacks and imperfections in practical implementations remains an ongoing challenge. In addition, the choice of the optimal decoy state configurations for a given scenario, such as the intensities and types of states, significantly affects the security and performance of the protocol and it is a complex problem that requires theoretical analysis and optimization techniques, as well as the analysis of the statistical fluctuations and finite-size effects.
In order to implement quantum cryptography and quantum key distribution technologically, it is necessary to take into account how they will integrate with the existing classical infrastructure and create layers of security while solving issues concerning system integration, stability, and scalability.
Before QKD can be regarded as a completely safe quantum technology, many types of vulnerabilities must be carefully considered. These weaknesses will become more evident as quantum cryptography develops as a field of science. However, the Decoy State Method could provide the solution to the raised problems, and research is already setting the path to implement systems that are capable of solving the threats brought by the power of quantum computers before they are even developed, in order to smooth the transition to a quantum reality.

Bibliography

[1] M. Nielsen, I. Chuang, "*Quantum Computation and Quantum Information: 10th Anniversary Edition*". Cambridge: Cambridge University Press (2010). DOI:https://doi.org/10.1017/CBO9780511976667

[2] W. Smythe, March 15, 2021. "*The Bloch sphere and eigenstates with their superpositions*" [Online]. Available from: https://logosconcarne.com/2021/03/15/qm-101-bloch-sphere/[Accessed 23 June 2023].

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "*Advances in quantum cryptography,*" Advances in Optics and Photonics 12, 1012 (2020). DOI:https://doi.org/10.48550/arXiv.1906.01645

[4] I. Bengtsson, "*Three Ways to Look at Mutually Unbiased Bases*", AIP Conference Proceedings 889, 40-51 (2007). DOI:https://doi.org/10.1063/1.2713445

[5] M. Planat, H.C. Rosu, S. Perrine, "*A Survey of Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements*". Foundations of Physics 36, 1662-1680 (2006). DOI:https://doi.org/10.1007/s10701-006-9079-3

[6] K. Jacobs, "*Quantum Measurement Theory and its Applications*". Cambridge University Press (2014). DOI:https://doi.org/10.1017/CBO9781139179027

[7] R. Wolf, "*Quantum Key Distribution*", Springer (2021). DOI:https://doi.org/10.1007/978-3-030-73991-1

[8] R. Griffiths "*Quantum Channels, Kraus Operators, POVMs*" (2012). Available from: https://quantum.phys.cmu.edu/QCQI/qitd412.pdf

[9] D. Griffiths, D. Schroeter, "*Introduction to Quantum Mechanics (3rd ed.)*", Cambridge: Cambridge University Press (2018). DOI:10.1017/9781316995433

[10] M. G. A. Crawford, "*Generalized coherent states and classical limits in quantum mechanics*" (2000). URI:http://hdl.handle.net/10012/550

[11] S.J. Blundell, and K.M. Blundell, "*Concepts in Thermal Physics*", Oxford University Press (2009). DOI:10.1093/acprof:oso/9780199562091.001.0001

[12] A.S. Trushechkin, E.O. Kiktenko, D.A. Kronberg, A.K. Fedorov. "*Security of the decoy state method for quantum key distribution*", Uspekhi Fizicheskikh Nauk Journal. Phys. Usp. 64, 88 (2021). DOI:https://doi.org/10.48550/arXiv.2101.10128.

[13] C.-H. F. Fung, X. Ma, H. F. Chau. "*Practical issues in quantum-key-distribution post-processing*", American Physical Society. Phys. Rev. A 81, 012318 (2009). DOI:https://doi.org/10.48550/arXiv.0910.0312

[14] E. Kiktenko, A. Trushechkin, Y. Kurochkin and A. Fedorov. "*Post-processing procedure for industrial quantum key distribution systems*". Journal of Physics: Conference Series 741, 012081 (2016). DOI:https://doi.org/10.1088/1742-6596/741/1/012081

[15] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "*Quantum cryptography*", American Physical Society. Rev. Mod. Phys. 74, 145-195 (2002). DOI:10.1103/RevModPhys.74.145

[16] S. Attal "*Lecture 6 Quantum Channels*". Available from http://math.univ-lyon1.fr/~attal/Quantum_Channels.pdf

[17] M. M. Wilde "*From Classical to Quantum Shannon Theory*", Cambridge University Press (2019). DOI:https://doi.org/10.1017/9781316809976.001

[18] IEEE Computer Society, Indian institute of science (Bangalore), IEEE Circuits and Systems Society "*International Conference on Computers, Systems Signal Processing*", Steering Committee (1984). DOI:https://books.google.com/books?id=JZetpwAACAAJ

[19] H. S. Singh, D. S. Gupta, A. K. Singh, "*Quantum Key Distribution Protocols: A Review*", IOSR Journal of Computer Engineering 16, 01-09 (2014). DOI:10.9790/0661-162110109.

[20] W. Wootters, W. Zurek, "*A single quantum cannot be cloned*", Nature 299, 802-803 (1982). DOI:https://doi.org/10.1038/299802a0.

[21] J. Ortigoso "*Twelve years before the quantum no-cloning theorem*", American Journal of Physics 86, 201-205 (2018). DOI:https://doi.org/10.1119/1.5021356

[22] I. Csiszar and J. Korner. "*Broadcast channels with confidential messages*", IEEE Transactions on Information Theory 24, 339-348 (1978). DOI:10.1109/TIT.1978.1055892

[23] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, W.-M. Shi, "*Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption*", Scientific Reports 6, 19788 (2016). DOI:10.1038/srep19788.

