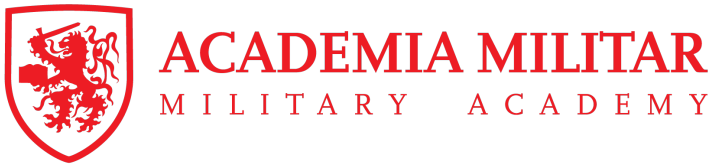


High-Speed Free-Space Quantum Key Distribution

Ricardo Figueiredo Ferreira

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisors: Prof. Emmanuel Zambrini Cruzeiro
Prof. Paulo Sérgio de Brito André

Examination Committee

Chairperson: Prof. José Eduardo Charters Ribeiro da Cunha Sanguino
Supervisor: Prof. Emmanuel Zambrini Cruzeiro
Member of the Committee: Prof. Manfred Niehus

December 2023

Declaration

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

First and foremost, I extend my heartfelt gratitude to my family. Specifically, to my parents and sister for their unwavering support, and to my uncle Carlos, the person who most encouraged me to pursue the path I have chosen to tread.

I am exceedingly grateful to my supervisors, Professors Paulo André and Emmanuel Cruzeiro. In particular to Professor Emmanuel for his consistent availability and the thoroughness with which he addressed any doubts or questions I had. I also wish to acknowledge Pedro Mendes, whose guidance and help was invaluable in the execution of the experimental work.

A sincere thank you to my closest friends, Bernando and Paulo, our friendship, spanning nearly two decades, has been a constant source of joy and motivation.

I would like to express my appreciation to my colleagues at Academia Militar, whose inspiration and encouragement have been vital in pushing me to realize my highest potential.

Finally, I extend my thanks to Instituto de Telecomunicações for offering a dedicated workspace conducive to this work, along with the valuable equipment that played a crucial role in the process of experimental quantum key distribution.

Abstract

The goal of cryptography is to encode data in such a way that no one can decode it unless they are the intended recipient. With the emergence of quantum computing, classical cryptography is not reliable enough to protect sensitive information. Nevertheless, there are alternatives. Quantum Key Distribution (QKD) is a method to secure communication based on the laws of quantum physics. Due to being impossible to measure the quantum state of a system without disturbing it, QKD provides a way to communicate between two parties while being, in theory, immune to eavesdropping.

In this work, a free-space high-speed QKD setup is proposed, with the objective of implementing the polarization three-state one-decoy variant of the BB84 protocol. An assessment of the best type of laser diode to use for free-space QKD is made between several options. The system's performance was assessed, incorporating a quantitative analysis of system losses and an estimation of the number of photons traversing the quantum channel. The system achieved a Quantum Bit Error Rate (QBER) of 1.58% for the Z basis and 1.46% for the X basis, for an average reception of two photons per pulse. Preliminary QBER measurements were also undertaken in the context of Quantum Keyless Private Communication protocols, focusing on the average number of photons per pulse.

Keywords

Quantum Key Distribution; Weak coherent pulses; Quantum states measurements; Secure optical communications.

Resumo

O objetivo da criptografia é codificar dados de tal forma que ninguém os possa descodificar, a não ser que seja o destinatário pretendido. Com o aparecimento da computação quântica, a criptografia clássica não é suficientemente fiável para proteger informações sensíveis. No entanto, existem alternativas. A Distribuição de Chaves Quânticas (DCQ) é um método de segurança das comunicações baseado nas leis da física quântica. Devido à impossibilidade de medir o estado quântico de um sistema sem o perturbar, a distribuição de chaves quânticas proporciona uma forma de comunicar entre duas partes, sendo, em teoria, imune a potenciais ouvintes.

Neste trabalho, é proposta uma configuração de DCQ de alta velocidade e em espaço livre, com o objetivo de implementar a variante de polarização de três estados um falso do protocolo BB84. É feita uma avaliação do melhor tipo de díodo laser a utilizar para DCQ em espaço livre. O desempenho do sistema foi avaliado, incorporando uma análise quantitativa das perdas do sistema e uma estimativa do número de fotões que atravessam o canal quântico. O sistema atingiu uma taxa de erro de bit quântico de 1.58% para a base Z e 1.46% para a base X, para um número médio de fotões de dois por pulso. Foram também efectuadas medições preliminares no contexto de Protocolos de Comunicação Privada Quântica Sem Chave, com um foco no número médio de fotões por pulso.

Palavras Chave

Distribuição quântica de chaves; Pulsos coerentes fracos; Medidas de estados quânticos; Comunicações ópticas seguras.

Contents

List of Figures

List of Tables

List of Symbols

I	Electric Current	A
P	Power	W
λ	Wavelength	m
ω	Angular Frequency	rad
c	Speed of Light	$m \cdot s^{-1}$
f	Frequency	Hz^{-1}
h	Planck's Constant	$J \cdot Hz^{-1}$
k	Wave Number	m^{-1}
t	Time	s

Acronyms

CW	Continuous Wave
DC	Direct Current
EOAM	Electro-Optic Amplitude Modulator
GEO	Geosynchronous Equatorial Orbit
HWP	Half-Wave Plate
IEEE	Institute of Electrical and Electronics Engineers
LED	Light-Emitting Diode
LEO	Low Earth Orbit
MASER	Microwave Amplification by Stimulated Emission of Radiation
NASA	National Aeronautics and Space Administration
PBS	Polarizing Beamsplitter
QBER	Quantum Bit Error Rate
QWP	Quarter-Wave Plate
QKD	Quantum Key Distribution
QKPC	Quantum Keyless Private Communication
RSA	Rivest–Shamir–Adleman
VCSEL	Vertical-Cavity Surface-Emitting Laser

1

Introduction

Contents

1.1 Introduction

Telecommunication is defined as the transmission of information between two or more parties using radio, optical, or other types of electromagnetic signals. In today's world, telecommunication has become the foundation for governments, businesses, and communities to connect and share information. From this technology arises an innate need to secure communication and make it theoretically invulnerable to potential eavesdroppers with malicious intents. Thus, telecommunication and cryptography are fundamental parts of how our society operates.

Conventionally, encrypting data is not a guarantee of protection; it is a way of making it harder to extract information for an eavesdropper. Quantum computation has the potential to make it easy to access conventionally encrypted data, meaning it breaks some important modern cryptography protocols. In this context, quantum algorithms are almost exponentially faster at inverting some (widely used) encryption functions than classical decryption algorithms. This raises concerns for data transfer security, and it is a problem that needs to be addressed as soon as possible.

Quantum physics is known to have counter-intuitive laws that describe the behavior of matter and energy at the atomic and subatomic levels. For example, measurements cause disturbances, so it is impossible to do a measurement without disturbing a quantum system (except if the quantum state is compatible with the measurement) [1]. This is the basis of quantum cryptography and one of the fundamental concepts that guarantee the security of Quantum Key Distribution (QKD).

Based on the idea that a measurement can change the state of a system, it is possible to detect eavesdropping, which leads to provably secure QKD [2]. This idea contrasts with classical cryptography systems, called computationally secure, which rely on how difficult it is to solve a mathematical function. These classical systems are also susceptible to passive eavesdropping because the encoding is done with measurable physical properties that can be observed without disturbance.

Currently, practical modern QKD systems are typically limited to approximately 100 km. Various solutions have been proposed for long-distance QKD, including quantum repeaters [3] (which lack extensive development) and satellite quantum communication [4]. The primary objective of this work is to develop a free-space QKD communication system, optimize its performance, and assess its capabilities. Additionally, the aim is to achieve the creation of quantum states with a Quantum Bit Error Rate (QBER) compatible with the implementation of various QKD protocols. Subsequently, this setup will be miniaturized and designed to fit within a nanosatellite, exemplified by a CubeSat.

2

State-of-the-Art

Contents

2.1 Communication Satellites

The first communication satellite, named Echo, was launched in 1960 by the United States National Aeronautics and Space Administration (NASA). It was a passive spacecraft based on a balloon design, made of Mylar, it required around 1800 kilograms of air to be inflated, thus measuring around 30 meters in diameter. Once in orbit, the air inside the balloon expanded, enabling the reflection of radio transmissions between two ground stations [5]. These types of satellites were credited with improving ground station technology and satellite tracking systems that were indispensable for the development of active satellites.

After two years of further development in the field, Telstar was launched. This satellite was developed by Bell Telephone Laboratories to become the world's first active communications satellite and "demonstrated the feasibility of transmitting information via satellite, gained experience in satellite tracking, and studied the effect of Van Allen radiation belts on satellite design" [6]. Telstar was responsible for relaying the world's first transatlantic television signal (from North America to Europe), operated in a Low Earth Orbit (LEO) (around 500 km), and the signals received were amplified by a low-noise Microwave Amplification by Stimulated Emission of Radiation (MASER), the predecessor of the modern laser [7]. With the continual development of satellites, it was proven the reliability and efficiency of satellite communication. Subsequent systems adopted a much higher orbit (35,900 km), staying in a Geosynchronous Equatorial Orbit (GEO) and matching the angular speed of the Earth's rotation, thus enabling constant coverage of specific areas and better control of these systems [8].

Since then, satellite communication has became an important technology that has played a significant role in the development of modern communication systems. It has several advantages, including transmitting signals over long distances and to remote locations where other forms of communication may not be possible or practical. Furthermore, with the growth of information technology, there is an increasing need to secure data transfer, so efficient encryption methods need to be developed. Classical encryption algorithms were able to cover this problem temporarily; however, due to the recent research in cryptography and quantum computing technology, it is proven that some of these widely used methods are not only unsecure, but even easy to break with quantum computers. This problem can be solved by using quantum cryptography, which will, in the near future, allow data to be securely sent and received over long distances.

2.2 Asymmetrical and Symmetrical Cryptosystems

Asymmetrical cryptosystems use a pair of keys for encryption and decryption. One key, called the public key, is used to encrypt the message, while the other key, called the private key, is used to decrypt it. So, if

Bob[1] wants to receive encrypted messages from a public cryptosystem, he has to first choose his private key. Then, he uses a one-way function to compute a public key, which he discloses to any interested party. Alice has to use Bob's public key to encrypt the message she wants to send. Finally, Bob can decrypt the message sent from Alice with his private key.

The security of these cryptosystems is based on computational complexity (how hard the one-way function is to inverse) [1]. Quantum computers pose a threat to these systems because they can perform these calculations exponentially faster than classical computers (section 2.3) [9].

Symmetrical cryptosystems, on the other hand, use the same key for both encryption and decryption. This means the same key must be shared between the sender and recipient for the message to be securely transmitted. These cryptosystems are based on the "one-time pad", a random key that must be as long as the message and is used only once to encrypt or decrypt a single message. In this scheme, Alice encrypts her message by performing a bitwise exclusive-or (XOR) operation between the message and the key [10]. The resulting string is sent to the recipient Bob. Bob then decrypts the string by simply performing the same XOR operation using the same key.

One-time pads are theoretically unbreakable (provably secure) because the key is random and used only once, thus resulting in a random string of bits [11]. One flaw of this cryptosystem is that the key has to be securely sent by trusted means from Alice to Bob. Quantum cryptography algorithms provide a solution to this problem, enabling insecure channels to share arbitrarily long keys (section 2.4).

2.3 Shor's Algorithm

Encrypting data using classical encryption algorithms isn't a guarantee of protection; it's a way of making it harder to access, hopefully, harder enough that it's not worth trying decrypting. This is why researchers in the field of cryptography have been trying to develop quantum algorithms that solve problems that are not solvable classically in polynomial time.

In 1994, the American mathematician Peter Shor developed a quantum computer algorithm for efficiently factoring integers [9]. Factoring integers has been used as the basis of several cryptography systems. The significance of this algorithm is highlighted by its potential to compromise established public key cryptography methods, such as Rivest–Shamir–Adleman (RSA), when applied with a sufficiently advanced quantum computer. In the case of RSA, a public key N is generated as the product of two large prime numbers; thus, the decryption of RSA is commonly achieved through the factorization of N. However, with classical algorithms, factoring becomes increasingly time-consuming as N grows large, making it necessary to spend a lot of time or resources in decryption. A method of encryption that is exponentially harder to solve with the increase of the public key N in classical computers can now be

[1] In cryptography, Alice, Bob, and Eve are commonly used as placeholder names for the three participants in a conversation, representing the sender, receiver, and eavesdropper, respectively.

solved in polynomial time by applying Shor's algorithm. If a quantum computer could systematically and reliably implement Shor's algorithm, it could potentially break many of the cryptographic systems currently in use, rendering them vulnerable to attacks and posing an immediate threat to today's security systems. With the discovery of this quantum factoring algorithm, it is proven that classical cryptography algorithms are unsafe and easily broken with the use of quantum computers.

In 2015, a team of physicists from the University of Innsbruck and the Massachusetts Institute of Technology reported the realization of a fully scalable Shor Algorithm [12]. The algorithm was implemented using a quantum computer comprised of a linear Paul trap in which an electric field holds five calcium-40 ions and uses them as qubits (section 2.5). This experiment exhibited success probabilities in excess of 90% and was the first implementation of the algorithm that did not use prior knowledge of the factors to simplify the computational procedure.

2.4 Quantum Key Distribution

In 1982, Charles H. Bennett, from IBM New York, and Gilles Brassard, from the University of Montreal, published the first-ever article on quantum cryptography, in which the term "Quantum Cryptography" was coined [13]. In this paper, it was proposed that "the use of quantum mechanical systems, such as polarized photons, to record information gives rise to novel cryptographic phenomena, not achievable with classical recording media" [13]. Although the objective of the paper was to use photon polarization as the carrier of quantum information, any degree of freedom can, in principle, be used; hence, this article stands as a foundation and initial approach to secure information with quantum cryptography.

One of the first ideas of quantum encryption was to encode a message in a quantum signal in such a way that it could be decoded if left undisturbed, but the action of an eavesdropper would spoil the encoded information and leave the eavesdropper detected. This system was meant to be unidirectional and use a one-time pad encryption [14]. This one-time pad could be reused if no eavesdropper was detected. Bennet and Brassard attempted to publish this paper; however, it was not accepted for publication at the time, although others have since then published the idea [15, 16].

As stated by Brassard, "quantum cryptography is the only approach to privacy ever proposed that allows two parties (...) to communicate with provably perfect secrecy under the nose of an eavesdropper endowed with unlimited computational power and whose technology is limited by nothing but the fundamental laws of nature" [17].

Based on the observer effect of quantum mechanics, the proposal has been advanced that information can be encoded in polarized photons and utilized as a cryptographic key. This effect suggests that the simple act of making a measurement on particular variables of a quantum system could lead to a consequential alteration of other variables within the same system. In this paradigm, any eavesdropping

attempt would inherently disturb the system's quantum state and thus be detectable [18].

In 1983, Bennet and Brassard realized it would be easier to use a quantum channel to generate a long secret key to encrypt and decrypt data [19]. The idea was born that a "quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else" [2]. Due to unavoidable disturbance, if an eavesdropped tried to access the quantum key, it would be discarded, if not, it could be used to transmit sensitive information safely. Moreover, the new scheme was much more robust against lost photons since a random of a random bit string is still a random bit string, albeit shorter.

Hence, QKD is a method for securely distributing a cryptographic key over a distance using the principles of quantum mechanics. It is a way to establish a shared secret key between two parties, that can be used to encrypt and decrypt messages sent between them. The key is generated and transmitted using quantum states of light. This is the foundation of QKD, which is still being researched and improved today. It remains, to this date, the most feasible of all proposed applications for the burgeoning field of quantum information science. To illustrate this, it should be noted that commercial QKD systems exist since 2001 [20].

Within the matrix of quantum key distribution systems, particularly in high-speed free-space architectures, the quantum bit or qubit serves as the fundamental information unit. Distinct from classical bits, qubits offer enhanced capabilities due to the principles of superposition and entanglement, giving rise to new paradigms in information security.

2.5 Quantum Bits and Quantum Superposition

The quantum bit (qubit), a quantum analogue to the classical bit, serves as the cornerstone of quantum information processing systems, from quantum computing to quantum key distribution. Governed by quantum mechanical laws, qubits facilitate complex computations and secure communication paradigms that are unfeasible within the classical domain. In classical computing, a bit exists in one of two discrete states: 0 or 1. Contrarily, qubits operate under the principle of superposition, allowing them to occupy a linear combination of these states. Mathematically, a pure qubit $|\psi\rangle$ state can be represented as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

where $|0\rangle$ and $|1\rangle$ denote two orthonormal basis states represented by the column vectors in (2.2), and α and β complex coefficients and describe probabilistic amplitudes. The state of a qubit is thus defined in a two-dimensional complex Hilbert space, which is a mathematical construct used to describe the state of a quantum system, such as a photon, and is composed of a vector space with an inner product.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.2}$$

The Born Rule provides the probability density of observing a system in a specific state upon measurement; it stipulates that if a quantum entity is described by a wavefunction $|\psi\rangle$, then the probability $P(x)$ of finding it in the state x is given by (2.3). Due to the probabilistic origin of this axiom, the coefficients of the system's wavefunction, α and β in the case of (2.1), are constrained by (2.4). Thus, a measurement made upon a quantum system disrupts its superposition, probabilistically collapsing it into one of the basis states.

$$P(x) = ||\psi\rangle|^2 \tag{2.3}$$

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.4}$$

2.6 Light Polarization

There are several physical implementations of qubits, such as photon polarization, discrete energy levels of ions, nuclear spins of an atom, spin states of electrons, etc. However, in the realm of quantum communication and cryptography, the obvious choice is photon polarization due to their high fidelity, easy manipulation, and capacity for long-distance transmission.

