UNIVERSIDAD DEL VALLE

Use of Decoy States as a Method for Increasing Security in a Quantum Key Distribution Protocol

Jorge Eduardo Arias Muñoz

Advisor: Omar Calderón Losada, Ph.D.
Co-Advisor: John Henry Reina Estupiñan, Ph.D.
Co-Advisor: Oscar Fernando Bedoya Leyva, Ph.D.

A thesis submitted in partial fulfillment for the degree of
Bachelor of Science in Systems Engineering

Faculty of Engineering
School of Systems and Computing Engineering

June 2025

“We can only see a short distance ahead, but we can see plenty there that needs to be done.”

Alan Turing

UNIVERSIDAD DEL VALLE

Abstract

Faculty of Engineering
School of Systems and Computing Engineering

Systems Engineer

Jorge Eduardo Arias Muñoz

This work investigates the BB84 Quantum Key Distribution (QKD) protocol enhanced with a Vacuum+Weak decoy-state configuration, through both software simulation and a low-cost optical experiment. An interactive simulation (built with Qiskit and Streamlit) models key-exchange under ideal, noisy, and adversarial conditions, and an additional decoy-state simulation quantifies photon-number yields Y_n to effectively reveal photon-number-splitting and beam-splitting attacks. Experimentally, a simplified free-space setup—using attenuated laser pulses, polarization optics, and single-photon detectors—implemented Vacuum+Weak BB84 with two mean photon numbers, enabling direct comparison of signal and decoy yields and error rates. Under normal operation, measured yields satisfied the decoy-state security conditions ($Y_n^\mu \approx Y_n^\nu$ and $e_n^\mu \approx e_n^\nu$) within statistical bounds. However, observed quantum bit error rates (QBERs) of 23.4% and 33.2% exceeded the theoretical secure threshold (11%), preventing secure key extraction. Evaluating these results with the developed simulation, they underscored the influence of source instability and polarization misalignment on overall error. In addition, the choice of mean photon numbers proved to be critical for increasing security in the protocol. Proposed next steps include upgrading to a stabilized pulsed laser source, matched polarization optics, and fiber-coupled components with active alignment, as well as extending simulation parameters to explore alternate mean photon numbers, occurrence ratios, and additional QKD protocols. This thesis findings provide a clear reference for implementing decoy-state QKD under resource-constrained conditions.

Acknowledgements

Estas palabras de agradecimiento son para todos aquellos que en algún momento contribuyeron en mi crecimiento personal y/o académico, moldeando a la persona que logró llegar hasta este punto. Inicialmente, agradezco enormemente a familia: a mi padre por ser un modelo de disciplina y perseverancia, a mi madre por su constante cariño y apoyo incondicional, y a mi hermana, quien me ha protegido y me ha hecho siempre sentir acompañado. Agradezco también a mis codirectores John Henry Reina y Oscar Bedoya por sus aportes a mi formación, y especialmente a mi director, Omar Calderón, quien me guió de inicio a fin, de quien aprendí tanto de la academia como de la vida, quien me instruyó dentro y fuera del aula, y a quien le debo enteramente el desarrollo de este proyecto, pues su paciencia y calidez hicieron de este proceso algo mucho más llevadero.

Quisiera agradecer también a los compañeros y amigos que se formaron con el paso del tiempo. Agradezco a Kevin López, quien se convirtió en alguien valioso gracias a nuestras discusiones académicas y momentos de ocio. Agradezco a Esteban Murillo, quien me brindó su apoyo incondicional de principio a fin dentro del laboratorio, y con quien las conversaciones esporádicas siempre fueron placenteras. Agradezco a Juan Camilo Moreno y a Miguel Rojas por su colaboración en el desarrollo de este proyecto, y especialmente a Miguel, de quien constantemente aprendía en el proceso. Agradezco también a Krystifer Campos, quien fue siempre mi mayor apoyo académico durante todos estos años, y a quien directamente le debo el inicio de este trabajo. Adicionalmente agradezco a los miembros de QuanTIC y CIBoFi, así como a mis compañeros de Ingeniería y Física, por los momentos compartidos y las sonrisas que me sacaron a lo largo de ellos.

Finalmente, quisiera agradecer a la persona más importante en mi vida desde que empezó toda esta travesía, Ariana Medina, por ser quien aguantaba mis quejas, por ser mi mejor amiga, por ser mi persona favorita, por ser mi compañera en la vida, por confiar en mí aunque dudara de mí mismo, por su amor absoluto e incondicional y, sin duda alguna, por ser el motivo por el cual hoy soy la mejor versión de mí que puedo ser.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Cryptography can be defined as a group of techniques aimed to maintain information transmission secure. Along with cryptanalysis, a group of techniques aimed to breach cryptographic methods; they compose what is called cryptology, a discipline that has evolved over time, allowing modern-day's technology to be secure [1].

Traditional cryptography focused on designing codes to allow two parties to communicate secretly in the presence of a third party who could intercept their communications [2]. These codes, now called encryption schemes, relied on a secret key shared by the communicating parties and unknown to the interceptor, a model known as private-key encryption [2]. In this model, the parties share a key that is used to encrypt plaintext into ciphertext, which is then sent to the receiver [2]. The receiver uses the same key to decrypt the ciphertext, keeping the plaintext hidden from any interceptor [2].

While this provides secure communication, the shared key must be exchanged securely in advance—a process known as key distribution, which is often impractical [1]. In public-key encryption, the receiver generates a public and a private key that are used to encrypt and decrypt the message, respectively. The public key can be distributed freely while the private key is kept secret. These key pairs are mathematically related in such a way that information encrypted with the public key can only be decrypted using the corresponding private key. Since the public key is easily accessible by anyone, the security of this scheme depends on the confidentiality of the private key [2].

Most modern secure communication protocols are based on private and public key encryption. Symmetric algorithms like AES, Twofish, and IDEA rely on complex transformations that require brute force attacks to break. Public-key algorithms such as RSA and ECC are based on problems considered computationally intractable for classical computers, like factoring large primes and computing discrete logarithms [2].

The security of these cryptographic systems, however, relies on the assumption that the mathematical problems in which they are based on, will remain computationally difficult to solve using classical computing architectures. This assumption is increasingly being challenged with the evolution of *quantum computing* [1]. Unlike classical computers that use bits with two stable states, quantum computers utilize *qubits* which can exist in superposition, allowing them to store significantly more information and perform certain calculations much faster by harnessing the laws of quantum mechanics [3].

Specific quantum algorithms have already been developed that could compromise today's cryptographic standards: Shor's algorithm can efficiently factor large integers and compute discrete logarithms [4], effectively breaking RSA and elliptic curve cryptosystems, while Grover's algorithm offers a quadratic speedup in brute-force attacks against symmetric encryption schemes [5]. However, the implementation of these quantum algorithms requires quantum computers with significant capabilities that do not yet exist.

Because of this, there is active work on new cryptographic techniques that are resistant to quantum computing's continuous development. One of them is called Quantum Key Distribution (QKD), and it focuses on solving the problem of securely exchanging a key between two parties in order to allow subsequent communication with a symmetric cryptosystem. Unlike traditional methods, QKD offers security based on the principles of quantum mechanics rather than computational hardness assumptions.

1.1 Problem Statement

1.1.1 Problem Description

The first QKD protocol was proposed by Bennett and Brassard in 1984, known as BB84 [6]. This protocol uses the polarization of single photons to encode classical bits, allowing two parties (Alice and Bob) to establish a shared secret key and detect the presence of an eavesdropper (Eve) by monitoring errors introduced during quantum transmission.

While theoretically offering unconditional security, translating QKD protocols like BB84 into practical systems faces significant experimental challenges. Ideal BB84 requires a perfect single-photon source, but real-world implementations often rely on attenuated lasers emitting weak coherent pulses. These pulses, while mostly containing zero or one photon, probabilistically can have multiple photons. This imperfection creates a critical vulnerability known as the Photon Number Splitting (PNS) attack, first proposed by Huttner et al. in 1995 [7], later established by Brassard et al. in 2000 [8], and extended further by Lütkenhaus and Jahma in 2002 [9]. Although other eavesdropping strategies such as Intercept-Resend and Beams-Splitting exist [10], mitigating the PNS attack had been of primary concern for practical QKD due to its theoretical power.

The PNS attack consists in Eve exploiting multi-photon pulses by intercepting them, retaining one photon for herself, and allowing the rest to pass to Bob. Eve can later measure her retained photons to gain information about the key without disturbing the photons that reach Bob, thus remaining undetected [8]. To overcome this, the decoy-state method was first proposed by Hwang in 2003 [11], where using pulses with varying intensities, alongside standard signal pulses used for key generation, serve as a way to monitor the presence of an eavesdropper by comparing the differences between decoy and signal state statistics caused by the PNS attack. The decoy-state method was quickly upgraded by Lo and colleagues in 2005 [12, 13], focusing on increasing the the speed at which secure cryptographic keys can be generated. For that, the Vacuum+Weak decoy-state configuration was proposed, where Alice generates vacuum and low intensity decoy pulses to monitor detection statistics such that they can limit Eve's information gain.

Not much work had been done regarding the ability of the decoy-state method to detect PNS attack's, until the work of Mailloux and colleagues [14–18]. Additionally, in the local context, work from Universidad de los Andes has explored aspects of QKD such as noise-assisted quantum key distribution schemes [19], the theoretical foundations and experimental advances in quantum cryptography [20] and the implementation of Hwang's original decoy-state method to enhance the security of the BB84 protocol [21]. However, to date, no experimental implementation or detailed analysis of the Vacuum+Weak decoy-state method's capability to detect PNS attacks has been reported.

In this undergraduate project, we address the problem of the absence of a local implementation and security condition evaluation of the BB84 protocol with Vacuum+Weak decoy states, through both a simulation-based approach and an accessible, low-cost experimental implementation, including systematic analysis of its practical limitations.

1.1.2 Problem Formulation

This project aims to implement the BB84 protocol with Vacuum+Weak decoy states in order to examine the practical challenges associated with this process and provide insights about its established security condition. In this context, the research question that guided the development of this undergraduate thesis is: How can the BB84 protocol with Vacuum+Weak decoy states be implemented in order to assess its practical challenges and evaluate its security condition under normal operation?

1.2 Justification

1.2.1 Academic Justification

The experimental implementation of QKD protocols has demonstrated great capacity for evolution. The use of decoy states as a technique to enhance security in the BB84 protocol poses practical challenges at various stages of development. Since the BB84 protocol is a cornerstone of QKD, this project serves as a resource regarding the limitations and possible solutions in the implementation process of this type of protocols.

1.2.2 Methodological Justification

The results obtained from experimental implementations of QKD protocols are generally affected by the type, quantity, and quality of equipment used throughout the project. The steps followed in each stage also vary depending on the focus of those involved. In the case of Systems Engineering, it provides contributions through the development of the technical and technological components involved in the process, both in terms of software development and simulation tools. This type of implementation contributes to general knowledge about the possible methods for carrying out such initiatives.

1.3 Objectives

1.3.1 General Objective

Implement a complete QKD system based on the BB84 protocol with decoy states and compare its efficiency with the standard BB84 and computational simulations.

1.3.2 Specific Objectives

1. Conduct a theoretical foundation of the BB84 protocol with decoy states, including a computational simulation and a design for experimental setup.

2. Implement an optical setup of the BB84 protocol with decoy states to distribute a key between two parties located in the same laboratory.

3. Characterize the implemented QKD system with decoy states in order to define limitations in the distribution rate, error mitigation, and its vulnerabilities.

1.4 Proposal Scope

This project deals with the implementation of a QKD system based on the BB84 protocol with Vacuum+Weak decoy-states to test its security condition under normal operation. Through a low-cost experimental setup, we seek to bring the development of quantum technologies closer to a local context. Additionally, by creating two distinct open-source simulations, we contribute tools to facilitate the understanding of the BB84 protocol and QKD systems capable of detecting the PNS attack. These include: an interactive BB84 protocol simulation designed to visualize the step-by-step process of QKD, and a more specific Vacuum+Weak decoy-state BB84 simulation, built with a modular, object-oriented design, leveraging a singleton configuration pattern, and employing distinct classes that represent the actions of each protocol role and manage quantum states.

1.5 Obtained Results

In this work, both the simulation and experimental implementation of the BB84 protocol with Vacuum+Weak decoy-states were achieved. The simulation results verify the stated security condition of the protocol under different scenarios, whereas the results obtained experimentally demonstrate the feasibility of an operational low-cost QKD system, while highlighting its hardware limitations for usable key generation. Finally, an analysis of the security condition over the experimental results point out the statistical nature of photon detection, where the mean photon numbers and occurrence percentages of decoy and signal states impact the discrepancies of the security condition.

Table 1.1: Specific objectives and their results

Specific Objective	**Obtained Result**
Conduct a theoretical foundation of the BB84 protocol with decoy states, including a computational simulation and a design for experimental setup.	BB84 protocol interactive simulation (Section 5.1), Vacuum+Weak decoy-states simulation (Section 5.2) and experimental setup design (Section 3.3).
Implement an optical setup of the BB84 protocol with decoy states to distribute a key between two parties located in the same laboratory.	Protocol implementation describing the optical setup specifications and control interface (Section 6.1).
Characterize the implemented QKD system with decoy states in order to define limitations in the distribution rate, error mitigation, and its vulnerabilities.	Description and discussion of experimental results (Section 6.2).

Chapter 2

Quantum Computing

The aspiration to harness quantum mechanics for computation requires meeting specific physical requirements for building and controlling quantum systems. A widely recognized set of criteria, proposed by David DiVincenzo, outlines the essential capabilities a system must possess to function as a scalable quantum computer [22]. These criteria highlight, among other requirements, the need for well-defined quantum bits, the ability to perform arbitrary operations on them (using a universal set of quantum gates), and the capacity to reliably extract information through measurement. This chapter develops some of these concepts, applied to the simulation component carried out in this work. First, the qubit as the fundamental unit of information is explained. Afterwards, the measurement process to obtain results is introduced. Finally, quantum gates and circuits are discussed as tools to manipulate states and represent computations.

2.1 Bits and Qubits

According to Claude Shannon, information is the measure of the reduction in uncertainty that results from knowing the outcome of an event [23]. A bit is the basic unit of information, corresponding to a choice between two equally likely alternatives, which describes a two-dimensional classical system. It can be represented by binary alternatives, usually denoted by 0 and 1. The most common representation is in terms of electrical states, where 0 corresponds to a low voltage and 1 corresponds to a high voltage.

Leveraging quantum mechanics, it is possible to represent a quantum bit, or qubit, as a unit of information describing a two-dimensional quantum system [3]. An example of this can be the state of a quantum particle, such as the spin of an electron or the polarization of a photon [3].

2.1.1 Bra-Ket Notation

In order to mathematically represent a quantum state, quantum mechanics makes use of bra-ket notation, a linear algebra notation used to write vectors and operators on Hilbert spaces, which are complex vector spaces equipped with an inner product such that the norm defined by the inner product is complete with respect to the metric induced by the norm [24]. A *ket* is written as $|\psi\rangle$, and it denotes a vector that represents the state of a quantum system. A *bra* is written as $\langle\psi|$, and it is the conjugate transpose of its corresponding ket. For a two-dimensional Hilbert space, this translates to:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \langle\psi| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}, \tag{2.1}$$

where α and β are complex numbers representing probability amplitudes of finding the system in each of the basis states. Using bras and kets, the *inner product* of two vectors $|\psi\rangle$ and $|\phi\rangle$ is denoted by $\langle\psi|\phi\rangle$ and computed through multiplication of $\langle\psi|$ and $|\phi\rangle$ as,

$$\langle\psi|\phi\rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \alpha^*\gamma + \beta^*\delta. \tag{2.2}$$

If a vector $|\psi\rangle$ satisfies $\langle\psi|\psi\rangle = 1$, it is said to be normalized. On the other hand, if two vectors $|\psi\rangle$ and $|\phi\rangle$ satisfy $\langle\psi|\phi\rangle = 0$, they are said to be orthogonal. For a set of vectors $\{|\psi_1\rangle \dots |\psi_n\rangle\}$ satisfying both conditions, it is said to be orthonormal and can be expressed as $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ where δ_{ij} is the Kronecker delta symbol defined as:

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases} \tag{2.3}$$

If an orthonormal set of vectors spans all the vector space it represents a basis. In the case of qubits, being a two-dimensional quantum system description, the basis known as the *computational basis* is formed by the following states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.4}$$

2.1.2 Superposition

Unlike a classic bit, a qubit takes advantage of a property of quantum mechanics known as superposition, where its state can be described by a linear combination of two or more possible basis states [3]. As a consequence, the most general state of a qubit is

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.5}$$

where α and β are complex numbers. A qubit in a superposition state has no corresponding classical bit value [25]. However, if the qubit is measured, it will not be found in that superposition. Instead, it is only going to be found in the states $|0\rangle$ or $|1\rangle$, with probabilities determined by $|\alpha|^2$ and $|\beta|^2$, respectively [25]. Therefore, α and β satisfy the condition $|\alpha|^2 + |\beta|^2 = 1$, ensuring that the total probability adds up to one.

The state of a single qubit can be visualized geometrically using the Bloch sphere (see Figure 2.1). In this representation, the computational basis states $|0\rangle$ and $|1\rangle$ are located at the north and south poles, respectively. The points on the surface of the sphere correspond to the *pure states* of the system, determined by the coefficients α and β in Eq. 2.5; whereas the interior points correspond to the *mixed states*. The concepts of pure and mixed states will be explained in more detail in a following section.

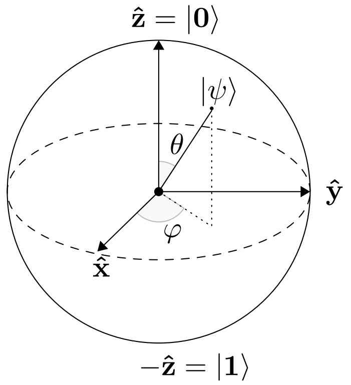

$\hat{\mathbf{z}} = |\mathbf{0}\rangle$
$|\psi\rangle$
θ
$\hat{\mathbf{y}}$
φ
$\hat{\mathbf{x}}$
$-\hat{\mathbf{z}} = |\mathbf{1}\rangle$

Figure 2.1: Representation of a quantum state $|\psi\rangle$ in the Bloch sphere.

2.2 Observables and Operators

In quantum mechanics, dynamical variables like position, momentum, angular momentum, and energy are known as observables [25]. They represent measurable properties used to describe and analyze the quantum state of a particle. According to one of the postulates of quantum theory, each observable is linked to a specific *operator*.

Formally, an operator represents a linear map that acts on a vector space, transforming one vector into another within the same space. When applied to a quantum state $|\psi\rangle$, an operator A maps it to a different state $|\phi\rangle$, as expressed by

$$A\,|\psi\rangle = |\phi\rangle\,. \tag{2.6}$$

For a chosen basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$, an operator can be represented as a matrix with the i-th column corresponding to the result of applying A to the basis state $|e_i\rangle$. For a matrix with elements A_{ij}, we define the trace as the sum of its diagonal elements:

$$\mathrm{Tr}(A) = \sum_i A_{ii}. \tag{2.7}$$

Different bases lead to different matrix representations for the same operator, however, the trace remains unchanged regardless of the chosen representation [26]. In the case of a single qubit, any operator acting on it is represented by a 2×2 matrix. A common example are the Pauli operators, whose representation in the computational basis are

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.8}$$

Operators can also be constructed by the *outer product* of two vectors [25]. Given two quantum states $|\psi\rangle$ and $|\phi\rangle$, their outer product is denoted by $|\psi\rangle\langle\phi|$ and calculated as:

$$|\psi\rangle\langle\phi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \gamma^* & \delta^* \end{pmatrix} = \begin{pmatrix} \alpha\gamma^* & \alpha\delta^* \\ \beta\gamma^* & \beta\delta^* \end{pmatrix}. \tag{2.9}$$

2.2.1 Hermitian, Unitary and Normal Operators

Three specific types of operators are of great importance in quantum theory: Hermitian, unitary, and normal operators [25]. They relate to the Hermitian adjoint, which is denoted as $A^\dagger$ and is defined as the conjugate transpose of the operator, or

$$A^\dagger = (A^*)^T. \tag{2.10}$$

An operator A is considered Hermitian if it satisfies $A = A^\dagger$. On the other hand, an operator U is unitary if it satisfies $UU^\dagger = U^\dagger U = I$ where I is the identity operator. Lastly, an operator A is normal if it satisfies $AA^\dagger = A^\dagger A$. An example of these operators are the Pauli operators (Eq. 2.8), which are Hermitian, unitary and normal. In quantum computing, they are used to manipulate the states of individual qubits [25].

