A Few-Mode-Fiber Platform for Quantum Communication Applications

Alvaro Alarcón Cuevas
To my Family, to my friends, to everyone who has supported my dreams
Society as we know it today would not have been possible without the explosive and astonishing development of telecommunications systems, and optical fibers have been one of the pillars of these technologies.

Despite the enormous amount of data being transmitted over optical networks today, the trend is that the demand for higher bandwidths will also increase. Given this context, a central element in the design of telecommunications networks will be data security, since information can often be confidential or private.

Quantum information emerges as a solution to encrypt data by quantum key distribution (QKD) between two users. This technique uses the properties of nature as the fundamentals of operation rather than relying on mathematical constructs to provide data protection. A popular alternative to performing QKD is to use the relative phase between two individual photon paths for information encoding. However, this method was not practical over long distances. The time-bin-based scheme was a solution to the previous problem given its practical nature, however, it introduces intrinsic losses due to its design, which increases with the dimension of the encoded quantum system.

In this thesis we have designed and tested a fiber-optic platform using spatial-division-multiplexing techniques. The use of few-mode fibers and photonic lanterns are the cornerstone of our proposal, which also allow us to support orbital angular momentum (OAM) modes. The platform builds on the core ideas of the phase-coded quantum communication system and also takes advantage of the benefits proposed by the time-bin scheme. We have experimentally tested our proposal by successfully transmitting phase-coded single-photon states over 500 m few-mode fiber, demonstrating the feasibility of our scheme. We demonstrated the successful creation of OAM states, their propagation and their successful detection in an all in-fiber scheme. Our platform eliminates the post-selection losses of time-bin quantum communication systems and ensures compatibility with next-generation optical networks and opens up new possibilities for quantum communication.
First of all, I would like to deeply thank the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT) for their financial support.

A long time ago in a galaxy far, far away I decided to start my doctoral studies and now it’s time to present my work. But before continuing, I must say that if I am where I am today, it is certainly not because of my effort or desire, but because of ALL the people who have supported me on this long road, and all those people who were there to encourage me during these nights when my heart was about to break.

To all my work team in the lab, to Joakim and my supervisor Guilherme for allowing me to grow every day, for allowing me to develop my academic and scientific dreams, thank you very much for being an important part of this story.

To Cristian and Pilar, to my dear niece, my grandmother, my close aunts and uncles, my cousins, my dog and my cat: Nothing, absolutely nothing would have been possible without your love, your support from the moment I opened my eyes to this day. There is no better balm than a conversation with all of you after hard days.

To my friends, ALL my friends, from my first days of school, those of high school, those warriors that I met in college while studying. I have no words for all of you other than infinite gratitude and unconditional love. Also for those friends I met in college from other careers, especially my dear law students, I really love you with my heart.

To the "Sapos", my dear and beloved friends, there really is no stage in life where I can be happy without you by my side. Thanks for everything!

To Aunt Eva, my dear Carlos and his whole family, for always receiving me with love, with joy, for feeding me, for showing me such a beautiful side in such hard times. They will always have a very special place in my heart.

To the Fuentes-Anguita family, my favorite couple in all of history. Really talking to you two is a constant injection of energy. I appreciate all your support
always and I hope we can remain friends forever.

To Camilo, one of the brightest people I’ve ever met, my current roommate and friend. I hope that we continue to have thousands of inspiring conversations and that gravity never fails in our environment.

To Yerko, that person who arrives at a very hard time for our country and for my life. If it wasn’t for you, I might have fallen into despair many times. Thanks for everything, let the crazy conversations continue for a long time.

For Lady Fahrenheit I should write a whole book giving thanks for her influence in my life, so here I will try try to summarize. Thank you for always being there, for giving me the infinite tranquility that I can always count on you, for being my accomplice in so many crazy thoughts. For supporting all my dreams and for being such an intense light in my darkest moments.

One paragraph will not do justice to everything I have to say about my friend Mario, but everything has already been said in informal conversations. I don’t know when life decided to cross our paths, but it has certainly been the most important moment in my history. There is no possible universe where we are not together living joys or overcoming the challenges that life gives us. Neither the separation of continents nor time could with our friendship, and I certainly hope that this lasts until the end of our days.

And finally to my parents, those people who have given me more than necessary to be who I am today. Infinite thanks for always being with me, for our long telephone conversations, for your immeasurable daily support. Life will not be enough to tell you how much I love you both.

To each person who reads this text, I wish you the best and I apologize if I was not explicit when writing your name. I am sure that from now on my life will be thanking those who have made me grow and be a better person. May the force be with you!!
# Contents

1 Introduction 3
   1.1 A Paradigm Shift: A Brief History of Quantum Mechanics . . . . . 6
   1.2 Motivation: The Mix of Two Worlds . . . . . . . . . . . . . . . 12

2 Theory 19
   2.1 Fundamentals of Quantum Mechanics . . . . . . . . . . . . . . . 19
      2.1.1 Linear Algebra for Quantum Mechanics . . . . . . . . . . 19
      2.1.2 Postulates and theorems of Quantum Mechanics . . . . . 22
      2.1.3 Mach-Zehnder Interferometer . . . . . . . . . . . . . . . . 24
   2.2 Spatial Modes in an Optical Fiber . . . . . . . . . . . . . . . . 27
      2.2.1 From Maxwell Equations to Linearly Polarized modes . . 27
      2.2.2 Types of Optical Fibers . . . . . . . . . . . . . . . . . . . 30
      2.2.3 Orbital Angular Momentum (OAM) . . . . . . . . . . . . . 32
   2.3 The Photonic Lantern: A Cornerstone . . . . . . . . . . . . . . . 33