In the early 1820s, Augustin-Jean Fresnel introduced the Fresnel Wave Theory, which provided a comprehensive framework for understanding three fundamental optical phenomena: interference, diffraction, and polarization. Additionally, through experimental collaboration with François Arago, Fresnel demonstrated that the optical field could be effectively described by two orthogonal components within the transverse plane to the direction of propagation, which are today represented by the electric field (2.5). This pivotal insight laid the foundation for our modern understanding of photon polarization.

$$\vec{E} = \begin{pmatrix} E_x(z,t) \\ E_y(z,t) \\ 0 \end{pmatrix} = \begin{pmatrix} E_x e^{i(\omega t - kz + \phi_x)} \\ E_y e^{i(\omega t - kz + \phi_y)} \\ 0 \end{pmatrix} = \begin{pmatrix} E_x e^{i(\phi_x)} \\ E_y e^{i(\phi_y)} \\ 0 \end{pmatrix} e^{i(\omega t - kz)} \tag{2.5}$$

For light propagating along the *z*-axis, the electric field can be described by the equation above, where $\omega = 2\pi f$ is the angular frequency, $k = \frac{2\pi}{\lambda}$ the magnitude of the wave number, E_{0x} and E_{0y} the peak amplitudes along the *x* and *y*-axis and ϕ_x, ϕ_x arbitrary phases. The polarization state of a quasi-monochromatic[2] can also be simplified and represented by the Jones Vector (2.6), which displays the phase and amplitude of the electric field in the x and y directions.

[2]Light radiation with a very narrow waveband.

$$E = \begin{pmatrix} E_x e^{i(\phi_x)} \\ E_y e^{i(\phi_y)} \\ 0 \end{pmatrix} \tag{2.6}$$

The physical representation of the electric field is the real part of (2.5), and summing or combining different electric fields enables the creation of new solutions, which are superpositions of the two orthogonal linearly polarized components and represent different polarization orientations (2.7). This is possible due to Maxwell's equations being linear in vacuum [21]. Let E_x represent horizontal polarization and E_y vertical polarization:

$$\vec{E} = E_{0x} cos(\omega t - kz + \delta_x) \left|H\right\rangle + E_{0y} cos(\omega t - kz + \delta_y) \left|V\right\rangle . \tag{2.7}$$

In the aforementioned equation, $|H\rangle$ and $|V\rangle$ serve as unit vectors for the horizontal and vertical components, or x and y planes, respectively. Light consists of perpendicular electric and magnetic fields and can be depicted graphically, as illustrated in Fig. 2.1. In the given example, light exhibits linear polarization along the *y*-axis, thus setting E_{0x} intensity to zero.

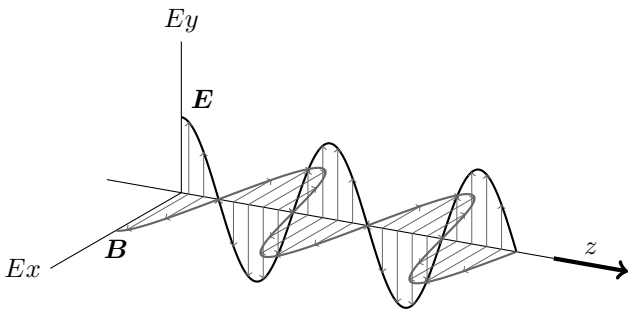


Figure 2.1: Graphical representation of an electromagnetic wave's components.

The intensity of light can be calculated by the sum of the squares of the absolute values of (2.6). It is common to normalize it to 1 which allows representing different polarizations states as the following:

$$\left|H\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \left|V\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.8}$$

$$\left|D\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\left|H\right\rangle + \left|V\right\rangle), \qquad \left|A\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\left|H\right\rangle - \left|V\right\rangle). \tag{2.9}$$

$$\left|R\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}} (\left|H\right\rangle + i \left|V\right\rangle), \qquad \left|L\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} = \frac{1}{\sqrt{2}} (\left|H\right\rangle - i \left|V\right\rangle). \tag{2.10}$$

These polarization states are identified as degenerate states, which can be broadly categorized into the following: Horizontal (H) and Vertical (V) represent states where the electric field intensity is exclusively

aligned with the x or y axes, respectively. In contrast, Diagonal (D) and Anti-diagonal (A) states are characterized by equivalent electric field intensities in both the x and y planes without any accompanying phase difference between the two orthogonal components. Additionally, Right Circularly Polarized (R) and Left Circularly Polarized (L) states are distinguished from the aforementioned linear states by an additional phase difference $\phi = \phi_x - \phi_y$, which assumes values of either $\frac{\pi}{2}$ or $-\frac{\pi}{2}$, respectively. These assorted polarization states can be geometrically illustrated within a three-dimensional construct known as the Poincaré sphere, as delineated in Fig. 2.2.

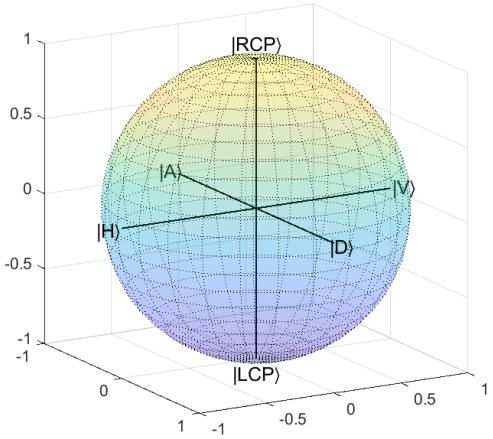


Figure 2.2: Poincaré sphere.

Within this three-dimensional framework, orthogonal polarization states are antipodal points on the sphere's surface, thereby providing a robust mapping between the mathematical abstraction and physical phenomena. For instance, the H and V states lie along the equator at opposing ends, as do the D and A states, which can be described as superpositions of the states before with a 45-degree phase shift in each direction. The R and L states are situated at the North and South poles of the sphere, respectively.

Leveraging these very quantum states of polarization, the BB84 protocol provides a secure methodology for cryptographic key exchange.

2.7 BB84

In December 1984, there was a coding and information theory session for an Institute of Electrical and Electronics Engineers (IEEE) conference in Bangalore, India. The resulting paper [22] was the first published article about QKD and remains the most relevant article on quantum information science.

In QKD, the polarization of individual photons is often used to encode information about the key being transmitted. Photons are particles of light that can be described as waves, and their polarization refers to the orientation of their electric field. Photons can have different polarizations, such as horizontal and vertical, diagonal, or circular (phase shift induced). The key is typically transmitted by sending a sequence

of photons, each with a specific polarization, from one party (Alice) to another (Bob). The polarization of each photon encodes one bit of the key, and the sequence of photons represents the entire key.

As a physical representation of a qubit, when subjected to a measurement in the rectilinear basis, a photon becomes either vertically or horizontally polarized with probabilities $(\cos(\alpha))^2$ and $(\sin(\alpha))^2$ respectively. These outcomes root from the qubit pure state in (2.1), after letting $|H\rangle$ and $|V\rangle$ represent the two qubit basis states, with $\alpha\,\epsilon\,[0, 2\pi[$ being the predominant polarization angle.

$$|\psi\rangle = \cos(\alpha)\,|H\rangle + \sin(\alpha)\,|V\rangle\,. \tag{2.11}$$

The protocol goes as follows:

1: If Alice wishes to send Bob a message, Alice initiates the process by sending Bob a key or stream of photons. The photons must first be polarized randomly to be either $|H\rangle$, $|V\rangle$, $|D\rangle$, or $|A\rangle$ (0, 90, 45, -45 degrees, respectively). Then, Bob receives these photons on the quantum channel and, for each one, decides at random to either use rectilinear (horizontal and vertical) or diagonal (diagonal and anti-diagonal) measurement basis;

2: After this, Bob uses a public channel to announce, for each photon, which type of measurement he made (rectilinear or diagonal), but not the result he obtained. Alice also has to publicly disclose whether each polarization Bob announced corresponds to the same polarization she encoded the photons with;

3: Basis reconciliation: Bob discards every photon he measured with a different orientation than the one Alice encoded and keeps the remaining. Each photon he keeps has perfectly correlated results with Alice, so disregarding the ones with a different basis is a simple error correction scheme;

4: Bob, at last, attributes the binary values 0 to $|H\rangle$, and $|D\rangle$, and 1 to $|V\rangle$, and $|A\rangle$. After basis reconciliation, this string with half the bit size is called a sifted key and can be used to encrypt and decrypt a single message. It should be noted that the public channel used should be authentic to guarantee an eavesdropper does not claim to be Bob and intercept the transmission. "Neither Alice nor Bob can decide which key results from the protocol. Indeed, it is the conjunction of both of their random choices which produces the key" [1]. Finally, Alice and Bob use the key to communicate via a classical (or quantum) communication protocol.

It is important to note that even though QKD was first developed by Bennet and Brassard, thus the name BB84, it was only later, in 1991, that Artur Ekert developed quantum entanglement-based QKD, relying on the violation of Bell's inequality [23], although not on the realm of this work. In this context, Table I delineates the various elements of this protocol. Herein, the characters Z and X symbolize the rectilinear and diagonal polarization states, respectively, while Y and N are indicative of affirmative and negative responses during the process of basis reconciliation.

In late October 1989, Bennett, Brassard, and Ekert established the world's first-ever secret quantum

Table I: BB84 Protocol Visualized

Alice's randomly chosen bit	0	1	0	1	0	1	0	1
Alice's random chosen basis	Z	X	X	Z	Z	X	X	Z
Photon polarization sent	$\|H\rangle$	$\|D\rangle$	$\|A\rangle$	$\|V\rangle$	$\|H\rangle$	$\|D\rangle$	$\|A\rangle$	$\|V\rangle$
Bob's random measurement basis	Z	X	X	Z	X	Z	Z	X
Bob's polarization measurement	$\|H\rangle$	$\|D\rangle$	$\|A\rangle$	$\|V\rangle$	$\|D\rangle$, $\|A\rangle$	$\|H\rangle$, $\|V\rangle$	$\|H\rangle$, $\|V\rangle$	$\|D\rangle$, $\|A\rangle$
Basis reconciliation	Y	Y	Y	Y	N	N	N	N
Secret key	0	1	0	1				

transmission over a distance of 32 cm [24]. This quantum system was able to transmit information in perfect secrecy. The design started with a Light-Emitting Diode (LED) that produced faint flashes of green light (Fig. 2.3), these faint flashes were then collimated with a pinhole, lens, and filter. After this collimation, a polarizer induced a horizontal polarization, and two Pockels cells (devices that have a controllable birefringence[3]) would change the polarization to 0, 45, 90, or 135 degrees. These polarized light flashes eventually reach the receiver, and another two Pockels cells would either shift the polarization a further 45 degrees or not at all. This shift allowed the receiver to choose between measuring rectilinear or diagonal polarization. In rectilinear polarization, a Wollaston Prism would separate horizontally and vertically polarized photons and send them to two separate photomultipliers, converting them into electric signals.

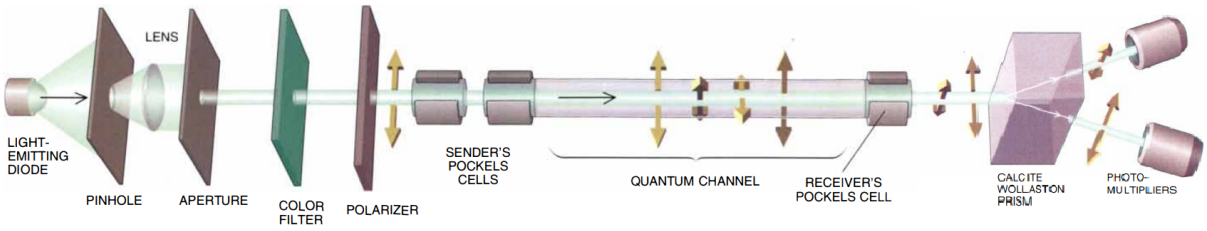


Figure 2.3: First quantum system prototype [25].

After this successful experiment, attention from the physics community shifted more towards this matter. It inspired prototypes capable of realizing QKD through optical fiber over several kilometers [26,27]. Furthermore, line of sight and the link of users through satellite (the objective of this article) were also inspired by this design; according to Brassard: "the use of entanglement could be instrumental in a truly secure satellite-based implementation of quantum cryptography" [17].

[3]Birefringence is the property of a material to refract light in different directions depending on the polarization of the light.

2.8 Performance Metrics

2.8.1 Secret Key Rate

The secret key rate is a pivotal metric that measures the efficiency of QKD protocols. The higher the secret key rate, the more secure and efficient the quantum communication is, making it a crucial determinant in the practical applicability of QKD systems.

The secret key rate is defined as the number of secure key bits generated per unit of time. Several factors affect the secret key rate, namely:

Sifted key rate: this rate, which refers to the remaining key bits after basis reconciliation, directly impacts the secret key rate. It is influenced by various protocol-specific parameters and is usually about 50%;

Error Rate: increased error levels jeopardize the key's integrity and the secret key rate. While error-correcting algorithms can moderate this impact, they also introduce a reduction in system efficiency.

The average secret key rate for state-of-the-art free-space quantum key distribution systems range from several thousand bits per second [28, 29] to tens of thousands of bits per second [30].

2.8.2 Quantum Bit Error Rate

In quantum communication, the QBER is a vital metric for evaluating the reliability and security of the transmission channel. It is defined as the ratio of the number of bits with errors to the total number of bits transmitted and received.

In quantum communication systems, a higher photon count typically contributes to a lower QBER, as it increases the signal-to-noise ratio, making the transmission more reliable. However, this benefit comes with a trade-off in terms of security. Higher photon counts increase the probability of multiphoton events, which can be exploited through several types of attacks, thereby compromising the integrity of the secure communication channel. A sudden or unexplained increase in the QBER could, therefore, indicate potential eavesdropping attempts.

Conversely, lower photon counts are generally more secure due to the reduced likelihood of multi-photon pulses that could be exploited in eavesdropping attacks. Thus, optimizing the photon count is a balancing act between improving QBER and ensuring the security of the quantum communication system. A typical average photon count per pulse in free-space QBER experiments is about 0.1 [31–33]; however, this metric is highly dependable on other variables, such as the transmission rate and the detector's properties. A higher QBER is typically caused by:

Noise in the communication channel: in free-space QKD, atmospheric turbulence, scattering, and

absorption are notable noise sources [34, 35];

Imperfections in the optical components: the quality and precision of the components used in a QKD setup, such as modulators can lead to polarization or phase errors;

Detector inefficiencies: alignment errors, and low-efficiency or high dark counts[4] detectors increase the QBER substantially [36];

Timing jitter: the misalignment in the timing of photon arrival can also contribute to errors in post-processing [36].

In the perspective of long-distance QKD, escalating channel losses result in fewer signals reaching the receiver, which in turn deteriorates the QBER. As dark counts start to dominate these attenuated signals, these error rates can cross protocol-specific acceptable thresholds, making secure key derivation unattainable from the obtained sifted keys. This constraint caps the maximum achievable distance for QKD; hence, for successful long-range QKD, the utilization of single-photon detectors with low dark count rates is indispensable [37].

The two primary causes affecting the elevation of QBER are the quantum efficiencies of the single-photon counting modules and their dark count rate. To quantify the effect of these factors, both the dark counts and incoming polarized photons are modeled using Poisson distributions (2.12).

$$P(n,\mu) = \frac{\mu^n}{n!}e^{-\mu} \tag{2.12}$$

Within this equation, the variable P represents the probability associated with the presence of precisely n photons within a laser pulse subjected to attenuation that results in a mean photon number μ per pulse.

Let $P_{dark}(n_d, \mu_d)$ denote the Poisson distribution governing the dark counts, characterized by an average rate of μ_d counts per pulse. Similarly, $P_{signal}(n_s, \mu_s)$ represents the Poisson distribution describing the polarized photons, with an average rate of μ_s photons per pulse. The Poisson distribution describes the probability of detecting n_d or n_s events in a single pulse and can be employed to encapsulate the stochastic nature of both dark counts and signal photon arrivals.

The lower bound on the QBER can be calculated using the following equation, under the assumption that a higher number of dark counts correlates with a higher incidence of key bit errors:

$$QBER_{LB} = \sum_{n_d=1}^{\infty}\left[P_{dark}(n_d,\mu_d) \times \sum_{n_s=0}^{\infty} P_{signal}(n_s,\mu_s)\right] \times 100. \tag{2.13}$$

The product of the probabilities $P_{dark}(n_d, \mu_d)$ and $P_{signal}(n_s, \mu_s)$ describes the joint probability of, in a single pulse, registering n_d dark counts in one detector not subjected to any incoming polarization states, and n_s signal counts in a different detector that is receiving such states, provided $n_d > n_s$. Equation

[4] Dark counts are detections registered by a single-photon detector even when no actual photons from the intended source are hitting the detector.