In the case of normal operators, they can also be represented by their *spectral decomposition* [27]. That is, writing them in terms of their eigenvalues and eigenvectors as

$$A = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|, \tag{2.11}$$

where λ_i and $|\lambda_i\rangle$ are the eigenvalues and corresponding eigenvectors of A. An example of this is the Pauli-Z operator, whose spectral decomposition is $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, with eigenvalues 1 and -1 corresponding to the eigenvectors $|0\rangle$ and $|1\rangle$. Notice that the trace of Pauli-Z is $\mathrm{Tr}(Z) = 1 + (-1) = 0$, which also matches the sum of its eigenvalues.

2.2.2 Expectation Value and Conmutator

The possible results of measurement of a dynamical variable A are the eigenvalues a_n of the operator A corresponding to that variable. The *expectation value* of an operator is the mean value of that operator with respect to a given quantum state, representing the average outcome obtained when a quantum state is prepared repeatedly and the same operator is measured each time. Mathematically, it is expressed as:

$$\langle A \rangle = \langle \psi | A | \psi \rangle . \tag{2.12}$$

Operators acting on a quantum system can either commute or not commute with each other. Two operators A and B are said to commute if their commutator, given by

$$[A, B] = AB - BA, \tag{2.13}$$

is equal to 0. If $[A, B] \neq 0$, they do not commute. The commutation between operators determines whether the physical properties they represent can be measured simultaneously with arbitrary precision. If two operators commute, the corresponding observables can, in principle, be measured simultaneously. If they do not commute, the precision with which their corresponding observables can be known simultaneously is limited.

2.2.3 Projection Operators

An operator satisfying $P^2 = P$ is called a projection operator. This condition is called *idempotence* and implies that applying the operator twice is equivalent to applying it once, which characterizes a projection onto a subspace of the vector space [24]. If the projection operator is also Hermitian, it is called orthogonal. An orthogonal projection operator can be formed using the outer product of a single quantum state. For a normalized quantum state $|\psi\rangle$, the corresponding projection operator is defined as:

$$P = |\psi\rangle \langle \psi | \tag{2.14}$$

When two projection operators P_1 and P_2 commute ($P_1 P_2 = P_2 P_1$), their product $P_1 P_2$ is also a projection operator. The combined action of commuting projections results in a projection onto the intersection of their respective subspaces [24].

Using projection operators, it is possible to rewrite the spectral decomposition of normal operators. If a normal operator A has eigenvalues λ_i and corresponding orthonormal eigenvectors $\{|\lambda_i\rangle\}$, its spectral decomposition can be written as

$$A = \sum_i \lambda_i P_i, \quad P_i = |\lambda_i\rangle\langle\lambda_i|, \tag{2.15}$$

where each projection operator P_i projects onto the eigenspace associated with λ_i. These projection operators satisfy the *completeness relation*, given by:

$$\sum_i P_i = I. \tag{2.16}$$

2.2.4 Pure States and Density Operators

As already established, the state of a quantum system can be represented by a single ket $|\psi\rangle$. This ket contains all the information about the system and is required to satisfy the condition $\langle\psi|\psi\rangle = 1$. When a system is completely described by such a ket, it is said to be in a *pure state*, meaning there is no uncertainty about its quantum state[1] [26].

However, there are situations in which the preparation of the system is not perfectly controlled or where the system interacts with an environment, resulting in loss of coherence—the capability of different components of a state to interfere. In these cases the system may be in one of several possible states $|\psi_i\rangle$ each occurring with a probability p_i, where $p_i \geq 0$ and $\sum_i p_i = 1$. This statistical ensemble of states is known as a *mixed state* [28], reflecting incomplete knowledge about which pure state the system is in.

To provide a unified description of quantum states, the density operator ρ is used. For a pure state the density operator is constructed directly from the state vector as:

$$\rho = |\psi\rangle\,\langle\psi|\,. \tag{2.17}$$

This operator is Hermitian, satisfies the idempotency condition $\rho^2 = \rho$ and has unit trace $\mathrm{Tr}(\rho) = 1$. These properties ensure that the purity of the state, quantified by $\mathrm{Tr}(\rho^2)$, is equal to one. In contrast, for a mixed state the density operator is defined as a convex combination of the density operators from the individual pure states:

$$\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|. \tag{2.18}$$

[1] This does not imply that the results of all measurements are predictable with certainty, but that the system has a complete description by means of the ket $|\psi\rangle$, without mixing with other possible states.

Although this density operator remains Hermitian and with $\mathrm{Tr}(\rho) = 1$, it does not satisfy the condition $\rho^2 = \rho$, and accordingly, the purity $\mathrm{Tr}(\rho^2)$ is different than one.

2.2.5 Projective Measurements

A projective measurements is used to determine the state of a quantum system by projecting it onto a set of mutually exclusive orthogonal subspaces [25]. It is characterized by a set of orthogonal projection operators $\{P_i\}$, each corresponding to a distinct measurement outcome. When a measurement is made on a quantum state $|\psi\rangle$, the probability of obtaining the i-th outcome is given by:

$$\Pr(i) = \langle\psi| P_i |\psi\rangle . \tag{2.19}$$

If outcome i is obtained, the quantum state right after the measurement becomes:

$$|\psi'\rangle = \frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}}. \tag{2.20}$$

In the computational basis, the projection operators $P_0 = |0\rangle \langle 0|$ and $P_1 = |1\rangle \langle 1|$ model a projective measurement where each operator corresponds to the outcomes $|0\rangle$ and $|1\rangle$, respectively. For a qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, the probabilities of measuring $|0\rangle$ or $|1\rangle$ are:

$$\Pr(0) = |\alpha|^2, \quad \Pr(1) = |\beta|^2. \tag{2.21}$$

The post-measurement state of the qubit for outcomes $|0\rangle$ and $|1\rangle$ becomes

$$|\psi'\rangle = \frac{P_0 |\psi\rangle}{\sqrt{\langle\psi| P_0 |\psi\rangle}} = \frac{|0\rangle \langle 0| (\alpha |0\rangle + \beta |1\rangle)}{\sqrt{|\alpha|^2}} = \frac{\alpha |0\rangle}{|\alpha|} = |0\rangle , \tag{2.22}$$

$$|\psi'\rangle = \frac{P_1 |\psi\rangle}{\sqrt{\langle\psi| P_1 |\psi\rangle}} = \frac{|1\rangle \langle 1| (\alpha |0\rangle + \beta |1\rangle)}{\sqrt{|\beta|^2}} = \frac{\beta |1\rangle}{|\beta|} = |1\rangle , \tag{2.23}$$

where $\alpha/|\alpha|$ and $\beta/|\beta|$ are global phase factors that do not affect measurement probabilities or observable physical properties, making the states physically equivalent. Hence, the post-measurement states collapse to pure $|0\rangle$ or $|1\rangle$ states.

2.3 Gates and Circuits

In classical computing, logic gates operate on bits, applying deterministic rules to manipulate binary values. Each gate processes inputs according to Boolean algebra and produces a definite output. In the circuit model of computation, computations are perfomed through fixed sequences of gates, each applying a specific logical operation [29].

On the other hand, in quantum computing, operations on qubits are performed by quantum gates, which are unitary transformations that modify the state of a qubit or a system of qubits. Like classical gates, quantum gates enable the description of computations, using quantum circuits with sequences of quantum operations [3].

2.3.1 Quantum Gates

A single-qubit quantum gate is described by a 2 × 2 unitary matrix. Some of the most basic quantum gates are the Pauli gates, which correspond to the Pauli operators introduced in Eq. 2.8, each performing a specific transformation.

Pauli-X: The Pauli-X gate, often called a quantum NOT gate, flips the state of a qubit. When applied, it swaps the basis states $|0\rangle$ and $|1\rangle$:

$$X|0\rangle = |1\rangle\,, \quad X|1\rangle = |0\rangle\,. \tag{2.24}$$

Pauli-Y: The Pauli-Y gate combines a bit flip with a phase shift, effectively rotating the qubit around the Y-axis of the Bloch sphere:

$$Y|0\rangle = i|1\rangle\,, \quad Y|1\rangle = -i|0\rangle\,. \tag{2.25}$$

Pauli-Z: The Pauli-Z gate performs a phase flip leaving $|0\rangle$ unchanged while inverting the phase of $|1\rangle$, corresponding to a rotation around the Z-axis of the Bloch sphere:

$$Z|0\rangle = |0\rangle\,, \quad Z|1\rangle = -|1\rangle\,. \tag{2.26}$$

Since the Pauli matrices are unitary and Hermitian, they are both reversible and self-inverse, meaning that applying the same gate twice restores the original state:

$$X^2 = Y^2 = Z^2 = I. \tag{2.27}$$

Hadamard: Another elementary gate is the Hadamard gate, which creates equal superpositions of the computational basis states. Its matrix representation is given by:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.28}$$

When applied to the basis states $|0\rangle$ and $|1\rangle$ it produces:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle\,, \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\,. \tag{2.29}$$

Here, $|+\rangle$ and $|-\rangle$ are called the **plus** and **minus** states. These states form an orthonormal basis $\{|+\rangle, |-\rangle\}$ known as the Hadamard or X-basis, which can be mapped back to the computational or Z-basis, since the Hadamard gate is also self-inverse:

$$H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle \tag{2.30}$$

From the above, it is possible to stablish a measurement in a different basis. That is, a measurement using the projection operators $\{|+\rangle\langle+|, |-\rangle\langle-|\}$. This can be viewed as performing a measurement in the computational basis, right after transforming the qubit state using the Hadamard gate. In other words, a measurement in the computational basis of the state $H|\psi\rangle$ is equivalent to measuring in the Hadamard basis [27]. This will be used later on to model the measurement process in the BB84 protocol.

2.3.2 Quantum Circuits

Although there are different models of quantum computation, the most common is the quantum circuit model or gate-based quantum computing, build from the circuit model of classical computation [29]. A basic single-qubit quantum circuit consists of a qubit initialized to a known state, followed by a sequence of quantum gates, and ending with a projective measurement. It can be represented by a quantum circuit diagram, where a wire represents the qubit and quantum gates proceed from left to right.

In Figure 2.2, a single-qubit quantum circuit is shown. The initial state $|\psi\rangle$ undergoes two unitary transformations, represented by gates U_1 and U_2. At the end, a measurement in the computational basis collapses the state to a classical outcome, and is recorded in a classical register—a classical memory—represented by the double wires at the end. The sequence of gates applied to the state is expressed as $U_2U_1|\psi\rangle$, where the gate acting last is written first. The combined action of the U_2 gate and measurement on the computational basis, represent a measurement in an arbitrary basis $\{|e_1\rangle, |e_2\rangle\}$.

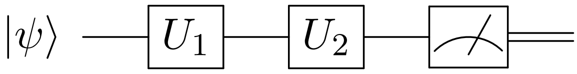


Figure 2.2: A quantum circuit with two unitary gates acting on an arbitrary initial state $|\psi\rangle$ followed by a final measurement in the computational basis.

A quantum circuit is executed in *shots*. In a single shot, the circuit is run once. As discussed in Section 2.2.5, the measurement causes the quantum state to collapse to one of the basis states. Because the outcome of a single measurement is probabilistic, a single run of the circuit only yields one possible result. To know the probability distribution of the outcomes—which is the true result of the quantum computation—the circuit must be executed multiple times. By repeating the experiment for a sufficient number of shots, the relative frequencies of observing each outcome can be calculated. These frequencies provide an estimate of the probabilities predicted by Eq. 2.19.

Quantum circuits can be implemented and run via simulation on classical computers or on real quantum hardware using platforms like Qiskit[2], Cirq[3], and PennyLane[4]. Currently available quantum computers are described as being in the Noisy Intermediate-Scale Quantum (NISQ) era [30]. This refers to the state of quantum processors which have a limited number of qubits (Intermediate-Scale) and are affected by significant noise and errors (Noisy). This noise limits the complexity (e.g., the number of gates and qubits) of circuits that can be reliably executed on current hardware, making simulations on classical computers a crucial tool for algorithm development and testing.

[2] `https://qiskit.org`

[3] `https://quantumai.google/cirq`

[4] `https://pennylane.ai`

Chapter 3

Quantum Key Distribution

This chapter compiles the main ideas of Quantum Key Distribution (QKD). It starts by presenting the theoretical foundations behind QKD, taking the BB84 protocol as the central discussion. It continues by explaining the concepts associated with the practical implementation of a QKD system and concludes with an explanation of the most studied configuration and model of this type of system.

3.1 Quantum Key Exchange

Quantum Key Distribution (QKD) is a technology that uses the principles of quantum mechanics to create and distribute secure cryptographic keys between two parties, which can then be used to encrypt a message in a one-time pad scheme, a technique that provides perfect secrecy if the key is truly random, never reused and kept secret [31]. Unlike traditional protocols, whose security depends on the complexity of certain mathematical problems, QKD relies on the principles of quantum mechanics, which theoretically makes it resistant to advances in computational power, such as quantum computing [32].

In general, QKD protocols can be classified in two main categories: *prepare-and-measure* and *entanglement-based*. In prepare-and-measure protocols, the security of the key exchange leverages the Heisenberg uncertainty principle, which states that certain pairs of quantum observables cannot be simultaneously measured with arbitrary precision. Thus, any eavesdropping attempt inevitably introduces detectable disturbances. In adition, the *no-cloning theorem* forbids creation of an identical copy of an unknown quantum state, ensuring that any attempt to copy quantum information leaves a trace [32, 33].

On the other hand, entanglement-based protocols rely on the phenomenon of quantum entanglement, a property of quantum systems composed of two or more subsystems, where the quantum state of the whole system cannot be described as a product of independent states for its constituent parts. The security in this category arises from the violation of Bell inequalities, which serve as a test for eavesdropping [34–36].

In the basic model of QKD protocols, two parties, commonly referred to as Alice and Bob wish to securely exchange a key while having access to classical and quantum communication channels. An eavesdropper, called Eve, is assumed to have access to both channels with no restrictions imposed on the resources she may utilize. Figure 3.1 presents a schematic diagram of the main components of a QKD protocol.

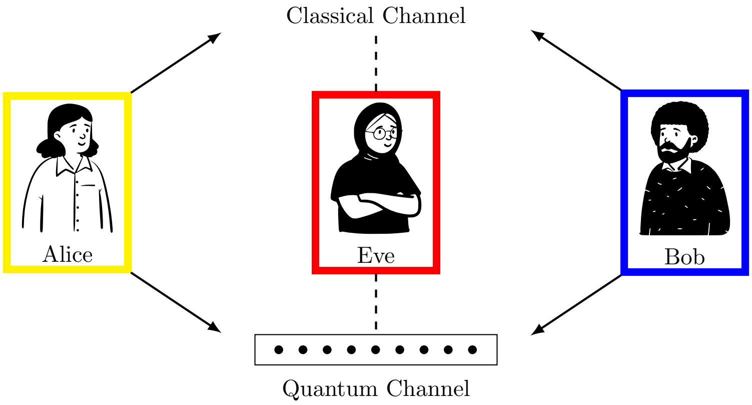


FIGURE 3.1: Basic Quantum Key Distribution (QKD) model. Alice and Bob exchange information through a quantum channel and a classical communication channel. Eve, attempts to intercept both channels to compromise the security of the exchange.

3.2 BB84 Protocol

The first QKD protocol, later known as BB84, was developed in 1984 by Charles Bennett and Gilles Brassard [6]. This protocol encodes classical bits into qubits based on photon polarization, and has become the most widely studied and implemented prepare-and-measure protocol to date. This is the implemented protocol in this work.

3.2.1 Polarization Qubits

Light, as an electromagnetic wave, consists of oscillating electric and magnetic fields perpendicular to its direction of propagation. In classical physics, polarization refers to the geometric orientation of the electric field as a function of time at a fixed point in space [37]. In quantum mechanics, polarization becomes a discrete degree of freedom of individual photons, which can be modeled as a two-level system. This makes the polarization state of a single photon a natural candidate for qubit implementation [38].

The polarization state of a photon can be represented using Jones vectors, which describe both the amplitude and phase of the electric field components [39]. For a photon traveling in the z-direction, its polarization state is characterized by the complex vector

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{3.1}$$

where α and β are complex amplitudes corresponding to horizontal and vertical polarization components, respectively. Notice that this representation is equivalent to the general qubit state described in Eq. 2.5, with the computational basis states $|0\rangle$ and $|1\rangle$ corresponding to horizontal $|H\rangle$ and vertical $|V\rangle$ polarization states, respectively. The BB84 protocol uses linear polarization states, as shown in Table 3.1.

Table 3.1: Linear polarization states used in the BB84 protocol.

Polarization	**Notation**	**Jones Vector**
Horizontal (0°)	$\|H\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
Vertical (90°)	$\|V\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
Diagonal (45°)	$\|D\rangle$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
Anti-diagonal (-45°)	$\|A\rangle$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

These polarization states form two *mutually unbiased* bases: the *rectilinear* basis $\mathcal{B}_+ = \{|H\rangle, |V\rangle\}$ and the *diagonal* basis $\mathcal{B}_\times = \{|D\rangle, |A\rangle\}$. Two bases are said to be mutually unbiased if a quantum system prepared in any state of one basis has equal probability of being measured in any state of the other basis [40]. Mathematically, for any state $|\psi_i\rangle$ from basis $\mathcal{B}_1$ and any state $|\phi_j\rangle$ from basis $\mathcal{B}_2$, it holds that

$$|\langle \psi_i | \phi_j \rangle|^2 = \frac{1}{d} \tag{3.2}$$

where d is the dimension of the Hilbert space ($d = 2$ for qubits). This property ensures that if an eavesdropper measures a qubit in the wrong basis, they gain no information while disturbing the state. The bases of the BB84 protocol satisfy this condition since the diagonal basis states are equal superpositions of the rectilinear basis states:

$$|\langle H|D\rangle|^2 = |\langle H|A\rangle|^2 = |\langle V|D\rangle|^2 = |\langle V|A\rangle|^2 = \frac{1}{2} \tag{3.3}$$

3.2.2 Experimental Preparation and Measurement

The preparation of polarization states needed for the BB84 protocol can be accomplished using a Half-Wave Plate (HWP). This optical element, known as a retarder, introduces a phase difference of half a wavelength between two orthogonal components of incident polarized light. When linearly polarized light passes through a HWP, the output remains linearly polarized but rotated by an angle of 2θ, where θ is the angle between the incident polarization direction and the fast axis of the retarder [41]. The matrix representation of the linear operator that accounts for the effects of a HWP in the rectilinear basis is

$$U_{HWP}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}. \tag{3.4}$$

For state preparation, Alice can generate all necessary polarization states using a horizontally polarized source and an appropriately oriented HWP, as shown in Table 3.2.

Table 3.2: Preparation of polarization states for BB84 using a half-wave plate with horizontally polarized input.

HWP Angle (°)	**Transformation**	**Result**
0	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \|H\rangle$
45	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \|V\rangle$
22.5	$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \|D\rangle$
67.5	$\begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = -\|A\rangle$

Note that the result for the anti-diagonal state differs from the conventional representation by a global phase factor of -1, however, as discussed in Section 2.2.5, both representations describe physically identical states.

For the measurement process, Bob needs to implement a projective measurement that allows him to distinguish between the possible polarization states sent by Alice. The projective measurements for rectilinear and diagonal bases are $\{|H\rangle\langle H|, |V\rangle\langle V|\}$ and $\{|D\rangle\langle D|, |A\rangle\langle A|\}$, respectively. To implement them, Bob passes the incoming photons through another HWP and a polarizing beam splitter (PBS), an optical element that separates light based on its linear polarization, typically transmitting horizontal and reflecting vertical. This way, Bob can model a measurement in both basis depending on the angle the HWP is set to. This process is depicted in Table 3.3.

TABLE 3.3: Transformations for each projective measurement: 0° (rectilinear) and 22.5° (diagonal)

Incoming State	Transformation with HWP	Result
$\lvert H\rangle = \begin{pmatrix}1\\0\end{pmatrix}$	$U_{HWP}(0)\lvert H\rangle = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix} = \lvert H\rangle$
$\lvert V\rangle = \begin{pmatrix}0\\1\end{pmatrix}$	$U_{HWP}(0)\lvert V\rangle = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\-1\end{pmatrix} = -\lvert V\rangle$
$\lvert D\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$U_{HWP}(22.5)\lvert D\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix} = \lvert H\rangle$
$\lvert A\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$U_{HWP}(22.5)\lvert A\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix} = \lvert V\rangle$

This process is analogous as the one described in Section 2.3.1 for a measurement in the Hadamard basis. The PBS models a measurement in the computational basis (here, rectilinear), while the operator $U_{HWP}(22.5)$ is equivalent to the Hadamard gate. In Figure 3.2 an schematic diagram of the prepare and measure process is shown.