[24] D. Pegg, S. Barnett, J. Jeffers. "*Quantum theory of preparation and measurement*", Journal of Modern Optics 49, 913-924 (2002). DOI:10.1080/09500340110109412

[25] C.A. Fuchs, N. Gisin, R. B. Griffiths, C-S Niu, A. Peres, "*Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy*", American Physical Society, Phys. Rev. A 56, 1163 (1997). DOI:10.1103/PhysRevA.56.1163

[26] C.M. Caves, C.A. Fuchs, R. Schack, "*Unknown quantum states: The quantum de Finetti representation*", Journal of Mathematical Physics 43, 4537 (2002). DOI:https://doi.org/10.1063/1.1494475

[27] J.I Cirac, N Gisin, "*Coherent eavesdropping strategies for the four state quantum cryptography protocol*", Physics Letters A 229, 1-7 (1997). DOI:https://doi.org/10.1016/S0375-9601(97)00176-X

[28] A. A. Gaidash, V. I. Egorov, A. V. Gleim "*Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices*". Journal of Physics: Conference Series 735, 012072 (2016). DOI:10.1088/1742-6596/735/1/012072

[29] X. Ma, B. Qi, Y. Zhao, H.-K. Lo, "*Practical decoy state for quantum key distribution*", American Physical Society. Phys. Rev. A 72, 012326 (2005). DOI:10.1103/PhysRevA.72.012326

[30] H.-K. Lo, X. Ma, K. Chen, Kai. "*Decoy State Quantum Key Distribution*", American Physical Society. Phys. Rev. Lett. 94, 230504 (2005). DOI:10.1103/PhysRevLett.94.230504

[31] G. Nogues, A. Rauschenbeutel, S. Osnaghi, et al. "*Seeing a single photon without destroying it*", Nature 400, 239-242 (1999). DOI:https://doi.org/10.1038/22275

[32] M. K. Bochkov and A. S. Trushechkin, "*Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds*", American Physical Society, Phys. Rev. A 99, 032308 (2019). DOI:10.1103/physreva.99.032308

[33] Z. Zhang, Q. Zhao, M. Razavi, X. Ma, "*Improved key-rate bounds for practical decoy-state quantum-key-distribution systems*", American Physical Society, Phys. Rev. A 95, 012333 (2017). DOI: 10.1103/physreva.95.012333

[34] A. S. Trushechkin, E. O. Kiktenko, A. K. Fedorov, "*Practical issues in decoy-state quantum key distribution based on the central limit theorem*", American Physical Society, Phys. Rev. A 96, 022316 (2017). DOI: 10.1103/PhysRevA.96.022316

[35] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, "*Practical challenges in quantum key distribution*", Springer Science and Business Media, npj Quantum Information 2, 16025 (2016). DOI: 10.1038/npjqi.2016.25

[36] H.-K. Lo, M. Curty, K. Tamaki, "*Secure quantum key distribution*", Springer Science and Business Media, Nature Photonics 8, 595-604 (2014). DOI: 10.1038/nphoton.2014.149

[37] A. V. Duplinskiy, E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, R. P. Ermakov, A. I. Kotov, A. V. Brodskiy, R. R. Yunusov, V. L. Kurochkin, A. K. Fedorov, Y. V. Kurochkin, "*Quantum-Secured Data Transmission in Urban Fiber-Optics Communication Lines*", Springer Science and Business Media, Journal of Russian Laser Research 39, 113-119 (2018). DOI: 10.1007/s10946-018-9697-1

[38] D. Gottesman, H.-K. Lo, N. Lutkenhaus, J. Preskill, "*Security of quantum key distribution with imperfect devices*", International Symposium on Information Theory, Quant.Inf.Comput. 5, 325-360 (2004). DOI: 10.1109/ISIT.2004.1365172

[39] G. Brassard, L. Salvail, "*Secret-Key Reconciliation by Public Discussion*", Springer Berlin Heidelberg, Advances in Cryptology - EUROCRYPT '93 765, 410-423 (1994). DOI: 10.1007/3-540-48285-7_35

[40] C. Gobby, Z. L. Yuan, A. J. Shields, "*Quantum key distribution over 122 km of standard telecom fiber*", Applied Physics Letters 84, 3762-3764(2004). DOI: 10.1063/1.1738173

[41] M. Bourennane, F. Gibson, A. Hening, A. Karlsson, P. Jonsson, T. Tsegaye, D. Ljunggren, E. Sundberg, "*Experiments on long wavelength (1550 nm) "plug and play" quantum cryptography systems*", Technical Digest. Summaries of Papers Presented at the Quantum Electronics and Laser Science Conference, 112-113 (1999). DOI: 10.1109/QELS.1999.807380

[42] J. W. Harrington, J. M. Ettinger, R. J. Hughes, J. E. Nordholt, "*Enhancing practical security of quantum key distribution with a few decoy states*", arXiv: Quantum Physics (2005). DOI: https://doi.org/10.48550/arXiv.quant-ph/0503002

[43] X.-B. Wang, "*Decoy-state protocol for quantum cryptography with four different intensities of coherent light*", American Physical Society, Physical Review A 72, 012322 (2005). DOI: 10.1103/physreva.72.012322