(2.13) is thus formulated to quantify the likelihood of incorrect polarization state estimation attributable to dark counts in the latter detector, with all other contributors to the QBER set aside.

Despite being unable to substantially lower dark counts on a single detector, their detrimental influence on QBER can be mitigated. By significantly increasing the transmission rate, i.e., the number of pulses, a lower effective average dark count rate μ_d per pulse can be achieved. This increase will lead to fewer polarization estimation errors, provided that the average signal photon count μ_s can be maintained constant.

This analysis elucidates the significant impact of dark counts on QBER. Lowering this particular metric has the potential to substantially reduce the error rate, in some instances by several orders of magnitude, as corroborated by existing literature [36]. In Fig. 2.4, the minimum QBER as a function of dark counts and mean photon number can be visualized.

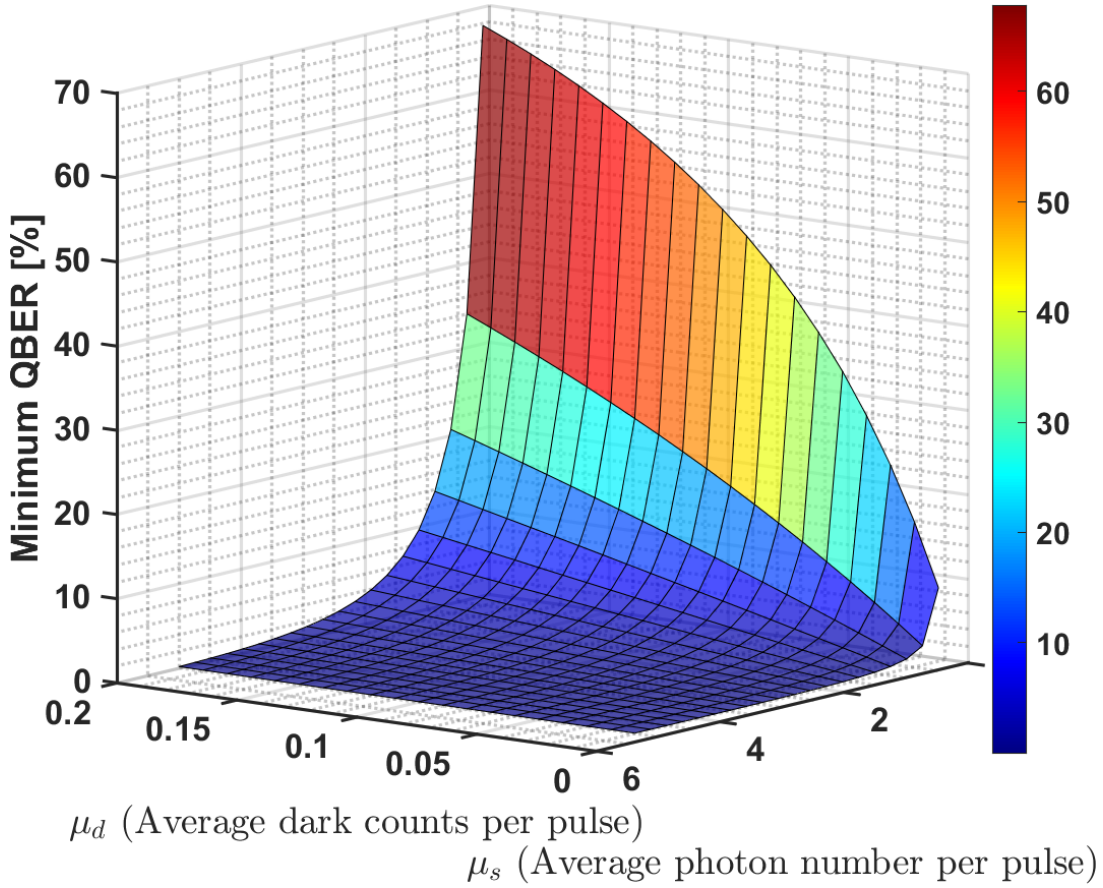


Figure 2.4: Minimum QBER as a function of dark counts and mean photon number.

Lowering the QBER allows QKD experiments to achieve higher transmission distances and secret key rates, thus enabling the further development of quantum networks and satellite quantum communication systems.

2.9 Quantum Networks and Satellite Quantum Communication

Until 2012, entanglement distribution had only been achieved up to a physical distance of 100 km [38], with the limitation being the photon loss in the optical quantum channel (exponential scaling with length). One solution is to use quantum repeaters (which can amplify and regenerate quantum states as they are transmitted over long distances) [3], thus dividing a transmission line into N smaller elements. However, quantum repeaters' usefulness is still hindered by challenges associated with storage and retrieval efficiency. Satellite and space-based technologies are interesting solutions to this problem because they can link very distant locations on the Earth's surface. The main advantage of this is that photon loss largely occurs in the lower ten thousand meters atmosphere; therefore, most of the photons' path is in a system of near-vacuum with almost zero absorption and loss of quantum coherence.

In 2016, China launched the first satellite designed to test quantum communication fundamentals in space. This satellite, named "Micius", weighed 635 kg and was launched to orbit at an altitude of approximately 500 km [39]. The main goal of this satellite was to demonstrate QKD with two ground stations, the Nanshan telescope, and the Xinglong Observatory. This demonstration was possible by distributing pairs of entangled photons to two locations separated by 1203 km on the Earth [40]. What made this possible was a Sagnac interferometer, which is used to generate two entangled photons (induce a phase shift by introducing angular velocity on the system) by shining an ultraviolet laser on a non-linear optical crystal. This experiment made possible the bidirectional distribution of entangled photons through downlink channels to the ground stations. Entanglement of two single photons was then achieved between both locations on Earth with a two-photon count rate of 1.1 Hz. Bell's inequality tests were then performed at a separation of over 1200 km to prove that entanglement can exist between particles separated by such a considerable distance.

In the matter of satellite-to-ground QKD, in 2017, "a kilohertz key rate from the satellite to the ground over a distance of up to 1,200 kilometers" [41], with the same satellite "Micious", was achieved. This further proves the necessity of satellite-based communication systems because this key rate is about 20 orders of magnitude higher than what would be possible by using optical fiber for the same length.

In 2019, an integrated space-to-ground quantum communication network combining both fiber network (700+ QKD links) and two satellite-to-ground free-space QKD links was achieved [42]. The fiber network covers more than two thousand kilometers, and by integrating the free-space links, a possible communication distance of up to 4.600 km is possible. The satellite-to-ground QKD link also realized a secret key rate of up to 47.8 kilobits per second, more than 40 times higher than two years before. It should be noted that this network is yet to be reliable due to only operating fully when the satellite flies over the ground station since it is not geosynchronous. Satellite-to-ground links for geosynchronous satellites have yet to be achieved.

Fully ground-based QKD networks are already implemented and reliable. In 2011, there was a

long-term performance review of the SwissQuantum QKD network after running for almost two years, with two nodes in Switzerland and one in France [43] (Fig. 2.5).

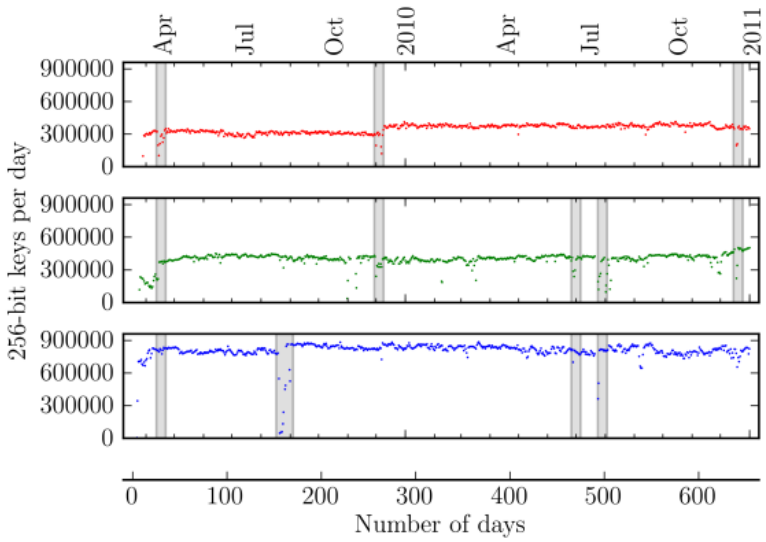


Figure 2.5: Number of 256-bit keys per day in the 3 links [43].

The ”most important prerequisite for the integration of QKD in a telecommunications network is reliability” [43], and this network proved this reliability could be achieved for future free-space systems by combining ground fiber optics with geosynchronous satellite-to-ground links.

3

Proposed QKD Setup

Contents

3.1 Methodology

In this dissertation, a three-state one-decoy BB84 protocol in polarization [44] is implemented. Furthermore, the original proposal of [44] is simplified by reducing the number of components on the emitter side, thereby making the setup more compact (in the perspective of nanosatellites QKD).

Two different approaches can be used for generating quantum states for QKD. These are:

Weak Coherent Pulses: pulses of light with low intensity and a long duration that are carefully prepared to be in a specific quantum state. Weak coherent pulses are generated using highly attenuated lasers or other light sources and can be transmitted over long distances through optical fibers or free-space [45];

Single-Photon Sources: designed to emit a single photon at a time. Single-photon Sources can be generated using various techniques, such as parametric down-conversion or quantum dots [46, 47].

Both technologies have advantages and disadvantages, and the choice of which technology to use will depend on the specific requirements and constraints of the QKD system.

One advantage of weak coherent pulses is that they can be generated and transmitted using existing optical communication systems, which makes them practical for widespread use. However, each pulse contains many photons, which makes it difficult to ensure that only a single photon is transmitted and received. One advantage of single-photon sources is that they can be used to transmit a single photon with high fidelity, which is important for QKD. However, single-photon sources are generally more complex and expensive than weak coherent pulses.

Because of their advantages relative to single-photon sources, weak coherent pulses are much more used in QKD systems. They were also used in this article because of their easy implementation. Due to quantum states being fragile and easily disrupted by noise or interference, the pulse must be strong enough to minimize these effects. At the same time, the pulse should be weak so it can't be reliably intercepted by a third party, making the pulse generation a process of delicate balance.

The most important variable when developing a satellite-to-ground QKD system is the emission frequency. It is established that operating within the first telecommunications window, typically around wavelengths of approximately 800 nm, offers distinct advantages. This wavelength regime leverages well-developed silicon-based single photon detectors and capitalizes on the low photon absorption characteristics of free-space, particularly in the vicinity of 770 nm radiation [48]. Such wavelength selection has yielded secret key lengths exceeding tenfold compared to sources operating at C-band, as documented by Abasifard et al. in their recent work [49].

As an alternative, the use of the second telecommunications windows, spanning the range of 1300 to 1500 nm, has also been contemplated. However, this wavelength region presents certain challenges, chiefly on single photon detectors. Detectors at these longer wavelengths, primarily relying on Ge and InGaAs/InP single-photon avalanche diodes, exhibit elevated dark count rates and afterpulsing

effects [50]. Nevertheless, it is noteworthy that optical fibers exhibit considerably lower attenuation at these wavelengths, rendering QKD systems in this spectral domain more efficient for ground-based communication.

Generating weak coherent pulses necessitates the initial production of Continuous Wave (CW) laser light.This can be done using a laser diode or some other type of laser that produces a stable, single-frequency output. The first proposed solution for creating these pulses was to use Vertical-Cavity Surface-Emitting Laser (VCSEL) diodes due to their high reliability, beam quality, and low cost. Another important feature is the comparatively low-temperature dependence of the emitted wavelengths. Another solution is also available but has yet to be implemented due to not being available in the laboratory. This solution is *Thorlabs' Fiber-Coupled Laser Source* (fiber coupling built into the laser package), this benchtop laser grants easy coupling using simple control of laser-diode-driven fiber optics. The laser diodes are operated from an independent, high-precision, low-noise, constant-current source and temperature control unit (Thorlabs 2022).

3.2 Characterization Setup

A VCSEL is a type of diode that emits light perpendicular to the semiconductor wafer surface. A typical VCSEL emits a low output power in a circular, nearly diffraction-limited beam, which is easier to collimate (or couple into a single-mode fiber) than the output of an edge-emitting laser [51].

VCSEL diodes function by having a couple of very thin active amplifying layers composed of quantum wells in the middle of two Bragg reflectors (Fig. 3.1). The output Bragg reflector has a slightly lower reflectivity which allows light to be emitted from that side.

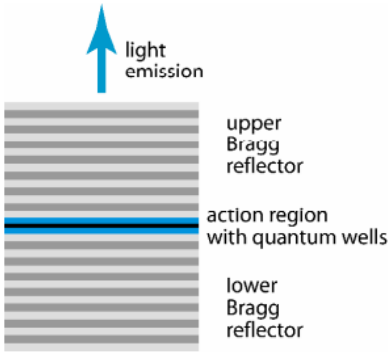
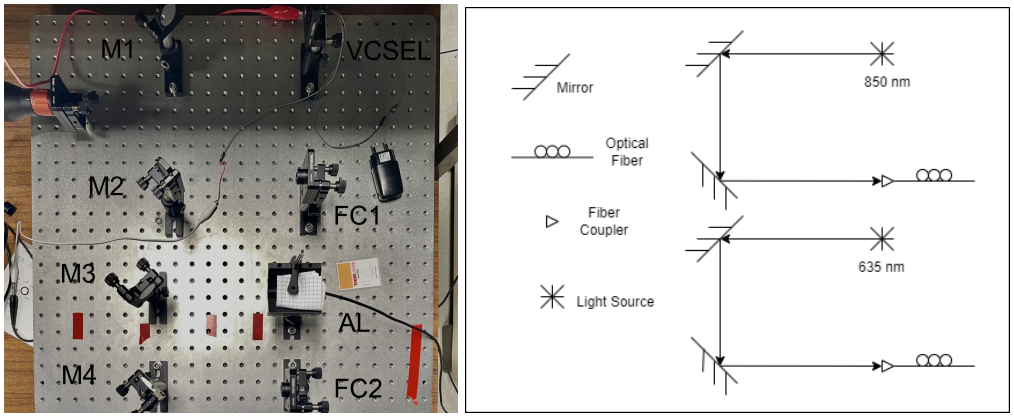


Figure 3.1: Vertical-Cavity Surface-Emitting Laser Diagram [51]

In Fig. 3.2(a), the characterization setup can be visualized. On the upper part, the VCSEL diode is mounted on a support, and two mirrors for collimation can be observed (M1 and M2). There are also two fiber coupler mounts (FC1 and FC2) connected by a single-mode 850 nm optical fiber, and two more

mirrors (M3 and M4) that provide degrees of freedom for collimation of the alignment laser (AL) into the fiber coupler number two. Mirrors number one and four were removed for the measurements performed in this chapter.



(a) Photo of the characterization setup. **(b)** Diagram of the characterization setup.

Figure 3.2: Characterization setup.

The characterization of the VCSEL diodes was done for several samples, the results shown only correspond to the VCSELs with the best performance. In Fig. 3.3, the response of the VCSEL diode to the input current is depicted. This power was measured with *Thorlabs' Analog Handheld PM100A Laser Power Meter Console*. The threshold current, which corresponds to the overtake of stimulated emission over spontaneous emission, is measured at about approximately 2 mA.

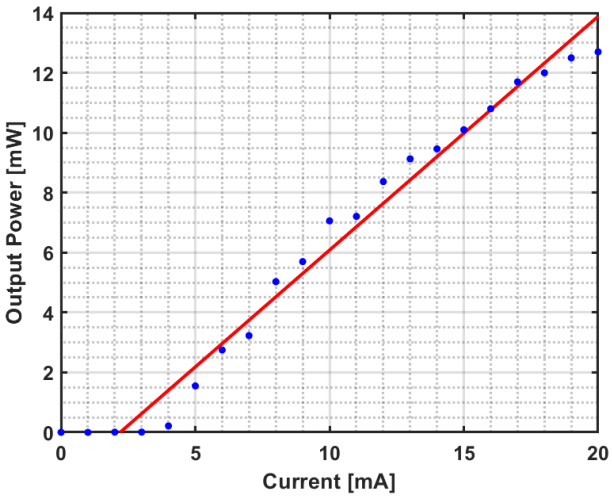


Figure 3.3: VCSEL diode's response to input current.

With this threshold current assessed, higher data points can be used to calculate the linear regression (3.1) and determine the slope efficiency (η), which corresponds to approximately 0.78 mW/mA (Fig. 3.3).