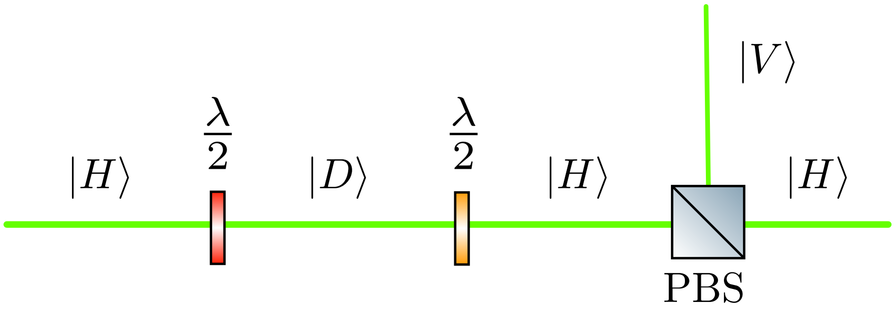


FIGURE 3.2: Example of state preparation and measurement. Red HWP ($\lambda/2$) rotated 22.5° prepares $\lvert D\rangle$ state. Orange HWP rotated 22.5° transforms back $\lvert D\rangle$ to $\lvert H\rangle$ state. The PBS splits the incoming state into its horizontal and vertical components.

3.2.3 Protocol Implementation

A classical bit can be encoded in photon polarization as shown in Table 3.4. In the rectilinear basis, 0 is represented by horizontal polarization, and 1 is represented by vertical polarization. In the diagonal basis, 0 is represented by diagonal and 1 is represented by anti-diagonal polarization.

TABLE 3.4: Photon polarization encoding in two mutually unbiased bases.

Basis	0	1
Rectilinear $\oplus$	$\lvert H\rangle$	$\lvert V\rangle$
Diagonal $\otimes$	$\lvert D\rangle$	$\lvert A\rangle$

The protocol consists of two stages: first is **quantum transmission**, in which Alice and Bob prepare, send and measure quantum states, and second is **classical post-processing**, where Alice and Bob communicate through the classical channel to convert the previously obtained bit sequences into secure keys [6].

Quantum Transmission

1. Alice generates a string of n random classical bits which denote her key.
2. Alice generates a sequence of n random polarization bases, choosing between the rectilinear $\oplus$ or the diagonal $\otimes$.
3. Alice encodes her bit string into a sequence of photons with polarization according to the selected bases, as shown in Table 3.4.
4. Bob receives the photons and decides randomly for each photon whether to measure it on the rectilinear basis or on the diagonal basis, obtaining his own key.

Classical Post-processing

5. Bob makes public the information about the bases he used to measure the photons sent by Alice.
6. Alice compares bases with the ones she used in the preparation process and tells Bob which of her choices matched. Then, both of them discard the bits where the encoding and measurement bases did not match.
7. Alice and Bob test for eavesdropping by publicly comparing some of the bits. Bob randomly reveals some bits of his key and Alice confirms them. If Eve has not interfered, all the comparisons must agree and the remaining bits can be used.

Table 3.5 illustrates a typical example of the BB84 protocol. If Eve attempts to intercept a quantum state sent by Alice, her intervention will disturb the state. When Bob and Alice use the same basis, Bob should normally receive the bit that Alice sent. However, Eve's interference can alter the quantum state so that Bob's measurement yields a random bit. During the eavesdropping check, Alice and Bob compare portions of their bit strings where any discrepancies reveal that the key exchange has been compromised.

TABLE 3.5: BB84 Protocol Example. Implementation of the BB84 protocol, assuming that no eavesdropping takes place.

Quantum Transmission								
Alice's random bits	0	1	1	0	1	0	0	1
Random preparation bases	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Photons sent by Alice	$\vert\swarrow\!\!\!\!\!\nearrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nwarrow\!\!\!\!\!\searrow\rangle$	$\vert\swarrow\!\!\!\!\!\nearrow\rangle$	$\vert\nwarrow\!\!\!\!\!\searrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\nwarrow\!\!\!\!\!\searrow\rangle$
Random measurement bases	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$
Bits received by Bob	0	1	1	1	0	0	0	1
Classical Post-processing								
Matching bases	OK	OK	OK				OK	OK
Presumably shared information	0	1	1				0	1
Bits revealed by Bob	0							1
Bits confirmed by Alice	OK							OK
Result								
Shared secret key		1	1				0	

3.3 Experimental Setup

The security of the BB84 protocol relies on theoretical assumptions such as the use of ideal single-photon sources and perfect detection devices [42]. This is because any deviation from these conditions can introduce vulnerabilities that an eavesdropper could exploit [8, 9, 43]. However, such technology is not entirely practical for industrial or large-scale applications. For this reason, many experimental implementations of QKD rely on weak coherent state sources and threshold detectors [7, 43].

A coherent source refers to a light source with a well-defined phase relationship, meaning that the electromagnetic waves maintain a consistent phase over time [38]. The most classic example of a coherent light source is the laser (Light Amplification by Stimulated Emission of Radiation). A highly attenuated laser results in a weak coherent source, which can serve as an approximation of an ideal single-photon source [42].

On the other hand, a threshold detector is a type of single-photon detector that provides only a binary response, indicating whether one or more photons have been detected, without distinguishing the exact number [44, 45]. A QKD setup based on these components is depicted in Figure 3.3.

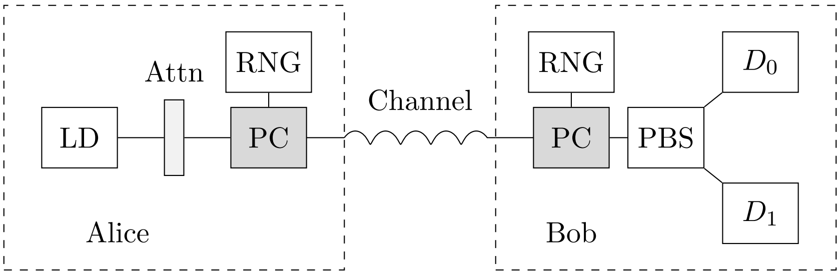


FIGURE 3.3: A schematic representation of a generic QKD setup based on a weak coherent source and threshold detectors. LD: laser diode; Attn: optical attenuator; RNG: random number generator; PC: polarization controller; PBS: polarization beam splitter; D_0, D_1: single-photon detectors. Adapted from [42].

In this layout, Alice attenuates the light from a laser diode (LD) using an optical attenuator (Attn) to generate weak coherent states. She uses a random number generator (RNG) to select a basis—either rectilinear or diagonal—and a corresponding bit value, encoding the information via a polarization controller (PC). Bob uses another polarization controller to randomly choose his measurement basis, also determined by an RNG. The photons then pass through a polarization beam splitter (PBS), which separates them based on their polarization toward one of the two threshold detectors, D_0 or D_1.

3.4 Experimental Model

A practical QKD system consists of three main components: the source, the quantum channel, and the detection system. The model described below follows a widely accepted theoretical framework for a QKD implementation based on weak coherent sources, where it is assumed that Alice sends quantum signals as laser pulses [43].

3.4.1 Weak Coherent State Source

A weak coherent source can be well described by a weak coherent state, which is as superposition of *number states* $|n\rangle$, representing well-defined photon numbers, where n indicates exactly n photons present in the laser pulse:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{3.5}$$

Assuming that the phase of the laser is randomized for each pulse, the emitted state can be described by the density operator [46]:

$$\begin{aligned}
\rho &= \frac{1}{2\pi}\int_0^{2\pi} d\theta\, |\alpha e^{i\theta}\rangle\langle\alpha e^{i\theta}| \\
&= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} e^{-|\alpha|^2}\frac{\alpha^n(\alpha^*)^m}{\sqrt{n!m!}}\,|n\rangle\langle m|\left(\frac{1}{2\pi}\int_0^{2\pi} e^{i(n-m)\theta}\,d\theta\right) \\
&= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} e^{-|\alpha|^2}\frac{\alpha^n(\alpha^*)^m}{\sqrt{n!m!}}\,|n\rangle\langle m|\,\delta_{nm} \\
&= \sum_{n=0}^{\infty} e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!}\,|n\rangle\langle n| \\
&= \sum_{n=0}^{\infty}\frac{\mu^n}{n!}\,e^{-\mu}\,|n\rangle\langle n|
\end{aligned} \tag{3.6}$$

where $\mu = |\alpha|^2$ is the mean photon number (MPN) of the source. Thus, the photon number follows a Poisson distribution:

$$P(n) = \frac{\mu^n}{n!}e^{-\mu}. \tag{3.7}$$

This probability distribution results in three relevant types of photon states:

1. **Vacuum state**: $|0\rangle\langle 0|$
2. **Single-photon state**: $|1\rangle\langle 1|$
3. **Multi-photon state**: $|n\rangle\langle n|$ for $n \geq 2$

Here, the worst case scenario is assumed, where every pulse transmitted by Alice is intercepted by Eve, attacking each signal individually [43]. Under this assumption, Eve is free to perform any operation on the intercepted pulse before forwarding to Bob either a vacuum state or a qubit. As a result, the qubits arriving at Bob are categorized into three types: vacuum qubits, single photon qubits, and multi photon qubits [42].

A vacuum state arises when Alice's pulse contains no photons; in scenarios without Eve's intervention, detections associated with such states are generated by detector dark counts or other sources of background noise, and they do not contribute to the secure key. On the other hand, multi-photon qubits are inherently vulnerable to *photon-number splitting attacks*,—explained in the following chapter—which compromise the security of the final key. Therefore, in this QKD model only the qubits corresponding to single-photon states are secure and can be used to extract the final secure key [42].

3.4.2 Quantum Channel and Detection System

After traversing the quantum channel, where they are subject to losses, quantum signals prepared by Alice reach Bob's detection system, which attempts to register their arrival. The overall efficiency and accuracy of this process affects the performance and security of the QKD protocol. To quantify these aspects, the metrics defined below are employed.

Transmittance: A beam splitter followed by an ideal single photon detector are employed to model both the channel and the detection process. The channel losses are related to the transmission distance l and the loss coefficient of the channel β measured in dB/km [13]. Therefore, the channel transmission efficiency is given by:

$$t_{AB} = 10^{-\frac{\beta l}{10}}. \tag{3.8}$$

The detection efficiency, η_B, on Bob's side includes both internal transmission efficiency of optical components, t_B, and detector efficiency η_D. Thus:

$$\eta_B = t_B \eta_D. \tag{3.9}$$

The overall transmission and detection efficiency between Alice and Bob is then:

$$\eta = t_{AB}\, \eta_B. \tag{3.10}$$

Since threshold detectors are employed, vacuum states can be distinguished from non-vacuum states. However the actual number of photons in the pulse cannot be resolved. In addition, independence in the behavior of the n photons of each n-photon state is assumed, due to separate interactions in the channel. As a result, the overall transmission efficiency for an n-photon state with respect to a threshold detector is given by:

$$\eta_n = 1 - (1 - \eta)^n. \tag{3.11}$$

Yield: The yield Y_n of an n-photon state represents the conditional probability of a detection event at Bob's end, given that Alice transmits an n-photon state. Y_0 corresponds to the background rate, which encompasses detector dark counts and other background disturbances. The yield comes of two parts: one coming from the detection of signal photons and the other from the dark counts of the detectors. Assuming that background counts are independent of the actual photon signal detection, the yield is given by:

$$\begin{aligned} Y_n &= Y_0 + \eta_n - Y_0 \eta_n \\ &\cong Y_0 + \eta_n. \end{aligned} \tag{3.12}$$

Where it is assumed that Y_0 and η are small.

Gain: The gain Q_n is the product of the probability of Alice sending out an n-photon state and the conditional probability of Alice's n-photon state will lead to a detection event in Bob's detection system. It is given by:

$$Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu}. \tag{3.13}$$

It represents the probability that Alice sends out an n-photon state and Bob obtains a detection. Summing over all Q_ns, we get the overall gain Q_μ, which is the probability for Bob to obtain a detection event in one pulse:

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu}. \tag{3.14}$$

Quantum Bit Error Rate (QBER): The error rate e_n for an n-photon state is defined as the ratio of the error contributions from Bob's detection events. It is given by:

$$e_n = \frac{e_0 Y_0 + e_d \eta_n}{Y_n}, \tag{3.15}$$

where e_d is the probability that a photon having successfully passed Bob's polarization controller (see Figure 3.3), hits the erroneous detector, which characterizes the alignment and stability of the optical system. e_0 is the error rate of the background, assumed random, thus $e_0 = 1/2$. The overall QBER is then expressed as:

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu}. \tag{3.16}$$

Because of Eve's interference, she can change Y_n and e_n. Without Eve, photon statistics remains the same, thus Eqs. 3.11 to 3.15 are satisfied for all $n = 0, 1, 2, \ldots,$ and the overall gain and QBER are:

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu}. \tag{3.17}$$

$$E_\mu Q_\mu = e_0 Y_0 + e_d (1 - e^{-\eta\mu}). \tag{3.18}$$

Chapter 4

Decoy States Protocol

This chapter examines common eavesdropping attacks on QKD protocols and introduces the decoy state technique as a solution to attacks exploiting multi-photon pulses. First, the fundamental Intercept-Resend attack is discussed. Next, the Photon-Number Splitting (PNS) is examined, explaining how an eavesdropper can evade detection with an extended version of the attack. Following this, the Beam Splitting attack is introduced as a more feasible method requiring less technology than PNS. Finally, the chapter details the decoy-state method as a countermeasure designed to detect attacks like PNS.

4.1 Eavesdropping Strategies

As already mentioned in previous chapters, imperfections in the hardware used for implementing a QKD setup can be exploited in order to allow an eavesdropper to gain information about the secret key. However, the strategies available to Eve are fundamentally limited by quantum mechanics and currently available technology.

4.1.1 Intercept and Resend Attack

When the source, channel and detectors used for quantum transmission are perfect, Eve's attack capability is greatly reduced. In fact, the only option available to her is the *intercept-resend* attack. It consists of Eve capturing the photons sent by Alice, measuring them and sending them back to Bob. Since Alice's source is perfect, the photons captured by Eve are individual photons, so she can do nothing more than select a random basis and measure them, just as Bob would do. Failure to resend the photons could compromise her presence during the quantum transmission stage.

As mentioned in Subsection 3.2.3, this can be easily detected by Alice and Bob after performing the eavesdropping check during the classical post-processing stage, however, it is worth identifying the possible scenarios when Eve is present.

Let $\mathcal{K}_{\mathcal{A}}$ be Alice's original random key string, $\mathcal{A}$ Alice's random preparation basis sequence, and let $\mathcal{E}$ and $\mathcal{B}$ be Eve's and Bob's random measurement basis sequence, respectively. Then, the following scenarios can happen during quantum transmission:

Eve chooses the correct basis: $\mathcal{E}_i = \mathcal{A}_i \longrightarrow$ Qubit is unaltered.

Bob chooses the correct basis: $\mathcal{B}_i = \mathcal{A}_i \longrightarrow$ Eve is undetected and has one key bit.

Bob chooses the incorrect basis: $\mathcal{B}_i \neq \mathcal{A}_i \longrightarrow$ Random outcome, Eve is undetected.

Eve chooses the incorrect basis: $\mathcal{E}_i \neq \mathcal{A}_i \longrightarrow$ Qubit is altered.

Bob chooses the correct basis: $\mathcal{B}_i = \mathcal{A}_i \longrightarrow$ Eve introduces error with 50% probability.

Bob chooses the incorrect basis: $\mathcal{B}_i \neq \mathcal{A}_i \longrightarrow$ Random outcome, Eve is undetected.

These scenarios reveal that Eve's action goes undetected 75% of the time. The remaining 25%, Bob could obtain an error even though he measured in the correct basis [47]. Applying the eavesdropping check, Alice and Bob sacrifice a fraction of the obtained key $\mathcal{K}_{\mathcal{B}}$ in order to discover Eve. The more bits they compare, the higher the probability of catching her. Thus, they have to compromise in the amount of bits they want to sacrifice in order to detect Eve's presence while still getting an usable key.

Assuming an initial key $\mathcal{K}_{\mathcal{A}}$ of n bits, the length of the resulting key, also called sifted key, is approximately $n/2$. If Alice and Bob compare one bit of their keys, the probability of having a match is 75%. For a selection of $\tilde{n}$ bits, the probability of every bit matching represents the chance of Eve's evading detection [47]. Therefore, the probability of detecting Eve that Alice and Bob wish to have above a confident threshold is given by:

$$p_d = 1 - (0.75)^{\tilde{n}}, \quad \tilde{n} < \frac{n}{2} \tag{4.1}$$

Figure 4.1 plots Eq. 4.1 as a function of the number of compared bits $\tilde{n}$. For an initial key $\mathcal{K}_{\mathcal{A}}$ of $n = 100$ bits, a reasonable value for $\tilde{n}$ of one third of the sifted key yields:

$$\tilde{n} = \left\lfloor \frac{|\mathcal{K}_{\mathcal{B}}|}{3} \right\rfloor = \left\lfloor \frac{n}{6} \right\rfloor = 16, \quad p_d = 0.9899$$

From the above it is possible to conclude that in order to have a high probability of detecting Eve, while also obtaining a sufficiently long usable key, Alice needs to increase the number of qubits she sends to Bob.

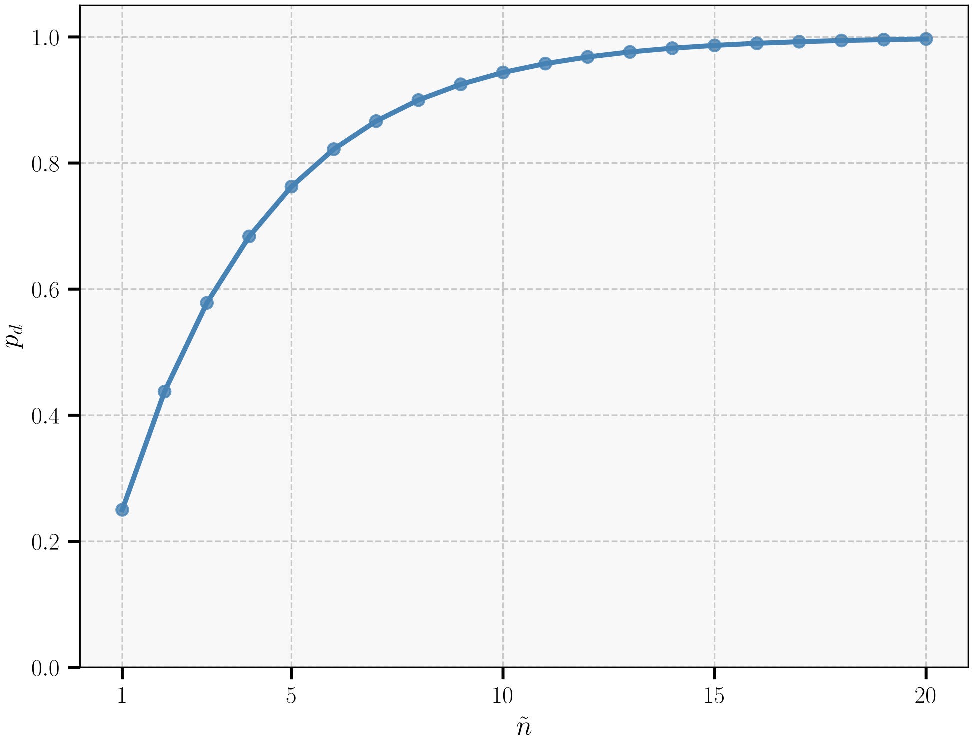


FIGURE 4.1: Eve's detection probability p_d as a function of the number of compared bits $\tilde{n}$. Adapted from [47].

4.1.2 Photon-Number Splitting Attack

Another strategy consists in exploiting imperfections in the quantum channel to gain information about the secret key. A critical vulnerability arises from multi-photon signals—pulses containing two or more photons—generated by weak coherent sources [7, 8]. If Eve replaces the noisy, lossy quantum channel with a superior one, the improved transmission gives her room to launch the photon-number splitting attack.

This attack consist in Eve performing a *quantum non-demoilition* (QND) measurement, which allows her to gain information about the photon number in the pulse without disturbing other degrees of freedom, such as the polarization of the photons [43, 48].

A QND measurement is a type of quantum measurement where the act of measuring a particular observable of a quantum system does not perturb the value of that observable itself for subsequent measurements. The core principle is to maintain the predictability of a subsequent measurement of the measured observable, while avoiding the random back-action[1] on this observable that would typically arise from the uncertainty introduced into a non-commuting observable due to the measurement process [48]. In the context

[1] The unpredictable disturbance inherent in quantum measurement that affects the system.