The variable P is the output power, I is the input current, and I_{th} is the threshold current.

$$P = \eta \times (I - I_{th}) \tag{3.1}$$

The dispersion of light in free-space from *Mouser's OPV314* VCSEL diodes with a wavelength of 850 nm will now be analysed (table I). The gaussian diameter metrics were acquired using *Thorlabs' BP209-VIS Scanning-Slit Optical Beam Profiler*. Measurements were made by directing the laser beam into the profiler's input aperture and successively scanning it with two slits of equivalent width but orthogonal orientations, under the control of *Thorlabs Beam 8.2 Software*. The current biasing the diode for the beam's characterization was 14 mA. The values obtained are averages with an uncertainty of 1.2 μm.

Table I: VCSEL's Diodes Beam Dispersion in Free-Space

Distance [cm]	Gaussian Diameter X [µm]	Gaussian Diameter Y [µm]
30	4716.2	4619.2
60	5928.2	5156.4
90	6471.4	5700.6
120	7080.1	6246.0

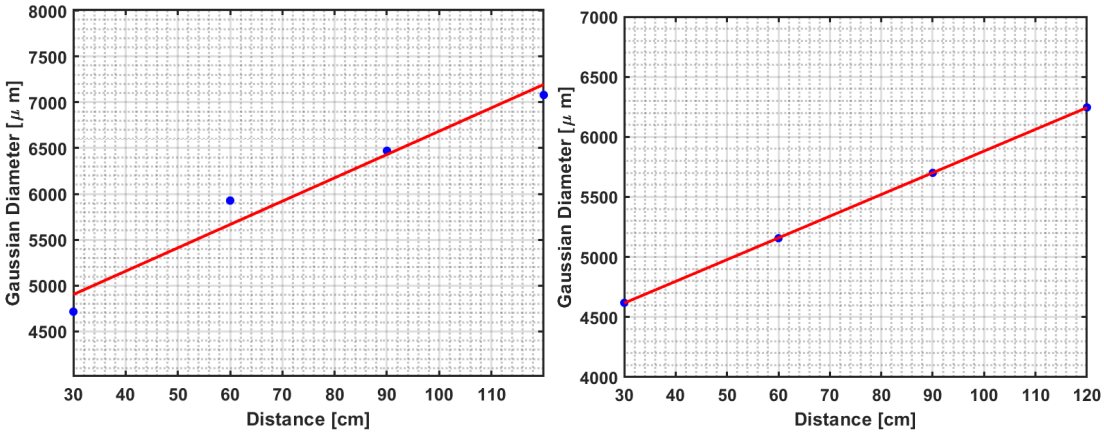
The Gaussian diameter of a laser diode is the size of the laser's beam at a particular point in its propagation, particularly where the intensity is $\frac{1}{e^2}$ (or about 13.5%) of the peak's intensity. This is an important parameter because it determines the size of the laser's beam at different points along its path. It is used to characterize the laser's beam quality and predict the beam's behaviour as it propagates through different optical systems.

On table I, it is possible to observe that the VCSEL diodes used have a high divergence in free-space, as depicted in Fig. 3.4(a), 3.4(b) as blue data points. This divergence causes high loss of power (Fig. 3.5) which occurs due to the beam becoming larger than receiving apertures for longer distances. Since VCSELs are usually fit for free-space applications, it is suspected that the samples in the lab are not of very good quality (their price is also a hint of this, being around six times cheaper than the ones from *Thorlabs*. A visual aid representing the behaviour of the VCSEL diode is provided in Fig. 3.4, 3.5 as a linear fit to the obtained data points, displayed in red.

Using (3.2), it is possible to calculate the beam's divergence (α), using the beam's diameter in two different points ($D_{\text{f}}, D_{\text{i}}$) and the horizontal distance between those points (l), with $D_f > D_i$. This value corresponds to approximately 2.62 milliradians for the X-axis, which is more pronounced in its divergence.

$$\alpha = 2 \times arctan\left(\frac{D_f - D_i}{2 \cdot l}\right) \tag{3.2}$$

In many experiments, it is convenient to couple the output of diode lasers into an optical fiber, in order to, for example, clean the spectral width of the beam. VCSEL's, being surface-emitting laser diodes, emit light in a single spatial mode, allowing the efficient coupling to a single-mode fiber with a lens or



(a) Gaussian diameter X. **(b)** Gaussian diameter Y.

Figure 3.4: Gaussian diameters in free-space.

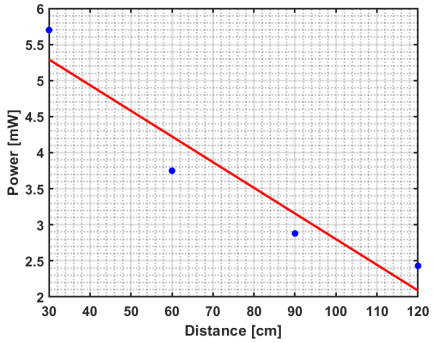


Figure 3.5: Power meter measurement.

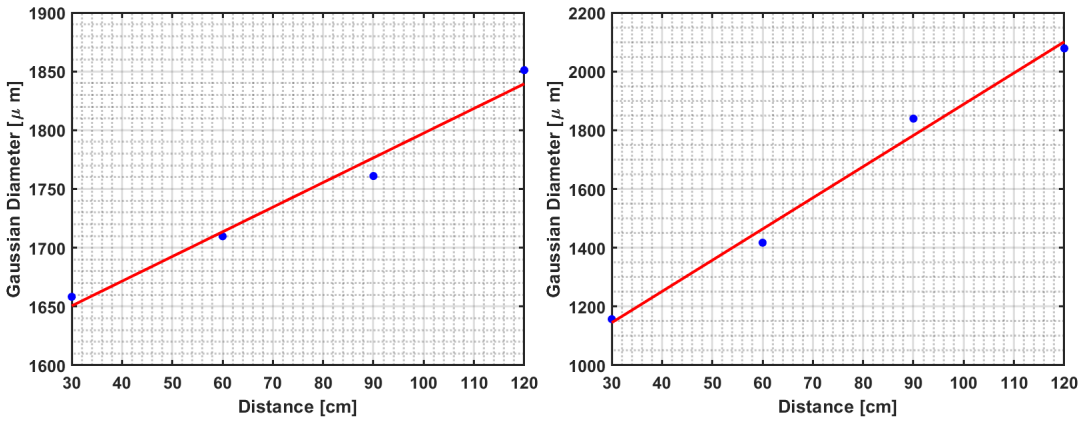
collimator. Thus, the dispersion of VCSEL diodes in free-space and the loss of power with distance were also analysed after the beam's propagation through an optical fiber (table II).

Table II: VCSEL's Diodes Beam Dispersion in Free-Space After Propagating Through Optical Fiber

Distance [cm]	Gaussian Diameter X [µm]	Gaussian Diameter Y [µm]
30	1658.3	1157.2
60	1709.8	1417.3
90	1761.0	1839.5
120	1851.1	2078.5

The optical fiber gives the beam an optimal spatial distribution in the form of a gaussian; however, the dispersion and loss of power are still observed. The beam's coupling was made possible by reflecting it on two mirrors that allow for four more degrees of freedom in the collimation process. The FiberPort collimator used was *Thorlabs' PAF2-A4C*, which provides an easy and precise coupling of the beam into the optical fiber with a very small focal length shift and a 5-axis adjustment of the lens.

It is possible to confirm that the spatial mode of the beam is much better and does not disperse as



(a) Gaussian diameter X.

(b) Gaussian diameter Y.

Figure 3.6: Gaussian diameters after beam's passage through optical fiber.

much (Fig. 3.6(a) and 3.6(b)). Once again a visual aid representing the behaviour of the VCSEL diode is provided in Fig. 3.6 and 3.7 in the form of linear fits to the obtained data points. The loss of power observed after the propagation of the beam through the optical fiber was negligible (Fig. 3.7).

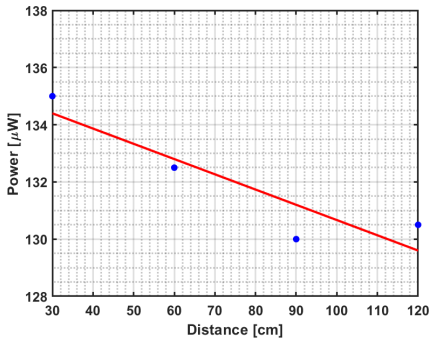
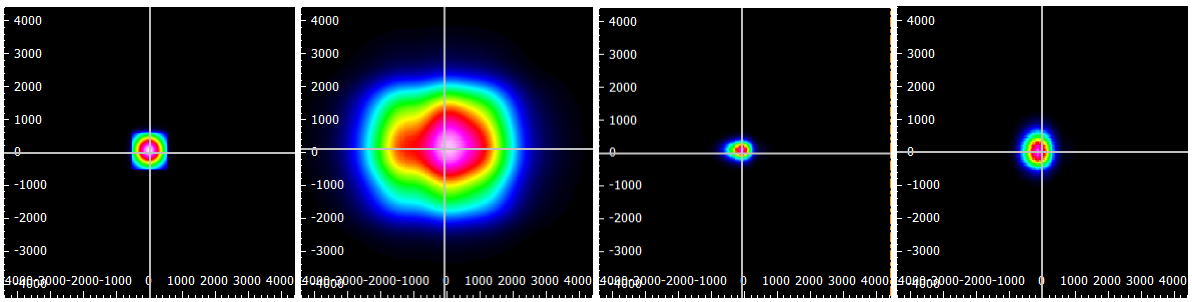


Figure 3.7: Power meter measurement.

Using (3.2), the beam's divergence was once again calculated. For the Y-axis, which is more divergent, this value amounts to approximately 1.09 milliradians. These measurements confirm that VCSEL diodes are not as good as other lasers (that do not diverge as much) but are a viable solution from the perspective of the setup's miniaturization, provided the produced beam is conducted through an optical fiber. It is also important to note that although the divergence of the worst axis decreased by a factor of 2.4, for the X axis, this decrease was factored in at more than 14 times (2.62 to 0.18 milliradians). In Fig. 3.8, the comparison of the beams' diameters before and after the propagation through the optical fiber can be visualized.

Furthermore, the principal factor contributing to the divergence of the beam prior to its transmission through the optical fiber appears to be the suboptimal adaptation of the collimating lens utilized to



(a) Reconstruction at a distance of 5 cm from the source.

(b) Reconstruction at a distance of 120 cm from the source.

(c) Reconstruction at a distance of 120 cm after propagating through optical fiber.

(d) Reconstruction at a distance of 120 cm after propagating through optical fiber.

Figure 3.8: 2D reconstructions of the beam's profile.

focus the output of the VCSEL at the exit of the laser diode. This adaptation issue may be attributed to the non-ideal characteristics of the VCSEL's spatial mode, which deviates from a perfectly Gaussian distribution.

Due to the improvement of the beam's divergence after its propagation through the optical fiber, this solution was employed in the setup's preliminary stages and later swapped for another VCSEL due to the losses this collimation introduced.

This CW laser source will be used as the carrier for the weak coherent pulses, which are created by modulating the amplitude and phase of the laser.

The light pulses are created by using square waves created using the waveform generator *TG330* from *Thurlby Thandar instrument* connected to the VCSEL diode's anode and cathode. As a pulse pattern generator, this device regulates the timing of the diode's emission. It dictates when a pulse is "on" (indicating the transmission of a quantum state) or "off" (indicating no transmission) by creating square waves with variable amplitude up to a frequency of 3 MHz. Since this CW source is pulsed and highly attenuated, photon probability distributions in the receiver follow a Poisson distribution.

This distribution is conveniently represented by the red scatter in Fig. 3.9, in which a VCSEL diode was set to a frequency of 50 kHz and attenuated to a mean photon number of 1 per pulse. In the same figure, the detector's dark counts are visible in blue. These events were calculated in post-processing and were, in the worst measurement, 0.06 counts per pulse. For the same pulse pattern generation with a frequency of 50 kHz, a simple Poisson distribution plot confirms these counts also follow the same distribution (Fig. 3.10).

The VCSEL input current is arbitrary as long as it is sufficient to provide photon arrival at the receptor; moreover, it can be fine-tuned to yield specific photon counts at the final part of the setup. This is assured after measuring losses occurring in both the emitter and receiver sides alongside those incurred during

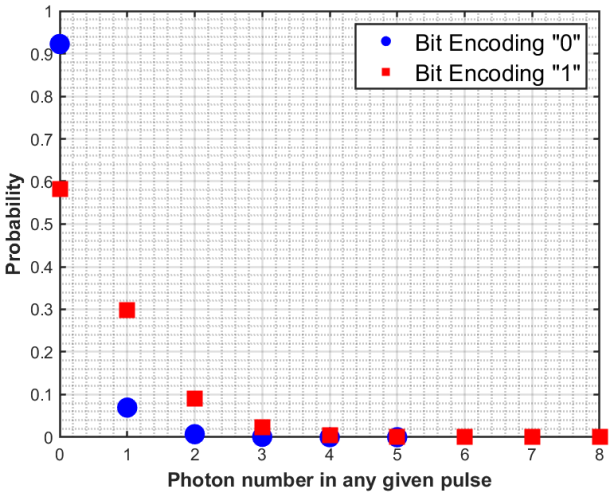


Figure 3.9: Probability of a photon detection in a single pulse for a mean photon number of 1.

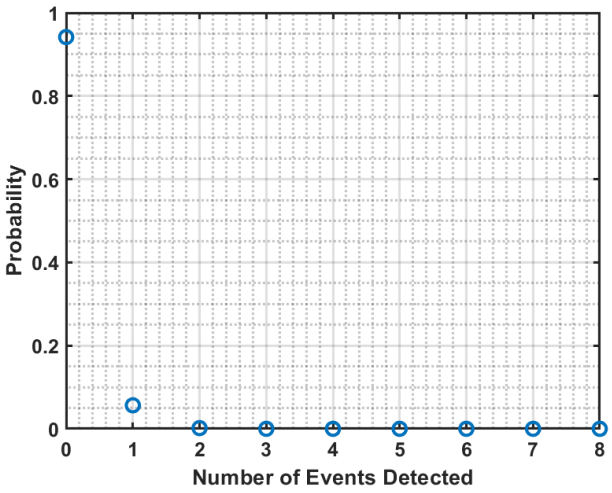


Figure 3.10: Dark counts Poisson distribution for a mean number of 0.06 per pulse.

free-space propagation, and applying further attenuation via optical filters.

3.3 State Preparation

After the creation of the 850 nm light pulses, for optical communication, there needs to be a polarization change in order for the cryptographic key to be created. The three states needed are horizontal, vertical, and diagonal. The rectilinear states horizontal and vertical (Z basis) are used to create the sifted key, while the remaining (X basis) are solely created with the purpose of detecting eavesdroppers. A potential eavesdropper cannot distinguish decoy states from signal states; therefore, decoy states allow Bob and Alice to detect deviations from normal ”behavior” due to eavesdropping attacks.

In order to create these polarizations, first, the light beam created from the VCSEL is guided through

a *Thorlabs' PBS102* Polarizing Beamsplitter (PBS) cube, this cube interacts with individual photons by separating horizontal and vertical polarizations according to their electrical components' predominance, since the incoming light is not strictly polarized, the PBS simply separates this beam into two horizontally and vertically polarized beams with a $50:50$ ratio. This separation is accomplished through the utilization of a specialized dielectric beamsplitter coating that reflects the vertical component while allowing the horizontal component to pass through.

After being horizontally polarized, the photons pass through the *Thorlabs' EO-AM-NR-C1* Electro-Optic Amplitude Modulator (EOAM). This modulator contains two matched lithium niobate crystals (Fig. 3.11); applying an electric field to these crystals induces a change in their indices of refraction, thus creating a birefringence that changes the polarization of the input beam. Thus, the electro-optic crystal assumes the role of a variable waveplate whose retardation properties exhibit a linear dependence on the magnitude of the applied electric field created by a Direct Current (DC) signal.

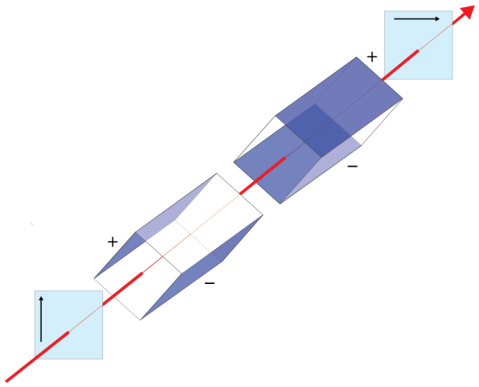


Figure 3.11: EOAM's lithium niobate crystals [52].

By controlling the DC voltage, different polarization phase shifts can be cycled and thus change polarization to several different orientations (Fig. 3.12). In electro-optic modulators, a noteworthy value of reference is the half-wave voltage, $V_\pi(\lambda)$, which is the voltage needed to induce a retardance of π radians, expressed in (3.3), with λ being the optical wavelength in nanometers.

$$V_\pi(\lambda) = 0.361\lambda - 23.844 \tag{3.3}$$

In order to achieve precise polarization states with a transmission wavelength of 850 nm, where the half-wave voltage stands at approximately 283 V, a meticulous synchronization between the waveform generator, responsible for driving the EOAM, and the waveform generator originating the light pulses is imperative. This synchronization ensures that the polarization shift occurs as closely as possible to the emission of the VCSEL beam.

Given the necessity to create a range of polarization states within the protocol, the process involves

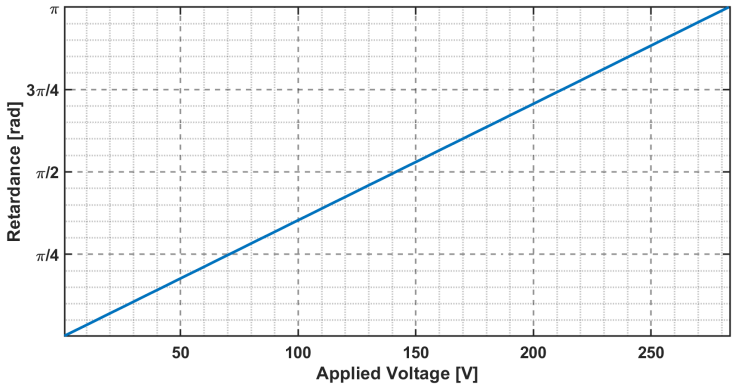


Figure 3.12: Linear relationship between the retardance of the electro-optic modulator and the applied voltage.

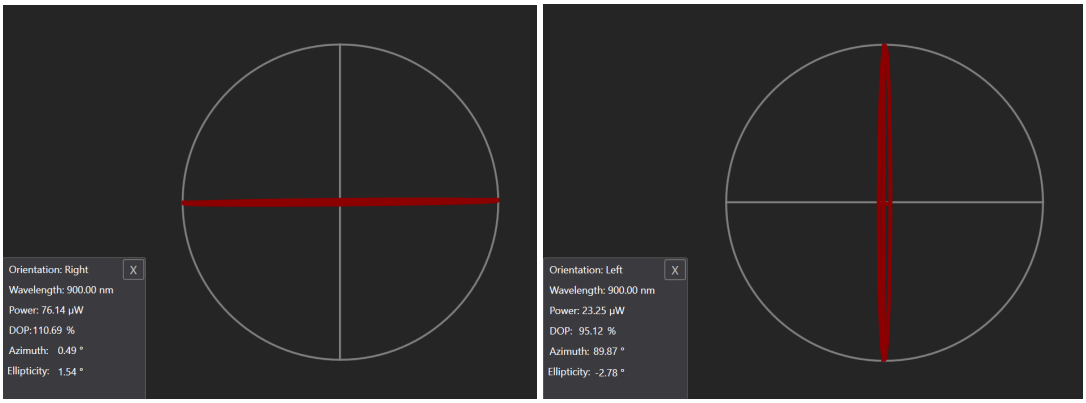
the creation of an arbitrary waveform. This waveform is crafted by a Python script (Appendix B) that takes an input string denoting the desired states, whether random or deliberate. The script transforms this string into a series of voltage points, ranging from -1 to 1, which are then loaded into the *Keysight 33250A Function Generator* and assume voltage levels corresponding to -5 to 5 V. This function generator plays a pivotal role in modulating the electro-optic crystal, thereby producing the intended polarizations for each pulse emitted by the VCSEL diode.

To ensure the effectiveness of this modulation process, synchronization between the function generator and the pulse pattern generator is meticulously maintained. The function generator operates at half of its frequency, aligning each voltage shift precisely with the commencement of a VCSEL pulse.

Subsequently, the polarization signal generated by the waveform generator undergoes amplification through the *Thorlabs' HVA200 High Voltage Amplifier*, which is set to a voltage gain of 20. This amplification is essential to attain the high voltages required for phase modulation within the setup. The amplified signal is then fed into the modulator through an SMA input, completing the process of achieving the desired polarization states for the quantum communication protocol.

The beam's polarization can then be confirmed using the *Thorlabs' PAX1000IR2/M Polarimeter* (Fig. 3.13), which measures the state of polarization of an input beam using the rotating-wave-plate method. In this method, a quarter wave plate modulates the input polarizations. After passing through this quarter wave plate, the beam is amplitude-modulated by a fixed polarizer, which controls the amount of light that reaches a photodiode. A Fast Fourier Transformation analysis allows the calculation of the three normalized Stokes vectors S_1, S_2 and S_3, and the degree of polarization which serve as the descriptors and characterize the beams' dominance of different polarization distributions.

In these figures, azimuth is the angle of polarization and ellipticity is the phase shift between orthogonal axis and can be translated as the level of circularity, in which 90° would be perfect circular polarization. In perfect conditions Fig. 3.13(a) would have an azimuth of 0°, and Fig. 3.13(b) an azimuth of 90°, both of these polarizations would ideally also have 0° ellipticity.



(a) Horizontal polarization. **(b)** Vertical Polarization.

Figure 3.13: Optical beams with different polarizations created by the EOAM.

3.4 Beam Attenuation

Subsequent to the generation of polarized pulses, the laser pulse has to be sufficiently attenuated in order to control the average number of photons emitted and consequently control the security with which the states are being transmitted. By adjusting these parameters, one can mitigate photon-number splitting[1] and beam splitting attacks[2], which are among the most common types of attacks and aim to secretly obtain information from the quantum channel, thereby undermining the security guarantees of QKD. This mitigation is achieved as a lower average photon number per pulse limits the information an adversary can obtain from the quantum channel.

To achieve the needed attenuation, *Thorlabs' Neutral Density Filters* are employed. The metric which dictates the attenuation factor provided by a given neutral density filter is denoted as optical density, OD, and can be calculated by (3.4) in which T is the transmission ratio, i.e., if a filter has a T of 0.01, then it reduces the incident beam's intensity to 1% of its original power.

$$OD = \log_{10}\left(\frac{1}{T}\right) \tag{3.4}$$

Several types of neutral density filters were available, with optical densities ranging from 0.44 to 3.5.

The energy, E, of a singular photon is elucidated by (3.5), where h represents Planck's constant, c denotes the speed of light in a vacuum, and λ is the wavelength of the incident photons.

$$E = \frac{hc}{\lambda} \tag{3.5}$$

[1] When a multi-photon pulse is emitted, the adversary intercepts it, keeps one photon for measurement, and lets the other photon(s) proceed to the legitimate receiver.

[2] The adversary employs a beamsplitter to divert a fraction of the quantum signal (i.e., some of the photons) to their own measurement apparatus.

This foundational equation enables the calculation of N_{det}, the rate of photon detection of a single photon detector, which correlates with the optical power P_{det} collimated into the optical fiber of each counting module, given its efficiency η, as shown in (3.6).

$$N_{det} = \frac{P_{det}}{E} \times \eta \tag{3.6}$$

The equation can be simplified as in (3.7), with λ_{nm} denoting the wavelength of incoming photons in nanometers. This linear correlation can be visualized in Fig. 3.14.

$$N(P) = 5.03 \times 10^{15} \times \lambda_{nm} \times P \tag{3.7}$$

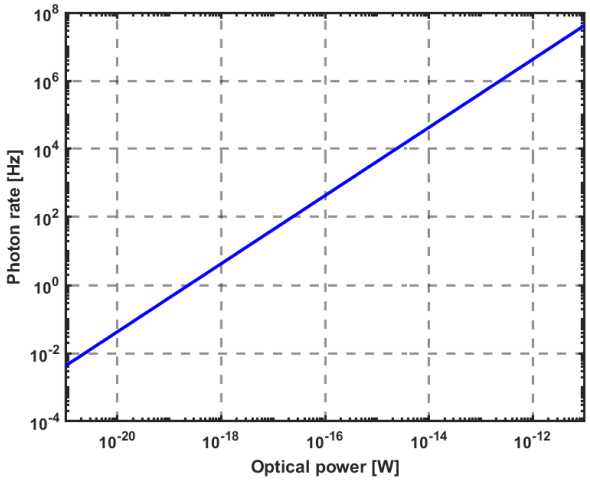


Figure 3.14: Photon number per second vs. optical power at 850 nm.

By measuring the VCSEL diode output optical power, estimating the emitter-to-receiver losses, and knowing rate of photon detection, one can employ straightforward computations to determine the required attenuation to achieve a specific photon detection rate.

After proper attenuation, two mirrors introduce an additional layer of control, providing increased degrees of freedom in directing the beam with maximum efficiency into the *Thorlabs' Beam Expander*, which generates a collimated and sufficiently large beam in order to decrease divergence effects. On the receiving end of the quantum communication setup, a counterpart beam expander is deployed. Its primary function is to focus the incoming beam, thereby enabling precise reception and further downstream processing.

3.5 Polarization Measurements

In the receiver end, incoming optical pulses are directed into a *Thorlabs' BS011 50:50 Non-Polarizing Beamsplitter Cube*. This device has the characteristic of being largely insensitive to the polarization states of the incoming light and it divides the optical beam into two separate trajectories, each responsible for measurements in distinct bases. One path is dedicated to projections in the Z basis (rectilinear), while the other is allocated for the X basis (diagonal) as shown in Fig. 3.15.

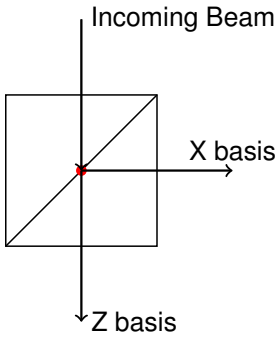
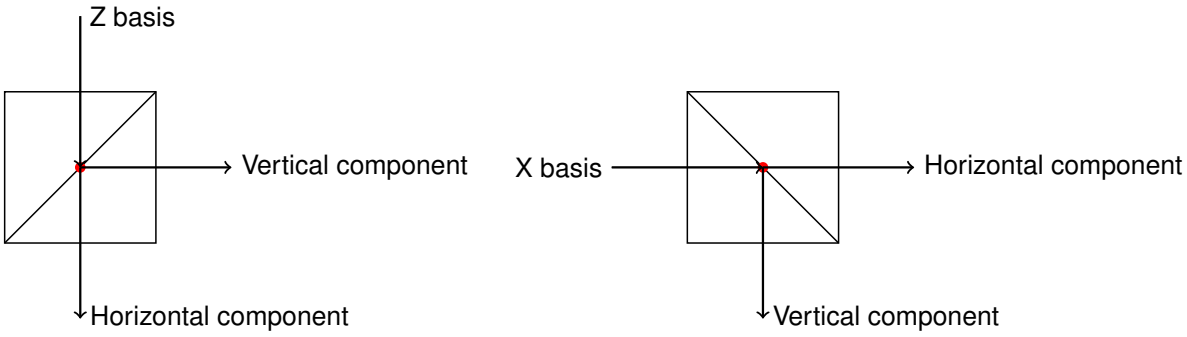


Figure 3.15: Non-polarizing beamsplitter cube polarization projections.

To facilitate the differentiation between measurements taken in these two bases during post-processing, a temporal delay is intentionally introduced in the X basis pathway, by collimating the beam in this trajectory through 1590 meters of single-mode optical fiber. This delay is discernible in the data outputs and can be computationally isolated in post-processing as analyzed in chapter 4.1.

To distinguish between horizontal and vertical polarizations in the Z basis projection, another *PBS102* PBS cube is implemented. As explained previously, horizontally polarized photons will pass through it and be collimated into one single-photon counting module, and vertically polarized photons will be reflected and directed into another single-photon counting module as shown in Fig. 3.16(a).



(a) Z Basis.

(b) X Basis.

Figure 3.16: Polarizing beamsplitter mode of operation.

With simplification and efficiency as the main goals, the PBS cube used for the Z basis polarization measurements is repurposed for capturing data in the X basis as well. After the insertion of a temporal delay in the X basis pathway, a Half-Wave Plate (HWP) is integrated into the system.

These plates are made from birefringent materials with distinct refractive indices along orthogonal axes, causing varying velocities for light polarized along the fast and slow axes. This velocity difference creates a phase difference between orthogonal polarization components. When linearly polarized light interacts with a HWP at an angle different from these axes, it results in rotated linear polarization (Fig. 3.17(a)). Quarter-Wave Plate (QWP) introduce a quarter-wavelength phase shift, producing elliptical polarization when interacting with linearly polarized light or circular polarization if aligned at exactly 45° (Fig. 3.17(b)). The HWP and QWP used were multi-order wave plates, meaning they induce specific phase shifts alongside the fractional design retardance. Often, when using HWP to rotate linnearly polarized light, ellipticity is introduced, which needed to be compensated with the use of a variable QWP.

(a) Half-Wave Plate. **(b)** Quarter-Wave Plate.

Figure 3.17: Quarter and half-wave plates set to an orientation of 45° degrees with vertically polarized light.

The quarter and half-wave plate used, thus, alter diagonal and anti-diagonal polarization states into their equivalent horizontal and vertical forms. Hence, X basis quantum states are equivalently mapped to temporally displaced Z basis states, as exemplified in Fig. 3.16(b).

Utilizing a pair of single-photon counting modules, the setup is configured to detect incoming photons and thereby discriminate polarization states in photons along the rectilinear and diagonal bases.

The single-photon counting modules used were *Laser Components' COUNT Photon Counter* and *Pacer's SPCM-AQRH*, which, through ultra-low loise VLoK and SLiK silicon avalanche photodiodes, provide a quantum efficiency[3] of about 45% and low dark count rates. Upon the detection of each incoming photon, these modules generate an electrical pulse characterized by a duration of 15 ns and an amplitude of 3 V. These pulses are then transmitted via a transistor-transistor logic output to a 50 Ω BNC to SMA cable connected to *Swabian Instruments' Time Tagger 20*.

[3]Quantum efficiency refers to the ratio of the number of photons successfully detected and converted into electrical signals to the total number of incident photons.

3.6 Post-Processing

The Time Tagger 20 is a high-resolution, multi-channel time-to-digital converter designed for capturing and timestamping the arrival times of electrical pulses. This allows for a precise synchronization of the detection events, thereby enabling detailed post-processing and analysis of the quantum states. Equipped to capture and log signal voltages exceeding 100 mV in amplitude and 1 ns in width, the device receives these signals and produces tags that denote their precise arrival time with picosecond accuracy.

In order for the post-processing to work properly, the pulse pattern generator should be detectable in the receptor to determine when the pulse is on or off in order to calculate if the signal is delayed or not. This can be done by using a mirror and reflecting the unused vertical polarization from the first PBS to redirect it to the receiver. For simplification and low cost, a biased detector can be used on the receiver end to detect this trigger.

One of the prerequisites for successful post-processing is precise temporal synchronization between the sender and the receiver. This involves aligning the time frames of both parties such that they can accurately associate each received photon with its corresponding quantum state. The ability to detect this pulse pattern at the receiver's end is critical for several reasons:

Temporal Synchronization: It aids in ensuring that Bob's measurements correspond accurately with Alice's sent states;

Delay Detection: By knowing when the pulse is "on" or "off", the receiver can calculate if there is any temporal delay in the signal, which is crucial for determining Bob's random basis of measurement.

In the early stage of this project, as the receiver and sender setups were only several meters away from each other, a simple cable was connected from the VCSEL generator to the Time Tagger 20; however, for bigger transmission distances, the vertically polarized beam from the first PBS can be used for this purpose, as it contains the same pulse pattern. In the interest of simplification and cost-effectiveness, a biased detector can be used at Bob's end to detect this timing pulse. By following this methodology, the receiver can detect the pulse pattern, thereby facilitating critical temporal synchronization for successful post-processing.

Presented in Appendix B is a Python script developed to instruct the Time Tagger in capturing signals from specific channels set to predetermined trigger voltages. The gathered timestamps are temporarily held within the device's own memory. Using a subsequent script, this data is then exported to a text document, a representation of which can be found in Fig. 3.18. Each captured event denotes either a signal's rise or fall time. Regarding photon detection, the timestamps correspond to the Low-to-High transition in the output of the single-photon counting modules. To effectively track the operations of the VCSEL, both Low-to-High and High-to-Low transition timestamps are saved.

Given that the data is recorded with picosecond precision, the time tagger's output can subsequently

TAG #	CHANNEL	TIMESTAMP (ps)	MISSED EVENTS
0	2	1672273614726	0
1	2	1672275508639	0
2	2	1672276138549	0
3	-4	1672279436135	0
4	4	1672289473349	0
5	1	1672292534722	0
6	1	1672295799725	0
7	1	1672296887058	0
8	1	1672297808285	0
9	1	1672299038941	0
10	1	1672299275894	0
11	1	1672299352069	0
12	-4	1672299546118	0
13	4	1672309583379	0
14	2	1672311206972	0
15	2	1672312933144	0

Figure 3.18: Timestamps extracted after a time tagger measurement.

be processed and examined in-depth. Specifically, one can scrutinize the delay in the photon's arrival in relation to the pulses of the VCSEL and the overall photon count. This intricate level of detail enables a comprehensive understanding of the photon dynamics, thus providing a foundation for further explorations on polarization measurements.

A complete diagram of the proposed setup is provided in Fig. 3.19.