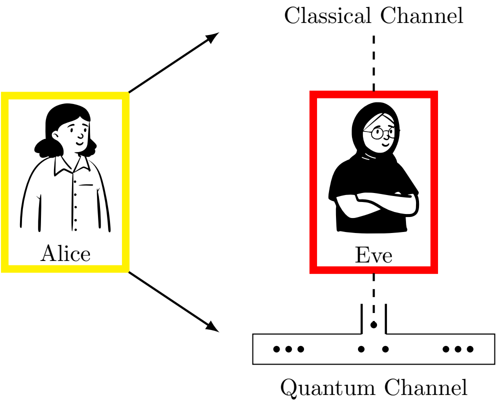


Figure 4.2: Photon-Number Splitting (PNS) attack. Eve performs a quantum non-demolition measurement to detect multi-photon signals, intercepting one photon from such signals while forwarding the remaining photons to Bob.

of the PNS attack, Eve's QND measurement is designed to determine the number of photons in a pulse without disturbing the polarization state of the photons.

For multi-photon signals, Eve retains one photon while forwarding the remaining ones to Bob, as illustrated in Figure 4.2. Eve then stores her captured photon in quantum memory until the public discussion phase, where Alice and Bob reveal the basis used for encoding. Once the basis is known, Eve measures her stored photon to deterministically learn the polarization—and thus the bit value—of the signal [7].

The attack's effectiveness depends on the channel's inherent loss. If losses are sufficiently high, Eve can selectively block single-photon pulses and forward only multi-photon signals to Bob, such that the rate at which he receives non-empty pulses remains as expected. This ensures she obtains full information about all bits received by Bob, as multi-photon pulses are entirely compromised. When losses are lower, Eve partially blocks single-photon signals and combines this with optimal eavesdropping strategies on the remaining single-photon pulses, maximizing her information gain [43].

4.1.3 Extended Photon-Number Splitting Attack

Even though the PNS attack compromises the BB84 protocol, its implementation alters the photon-number statistics observed by Bob, potentially revealing Eve's presence. For instance, the attack reduces the fraction of single-photon signals while increasing multi-photon counts, which could be detected through monitoring of the received photon-number distribution. As a result, Eve must ensure that the photon-number distribution arriving at Bob's detectors matches the expected Poissonian distribution of a lossy channel. This motivates an extended PNS attack that preserves the complete photon-number statistics so that Eve can remain undetected. The following section summarizes the extended PNS attack as developed by Lütkenhaus and Jahma [9].

In a lossy channel with transmission efficiency η_c, the photon-number distribution at Bob's end follows a Poissonian distribution with mean photon number $\eta_c\mu$:

$$P_{loss}[n] = \frac{(\eta_c\mu)^n}{n!}e^{-\mu\eta_c} \tag{4.2}$$

In contrast, the PNS attack where Eve blocks a fraction b of the single-photon signals results in a non-Poissonian photon number distribution:

$$P_{\mathrm{PNS}}[n] = \begin{cases} (1+b\mu)e^{-\mu} & n=0 \\ [(1-b)\mu + \frac{\mu^2}{2}]e^{-\mu} & n=1 \\ \frac{\mu^{n+1}}{(n+1)!}e^{-\mu} & n \geq 2 \end{cases} \tag{4.3}$$

As a first step to remain undetected, Eve adjusts b to match the vacuum probability $P_{loss}[0] = P_{PNS}[0]$. While this condition ensures that the probability of vacuum events at Bob's detectors remains unchanged, it does not yet guarantee that the entire photon-number distribution is indistinguishable from a lossy Poissonian source. The remaining discrepancies come from the altered distribution of single-photon and multi-photon pulses, which must be adjusted to avoid detection.

However, since Eve cannot increase the number of single-photon pulses but can redistribute the multi-photon pulses, she must rely on an additional strategy to eliminate the statistical discrepancies. The key observation is that multi-photon pulses can be selectively manipulated to rebalance the photon-number distribution while preserving the expected mean photon count.

This is achieved by probabilistically extracting additional photons from multi-photon signals. Specifically, Eve can introduce a controlled redistribution such that the probability of detecting a given photon number at Bob's detectors matches the expected Poissonian statistics of a lossy channel. This redistribution is constrained by the requirement that no photons be artificially inserted into a pulse, ensuring that:

$$\sum_{i=0}^{n} P_{PNS}[i] \leq \sum_{i=0}^{n} P_{loss}[i], \quad \forall n. \tag{4.4}$$

This condition guarantees that the probability flow is always directed from higher photon-number states to lower ones, a process that Eve can implement by strategically extracting photons from pulses containing two or more photons.

Since Eve can manipulate photon statistics without introducing detectable anomalies, conventional countermeasures such as monitoring the photon-number distribution are insufficient. The security of QKD thus requires additional safeguards, such as protocols that actively test for inconsistencies in photon detection (e.g. the decoy-state protocol) [11] or encoding strategies that minimize the impact of multi-photon pulses [12, 13].

4.1.4 Beam Splitting Attack

While the PNS attack represents a significant threat to QKD protocols, its implementation requires sophisticated technology in terms of performing the QND measurement. A simpler and more feasible eavesdropping strategy, requiring less advanced technology than PNS, is the Beam-Splitting (BS) attack [10, 49].

In a beam splitting attack, Eve positions herself in the quantum channel and uses a beam splitter[2] to divert a portion of the transmitted pulse's intensity towards her, while the remaining part of the pulse continues towards Bob. Similarly to the PNS attack, the BS attack can be viewed as Eve simulating the effect of a lossy quantum channel. In this case, the lossy channel acts as combination of a perfect channel followed by a beam splitter with a certain transmission efficiency η which accounts for the losses.

Eve could potentially perform a delayed measurement analogously to the PNS attack, if a multi-photon signal is split such that Bob and Eve both get at least one photon from the signal, thus gaining complete knowledge of that bit. For a pulse with a mean photon number μ transmitted through a channel with single-photon transmission efficiency η_c, the probability that Bob receives a non-vacuum signal is given by:

$$P_{BS}[n] = 1 - e^{-\mu\eta_c}, \quad n \geq 1. \tag{4.5}$$

On the other hand, the probability that both Bob and Eve receive a signal is

$$P_{BS}^{Succes} = [1 - e^{-\mu\eta_c}][1 - e^{-\mu(1-\eta_c)}]. \tag{4.6}$$

Despite its simplicity and accurate simulation of a lossy channel, the BS attack becomes highly ineffective when used to replace channels with significant losses. This is because multi-photon pulses are more likely to be entirely directed to Eve, rather than being split such that both Eve and Bob receive photons from the same pulse. However, the BS attack remains a more technologically accessible strategy compared to the PNS attack.

[2] A beam splitter is an optical device that divides a beam of light into two separate beams. Unlike a polarizing beam splitter, which separates light based on its polarization, a standard beam splitter splits light based on its intensity, allowing a certain fraction to pass through and reflecting the rest.

4.2 Decoy States

The decoy state method was originally proposed by Hwang [11] as a solution to the PNS attack, and subsequently refined and optimized by Lo and colleagues [12, 13]. It addresses the vulnerability to PNS attacks by enabling Alice and Bob to detect eavesdropping through statistical monitoring of photon yields. It consists in introducing *decoy* states with varying intensities, to allow the legitimate parties to verify the integrity of the quantum channel and identify anomalies caused by Eve's interference.

4.2.1 Security Condition

To ensure security, Alice randomly alternates between two types of pulses: signal states, used for key generation, and decoy states, used channel monitoring. The essence of the method is that Eve cannot distinguish between signal and decoy pulses, as they share identical physical characteristics (e.g., wavelength, timing, etc.), she can only determine the number of photons in each pulse and therefore, she has to apply the same strategy to all of them. Hence, the yield Y_n and QBER e_n are determined only by the photon number n regardless of whether the state comes from a decoy or a signal source, satisfying:

$$\begin{aligned} Y_n &= Y_n^{signal} = Y_n^{decoy} \\ e_n &= e_n^{signal} = e_n^{decoy} \end{aligned} \tag{4.7}$$

In the ideal theoretical case, it is considered that Alice could use an infinite number of possible intensities for the decoy states. When Alice randomly varies the intensity μ of each pulse, she and Bob can experimentally measure the overall gain Q_μ and the overall QBER E_μ for each intensity used. Since the relationships between Q_μ's and Y_n's and between E_μ and e_n are linear, given Q_μ's and E_μ's, they can mathematically deduce with high confidence Y_n and e_n for each photon number n [12].

This means that Alice and Bob can simultaneously verify the yields and error rates for all n-photon states and, knowing the normal properties of their channel, determine which ranges of values are acceptable. Any attempt by Eve to manipulate the channel will inevitably alter some of these Y_n or e_n values, which will be detected with high probability. To avoid being discovered, Eve is left with very limited options in her attack, which significantly strengthens Alice and Bob's ability to detect eavesdropping.

Generally speaking, decoy-state research has focused on increasing two important aspects of QKD performance: *secure key rate*, which is the average number of final secure key bits from one pulse; and *maximal secure distance*, which is the maximal QKD transmission distance that can yield a positive key rate for a certain setup. For that, a widely adopted implementation of the decoy state method has been the **Vacuum+Weak** decoy scheme, which uses one weak decoy state with a mean photon number lower than that of the signal state, and an additional vacuum state with zero photons [13, 42]. Nonetheless, not much discussion had been made about the decoy-state protocol's effectiveness to detect PNS attacks until the work of Mailloux and colleagues [14–18].

4.2.2 Vacuum+Weak Decoy State

In Vacuum+Weak, the vacuum state is used to detect background and dark counts in the detector, while the weak decoy state helps estimate the fraction of single-photon events and detect the PNS attack. Using Eqs. 3.17 and 3.18 for the *vacuum* state:

$$\begin{aligned} Q_{vac} &= Y_0 \\ E_{vac} &= e_0 = \frac{1}{2} \end{aligned} \tag{4.8}$$

During quantum transmission, Alice randomly prepares each pulse as either a signal, decoy, or vacuum state according to predefined probability distributions and mean photon numbers [16]. Alice and Bob then proceed with the classical post-processing phase, where they publicly announce the bases used for each pulse while also disclosing whether each pulse was a signal, decoy, or vacuum state. Denoting μ as the signal state MPN and ν as the decoy state MPN, Alice and Bob can measure Q_μ, Q_ν and Q_{vac} as:

$$Q_\mu = \frac{\text{Number of signal state detections}}{\text{Number of signal state pulses sent}}, \tag{4.9}$$

$$Q_\nu = \frac{\text{Number of decoy state detections}}{\text{Number of decoy state pulses sent}}, \tag{4.10}$$

$$Y_0 = \frac{\text{Number of vacuum state detections}}{\text{Number of vacuum state pulses sent}}. \tag{4.11}$$

Solving Eq. 3.17 for η and plugging the measured gains, we obtain each state efficiency:

$$\begin{aligned} \eta^{(\mu)} &= -\frac{\ln|1 + Y_0 - Q_\mu|}{\mu} \\ \eta^{(\nu)} &= -\frac{\ln|1 + Y_0 - Q_\nu|}{\nu} \end{aligned} \tag{4.12}$$

Finally, we can compute the n-photon expected yields Y_n, signal state yields Y_n^μ and decoy state yields Y_n, using Eqs. 3.10, 3.12, and 4.12. Since higher order contributions of Y_n in 3.14 decay by a factorial factor, the unknowns can be chopped off to a finite small number $n = 1 \ldots 5$. If no eavesdropping took place, the security condition 4.7 should hold, otherwise, Eve's prescience is detected [17, 18].

Chapter 5

Simulation Results

This chapter shows the simulations performed for both the implementation of the BB84 protocol and the integration of the decoy state technique. The construction performed in each case is described, as well as the results obtained for each of the implementations.

5.1 BB84 Protocol Simulation

In order to visualize the implementation of the BB84 protocol, an interactive simulation was developed using Qiskit and Streamlit. Qiskit is an open source Software Development Kit (SDK) developed by IBM to run programs via the cloud on IBM quantum computers, or locally via simulation backends. On the other hand, Streamlit is an open source framework that enables the generation of dynamic web applications for data visualization through Python scripting.

5.1.1 Qiskit Implementation

From Chapters 2 and 3, we see that the states used in the BB84 protocol can be represented through the computational basis states, and the Hadamard basis states, as:

$$\begin{aligned} |H\rangle &\longmapsto |0\rangle \\ |V\rangle &\longmapsto |1\rangle \\ |D\rangle &\longmapsto |+\rangle \\ |A\rangle &\longmapsto |-\rangle \end{aligned} \tag{5.1}$$

Using Qiskit, we can generate these states through the combined action of the X and H gates, as discussed in Section 2.3.1. Additionally, the respective process of measuring in the rectilinear and diagonal basis, can be modeled with the corresponding projection operators of the Z and X basis, where a measurement in the X basis is equivalent to applying a Hadamard gate followed by a measurement in the Z basis.

Figure 5.1 shows the corresponding circuit diagram for preparing and measuring each of the states in the correct basis. As explained in Section 2.3.2, each horizontal line in the diagram represents a qubit, initialized in an initial state—$|0\rangle$ by default—on which quantum gates act from left to right. The measurement symbol indicates a projective measurement, and the double horizontal line represents the classical register where the outcome of the measurement is recorded. The dashed vertical line indicates a separation between the state preparation stage on the left and the measurement stage on the right.

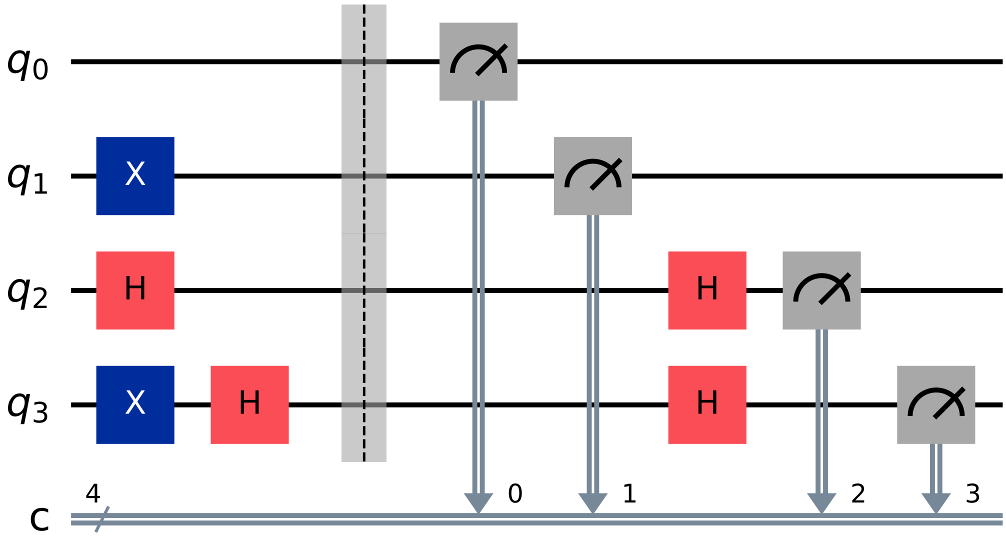
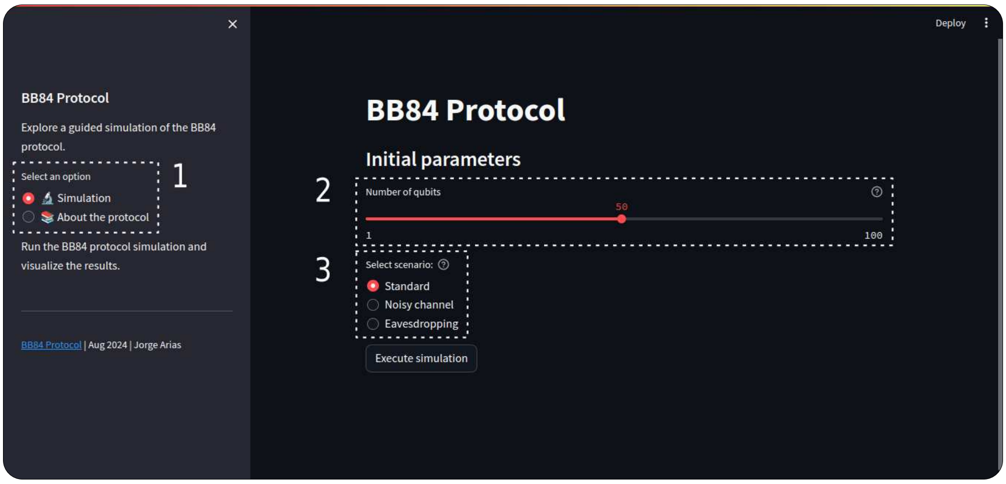


FIGURE 5.1: Quantum circuit showing the preparation and measurement of the Computational and Hadamard basis states. From top to bottom: $|0\rangle$ (default setting, measured in Z-basis), $|1\rangle$ (prepared with X-gate, measured in Z-basis), $|+\rangle$ (prepared with H-gate, measured in X-basis) and $|-\rangle$ (prepared with X and H-gates, measured in X-basis).

Although Figure 5.1 represents a 4-qubit circuit, each row can be seen as an individual single-qubit circuit demonstrating the state preparation and measurement in the correct basis. As mentioned in Section 3.2.1, if a qubit from the computational basis is measured in the Hadamard basis, it would yield a classical outcome of 0 or 1 with equal probability. In this BB84 Protocol Simulation, each circuit is run using exactly one shot (see Section 2.3.2), so that one circuit execution corresponds directly to one photon detection event. Since each shot incorporates the intrinsic randomness of a the measurement, increasing the number of shots would not alter the statistics, only the runtime.

5.1.2 Interactive Simulation

The result of the simulation is a Streamlit application with an interactive GUI (see Figure 5.2), which shows the step-by-step of the protocol described in Subsection 3.2.3.



BB84 Protocol

Explore a guided simulation of the BB84 protocol.

Select an option

● Simulation

○ About the protocol

Run the BB84 protocol simulation and visualize the results.

BB84 Protocol | Aug 2024 | Jorge Arias

BB84 Protocol

Initial parameters

Number of qubits: 50 (1–100)

Select scenario:

● Standard

○ Noisy channel

○ Eavesdropping

FIGURE 5.2: User interface of the Streamlit web application developed for simulating the BB84 protocol.

Segment 1 presents two options, About the Protocol, which displays general information about the protocol operation, and Simulation, which presents the simulation startup interface. Segment 2 is a slider component to select the number of initial qubits Alice sends to Bob. Segment 3 shows a radio button to select a simulation scenario: standard, with no eavesdropping; noisy channel, in which photon polarization may change due to the channel; and eavesdropping, where the intercept-resend attack is implemented.

The application can be found on GitHub and deployed on Streamlit Community Cloud, we encourage the reader to access these links and interact with the simulation.

5.2 Decoy States BB84 Simulation

To study the behavior of the BB84 protocol with decoy states following the Vacuum+Weak configuration, an additional and independent simulation was developed. This simulation follows the structure shown in Figure 5.3, implementing each element involved in the protocol according to the experimental model described in Section 3.4.