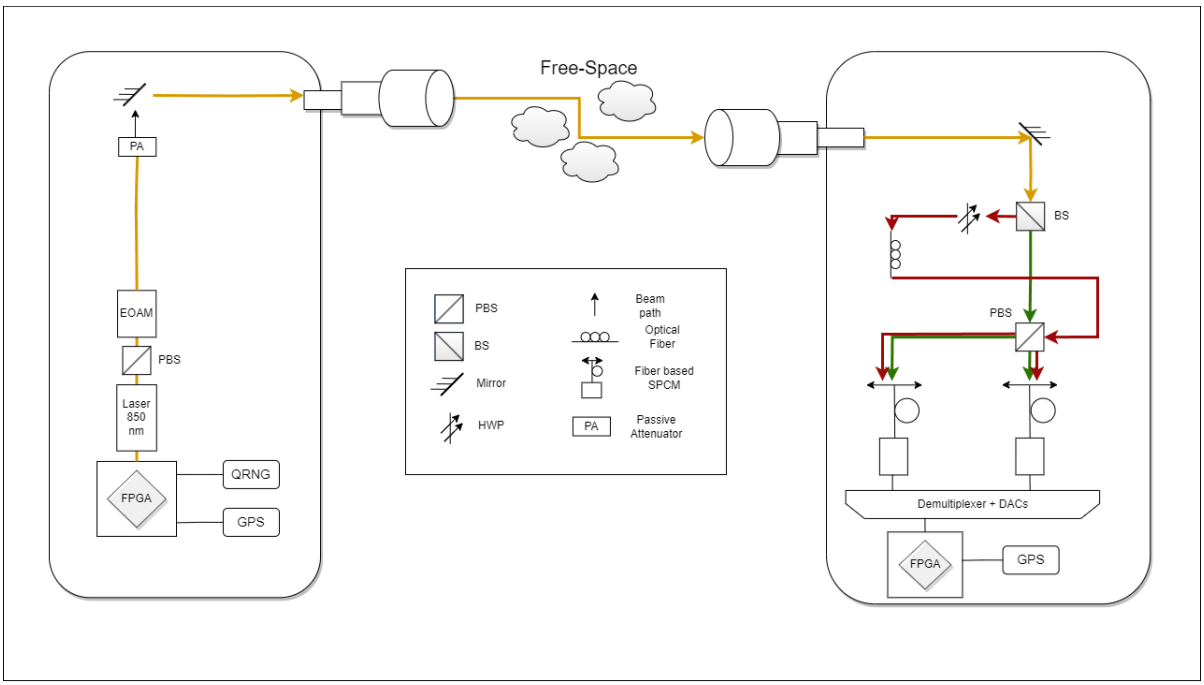
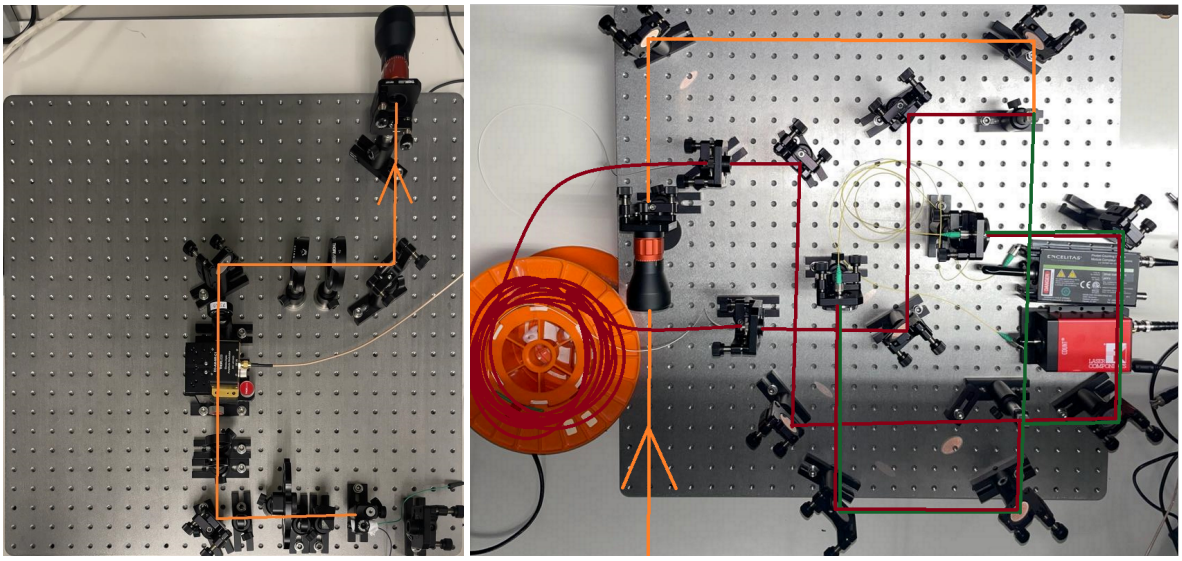


Figure 3.19: Illustration of the experimental setup, QRNG: quantum random numbers generator, FPGA: field-programmable gate array, EOAM: electro-optic amplitude modulator, PBS: polarizing beamsplitter, BS: beamsplitter, DAC: digital-to-analog converter, SPCM: single-photon counting module. HWP: half-wave plate.

As the culmination of the methodology and characterizations discussed, a comprehensive representation of the envisioned setup is delineated in Fig. 3.19. It is imperative to elucidate certain deviations in

the actual experimental setup from this schematic representation:

- The integration of FPGA, QRNG, and GPS, as depicted, was not realized in the initial experimentation phase;
- The passive attenuator, represented in the diagram, was substituted in practice by neutral density filters to achieve the desired beam attenuation;
- The elements denoting the demultiplexers and DAC, while represented in the figure, were not incorporated in the current setup. These components signify prospective enhancements and are earmarked for future iterations of the system.



(a) Emitter setup. **(b)** Receiver setup.

Figure 3.20: Characterization setup.

In Figure 3.20, the experimental configuration for both the emission and reception modules is delineated. The visual representation employs red and green beams to signify the distinct pathways of the X and Z bases, respectively (Fig. 3.20, 3.19). Upon traversing a 50:50 non-polarizing beamsplitter, these quantum states are effectively separated into their respective channels.

4

Results

Contents

4.1 Orthogonal Basis Delay

In order to measure and visualize the orthogonal basis delay, a string of bits consisting of vertical and diagonal polarizations was translated to DC voltages and loaded into the *33250A function generator*. These polarizations were used for delay calculations since they correspond to photons arriving in the same detector, following the same trajectory after traversing the non-polarizing beamsplitter. The *TG330 waveform generator* was set to output 7.2 V to the VCSEL diode with square waves with a duty cycle of 50% and a frequency of 50 kHz.

The polarization measurement basis estimation in post-processing was done by collimating the X basis path into a single-mode optical fiber, thus making the photons traverse a longer path and reach the detector with a delay. The speed of light in an optical fiber is inversely proportional to the refractive index (n) of that fiber, defined in (4.1) where c is the speed of light in vacuum and v is the speed of light in the medium.

$$v = \frac{c}{n} \tag{4.1}$$

There is no documentation for the refraction index of the optical fiber used; however, for 850 nm single-mode fibers, the typical refractive index of the core generally falls within the range of 1.45 to 1.48. Thus, for the 1590 meters of optical fiber used, the observed delay should be about 8.4 µs in the worst-case scenario.

This delay can be confirmed by calculating the average delay in photon detection after the VCSEL trigger pulse reaches the time tagger (Fig. 4.1).

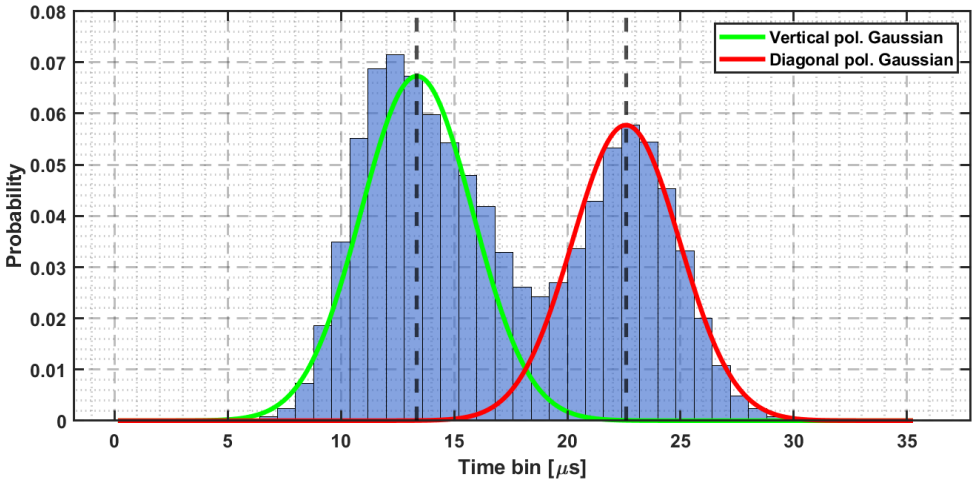


Figure 4.1: Temporal delay observed between vertical and diagonal polarizations.

By applying a two-parameter Gaussian fit, the average delay of both Gaussian distributions reaching the same single photon detector can be determined, as depicted in Fig. 4.1. The temporal delay between

these distributions can subsequently be verified through the subtracting of these obtained mean values, as delineated by (4.2).

$$delay = 22.6 \times 10^{-6} - 13.3 \times 10^{-6} = 9.3\mu s \tag{4.2}$$

With a characteristic time delay of approximately 9.3 µs, the optimal frequency, F, for polarization discrimination is one that aligns with the termination of the VCSEL's emission with the delayed photons reaching the detectors. The "signal off" event is registered by the time-tagger, so any photons detected during this specific interval unambiguously indicate an X-basis measurement. Moreover, the active detector at this interval specifies whether the received photon is polarized either diagonally or anti-diagonally.

$$F = \frac{1}{2 \times delay} \tag{4.3}$$

A small frequency increase was made due to there not being delayed photons arriving at the beginning of the next pulse. Considering this, a frequency of emission of around 50 kHz was used. It is worth noting that in this measurement, the capacity to measure polarizations was limited to the horizontal, vertical, and diagonal orientations. This limitation was a direct consequence of the operational range of the EOAM waveform generator, which is confined between -5 and 5 V. Due to this constraint, only three polarization states could be synthesized simultaneously, thereby precluding the possibility of generating anti-diagonal polarization in the same experimental run.

A noteworthy constraint in the current setup is the requirement of utilizing square waves with a 50% duty cycle for the VCSEL pulse pattern generation. Maintaining this duty cycle ensures that the temporal delay should consistently be aligned with the VCSEL "off signal", which in turn confines the transmission frequency to resonate with the available optical fiber lengths. By potentially reducing the duty cycle, it would grant greater adaptability regarding the optical fiber length of choice and, consequently, the preferred transmission frequency. Moreover, with a decreased duty cycle, the temporal delays would become more evident, as the dual Gaussian profiles would remain distinct and avoid overlapping. Such overlap, such as the one present in Fig. 4.1, can exacerbate the error rate, underscoring the pertinence of using a waveform generator which does not have this limitation for arbitrary waveforms.

4.2 System Losses

The efficiency of a quantum key distribution system is intricately linked to the cumulative losses accrued at various stages of its operation. A quantitative analysis of these losses is indispensable for gauging the overall performance and reliability of the system. Table I presents a methodical breakdown of these

losses, delineating both average and worst-case scenarios for the emitter, free-space transmission, and receiver.

Table I: Average and Worst-Case Losses

	Average [dB]	Worst-Case [dB]
Emitter	11.2	11.6
Free-Space	0.6	0.7
Receiver	15.1	17.0

4.2.1 Emitter Losses

In the emitter configuration, the bulk of the losses occurs from the reflection of the vertical polarization of the beam in the first PBS, resulting in half of the output power being wasted. Several approaches and VCSEL diodes were used in order to find the implementation with the best results. The first implementation involved using *Mouser's OPV314* VCSEL diodes, which needed to be collimated into 850 nm single-mode optical fiber to achieve proper spatial modes and resulted in losses of about 15 to 20 dB on the first part of the setup. These losses come from the fact that only around 1% to 3% of the laser power could be collimated into the optical fiber.

The second implementation used VCSEL arrayed laser diodes, which were superior to their predecessors but needed to be orientated through a pin-hole to remove the excess beams, which had to be done due to different beams adopting different polarization orientations inside the EOAM crystal. This led to comparatively lower but still noteworthy losses in the range of 7 to 10 dB.

It should be noted *Mouser's OPV314* VCSEL diode had much higher losses due to collimation; however, its divergence was much lower than the latter solution.

Both implementations highlight the trade-offs between the types of VCSEL diodes used and the resulting losses incurred during the collimation and attenuation processes, thereby underscoring the complexity of optimizing emitter efficiency in QKD setups.

Residual losses also occurred inside the EOAM. Overall, losses on the emitter side of the setup accounted for up to 11.6 dB.

4.2.2 Free-Space Losses

In the constraints of the experimental setup, a comprehensive evaluation of free-space losses was not feasible owing to the limited separation achievable in the laboratory environment. However, it is instructive to consider related works for extrapolative insights. For instance, Schmitt-Manderbach et al. [53] reported an atmospheric attenuation rate of 10 dB over a 144 km free-space optical link operating with an 850 nm laser. This approximates a loss rate of approximately 0.07 dB/km.

It is essential to account for multiple loss mechanisms in free-space quantum key distribution (QKD) systems; beyond diffraction-induced geometric loss, there are additional complexities, mainly atmospheric extinction and absorption and scattering effects [35].

In the case of quantum key distribution situated above Earth's atmosphere, which is the main goal of this work, many of these limiting factors are mitigated. Specifically, the vacuum environment substantially negates absorption-induced attenuation. Furthermore, the atmospheric medium is almost devoid of birefringence, thereby offering a more conducive environment for transmitting quantum states with specific polarization properties, thus maintaining the quantum coherence of these states.

4.2.3 Receiver Losses

The primary source of loss at the receiving end is associated with the process of collimating the optical beams into optical fibers. This step is vital for introducing a temporal delay between the distinct bases, thereby enabling successful basis discrimination.

This is followed by a subsequent collimation of all the optical beams into fibers that direct the photons to the single-photon counting modules. These collimation steps inherently introduce losses, which depend on the efficiency of the optical-to-fiber coupling. Based on empirical data, these losses can range between 8 to 13 dB, corresponding to a collimation efficiency of approximately 15 to 5%.

The *Thorlabs' FiberPort collimator PAF2-A4C* offers enhanced collimation capabilities. Utilizing this specific model, a higher percentage of the beam can be successfully collimated into the optical fiber, thereby reducing the incurred losses. However, it should be emphasized that only a limited number of these advanced collimators are available—specifically, three units—posing constraints on the extent to which these losses can be minimized in a given setup, which is why collimation losses were higher on the emitter side when considering the use of *Mouser's OPV314* VCSEL diodes, which were later disregarded in favor of the arrayed VCSEL. However, this is not of relative importance due to the results being obtained with the best solution available, which was the arrayed VCSEL diode.

In total, the measured diode-emission to photon-reception losses were, in the worst-case, about 30 dB for the Z basis and about 43 dB for the X basis.

4.3 Average Photon Emission and Reception Estimation

Determining the average photon count reaching the detector is pivotal for maintaining a low photon emission. The relationship between the power reaching the detectors P_{det} and the beam power post-polarizing beamsplitter (PBS), denoted as $P_{emitted}$, is given by:

$$P_{det} = P_{emitted} \times 10^{-\frac{30+OD\times 10}{10}}. \tag{4.4}$$

In the equation above, the fixed exponent of 30 dB accounts for the worst-case fixed losses from the VCSEL diode to the single-photon counting modules. The factor $OD \times 10$ represents losses caused by the beam's attenuation via neutral density filters.

Sourcing a 7.2 V output to the VCSEL diode during its active phase yielded an optical power of 2.38 mW ($P_{emitted}$). Taking into account inherent losses—spanning from the emitter, through propagation, to the receiver—amounting to 30 dB (worst-case), the required optical density (OD) to achieve a specified average photon arrival per pulse during $\Delta t = \frac{1}{2\times f}$ is given by (4.5). This equation is derived from (3.6) after substituting P_{det} by (4.4) and isolating OD. This relationship is further illustrated in Fig. 4.2.

$$OD = \frac{-10\log_{10}\left(N_{det} \times \Delta t \times \frac{E}{2.38\times10^{-3}\times\eta}\right) - 30}{10} \tag{4.5}$$

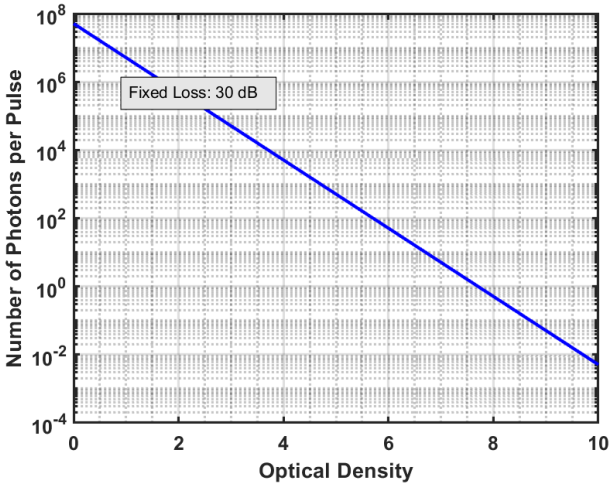


Figure 4.2: Relation between optical density and average photon arrival per pulse.

By knowing the optical power leaving the receiver apparatus, the number of photons traveling through free-space until they reach the receiver side can also be calculated. This is useful for providing critical insights into the security of the quantum channel and how many photons can, in principle, be intercepted by an eavesdropper. Since the number of photons is linearly dependent on the optical power, the ratio of photons between the emitter and receiver side can be defined as R_p:

$$R_p = \frac{N_{emitter}}{N_{receiver}}. \tag{4.6}$$

Given that the number of photons, N, for both the emitter and receiver can be represented as the ratio of power to the energy of a single photon multiplied by the detector's efficiency, η, this equation becomes:

$$R_p = \frac{P_{emitter}}{P_{receiver}}. \tag{4.7}$$

At last, the proportion of power between the emitter and the receiver, is determined by ten, raised to the power of the channel loss (spanning from the emitter to the receiver) divided by ten (4.8).

$$R_p = 10^{\frac{Ch_{loss}}{10}} \tag{4.8}$$

For a quantum-channel to detector loss of 17.72 dB, the photon ratio R_p is approximately 39.16. Table II delineates the relationship between typical average photon counts reaching the detector and those emitted from the source, providing a quantitative measure of the transmission efficiency.

Table II: Correlation Between Source-Emitted Photons, Detected Photons, and Required Optical Density

Photons reaching detector	Optical Density needed	Photons exiting emitter
0.1	8.71	3.92 ± 1.48
0.5	8.01	19.58 ± 7.42
1	7.71	39.16 ± 14.84
3	7.23	117.48 ± 44.52

It is important to note that the values in this table were calculated for the combined worst-case scenario between free-space and receiver losses; however, for the experiment with the least losses, a photon ratio of only 21.63 was achieved.

4.4 Quantum Bit Error Rates

In a 3-state 1-decoy scheme, the QBER for the X and Y bases contribute to the composite QBER, affecting the final key rate and security level. It is often essential to keep track of the QBER for individual bases to acquire sufficient statistical evidence for security proofs.

Finally, QBER metrics serve as the foundation for error correction algorithms and privacy amplification. Knowing the QBER for each basis assists in isolating which part of the channel or protocol may require optimization. Monitoring this parameter for both bases provides a deeper understanding of the security lapses that may need to be apparent when looking at the overall QBER.

As mentioned in section 3.2, the single-photon counting modules used in this experiment exhibited an average of 0.06 dark counts per pulse for a transmission frequency of about 50 kHz in the worst case. Due to this high number, an average photon count per pulse of about 0.1 can't be used as it would cause an exceptionally high QBER (37.0% according to (2.13)). Instead, in order to maintain the error rate lower than the maximum for a decoy-state BB84 protocol of about 3.5% [30, 54], an average photon detection of 1 or higher has to be maintained (Fig. 4.3).

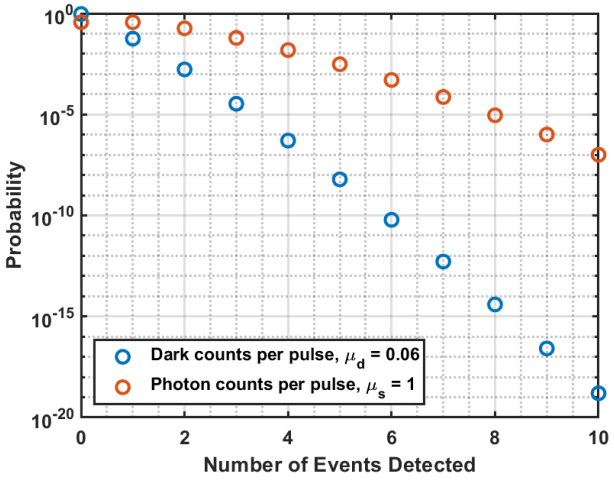


Figure 4.3: Number of events detected per pulse

4.4.1 Z Basis

The QBER in the Z basis was evaluated by directing photons polarized in horizontal and vertical orientations towards the receiver assembly, where they were subsequently processed through a PBS. In this setup, photons with horizontal polarization traverse the PBS, whereas those with vertical polarization are reflected. Following this separation, the photons are guided into the apertures of two distinct single photon counting modules. These modules can detect the incoming photons and effectively differentiate between the horizontal and vertical polarization states.

For the QBER calculation in the Z basis, the polarization states created were horizontal and vertical alternately, so the most straightforward method for calculating the error rate involves evaluating the photon counts at each detector for every ”on” pulse emitted by the VCSEL. It is feasible to deduce the transmitted state by identifying which detector registers a higher photon count and thus reliably distinct between these polarizations.

In the post-processing stage, calculating parity for particular time intervals when a detector is operational becomes indispensable, as detailed in (4.9). The computational approach outlined in appendix B begins by associating a specific parity to each polarization state. For example, if an exceptionally high ratio of photons is detected by detector α for odd-numbered intervals, and this detector is aligned to the horizontal polarization path, then the even intervals exhibiting a bias toward detector α are classified as contributing to error events, and vice-versa.

$$QBER = \frac{I_{\alpha,p} + I_{\beta,\overline{p}} + E}{f_T} \tag{4.9}$$

In (4.9), $I_{\alpha,p}$ denotes the number of pulses where detector α registers a photon count ratio that deviates from the expected, based on its assigned parity p. Conversely, $I_{\beta,\overline{p}}$ represents the analogous

count for the complementary detector β, but where the observed photon ratio defies expectations based on the negation of the parity $\overline{p}$. The term E signifies the pulses where both detectors capture an equal number of photons, leading to an inconclusive ratio of 1 and, hence, an indeterminate polarization state. The denominator f_T represents the total number of pulses for the measurement time.

Based on the method explained above, and for a measurement time of 10 s, the Z-basis QBER was calculated to be the following.

Table III: Z-Basis QBER

	$QBER_Z$
N=2	$1.58 \pm 0.15\%$

4.4.2 X Basis

The X basis QBER was performed similarly; however, the created states were diagonal and anti-diagonal polarizations, with a polarization shift being introduced in the receiver as explained in chapter 3.5 in order to comply with the proposed setup and use a single PBS to perform these measurements (Fig. 4.4).

(a) Diagonal to horizontal. **(b)** Anti-diagonal to vertical.

Figure 4.4: Half-Wave plate polarization shift.

The QBER for this base can also be calculated by (4.9) and is presented in the following table.

Table IV: X Basis QBER

	$QBER_X$
N=2	$1.46 \pm 0.03\%$

It should be noted that much lower error rates were achieved (in the order of 0.03%) although they compromise the security of the system due to the high number of photons being transmitted through the quantum channel.

4.5 Quantum Keyless Private Communication

In the domain of quantum communications, Quantum Keyless Private Communication (QKPC) presents a unique paradigm that eliminates the necessity for key distribution, thereby streamlining the overall process.

This framework enables the secure transmission of confidential data via a quantum channel devoid of any preliminary key establishment. This is in stark contrast to QKD, which necessitates a two-step procedure involving both quantum and classical communications to establish and employ a cryptographic key for secure data exchange.

Although not the main focus of this dissertation, preliminary results have been acquired for the initial stages of potential protocols.

Instead of orthogonal polarization states to create a cryptographic key, one protocol idea is to use one fixed polarization (horizontal) and an arbitrary one, β, which can vary up to 90 degrees. In the implementation of the present protocol, an inherent rise in the QBER is observed, a consequence directly attributable to the employment of non-orthogonal polarization states. The non-orthogonality of these states introduces an element of higher probabilistic uncertainty into the outcomes. However, according to the law of large numbers[1], this limitation can be substantially mitigated by amplifying the number of photons deployed per pulse. Simply put, statistical fluctuations can be minimized by increasing the number of photons per pulse. Theoretically, by sufficiently increasing the number of photons, the QBER should tend to zero. This error rate reduction is thus caused by the improved statistical accuracy in distinguishing between various polarization states, given that higher photon counts enable more precise identification of the measurement with the higher number of photons.

In the present experimental framework, where polarization measurements are predominantly aligned with horizontal and vertical basis states owing to the intrinsic properties of the PBS, a distinct problem arises in the case of diagonal polarization. Specifically, a photon exhibiting diagonal polarization displays equiprobable collapse to either a vertical or horizontal state during the measurement process.

With this understanding, it becomes advantageous to focus on polarization states that are strongly aligned with either the horizontal or vertical components. Such an approach is predicated on the notion that a dominant horizontal or vertical component would reduce the stochastic variability associated with diagonal polarization, thus mitigating the QBER.

To execute this strategy, the polarization states utilized in this experiment are deliberately constructed to distribute their horizontal and vertical components symmetrically, utilizing diagonal polarization as a referential midpoint in the design schema. The probability that a state β is measured as either vertical or horizontal can be calculated by (4.10), and (4.11) respectively.

$$H_{error} = sin(\frac{\pi}{2} - \frac{\beta}{2})^2 \tag{4.10}$$

$$V_{error} = cos(\frac{\pi}{2} + \frac{\beta}{2})^2 \tag{4.11}$$

[1] The law of large number states that as a sample size approaches infinity, the sample average converges towards the expected value or true mean.

Under the assumption that each polarization encoding state has an average presence of 50% within a random key, the QBER can be derived by taking the weighted average of the errors associated with each state. Given their equal presence, this amounts to summing the individual errors and dividing by two (4.12). This QBER can be visualized in Fig. 4.5. It is important to note that this calculation ignores other variables that further increase the QBER.

$$QBER = \frac{H_{error}}{2} + \frac{V_{error}}{2}. \tag{4.12}$$

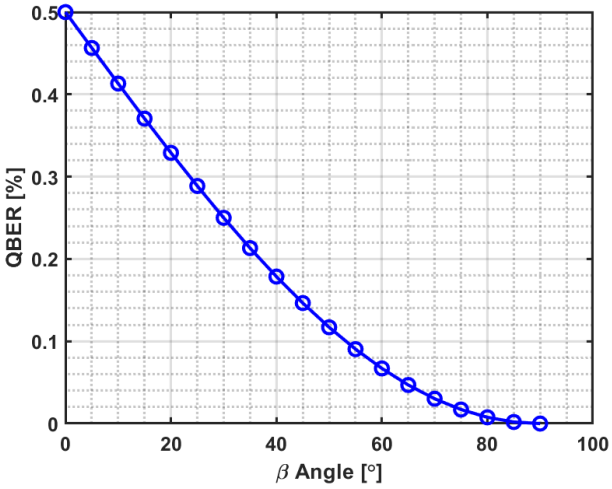


Figure 4.5: QBER in relation to β angle.

The figures present in appendix A elucidate the polarization states created with the EOAM in the emitter setup and the angle shifts induced in the receiver side, which allow proper quantum state measurements.

Building upon the preceding theoretical discussion, the study was conducted to evaluate angles of β ranging from 20 to 80 degrees in 20-degree increments. To scrutinize how the QBER fluctuates in relation to the photon count detection rate, this metric was adjusted to 0.5, 1, and 3 photons per pulse.

Table V: 20 Degrees QBER

	QBER
N=0.5	41.0 %
N=1	40.2 %
N=3	33.0 %

In accordance with (4.12), the QBER should be contingent on the angle β, manifesting greater error rates when β approaches diagonal orientations. Consistently, the tables indicate a discernible reduction in QBER as the angle shifts from $20°$ to $80°$, thus corroborating the theoretical estimations.

These measurements also demonstrate the law of large numbers is, in fact, working towards the receiver advantage in the sense that the more polarized photons are received, the better a given

Table VI: 40 Degrees QBER

	QBER
N=0.5	25.8 %
N=1	21.9 %
N=3	9.1 %

polarization can be distinguished. It is critical to acknowledge that while higher photon counts permit greater statistical accuracy, the presence of other noise and experimental inaccuracies could obscure this benefit.

Table VII: 60 Degrees QBER

	QBER
N=0.5	20.2 %
N=1	16.7 %
N=3	8.6 %

Ultimately, the experimental setup characterized by the largest angle, β, yielded remarkably reduced values in terms of QBER. Notably, under this configuration, QBER values were reduced by a factor of up to 35, given an average photon count of three per pulse.

Table VIII: 80 Degrees QBER

	QBER
N=0.5	7.2 %
N=1	5.2 %
N=3	0.9 %

The data and insights garnered from this dissertation will directly contribute to two subsequent publications: one focusing on Quantum Key Distribution and the other on Quantum Keyless Private Communication. It is essential to note that the experimental setup employed herein serves as a preliminary proof of concept. Future work aims to employ enhanced equipment, fine-tuning the existing framework for eventual integration into a CubeSAT-based communication system.

5

Conclusion and System Limitations

Contents

5.1 Conclusion

In summary, this dissertation has sought to provide a comprehensive examination of key elements in Free-Space QKD, with a particular focus on the generation and manipulation of weak coherent pulses, beam divergence metrics, and statistical models for event probability distribution. Various computational and analytical methods have been employed to dissect these intricate components, offering a more complete understanding of the system's operation and limitations.

In the quest to identify an optimal source for weak coherent pulses, various options were scrutinized with particular emphasis on beam divergence—a key parameter for long-distance free-space propagation. Vertical-cavity surface-emitting Laser diodes emerged as candidates that met these stringent requirements. However, it was observed that some level of collimation or beam isolation losses would need to be tolerated in order to implement this solution.

An optimal emitter setup should integrate both free-space and fiber-based optical components. This integration enables significantly faster repetition rates, especially in the polarization induction process, which is constrained by the limitations of the electro-optic modulator and its power source.

An in-depth analysis of power attenuation was conducted, pinpointing the elements within the system that are primary contributors to signal losses. By quantifying these loss factors and aligning them with known further attenuation applied via neutral density filters, an interdependent relationship was established among the emitted power, the photon count at the detection stage, and the photons successfully traversing free-space. Focused reduction of loss factors, particularly between the emitting mechanism and the single-photon counting modules—chiefly attributed to issues with collimation—offers a pathway for optimizing this intricate relationship and making the quantum channel more secure and attack-resistant.

This work also scrutinizes the quantum bit error rate associated with distinct polarization bases, namely Z and X, which accounted for 1.58% and 1.46%, respectively. A quantitative analysis of the influence that dark counts exert on the QBER was made. It is important to note that no error correction algorithm was applied to the acquired results, so the error can be further reduced.

A script was developed (appendix B) which, based on photon arrival delay and active detectors, provides basis of polarization estimation as long as states of polarization measured. With this output, basis reconciliation can be made, and a subsequent key can be extracted. Preliminary tests for implementing QKD were conducted; however, the results were distorted owing to the excessive photon count utilized in the tests. This work was not further developed due to time constrains.

Preliminary results were undertaken in order to gauge the effectiveness of QKPC, which can be a better alternative to QKD for simplicity, cost-effectiveness, and scalability.

5.2 System Limitations

The main limitations encountered in this work were the damage of a high-quality laser diode due to back reflections leaving as an alternative solution the use of VCSEL diodes.

High repetition rates measurements were not performed due to the high voltage amplifier utilized being limited to 1 MHz, showing signal deterioration as this frequency was approached, for high-quality and reliable signal amplification a maximum frequency of 100 KHz was measured.

The QBER obtained is higher than what can be achieved due to the high dark count rate of the single-photon counting modules used, relative to the repetition rate of the photon source. To counter this higher QBER, a much higher photon count at the receiver had to be assured relative to state-of-the-art QKD experiments. This high dark count can be improved by further and better isolating light entering the optical fibers employed and their effects can be mitigated by significantly increasing the repetition rate.

Despite these hurdles, the insights garnered herein contribute to the broader endeavor of advancing and contributing to Instituto de Telecomunicações' QKD investigation.

Bibliography

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.

[3] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, pp. 5932–5935, Dec. 1998.

[4] M. Pfennigbauer, M. Aspelmeyer, W. R. Leeb, G. Baister, T. Dreischer, T. Jennewein, G. Neckamm, J. M. Perdigues, H. Weinfurter, and A. Zeilinger, "Satellite-based quantum communication terminal employing state-of-the-art technology," *Journal of Optical Networking*, vol. 4, no. 9, p. 549, 2005.

[5] "Project echo," accessed: Out. 5, 2022. [Online]. Available: https://www.nasa.gov/image-article/echo-nasas-first-communications-satellite/

[6] "Nasa's first communications satellite," accessed: Out. 5, 2022. [Online]. Available: https://www.nasa.gov/image-article/echo-nasas-first-communications-satellite/

[7] W. J. Tabor and J. T. Sibilia, "Masers for the telstar satellite communications experiment," *Bell Syst. Tech. J.*, vol. 42, no. 4, pp. 1863–1886, Jul. 1963.