5.2.1 Simulation Structure

The simulation is structured as a modular system with the following components:

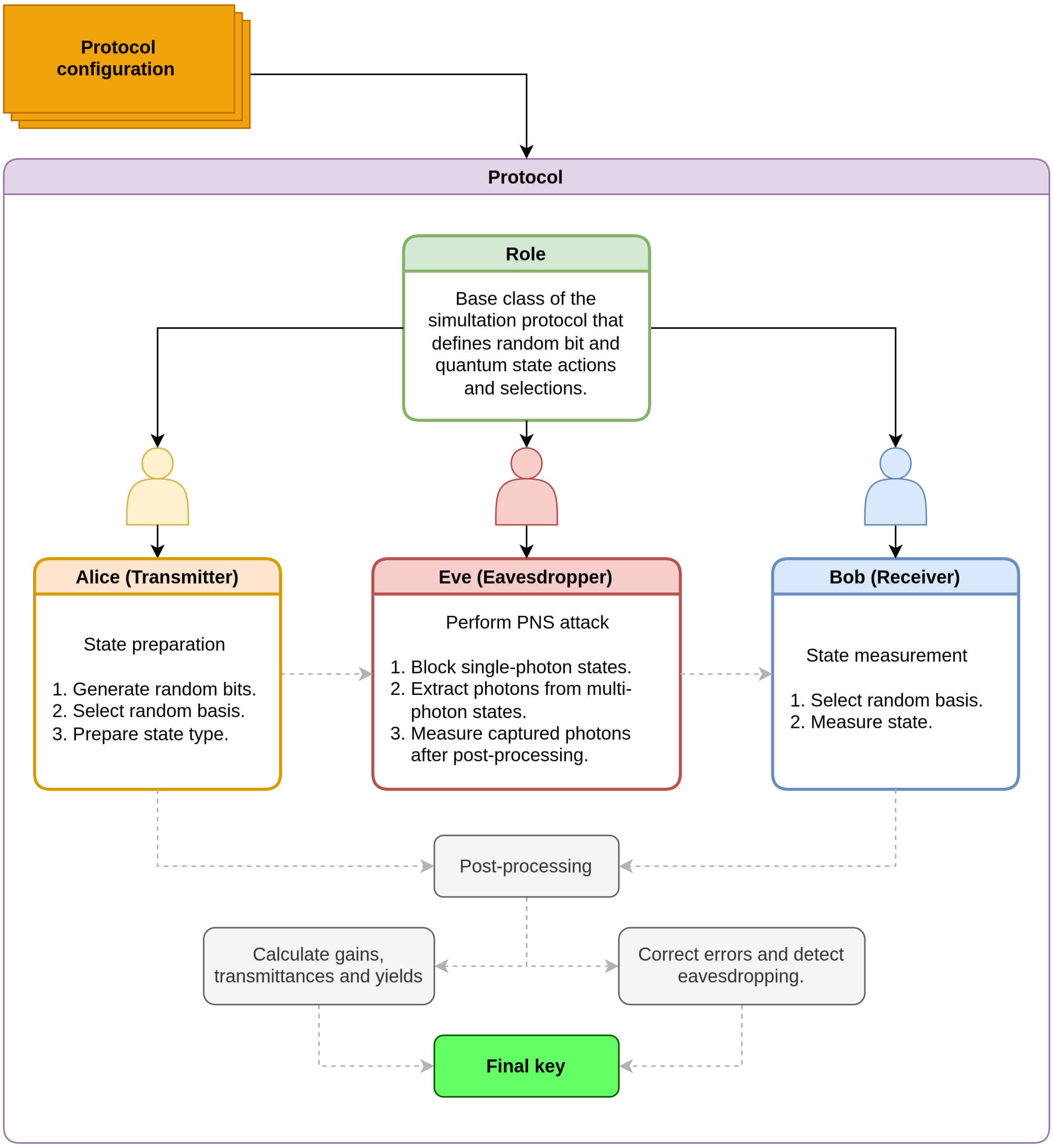

Protocol configuration
Protocol
Role
Base class of the simultation protocol that defines random bit and quantum state actions and selections.
Alice (Transmitter)
State preparation
1. Generate random bits.
2. Select random basis.
3. Prepare state type.
Eve (Eavesdropper)
Perform PNS attack
1. Block single-photon states.
2. Extract photons from multi-photon states.
3. Measure captured photons after post-processing.
Bob (Receiver)
State measurement
1. Select random basis.
2. Measure state.
Post-processing
Calculate gains, transmittances and yields
Correct errors and detect eavesdropping.
Final key

FIGURE 5.3: Schematic diagram of the BB84 protocol simulation with decoy states.

- **Quantum States**: Represented by a `State` class encapsulating a Qiskit circuit with a variable number of qubits following a Poisson distribution based on the type of state (signal, decoy, or vacuum).

- **Protocol Roles**: Implemented through a class hierarchy with a base `Role` class and specialized extensions (`Sender`, `Receiver`, `Eavesdropper`), each handling their specific protocol functions.

- **Protocol Implementation**: Provided by the `Protocol` class that manages the exchange of quantum states between roles, processes measurement results, and calculates security metrics to detect eavesdropping.

The simulation employs a singleton configuration pattern through a `Config` class to access shared parameters across components. During execution, Alice generates quantum states with Poisson-distributed photon numbers according to the intensity levels with configurable probability distributions. Each state carries a random bit value encoded in the randomly selected basis, following the BB84 protocol. If present, Eve implements the standard PNS attack described in Section 4.1.2 for a lossy channel. An optional case simulates the BS attack described in Section 4.1.4 using a variable beam splitter transmittance. Bob measures incoming states in randomly chosen bases recording detection events, while the simulation tracks which pulses resulted in successful detections. Similar to the BB84 simulation, each circuit is also run with a single shot, but because these circuits may contain multiple qubits per `State`, the logical bit is obtained by taking the majority outcome across all qubit measurements in that one shot.

5.2.2 Simulation Results

The simulation was conducted under two scenarios: standard BB84 with decoy states with and without Eve. Both scenarios maintained identical parameters and configurations to enable direct comparison of the resulting metrics. Each scenario was run 500 times with 1,000,000 initial pulses per run. Table 5 shows the parameters used for the simulation, which are based on the experimental USTC-Xingling link QKD system that is part of a three-node network communication system utilizing decoy-state quantum cryptography implemented in Hefei, China and described in [50].

Table 5.1: Simulation parameters based on the USTC-Xingling link QKD system [50]

System configuration			
Signal MPN (μ)	0.65	Signal state (%)	75
Decoy MPN (ν)	0.08	Decoy state (%)	12.5
Dark count rate	10^{-5}	Vacuum state (%)	12.5
System architecture			
Channel length	20 km	Channel loss	5.6 dB
Receiver loss	3.5 dB	Detector efficiency	10 %

The result from the scenario without eavesdropping is shown in Figure 5.4. The figure illustrates a box-plot where the expected and simulated yields for photon numbers $n = 1, 2, 3$ for both signal and decoy states are shown. The expected values Y_n were directly calculated using Eq. 3.12 with the known transmittance η, computed from the system's architecture parameters in Table 5.1. The signal and decoy state yields Y_n^μ and Y_n^ν were calculated from the derived channel efficiency based on each state's type measured gain (Eq. 4.12). Figure 5.4 demonstrates an overlap between the expected and simulated photon-number-dependent yields for each n, indicating that the system is functioning normally and is not under a PNS attack. The variation of the decoy state yields is attributed to its lower MPN, which reduces detections and thus increases deviation.

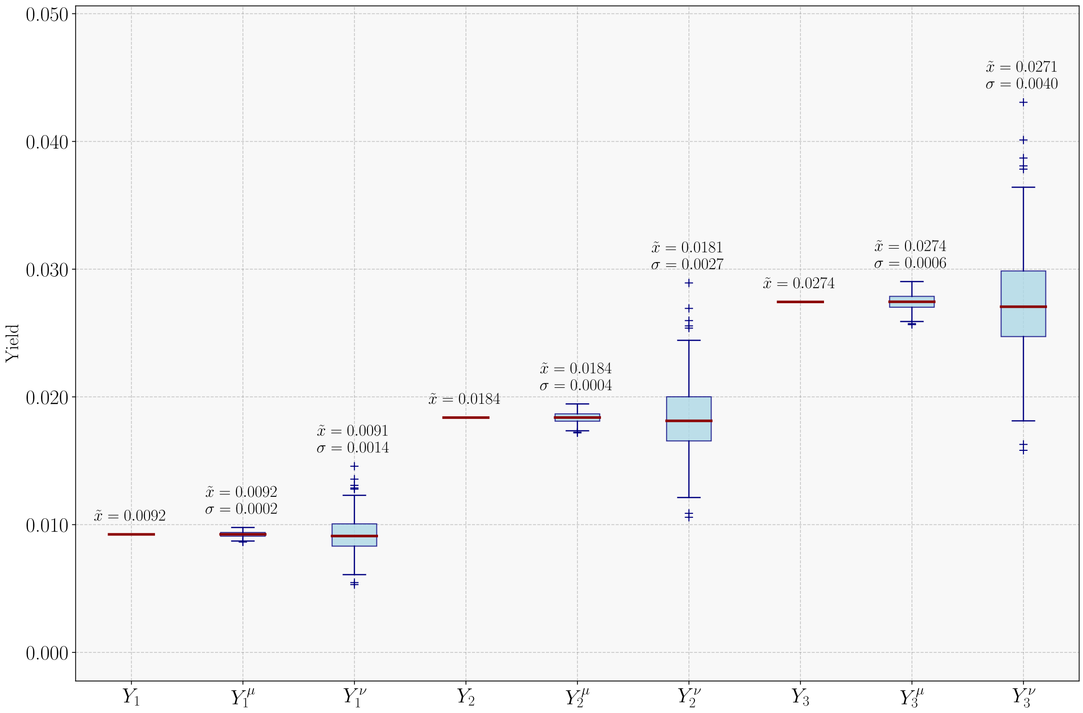


FIGURE 5.4: Results for the Vacuum+Weak QKD simulation under no eavesdropping.

In contrast, Figure 5.5 illustrates the simulation results when a standard PNS attack is implemented. The comparison between the expected and simulated yields clearly deviates for all photon numbers, indicating the presence of an eavesdropper. This deviation in yields illustrates how Eve's blocking of single-photon states and interception of multi-photon states alters detection statistics at Bob's end.

It can be noted that if Eve had knowledge of the channel's transmittance η, she could implement the Extended PNS attack discussed in Section 4.1.3 by constantly monitoring the overall photon number distribution she's sending to Bob, and comparing with the target Poissonian distribution she needs to mimmick. This would result in a matching in the expected and signal state yields $Y_n = Y_n^\mu$, but not for the decoy state yields Y_n^ν, since the lower MPN for the decoy state $\nu < \mu$ would cause fewer multi-photon states leaving Alice's source, making the redistribution from higher photon number pulses to not be as effective as with the signal state, thus revealing her presence.

Finally, an scenario of interest is the one shown in Figure 5.6, where the implementation of the most feasible BS attack is visualized. In this case, Eve's attack is carried out with a 90/10 beam splitter, which allows 90% of the photons from each pulse to pass

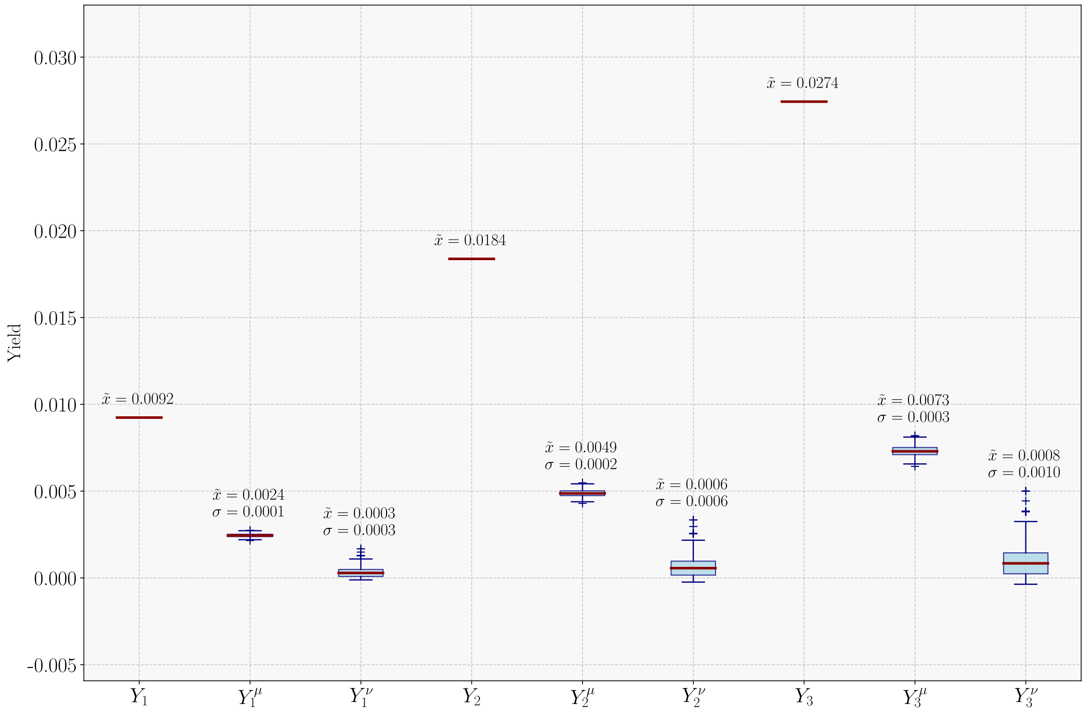


FIGURE 5.5: Results for the Vacuum+Weak QKD simulation under standard PNS attack.

through, while retaining 10% of the photons. This can be translated to an additional loss corresponding to 10% of the overall transmittance, thus $\eta_{BS} = 0.9 \times \eta$.

It can be seen that there's no overlapping between Y_n's and Y_n^μ's, with the signal state yields corresponding to effectively, 10% of the expected yields. However, overlapping between the decoy state yields and the expected yields is evident. This is due to two factors: the first, as with the previous two scenarios, has to do with the lower MPN of the decoy state. The Poissonian distribution resulting from the decoy MPN ν accounts for a decreasing in both multi-photon and single-photon states, causing fewer photon detections and increasing the variation. On the other hand, the second factor is the number of sent pulses by Alice, which is significantly small taking into account discarded pulses due to basis mismatch and occurrence percentage of decoy states.

Notice that Figure 5.6 shows how the losses caused by Eve's BS attack are applied to both signal and decoy states sent by Alice, where Y_n^μ's Y_n^ν's can be considered equal, despite the variations of the decoy states. Thus, the BS attack cannot be detected by the security condition $Y_n^\mu = Y_n^\nu$ since both photon number dependent yields are uniformly degraded. Instead, Alice and Bob can only detect Eve's presence by comparing the expected yields with those of the signal and decoy states. This requires that the quantum channel is well characterized in a secure manner, where the transmission efficiency has not been affected by Eve. If Eve manages to alter this value by inserting herself before transmission, she will remain undetected. Nonetheless, the key's information gain from the BS attack will be dependent on Eve's capability of performing a delayed measurement.

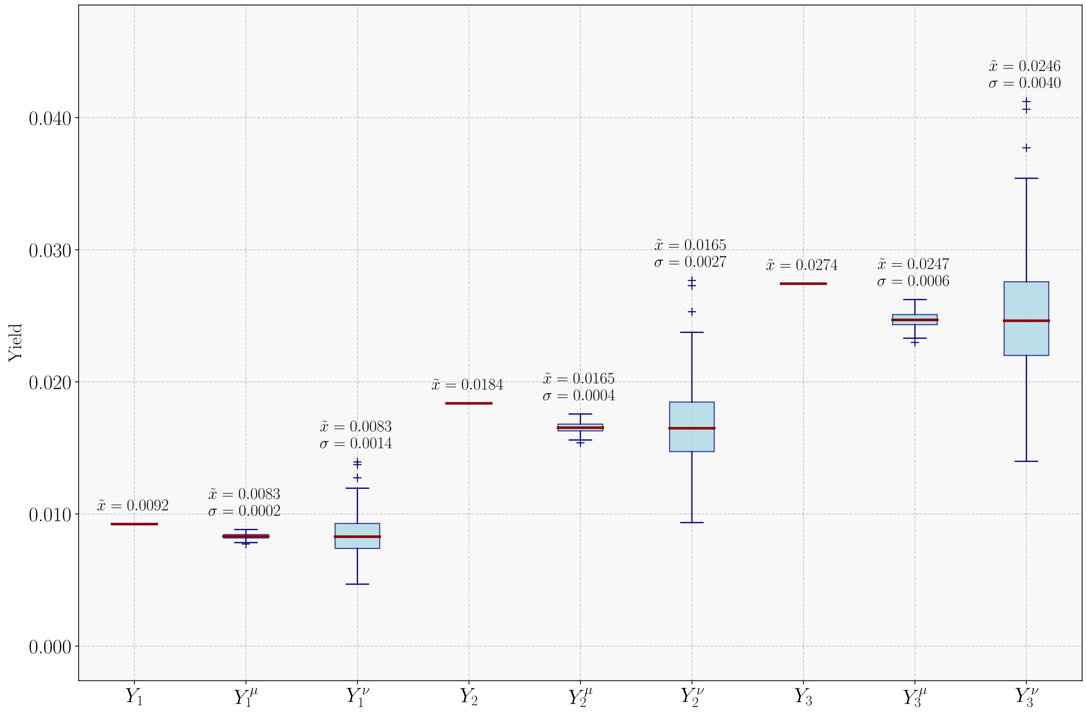


Figure 5.6: Results for the Vacuum+Weak QKD simulation under the BS attack.

Chapter 6

Experimental Results

This chapter compiles the experimental results achieved in this project. It describes the elements regarding the experimental setup used, as well as the tools developed to implement the Vacuum+Weak decoy-state BB84 protocol. The key metrics corresponding to the protocol's normal operation for two different executions are shown and discussed.

6.1 Protocol Implementation

To implement the protocol, an optical setup based on Figure 6.1 was employed. A laser pointer served as a 532 nm Laser Diode (LD) for Alice's photon source. Since the laser pointer generates a continuous wave (CW), it was connected to the FL591FL laser diode driver from Wavelength Electronics, which received an external modulation signal via its BNC connector to control the setpoint voltage, directly modulating the output current supplied to the laser. By adjusting the modulation signal, pulsed laser operation was obtained. In addition, the weak coherent states were produced by attenuating the laser with two fixed neutral density (ND) filters and a circular continuously variable neutral density filter. Finally, variable intensities required to generate signal and decoy states were generated by varying the time width of the external modulation signal, while the circular variable ND filter was kept at a fixed angle to maintain a constant attenuation.

To have an initially prepared horizontal state $|H\rangle$, a polarizing beam-splitter (PBS) served as a polarizer (POL) with the transmitted port aligned with the optical path. The incoming light reaches Alice's Half-Wave Plate (HWP) which is rotated using a custom-made automated rotational mount. After preparing the state, a first mirror (M1) changes the direction of light propagation to then reach Bob's HWP, which operates in the same way as Alice's. Next, a second mirror (M2) redirects the laser pulse to Bob's

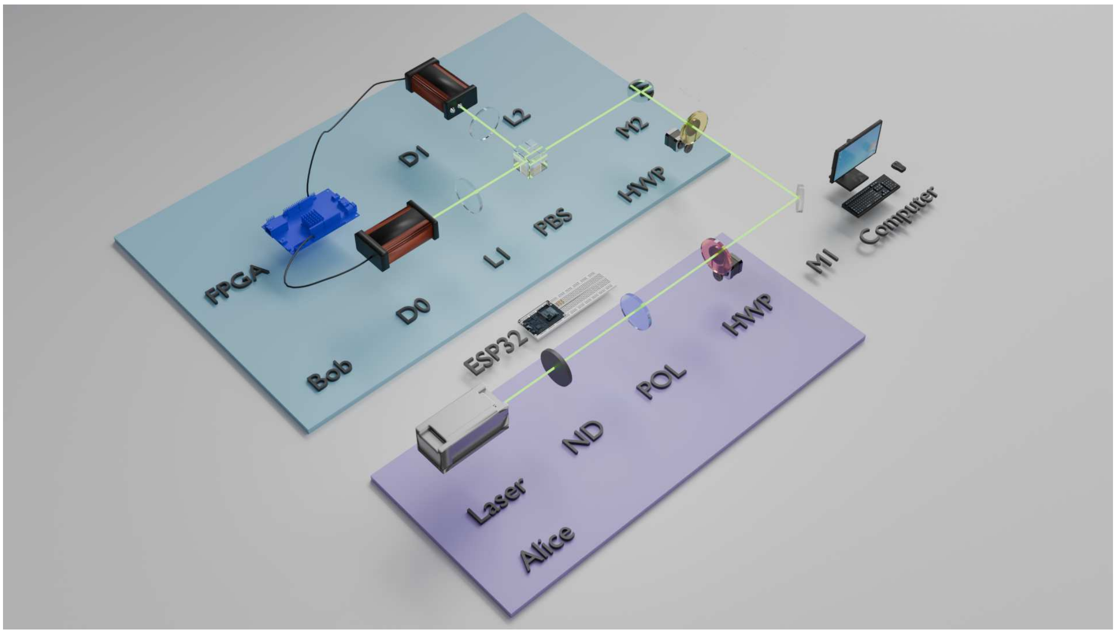


Figure 6.1: 3D rendering of the experimental setup. It showcases Alice's station in purple and Bob's station in blue. Here: Neutral Density Filter (ND), Polarizer (POL), Half-Wave Plate (HWP), Lens (L1 and L2), Mirrors (M1 and M2), Detectors (D0 and D1).

PBS which separates the incoming light into horizontal and vertical components. Each output port of the PBS is equipped with a lens (L1 and L2) to focus the light onto the active area of a Single Photon Avalanche Diode (SPAD) detector (D0 and D1). These detectors generate 20 ns TTL output pulses in response to detected photons, which are then counted and processed by an FPGA-based system for real-time acquisition.

The synchronization between the laser pulses and the photon counting was inherently managed within the FPGA design, as the same FPGA was the one responsible for generating the external modulation signal sent to the laser driver. The resulting counting data was transmitted via a UART interface to an ESP32 microcontroller, which also handled the control of the rotational mounts with the Half-Wave Plates.

The ESP32, programmed in C++ using Arduino's framework, connects to a Wi-Fi hotspot hosted by the control computer and runs a WebSocket server to enable real-time communication. A Jupyter Notebook client was scripted to act as the interface, consuming the counting data streamed over the WebSocket and allowing live monitoring and control of the system. A single round of the protocol begins with the Jupyter client sending a configuration packet—containing the laser pulse width and the photon counting interval—through the WebSocket interface. The ESP32 receives this configuration and forwards it to the FPGA via the UART connection. Then, using a pseudo-random number generator, the ESP32 selects Alice's bit value and preparation basis, and Bob's measurement basis. These values determine the pre-established angles at which each of

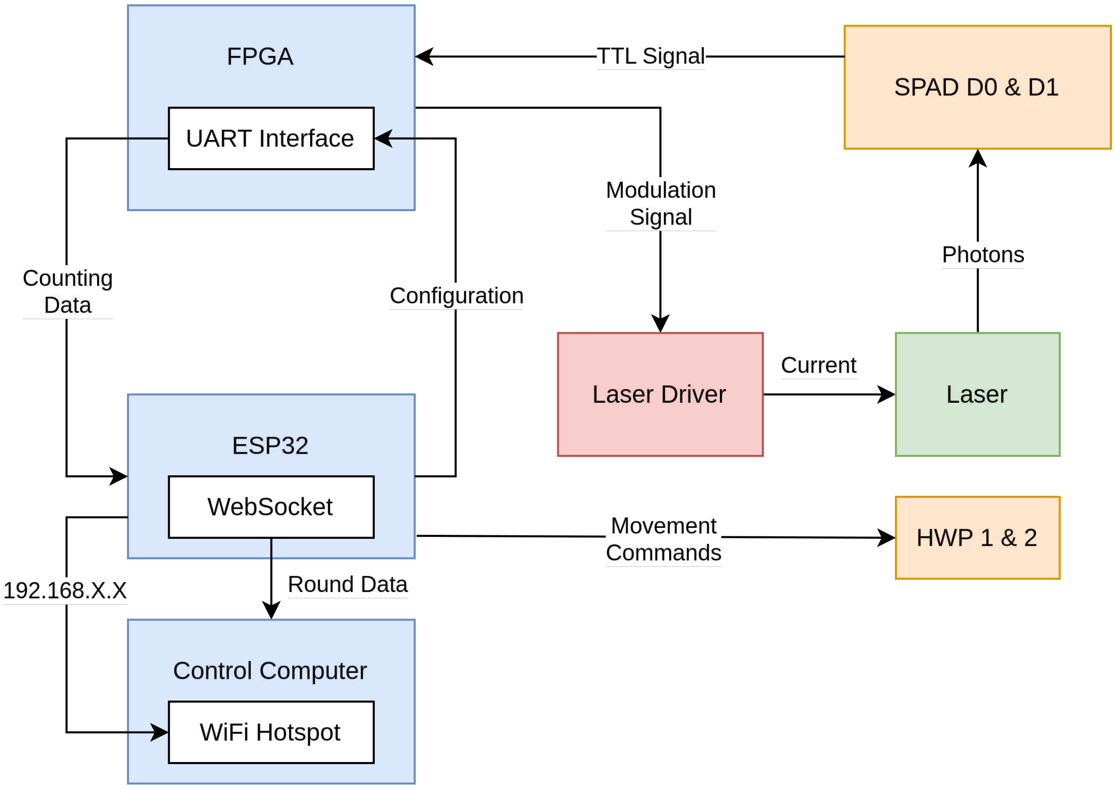


Figure 6.2: Schematic diagram of the electronic components workflow.

the HWP's rotate to. After the laser pulse is fired, the FPGA records the photon counts from both detectors and forwards it back to the ESP32, which transmits this data to the Jupyter Notebook client for a subsequent processing. The workflow of the electronic components and their communication is illustrated in Figure 6.2. The data processing determines a detection if the sum of the detection events from each detector is greater than 0, while the detected bit value corresponds to the detector with the most counts for that specific round: D0 for a bit 0, D1 for a bit 1. In the case that the counts for each detector are the same, the resulting detected bit value is randomly assigned.

6.1.1 Component Specifications

The employed laser pointer is a generic model with a maximum output power of less than 200 mW and a reported wavelength of 532 ± 10 nm. The variable ND filter was a Thorlabs NDC-50C-4M, which offers a continuously variable Optical Density (OD) attenuation range from 0.04 to 4.0. The two PBSs used were a Thorlabs PBS251 Polarizing Beamsplitter Cube, designed for an operational wavelength range of 420 to 680 nm. For the fixed attenuation, Thorlabs NE30A (3.0 OD) and NE40A (4.0 OD) absorptive neutral density filters were used. The initial state preparation is shown in Figure 6.3.

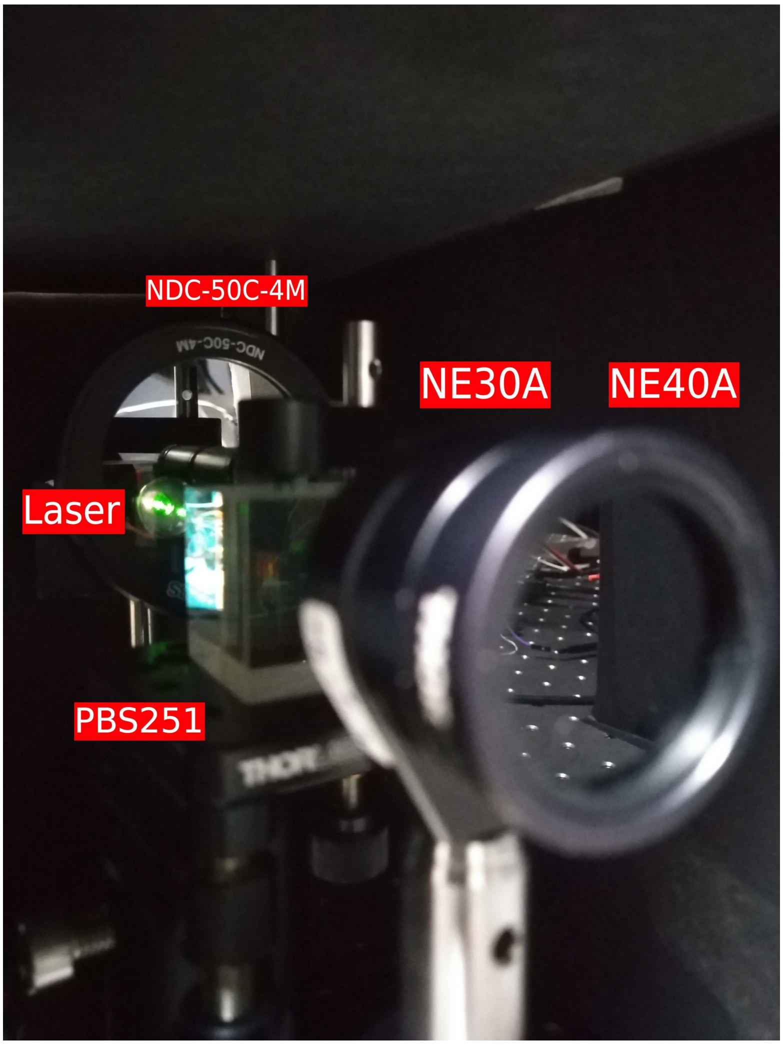


Figure 6.3: Optical elements used for the initial state preparation. To avoid residual light from the second output port of the PBS, it was covered with black cardboard.

The HWP used in Alice's station was a Thorlabs WPH10M-532, a zero-order plate optimized for 532 nm, with a clear aperture of 22.6 mm and a retardance tolerance of $\lambda/300$. Due to the lack of an adittional 532 nm HWP, Bob's Half-Wave Plate was implemented using a stretched sheet of commercial cellophane film, cut and mounted to approximate half-wave retardance at 532 nm [51]. Both HWPs are shown in Figure 6.4. The main cylindrical housing is held within a quartz frame and is rotated using a timing belt mechanism connected to a toothed pulley, which is driven by a stepper motor. A Hall sensor is mounted at the top of the frame to detect two magnets attached to the rotating housing, providing a zero reference point such that the stepper motor sets the desired angle of the HWP. The rotational mounts and the counting system used in the experimental setup were adapted for the Vacuum+Weak decoy-state protocol, from a previously developed undergraduate project used for a BB84 protocol implementation.

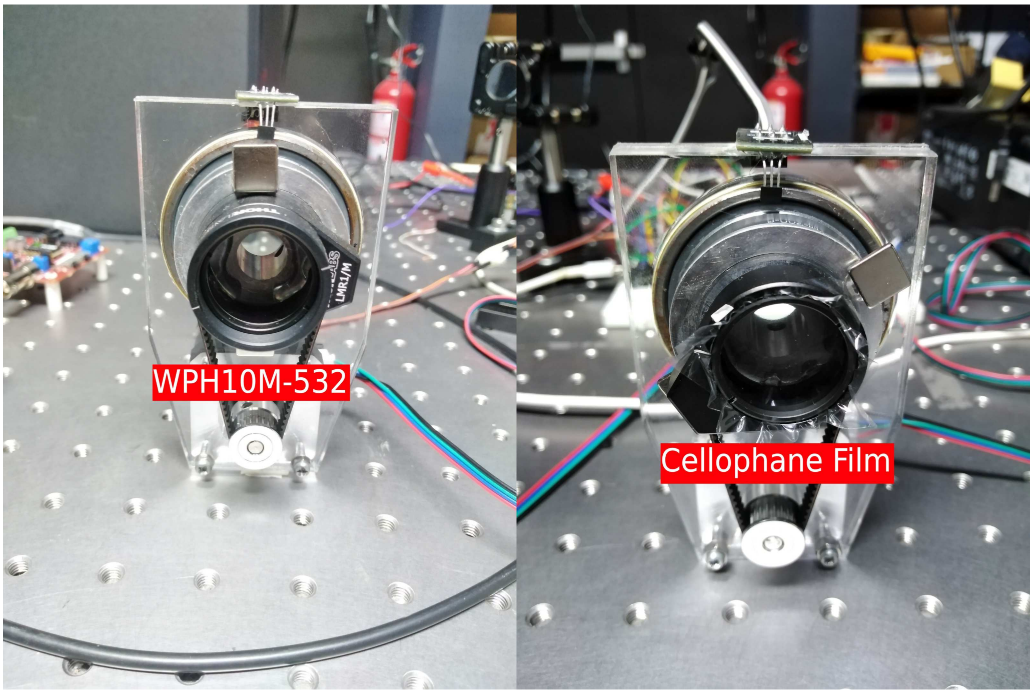


Figure 6.4: Mounted HWPs used in the experiment. Left: Alice's WPH10M-532 zero-order wave plate from Thorlabs. Right: Bob's adapted HWP made from stretched cellophane film. Both mounts are motorized and equipped with belt drives for rotation, with Hall sensors on top providing zero reference points.

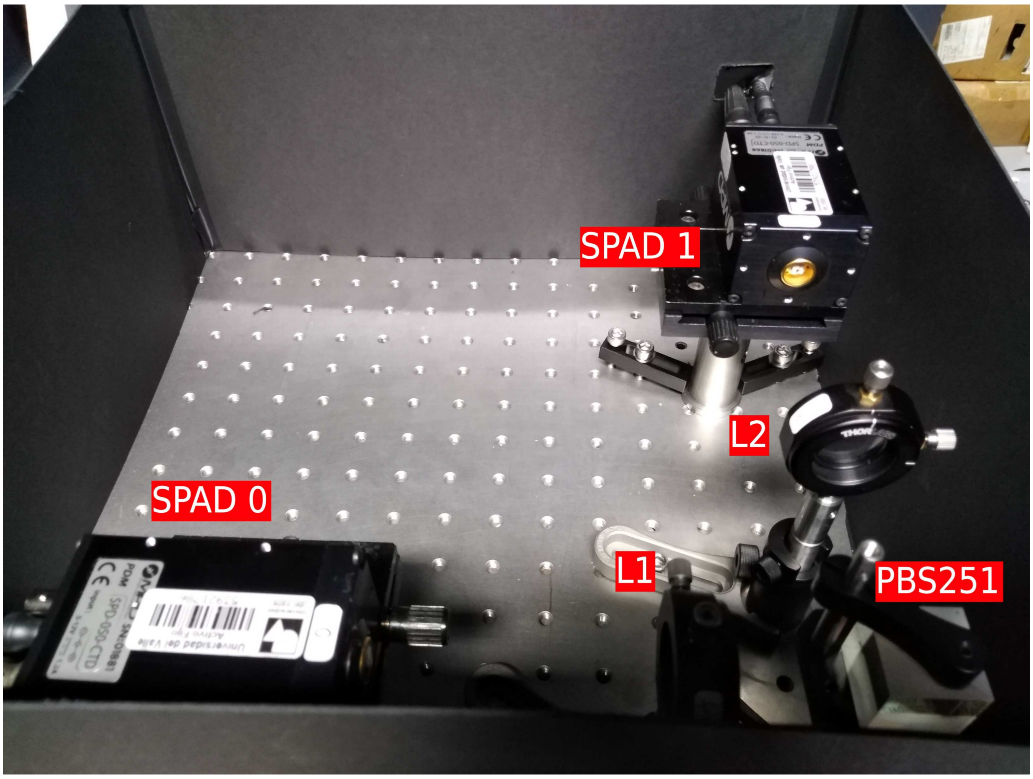


Figure 6.5: Bob's measurement station encompassing polarization-splitting, focusing optics, and single-photon detectors used for signal detection.

The second Thorlabs PBS251 separates the incoming light into its horizontal and vertical polarization components. Each output was focused using Thorlabs lenses with focal length of 90 mm onto the active area of a PDM Series Single Photon Avalanche Diode (SPAD) from Micro Photon Devices (MPD). Specifically, the model used was PD-050-CTD, a PDM Series detector with a 50 μm active area diameter and a dark count rate of less than 50 cps. At the operating wavelength of 532 nm, the detectors offer a typical photon detection efficiency of approximately 47%, as inferred from the device's spectral response. The detectors were powered via a 5–12 V DC supply and operated in free-space mode without fiber coupling. To reduce the background count rate, these elements were also covered with black cardboard. Figure 6.5 shows Bob's measurement station. The full circuit integrating all described elements is shown in Figure 6.6.

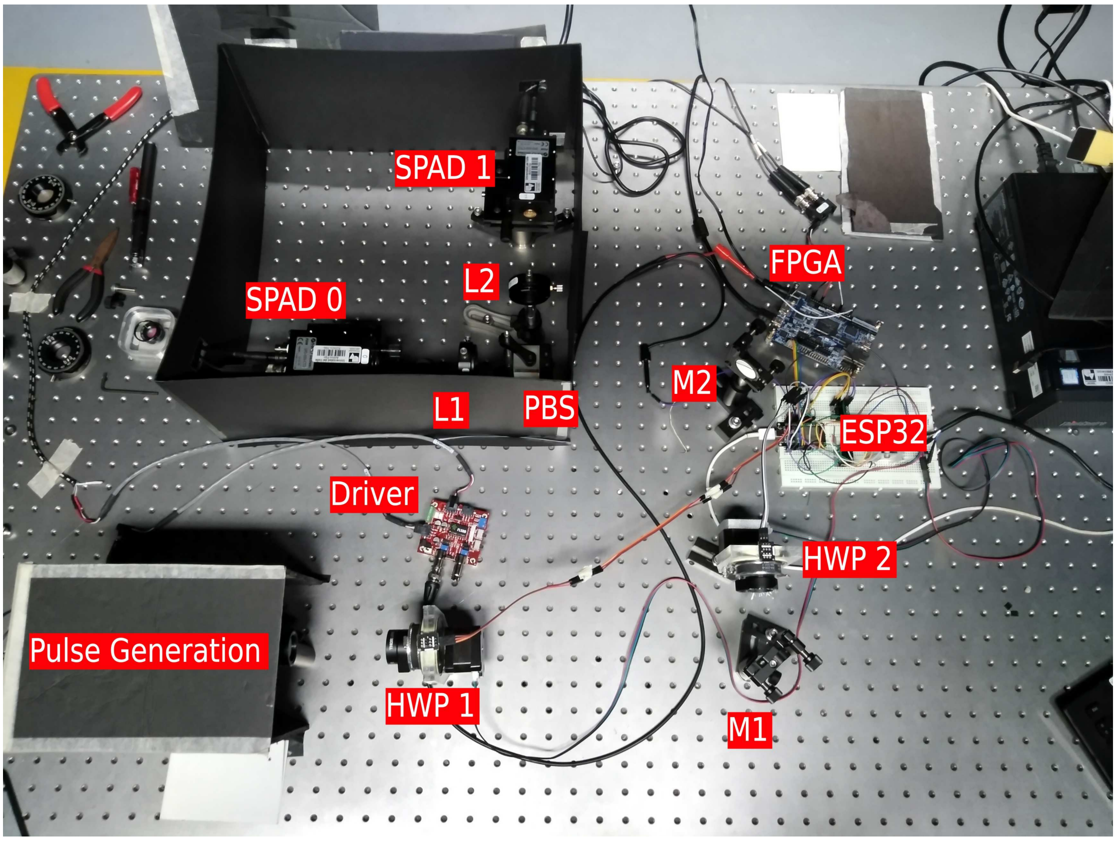
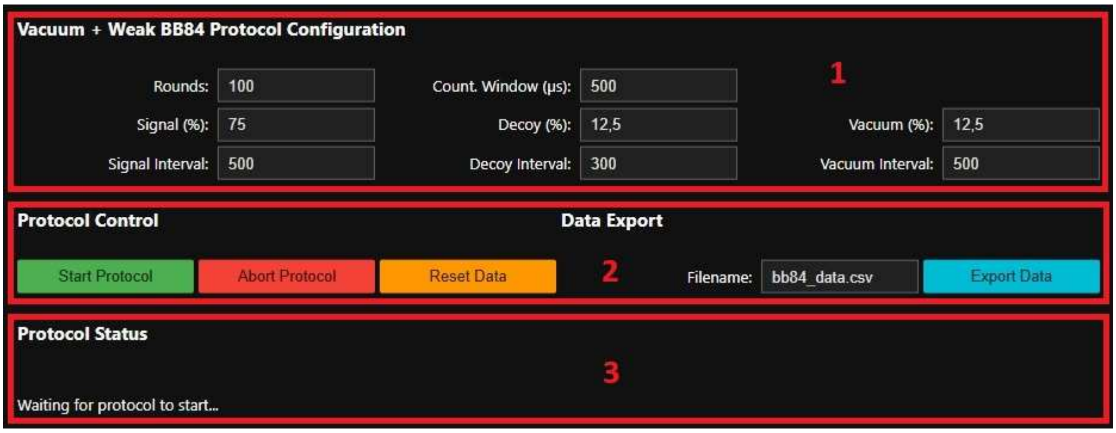


FIGURE 6.6: Complete circuit for implementing the Vacuum+Weak BB84 Protocol.

6.1.2 Control Interface

In order to interact with the electronic system in charge of executing a complete run of the protocol, an interactive interface was developed, running within the Jupyter Notebook on the control computer. Figure 6.7 shows a screenshot of the interface for running the protocol. Section 1 provides numeric input text fields to specify the number of rounds of the protocol to run, the occurrence percentages of each type of state, the duration of



Vacuum + Weak BB84 Protocol Configuration

Rounds: 100
Count. Window (µs): 500
Signal (%): 75
Decoy (%): 12,5
Vacuum (%): 12,5
Signal Interval: 500
Decoy Interval: 300
Vacuum Interval: 500

Protocol Control

Data Export

Filename: bb84_data.csv

Protocol Status

Waiting for protocol to start...

FIGURE 6.7: Interactive configuration and control interface for execution of the Vacuum + Weak BB84 Protocol.

the FPGA's counting window in μs and the laser pulse width for each state type also in μs. In the case of the vacuum state, the internal logic of the ESP32 is in charge of shutting down the modulation signal such that the laser remains off. A necessary requirement is that the laser pulse width be less than or equal to the count window.

Section 2 provides control buttons which allow to start the protocol, abort the protocol, and reset and export last's execution data. The exported data format is csv, to allow better subsequent data processing. Finally, section 3 displays update messages to know the status of the current protocol execution, such as the current round number.