[8] "The first geosynchronous satellite," accessed: Out. 5, 2022. [Online]. Available: http://www.nasa.gov/multimedia/imagegallery/image_feature_388.html

[9] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, p. 24, Oct 1997.

[10] G. J. Simmons, "Symmetric and asymmetric encryption," *ACM Comput. Surv.*, vol. 11, no. 4, pp. 305–330, Dec. 1979.

[11] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[12] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, “Realization of a scalable shor algorithm,” *Science*, vol. 351, no. 6277, pp. 1068–1070, Mar. 2016.

[13] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, “Quantum cryptography, or unforgeable subway tokens,” in *Advances in Cryptology*. Springer US, Jan. 1983, pp. 267–275.

[14] C. H. Bennett, G. Brassard, and S. Breidbart, “Quantum cryptography ii: How to re-use a one-time pad safely even if p=np,” *Natural Computing*, vol. 13, no. 4, p. 7, Dec 2014.

[15] I. Damgård, T. B. Pedersen, and L. Salvail, “A quantum cipher with near optimal key-recycling,” in *Advances in Cryptology – CRYPTO 2005*, ser. Lecture notes in computer science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, p. 494.

[16] ——, “On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission,” in *Advances in Cryptology - EUROCRYPT 2004*, ser. Lecture notes in computer science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 91–108.

[17] G. Brassard, “Brief history of quantum cryptography: A personal perspective,” in *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, 2005, p. 19–23.

[18] L. Goldenberg and L. Vaidman, “Quantum cryptography based on orthogonal states,” *Physical Review Letters*, vol. 75, no. 7, p. 2, Aug. 1995.

[19] C. H. Bennett and G. Brassard, *An Update on Quantum Cryptography*, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, vol. 196, p. 475–480.

[20] “Quantum-safe security,” accessed: Jan. 12, 2023. [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/

[21] W. Greiner and J. Reinhardt, *Quantum Electrodynamics*, 4th ed. Berlin, Germany: Springer, Dec. 2008.

[22] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, ser. Proceedings of IEEE International Conference on Computers, Systems & Signal Processing. Bangalore, India: Steering Committee, Dec. 1984.

[23] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, p. 1, Aug. 1991.

[24] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Journal of Cryptology*, vol. 5, no. 1, p. 11, Jan. 1992.

[25] C. H. Bennett, G. Brassard, and A. K. Ekert, “Quantum cryptography,” *Scientific American*, vol. 267, no. 4, p. 56, 1992.

[26] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, “Secure quantum key distribution over 421 km of optical fiber,” *Physical Review Letters*, vol. 121, no. 19, p. 190502, Nov. 2018.

[27] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, “Twin-field quantum key distribution over 830-km fibre,” *Nature Photonics*, vol. 16, no. 22, p. 154–161, Feb. 2022.

[28] S. Mishra, A. Biswas, S. Patil, P. Chandravanshi, V. Mongia, T. Sharma, A. Rani, S. Prabhakar, S. Ramachandran, and R. P. Singh, “BBM92 quantum key distribution over a free space dusty channel of 200 meters,” *Journal of Optics*, vol. 24, no. 7, p. 9, Jul. 2022.

[29] A. Kržič, S. Sharma, C. Spiess, U. Chandrashekara, S. Töpfer, G. Sauer, L. J. González-Martín del Campo, T. Kopf, S. Petscharnig, T. Grafenauer, R. Lieger, B. Ömer, C. Pacher, R. Berlich, T. Peschel, C. Damm, S. Risse, M. Goy, D. Rieländer, A. Tünnermann, and F. Steinlechner, “Towards metropolitan free-space quantum networks,” *Npj Quantum Information*, vol. 9, no. 1, Sep. 2023.

[30] A. Jain, A. Khanna, J. Bhatt, P. V. Sakhiya, and R. K. Bahl, “Experimental demonstration of free space quantum key distribution system based on the BB84 protocol,” in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, Jul. 2020.

[31] ——, “Experimental demonstration of free space quantum key distribution system based on the BB84 protocol,” in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, Jul. 2020.

[32] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,” *New Journal of Physics*, vol. 4, pp. 43–43, Jul. 2002.

[33] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, “Practical Free-Space quantum key distribution over 1 km,” *Physical Review Letters*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.

[34] M. Avesani, “Long-range quantum cryptography gets simpler,” *Physics*, vol. 16, p. 104, Jun. 2023.

[35] M. Sisodia, Omshankar, V. Venkataraman, and J. Ghosh, “FSO-QKD protocols under free space losses and device imperfections: a comparative study,” Sep. 2023.

[36] B. Baek, L. Ma, A. Mink, X. Tang, and S. W. Nam, “Detector performance in long-distance quantum key distribution using superconducting nanowire single-photon detectors,” in *Advanced Photon Counting Techniques III*, M. A. Itzler and J. C. Campbell, Eds. SPIE, May 2009.

[37] H. Shibata, T. Honjo, and K. Shimizu, “Quantum key distribution over a 72 db channel loss using ultralow dark count superconducting single-photon detectors,” *Opt. Lett.*, vol. 39, no. 17, pp. 5078–5081, Sep. 2014.

[38] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, “Quantum teleportation and entanglement distribution over 100-kilometre free-space channels,” *Nature*, vol. 488, no. 7410, pp. 185–188, Aug. 2012.

[39] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, “Micius quantum experiments in space,” *Reviews of Modern Physics*, vol. 94, no. 3, Jul. 2022.

[40] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Satellite-based entanglement distribution over 1200 kilometers,” *Science*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017.

[41] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, no. 7670, p. 43–47, Sep. 2017.

[42] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, vol. 589, no. 78417841, p. 214–219, Jan. 2021.

[43] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, and H. Zbinden, “Long term performance of the swissquantum quantum key distribution network in a field environment,” *New Journal of Physics*, vol. 13, Dec. 2011.

[44] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, “Simple and high-speed polarization-based QKD,” *Applied Physics Letters*, vol. 112, no. 5, p. 3, Jan. 2018.

[45] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” *Applied Physics Letters*, vol. 87, no. 19, p. 3, Nov. 2005.

[46] T. B. Pittman, B. C. Jacobs, and J. D. Franson, “Heralding single photons from pulsed parametric down-conversion,” *Optics Communications*, vol. 246, no. 4-6, pp. 545–550, Feb. 2005.

[47] R. Alleaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, “Experimental open air quantum key distribution with a single photon source,” *New Journal of Physics*, vol. 6, p. 92, Jul. 2004.

[48] V. Fernandez, K. J. Gordon, R. J. Collins, P. D. Townsend, S. D. Cova, I. Rech, and G. S. Buller, “Quantum key distribution in a multi-user network at gigahertz clock rates,” in *Photonic Materials, Devices, and Applications*, G. Badenes, D. Abbott, and A. Serpenguzel, Eds. SPIE, Jul. 2005.

[49] M. Abasifard, C. Cholsuk, R. G. Pousa, A. Kumar, A. Zand, T. Riel, D. K. L. Oi, and T. Vogl, “The ideal wavelength for daylight free-space quantum key distribution,” Mar. 2023.

[50] P. C. M. Owens, J. G. Rarity, P. R. Tapster, D. Knight, and P. D. Townsend, “Photon counting with passively quenched germanium avalanche,” *Applied Optics*, vol. 33, no. 30, p. 6895, Oct. 1994.

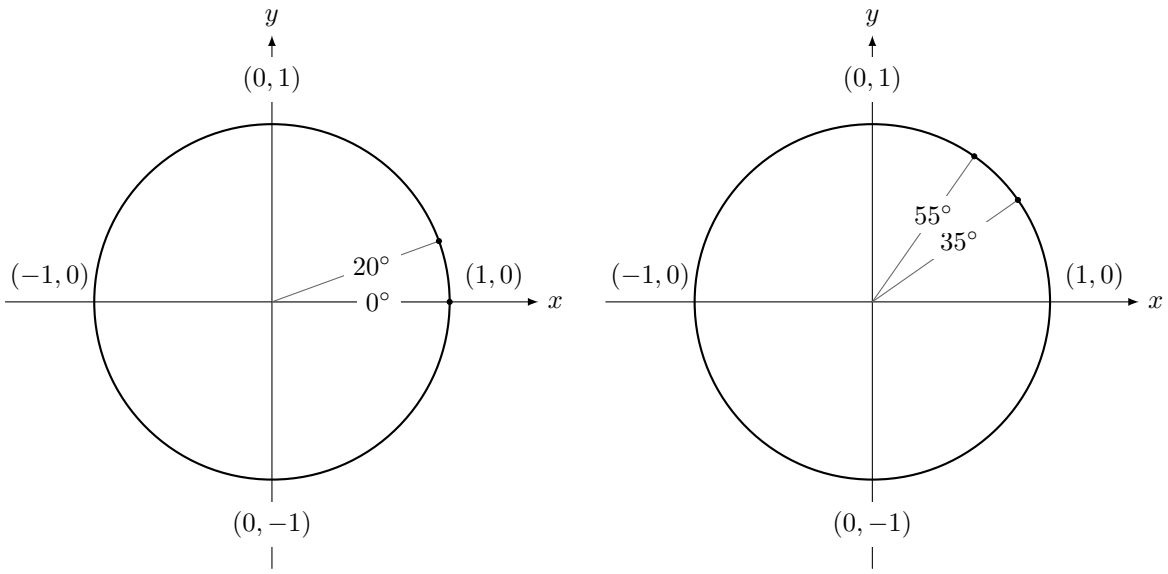
[51] R. Paschotta, *Field guide to lasers*. Bellingham: SPIE press, 2008, vol. 12.

[52] “Free-space electro-optic modulators,” accessed: Fev. 25, 2022. [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=2729

[53] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” *Physical Review Letters*, vol. 98, no. 1, Jan. 2007.

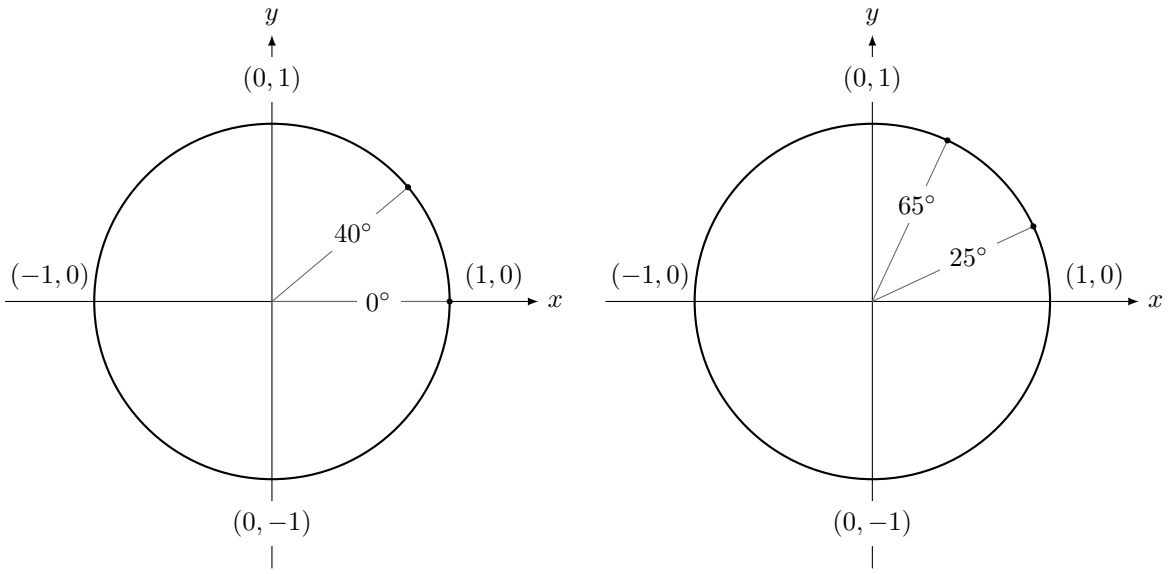
[54] Y. Chu, R. Donaldson, R. Kumar, and D. Grace, “Feasibility of quantum key distribution from high altitude platforms,” *Quantum Science and Technology*, vol. 6, no. 3, Jul. 2021.

Polarization Shifts in Receiver Setup



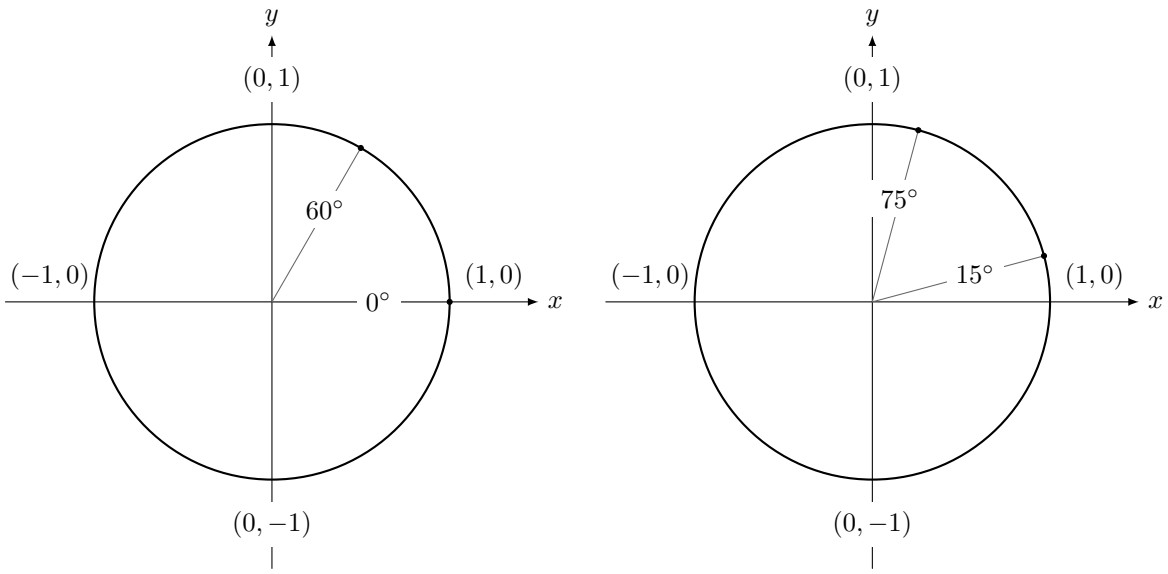
(a) States created. **(b)** Measurement states.

Figure A.1: States created for a β of 20 degrees and polarization shift induced via half-wave plate.



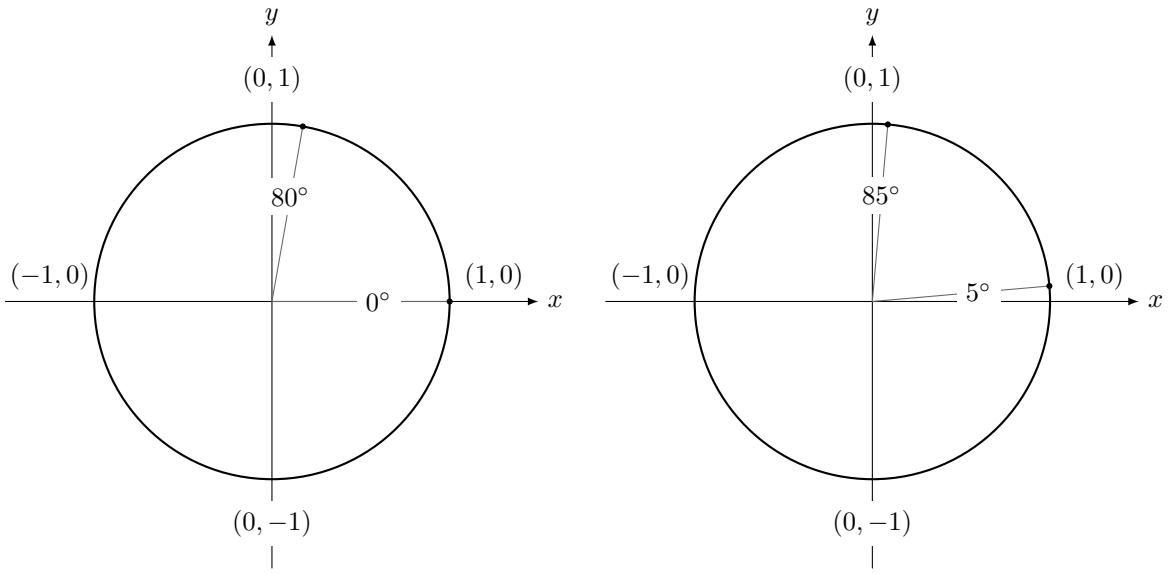
(a) States created. **(b)** Measurement states.

Figure A.2: States created for a β of 40 degrees and polarization shift induced via half-wave plate.



(a) States created. **(b)** Measurement states.

Figure A.3: States created for a β of 60 degrees and polarization shift induced via half-wave plate.



(a) States created. **(b)** Measurement states.

Figure A.4: States created for a β of 80 degrees and polarization shift induced via half-wave plate.

B

Code of Project

The code used in this project can be found in a public GitHub repository in the following link:

- https://github.com/ferreirar8/Quantum-Key-Distribution