6.2 Experimental Results

Two main executions were carried out with the same parameters, except the effective attenuation of the laser, where the second execution was the more attenuated. Each run consisted of 25,000 rounds of the protocol. The occurrence percentages for each state state were: 75% for signal, 12.5% for decoys, and 12.5% for vacuum. The FPGA counting window was set to 500 μs. The laser pulse width was set to 250 μs for signal states and 100 μs for decoy states. Alice and Bob chose their bases pseudo-randomly.

High MPN Execution

For the first execution, the continuously variable neutral density filter was adjusted such that the effective attenuation of the laser produced high MPN values (i.e., > 1) in both signal and decoy states. Table 6.1 breaks down detection statistics by state type. The left plot from Figure 6.8 shows the corresponding detection rate, where most of the signal and decoy states were detected (98.18% and 80.66%, respectively) and only a few of the vacuum states accounted detections (3.17%). This behavior follows from the results shown in the right plot of Figure 6.8, where a histogram of the sum of counts from both detectors is shown for each state type. Each histogram shows a Poissonian fit from which the parameter λ, corresponding to the average number of counts per pulse in the detectors, is derived. This value is then used to estimate the MPN for both signal and decoy states by dividing it over the overall expected transmittance.

Table 6.1: Statistics by state type for the first execution.

State Type	**All Pulses**		**Same Basis**	
	Detections	Total Pulses	Detections	Total Pulses
Signal	18406	18746	9330	9494
Decoy	2583	3202	1286	1606
Vacuum	97	3052	51	1498

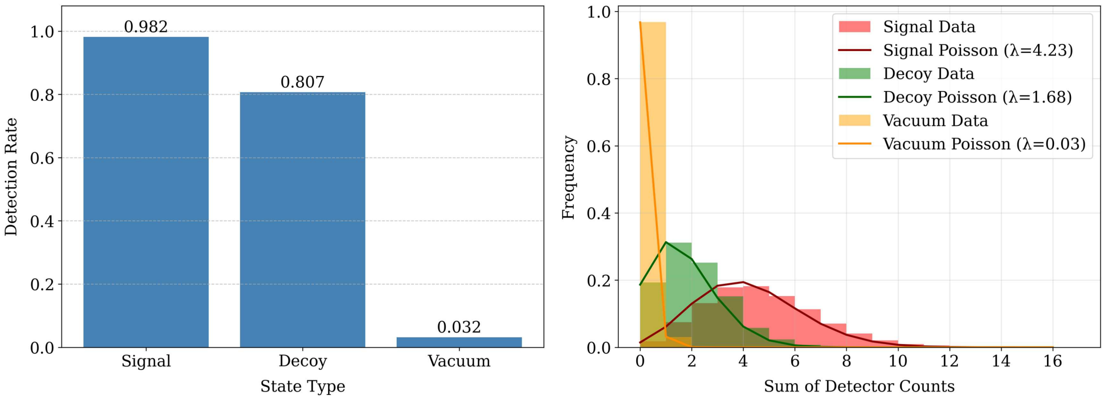


Figure 6.8: Detection statistics and photon number distributions for the first execution. Left: Detection rates for each state type. Right: Histograms of total detector counts per pulse for each state type, fitted with Poisson distributions from which the mean photon number (MPN) per pulse is estimated.

The experimental parameters of the first execution are summarized in Table 6.2, showing the MPN, transmittance, overall gain and QBER calculated for each state type. Since the protocol does not make use of the vacuum state transmittance, it is not calculated. The expected transmittance, computed as described in Section 3.4.2, was $\eta = 0.739973$. In this setup, negligible channel losses were considered, since no optical fiber was used.

Table 6.2: First execution experimental parameters per state type.

State	**MPN**	**Transmittance**	**Gain**	**QBER**
Signal	5.722507	0.518948	0.982726	0.233655
Decoy	2.268934	0.641463	0.800747	0.284603
Vacuum	0.032765	———	0.034045	0.470588

The expected and estimated yields Y_n and QBERs e_n for signal and decoy states for photon numbers $n = 1 \ldots 5$ are shown in Table 6.3. Of main interest, we sought to evaluate the security condition given by Eq. 4.7. When a PNS attack is not implemented, the photon-number-dependent yields should be equal for every photon number.

TABLE 6.3: Expected, signal and decoy Y_n and e_n values for $n = 1 \dots 5$.

n	Y_n	Y_n^μ	Y_n^ν	e_n	e_n^μ	e_n^ν
1	0.748826	0.535326	0.653670	0.055342	0.063789	0.058425
2	0.934688	0.776468	0.875828	0.051131	0.054588	0.052271
3	0.983017	0.892469	0.955480	0.050297	0.051934	0.050762
4	0.995584	0.948272	0.984038	0.050093	0.050888	0.050280
5	0.998852	0.975116	0.994277	0.050041	0.050427	0.050114

From Table 6.3, two things can be noticed. The first one is that the expected yields differ from the estimated signal state yields for all n, where the major variation happens for pulses containing 1, 2 and 3 photons. The second one corresponds to the differences between the decoy and signal state yields, where the main discrepancies also happen for $n = 1, 2, 3$. Although both of these behaviors would normally indicate a possible PNS attack, the discrepancies here are associated with practical considerations in the execution, such as the number of detections and hardware imperfections.

To understand this, we can see first in Table 6.2 that a gain difference of 18% between signal and decoy states appear. If the relationship between the estimated gain with respect to the MPN for signal and decoy states does not hold, the measured transmittance (Eq. 4.12) will be different, and consequently so will the yields, as Tables 6.2 and 6.3 show. This is likely to happen when the differences between the MPN for signal and decoy states is too steep, which can be noticed in the histograms shown in Figure 6.8, where the frequency of 1- and 2-photon detections is higher for the decoy data.

In the case of higher n-values, the gap between signal and decoy state yields was reduced, a result attributed to an increase in the number of detections of larger photon numbers, which corresponds to the opposite behavior to the one analyzed in the simulation from Section 5.2. This can be easily verified by replicating the experimental results, with the simulated environment under normal operation. A boxplot displaying the respective expected, signal and decoy yields for 5000 runs is shown in Figure 6.9, where the previously described behavior can be observed. No clear overlap can be seen between yields for all n, indicating $Y_n \neq Y_n^\mu \neq Y_n^\nu$ for this execution. Additionally, the largest deviation occurs for decoy pulses with low photon number, caused by a small number of detections, with the signal-to-decoy pulse ratio being the main influencing factor.

On a side note, Table 6.3 also demonstrates an important statement from the decoy-state method, which is that the error rate for an n-photon state should also remain the same for both signal and decoy states when no eavesdropping of any kind took place; the error based security condition in Eq. 4.7. If a PNS attack is considered, this security condition

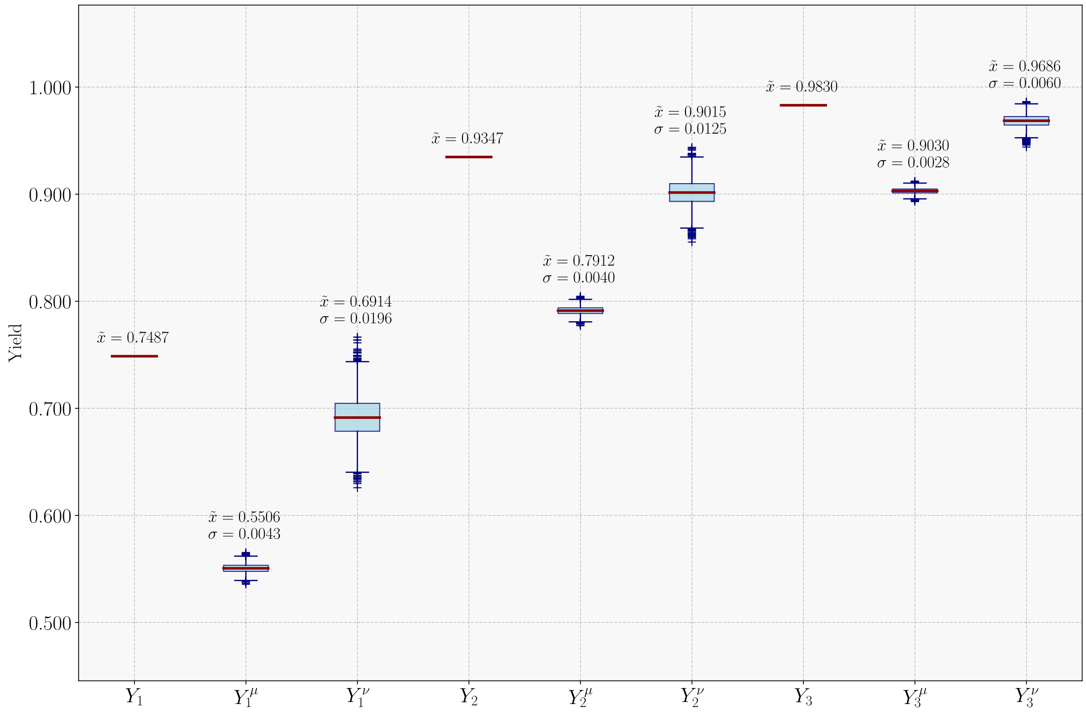
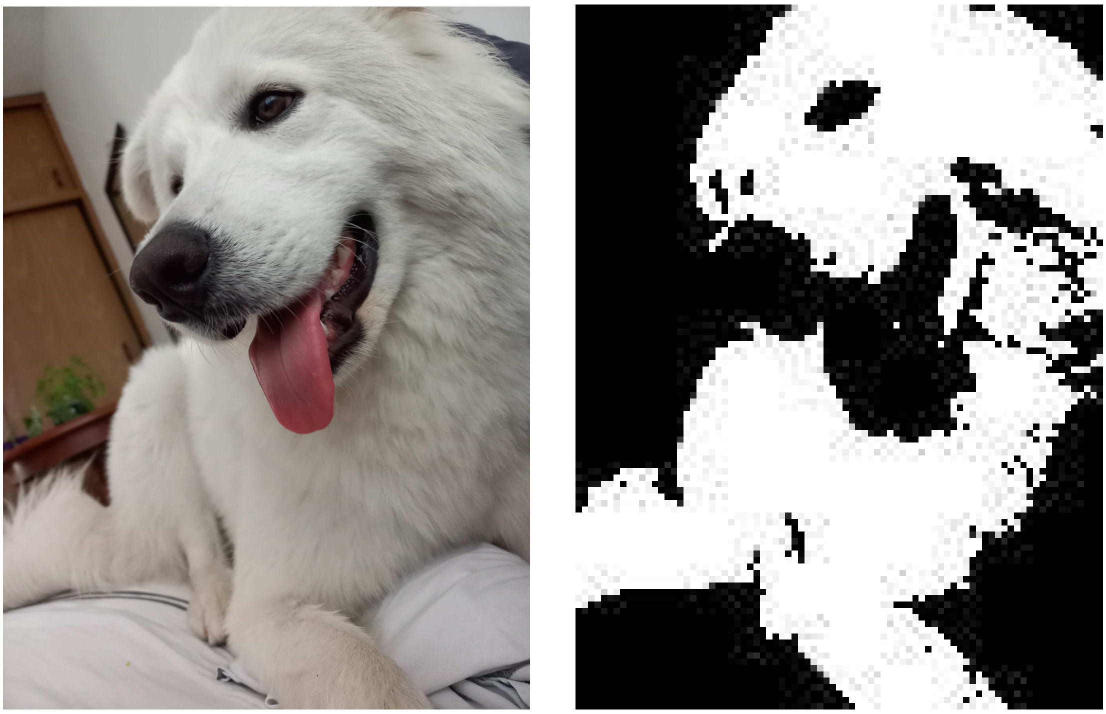


Figure 6.9: Replicated results for the high MPN execution using the Vacuum+Weak QKD simulation under no eavesdropping.

by itself would not reveal Eve's presence, since the PNS attack does not introduce errors during quantum transmission. Therefore, monitoring both photon-number-dependent yields and QBERs is needed to confirm the integrity of the channel.

Finally, to conclude the analysis of this execution, we note that the overall QBER for the signal state is 23.37%, which translates to 2180 error bits from the 9330 detected. Again, this would be indicative of eavesdropping if there was no knowledge about what was happening in the quantum channel. However, similarly to the discrepancies in the measured yields, the experimental conditions implicated in the execution affected the error rate statistic. In this case, a major element of the experimental setup was most likely the one inducing the errors: the laser source. As described in Section 6.1, a laser pointer operating with the driver FL591FL was used. Despite being supplied with a constant current, the laser often showed variations in its output optical power. In addition, the intrinsic instability of the laser output polarization would commonly translate in a difference between the counting data from the two detectors without changing the setup. These imperfections potentially affected the system's capability of obtaining correct detections during the execution of the protocol. To contrast this with the simulation from Figure 6.8, the obtained average value of the signal overall QBER was 7.41%, indicating that with a stable source, the errors obtained during quantum transmission are only caused by detector error probability and dark counts.

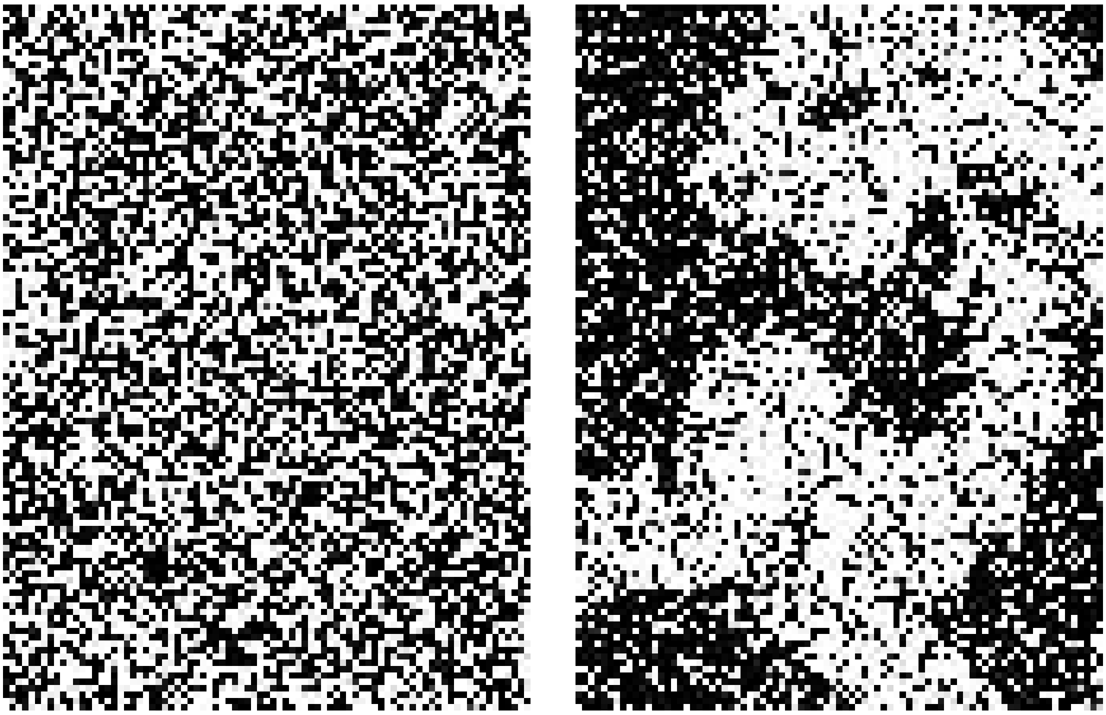
To illustrate the resulting key in action, a picture of my dog, named Antares, was converted to a black and white pixel art of the same number of signal bits as the resulting key. This can be seen in Figure 6.10. Applying the one-time pad (OTP) scheme between the image data and Alice's key, the image is encrypted (Figure 6.14a). On the other hand, the image is decrypted by applying the OTP scheme back with the encrypted image and Bob's resulting key (Figure 6.14b). Evident discrepancies between the decrypted image and the original image can be noted, which illustrates the QBER obtained between Alice's and Bob's keys. Since the QBER surpasses the theoretical secure threshold of 11% [52], the correct course of action would be to abort the protocol and start over again. In the case that the QBER was below this threshold, we would proceed with the *error correction* phase in which the bit flips generated during quantum transmission are corrected; and the *privacy amplification* phase, in which a smaller final key length is obtained, to reduce the amount of information leaked throughout the protocol. Since the main focus of this work is to test the security condition of the Vacuum+Weak decoy-state protocol, the details of these additional phases will not be discussed any further.



(A) Original photo of Antares.

(B) Resulting black and white pixel art.

FIGURE 6.10: Visual comparison between the original photo and the generated pixel art version of Antares.



(A) Encrypted image.

(B) Decrypted image.

Figure 6.11: Visual comparison between the encrypted and the decrypted images of the generated pixel art version of Antares for the first execution.

Low MPN Execution

In this run the continuously variable neutral density filter was set to yield much lower mean photon numbers (i.e., < 1) in both signal and decoy pulses. Table 6.4 summarizes the raw detection counts: only about 26.64% of signal pulses and 12.36% of decoy pulses produced a click in the detectors, whereas vacuum pulses triggered a detector merely 2.89% of the time. These detection rates are plotted in the left panel of Figure 6.12, while in the right panel, histograms of the total counts per pulse for each state are overlaid with Poisson fits, from which the new MPN values were extracted (see Table 6.5).

Table 6.4: Statistics by state type for the second execution.

State Type	**All Pulses**		**Same Basis**	
	Detections	Total Pulses	Detections	Total Pulses
Signal	4984	18707	2553	9482
Decoy	405	3278	223	1659
Vacuum	87	3015	37	1532

The experimental parameters for the low-MPN regime are listed in Table 6.5. The estimated MPNs drop to 0.4259 for the signal state and 0.1810 for the decoy, with the vacuum background remaining at 0.0318 photons per pulse. Here, a less pronounced difference between the measured transmittance for the signal state with respect to the

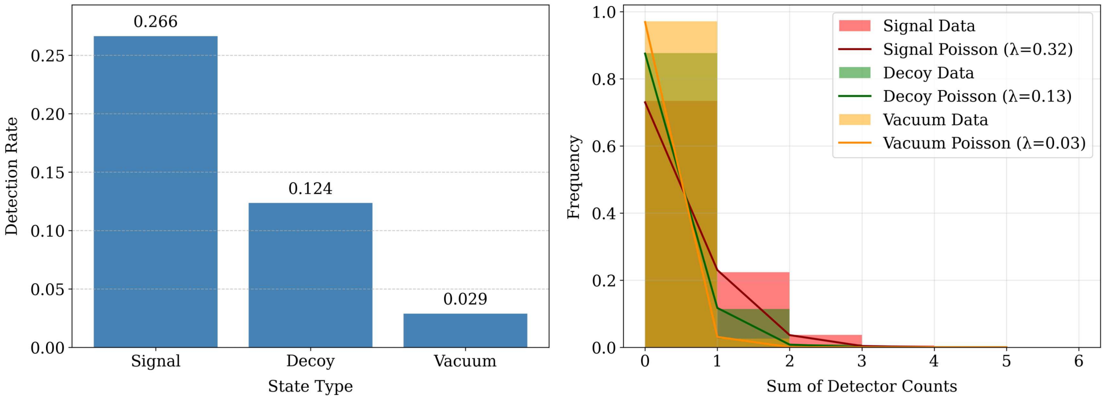


FIGURE 6.12: Detection statistics and photon number distributions for the second execution. Left: Detection rates for each state type. Right: Histograms of total detector counts per pulse for each state type, fitted with Poisson distributions from which the mean photon number (MPN) per pulse is estimated.

expected value can be noted, while both signal and decoy measured transmittance remained close, with a mere difference of 2%. The resulting gains fall to 0.2693 for signal and 0.1344 for decoy, and the signal QBER rises up to 33.18%, reflecting the increased impact of background counts and statistical fluctuations at lower intensity levels.

TABLE 6.5: Second execution experimental parameters per state type.

State	**MPN**	**Transmittance**	**Gain**	**QBER**
Signal	0.425857	0.660232	0.269247	0.331767
Decoy	0.180984	0.645548	0.134418	0.313901
Vacuum	0.031841	———	0.024151	0.324324

The yields and QBERs results for this execution are shown in Table 6.6, where an analogous behavior to the run with a high MPN can be observed: detections corresponding to pulses containing 1 and 2 photons exhibit a greater variation with respect to the pulses with a higher number of photons. However, in contrast with the first run, the yields for the signal and decoy state show a greater similarity for all n-values, a result that follows directly from the resemblance between the estimated transmittance of the signal and decoy states, which can be achieved when the photon number distributions for both types of states are similar, i.e., the MPNs remain on the order 10^{-1}.

TABLE 6.6: Expected, signal and decoy Y_n and e_n values for $n = 1 \dots 5$.

n	Y_n	Y_n^μ	Y_n^ν	e_n	e_n^μ	e_n^ν
1	0.746253	0.668438	0.654109	0.048904	0.050660	0.051029
2	0.934019	0.887346	0.877398	0.045871	0.046505	0.046649
3	0.982843	0.961724	0.956544	0.045272	0.045524	0.045587
4	0.995539	0.986995	0.984597	0.045126	0.045224	0.045252
5	0.998840	0.995581	0.994540	0.045089	0.045126	0.045138

Once again, the above can be compared to the corresponding simulated execution in Figure 6.12, where a noticeable overlap between photon-number-dependent yields is depicted, which is the expected behavior under normal operation described in Section 5.2. Nonetheless, as in Figure 6.8, the recreation shows a yield variation decrease as the photon number increases, which illustrates the case of small detection statistics if not sufficient amount of n-photon pulses are generated. The specific example of $n = 3$ can be examined; the probability of obtaining a 3-photon pulse from a Poissonian source with MPN $\nu = 0.18$, is $P(\nu; n) = 0.00082$. If we multiply this value with the total of decoy pulses generated in the execution, we obtain $\langle N_3 \rangle = 2.73$, which is the expected number of 3-photon decoy pulses during this run. From here it is clear that, if only about three such pulse are expected per execution, the yield estimate Y_3^ν is based on an extremely limited sample. This constrains statistical variation, not because the estimate is precise, but because the lack of data prevents observable fluctuations, ultimately leading to an artificially reduced dispersion in the yield distribution for higher photon numbers.

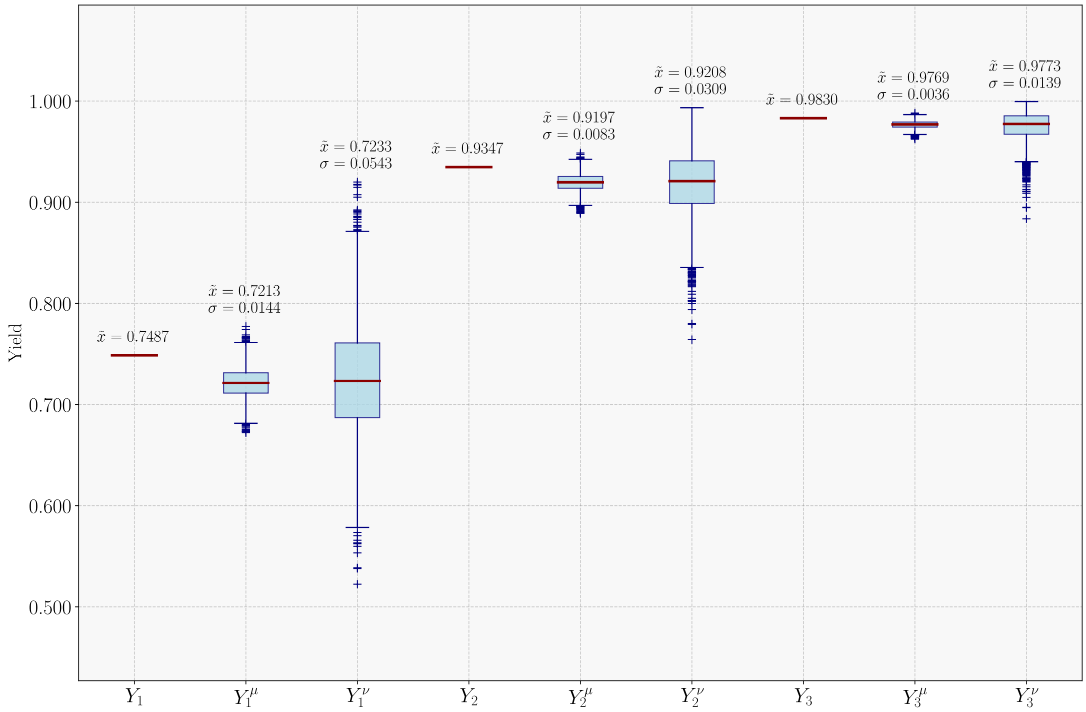
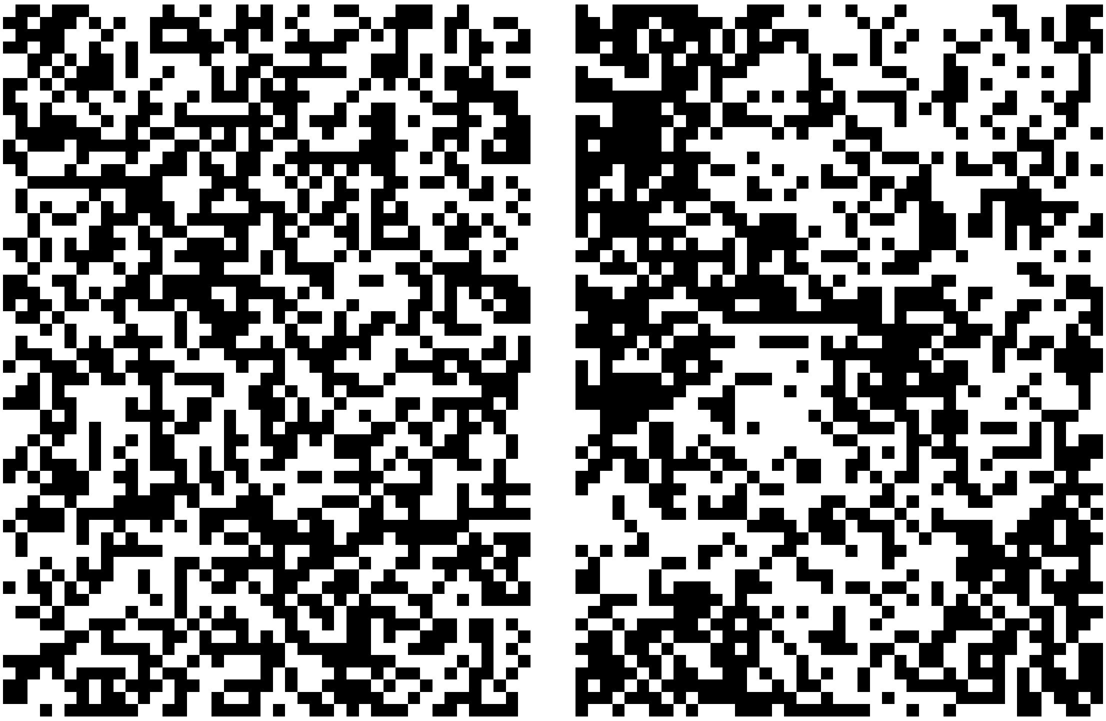


FIGURE 6.13: Replicated results for the low MPN execution using the Vacuum+Weak QKD simulation under no eavesdropping.

Furthermore, when we check the error-based security condition, we find that for all n-values, the photon-number-dependent error rates e_n^μ and e_n^ν differ by no more than 0.0003. This uniformity confirms again that, despite the high overall QBER of 33.18% in this case (which also exceeds the 11% secure threshold), no additional errors were introduced selectively in either the signal or decoy pulses. As for the simulation, the average value of the signal QBER was 7.04%, supporting the already stated hypothesis about shifts in polarization causing detection counts to drift and result in incorrect bit values. It is worth mentioning that the use of the cellophane film as Bob's HWP could also have influenced in this problem, since its behavior over time was not characterized.

The exercise of encrypting and decrypting the photo of Antares was repeated, taking into account the new max length of 2553 bits, corresponding to the amount of signal state detections. The results are shown in Figure 6.14. Here, both the effects of shortening the number of bits used to scale the photo, and the increase in the overall QBER in the effective key, make it difficult to see the original photo, although a somewhat vague silhouette is visible. As discussed in Section 5.2, smaller MPN values reduce the number of detections, making the length of the sifted key considerably smaller if no sufficient amount of pulses are sent. In our experimental results, 25,000 initial pulses was a compromise between the time taken to run the protocol and statistical value.



(A) Encrypted image.

(B) Decrypted image.

FIGURE 6.14: Visual comparison between the encrypted and the decrypted images of the generated pixel art version of Antares for the second execution.

Overall, the low-intensity run uphold the decoy-state security condition given by Eq. 4.7, within statistical and systematic uncertainties. In the case of high-intensity levels, the discrepancies in both estimated transmittances and yields for signal and decoy states make the obtained results an illustrative example of how photon detection statistics can be affected by changes in the MPN, which enforces better polarization control in order to not rely on the use of majority detection counts to determine bit values. In addition, the complementary simulation results for the low MPN regime showcase the need for previous characterization of a QKD system detection statistics fluctuations. While the experimental results had small discrepancies, its corresponding recreation in the simulation environment shows the possibility of deviations as high as the order of 10^{-2} for decoy states. From this, the more accurate security condition $Y_n = Y_n^{\mu} = Y_n^{\nu} \pm \Delta$ can be considered, where Δ represents the expected variation during quantum exchange.

On the other hand, the overall QBERs of 23.37% and 33.18% exceeding the security threshold for key extraction underscore that, although the Vacuum+Weak decoy-state method imposes matched photon-number-dependent yields and error rates, practical key generation further demands better control of laser stability and background counts to drive the overall QBER below the security limit in order to have an usable key.

Finally, it is important to consider the intrinsic trade-off for selecting the signal state MPN. A larger μ increases the fraction of single-photon pulses—the only ones contributing to secure key generation—but also raises the multi-photon fraction and thus the vulnerability to PNS attacks. For a Poissonian source, the single-photon probability is maximized at $\mu = 1$, whereas keeping $\mu \lesssim 1$ ensures that the fraction of all detection events that originated from single-photon signals, Q_1/Q_μ, remains high [13]. Consequently, for practical implementations, the signal state μ should have a balance between single-photon gain with security against multi-photon leaks.

Chapter 7

Conclusions and Perspectives

7.1 Conclusions

This thesis explored the implementation and behavior of the BB84 Quantum Key Distribution (QKD) protocol, specifically focusing on the integration of Vacuum+Weak decoy-states to enhance security against photon-number splitting (PNS) attacks. Our investigation encompassed both a simulation-based approach and a low-cost experimental realization, providing a comprehensive understanding of the protocol's practical challenges and implications of the security condition to conclude normal operation.

The interactive Qiskit and Streamlit simulation proved to be an effective tool for visualizing step by step the BB84 protocol along with the impact of fundamental scenarios, such as noisy-channels, the presence of an eavesdropper and ideal-theoretical conditions. On the other hand, the Vacuum+Weak decoy-state simulation effectively demonstrated how this configuration enables the detection of Eve's presence by revealing discrepancies in the photon-number-dependent yields Y_n. The simulation results showed the distinct signatures of a standard PNS attack and a beam-splitting (BS) attack, highlighting the importance of monitoring signal and decoy state yields for different photon numbers. The statistical match between expected and simulated yields in the absence of an eavesdropper validated the theoretical framework of the decoy state method, confirming its ability to characterize the quantum channel in order to test for eavesdropping.

The experimental implementation of the Vacuum+Weak decoy-state BB84 protocol, built upon a customized optical setup, provided meaningful insights into the practical complexities and limitations of QKD. Despite utilizing a simplified setup with a laser pointer and an homemade rotational mounting for the Half-Wave Plates, the experiment successfully demonstrated the core functionality of the protocol.

Two experimental runs, operating at different mean photon numbers (MPNs), were analyzed: a high MPN execution ($\mu > 1$) and a low MPN execution ($\mu < 1$).

For the high MPN scenario, the overall QBER was 23.37%, significantly exceeding the theoretical secure threshold of 11%. This high error rate, primarily attributed to the instability of the laser source and imbalance in initial polarization preparation, prevented the generation of a usable secure key. While this run showed discrepancies between expected and estimated yields ($Y_n \neq Y_n^\mu \neq Y_n^\nu$), particularly for low photon numbers, these were linked to practical considerations like the steep difference in MPN between signal and decoy states and limited detection statistics, rather than an active PNS attack. The gain difference of 18% between signal and decoy states underscored how variations in MPN can impact measured transmittance and, consequently, estimated yields. The visual demonstration with the image of Antares clearly illustrated the impact of this high QBER on key usability, showing the degradation of the decrypted image.

In contrast, the low MPN scenario, with an overall QBER of 33.18%, still above the secure threshold, demonstrated a more consistent adherence to the security condition $Y_n^\mu \approx Y_n^\nu$ and $e_n^\mu \approx e_n^\nu$ within statistical variation. This was primarily due to the closer resemblance between the estimated transmittances of the signal and decoy states, achieved by maintaining similar MPNs of order 10^{-1}. Although small discrepancies were observed, especially for large photon numbers, these were attributed to limited detections of higher n-photon pulses, as illustrated by the simulated replication. This highlights the importance of sufficient statistical sampling for accurate yield estimation and suggests that the security condition might be more accurately expressed as $Y_n = Y_n^\mu = Y_n^\nu \pm \Delta$, where Δ accounts for expected statistical variations. Both runs consistently upheld the error-based security condition ($e_n^\mu \approx e_n^\nu$), indicating that no additional errors were selectively introduced by an eavesdropper. However, the persistently high overall QBERs, in contrast to the significantly lower simulated values (7.41% and 7.04%), stemmed from inherent experimental limitations such as laser instability and polarization misalignment, which introduced systematic noise across all pulse types.

In summary, this work has demonstrated the efficacy of the Vacuum+Weak decoy state method in characterizing normal operation in practical QKD, both through robust simulation and a proof-of-concept experimental setup. It concurrently elucidated the stringent requirements for component stability and channel characterization necessary to achieve secure and practical QKD in real-world scenarios. While the decoy state method effectively monitors the channel for eavesdropping by comparing photon-number-dependent yields and error rates, practical key generation necessitates further improvements in laser stability and control over background counts to drive the overall

QBER below the secure threshold. Furthermore, the experiments highlighted the intrinsic trade-off in selecting the signal state MPN, emphasizing the need for a balance between maximizing single-photon gain and mitigating multi-photon pulse generation.

7.2 Perspectives

Addressing the limitations identified in our experimental setup would be our most logical next step, leading to a more robust and reliable QKD implementation. Firstly, a primary focus should be on improving the photon source quality, by replacing the laser pointer with a more stable weak coherent pulse, source featuring a more controlled polarization, in order to drastically reduce the overall QBER and enable the generation of truly secure keys. Investigating pulsed laser diodes with better stability would be crucial.

Secondly, enhancing the optical components would significantly impact performance. Using a matched HWP for Bob, similar to Alice's, would improve the consistency of polarization measurements. Furthermore, exploring fiber-coupled components instead of free-space optics could mitigate environmental noise and simplify alignment, leading to a more stable and efficient quantum channel. Implementing active feedback mechanisms for HWP alignment could also compensate for misalignments over time.

Future work could also delve into expanding the decoy state implementation in terms of secure key generation and maximal secure distance. Although the Vacuum+Weak configuration allows eavesdropping detection, its main focus has been increasing performance metrics, something that can be tested in a long field practical QKD implementation.

Finally, the Vacuum+Weak simulation developed in this work is open for further exploration. Additional discussion elements such as studying further the effects of different combinations of MPN values and occurrence percentage ratios might better illustrate the obtained experimental results in this work. In addition, the simulation could be extended to include other QKD protocols and types of eavesdropping, or be restructured to better model the optics behavior by including photon polarization angles and physical interactions with optical elements under different environment conditions. This would provide an accessible educational and research tool for the QKD community.

Bibliography

[1] J. F. Dooley, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms.* Springer International Publishing, 2018.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography.* CRC Press, 2015.

[3] N. S. Yanofsky and M. A. Mannucci, *Quantum Computing for Computer Scientists.* Cambridge University Press, 2008.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, 1997.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, pp. 212–219, 1996.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the International Conference on Computers, Systems and Signal Processing*, vol. 1, pp. 175–179, 1984.

[7] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Physical Review A*, vol. 51, pp. 1863–1869, 1995.

[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, pp. 1330–1333, 2000.

[9] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics*, vol. 4, p. 344, 2002.

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[11] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, p. 057901, 2003.

[12] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, p. 230504, 2005.

[13] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, p. 012326, 2005.

[14] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner, and C. McLaughlin, "Performance evaluations of quantum key distribution system architectures," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 30–40, 2015.

[15] L. O. Mailloux, R. D. Engle, M. R. Grimaila, D. D. Hodson, J. M. Colombi, and C. V. McLaughlin, "Modeling decoy state quantum key distribution systems," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 12, pp. 489–506, 2015.

[16] L. O. Mailloux, M. R. Grimaila, J. M. Colombi, D. D. Hodson, R. D. Engle, C. V. McLaughlin, and G. Baumgartner, "Quantum key distribution: examination of the decoy state protocol," *IEEE Communications Magazine*, vol. 53, pp. 24–31, 2015.

[17] R. D. Engle, L. O. Mailloux, M. R. Grimaila, and D. D. Hodson, "Modeling, simulation, and performance analysis of decoy state enabled quantum key distribution systems," *Applied Sciences*, vol. 7, p. 212, 2017.

[18] R. D. Engle, L. O. Mailloux, M. R. Grimaila, D. D. Hodson, C. V. McLaughlin, and G. Baumgartner, "Implementing the decoy state protocol in a practically oriented quantum key distribution system-level model," *The Journal of Defense Modeling and Simulation*, vol. 16, pp. 27–44, 2019.

[19] A. F. Herrera Fernández, "Noise assisted quantum key distribution." Bachelor's thesis, Universidad de los Andes, 2019.

[20] K. A. Suárez Molano, "Fundamentos y avances en criptografía cuántica." Bachelor's thesis, Universidad de los Andes, 2020.

[21] D. R. Sabogal Pérez, "Use of decoy states in quantum key distribution." Bachelor's thesis, Universidad de los Andes, 2021.

[22] D. P. DiVincenzo, *Topics in Quantum Computers*, pp. 657–677. Springer Netherlands, 1997.

[23] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[24] W. Scherer, *Mathematics of Quantum Computing: An Introduction.* Springer International Publishing, 2019.

[25] D. McMahon, *Quantum Computing Explained.* Wiley-IEEE Computer Society Press, 2007.

[26] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics.* Cambridge University Press, 2018.

[27] S. Gharibian, "Introduction to quantum computation." Lecture Notes, Paderborn University, 2021.

[28] J. J. Sakurai and J. Napolitano, *Modern Quantum Mechanics.* Cambridge University Press, 2020.

[29] P. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing.* Oxford University Press, 2007.

[30] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[31] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010.

[32] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.

[33] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises*, vol. 988 of *Lecture Notes in Physics.* Springer, 2021.

[34] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, 1991.

[35] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Physical Review Letters*, vol. 69, pp. 2881–2884, 1992.

[36] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, 2009.

[37] B. E. Saleh and M. C. Teich, *Fundamentals of Photonics.* Wiley, 2019.

[38] M. Fox, *Quantum Optics: An Introduction.* Oxford University Press, 2006.

[39] R. Chipman, W. S. T. Lam, and G. Young, *Polarized Light and Optical Systems.* CRC Press, 2018.

[40] T. Durt, B.-G. Englert, I. Bengtsson, and K. kowski, "On mutually unbiased bases," *International Journal of Quantum Information*, vol. 8, pp. 535–640, 2010.

[41] D. H. Goldstein, *Polarized Light, Revised and Expanded.* Marcel Dekker, 2003.

[42] X. Ma, *Quantum cryptography: theory and practice.* PhD thesis, University of Toronto, 2008.

[43] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, p. 052304, 2000.

[44] M. Koashi, "Efficient quantum key distribution with practical sources and detectors," 2006.

[45] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photonics*, vol. 3, pp. 696–705, 2009.

[46] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics.* Cambridge University Press, 1995.

[47] M.-Z. Mina and E. Simion, "A scalable simulation of the bb84 protocol involving eavesdropping," in *Innovative Security Solutions for Information Technology and Communications (SecITC 2020)*, vol. 12596 of *Lecture Notes in Computer Science*, pp. 91–109, 2021.

[48] C. S. Unnikrishnan, "Quantum non-demolition measurements: Concepts, theory and practice," *Current Science*, vol. 109, pp. 2052–2060, 2015.

[49] J. Calsamiglia, S. M. Barnett, and N. Lütkenhaus, "Conditional beam-splitting attack on quantum key distribution," *Physical Review A*, vol. 65, 2001.

[50] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Optics Express*, vol. 17, pp. 6540–6549, 2009.

[51] M. Ortiz-Gutiérrez, A. Olivares-Pérez, and V. Sánchez-Villicaña, "Cellophane film as half wave retarder of wide spectrum," *Optical Materials*, vol. 17, no. 3, pp. 395–400, 2001.

[52] N. Lütkenhaus, "Estimates for practical quantum cryptography," *Physical Review A*, vol. 59, p. 3301–3319, 1999.