3 Methods 37
   3.1 Quantum Communication Systems Over Optical Fibers . . . . . 37
   3.2 Our Proposal: A Few-Mode-Fiber Platform for Quantum Commu-
      nication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42

4 Conclusions 47
   4.1 Discussions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
   4.2 Future work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49

Bibliography 51

Paper I 61

Paper II 65

vii
Contents

Paper III 69
We must be clear that when it comes to atoms, language can be used only as in poetry. The poet, too, is not nearly so concerned with describing facts as with creating images and establishing mental connections.

- Niels Bohr (Discussions about Language (1933))
Telecommunications have been a fundamental component of many cultural and social changes in the world and we will have them as part of our lives for many more years. In a communication system, we could argue that both high bandwidth and security are essential parameters when evaluating its performance. Given the advances and large cultural changes of the last decades, technological challenges are highly complex but undeniably necessary. It has been shown that both the increase in internet traffic and users on social networks has an exponential increase every year [1], and along with them, cyber attacks increase and become more sophisticated and powerful [2].

Regarding to the channel capacity, optical communications have proven since their inception to be the preferred and indisputable alternative to withstand the explosive increase in data traffic around the world [1,3]. The current evolution of the internet, social networks and digitization would not have been possible without this technology. The enormous traffic of information around the world has fueled one of the greatest technological revolutions in human history: Countless digital resources such as online jobs, online shopping, streaming services, payments and many other examples could be cited to demonstrate how deep this revolution has been in our lives.

According to the GSM Association (Global System for Mobile Communications), the future does not seem to be different in terms of challenges for optical communications, for example, within the promises that 5G brings (fifth generation technological standard for broadband cellular networks) there will be more than 1.7 billion new subscribers in worldwide by 2025. Along with this, the Internet of Things (IoT) will also be a key element in the digitization and processing of information in the new generation [4,5]. A study from Juniper Research found that the total number of IoT connections will reach 83 billion by 2024, compared to 35 billion connections in 2020 [6], showing the tremendous current and projected
growth of these technologies.

It seems impossible to think of a scenario where fiber optics is not the preferred channel to transport such a huge amount of data, and that is why there are currently numerous local, regional, national and international optical fiber links capable of carrying out these transport tasks [7]. This type of communication systems transmit information through optical fibers (more details in 2.2.1): Electronic signals are converted into light using light sources (mainly lasers). The light is propagated and detected by photodiodes and is converted back into electronic signals. Thanks to the combination of these elements, it is possible to transmit light with both minimal attenuation and low dispersion, which implies in high bandwidths and ultra-fast data transmission.

The optical communication has allowed permanent communication between users located in different geographical places at a relatively low cost. Due to this, it is also necessary to do a small review of the security aspects of these technologies. For example, according to F-Secure, in 2019 the number of cyber attacks measured from January to June was twelve times higher compared to the same period in 2018, an increase largely driven by IoT-related traffic that led to a total of 760 million reported cases [8]. Security becomes a fundamental aspect when having a communication system. Various security systems have been implemented around the world as a black box where security depends on the skills of the programmers: The level of security will be as high as the complexity required to break the algorithm created. The problem is that if the system is hacked only once, the system is no longer useful.

Currently, we know that there is an alternative that can improve the disadvantage of only relying on the skill of the programmer and bet that the security of a system will lie in the physical properties of nature itself. These types of technologies are commonly called quantum communications, and as their name implies, they are a branch of quantum information.

More than 100 years have passed since the birth of quantum mechanics and we are still unable to fully understand their conceptual structure and how to interpret it. Its properties are often counterintuitive and defy classical logic. Both the results obtained in the experiments and the theory presented over the years have given rise to arduous debates among the scientific community [9] and to this day, controversies persist. Concepts such as non-locality [10], the axiom of considering nature inherently random [11], the lack of realism of physical properties [12], superpositions and quantum entanglement [13-15] are some of the premises and conclusions that motivate controversy in classical sciences. To paraphrase Thomas Kuhn [16], a scientific revolution occurs when current paradigms of science are unable to reliably explain the results or observations of some physical experiment or event. Classical physics was not able to explain some questions that arose from the development of the foundations of quantum mechanics, which generated a crisis in the scientific world. A revolution then took place in the prevailing scientific structure that allowed the establishment of quantum Mechanics. It brought with itself a series of new mathematical tools that made possible the development of new hypotheses and a new technological age for humanity.

In this text we will not discuss in much depth the implications of quantum me-
mechanics, nor will we consider its many discussions closed, rather we will accept that quantum mechanics by itself is capable of explaining, through a set of philosophical, mathematical and physical tools, the behavior of nature, and we will take advantage of this to implement quantum communication systems in a practical way [17-20]. In particular, we will try to explain that theoretically, unconditional security can be obtained through quantum communications, if we apply the properties of nature in the construction of encryption protocols. A cornerstone of this work is the fact that communication is possible over optical fibers.

The main goal of this work is therefore to present a platform for future quantum communications (especially for QKD applications). Among the main challenges is to generate a compatible platform between quantum and optical communications. In addition, we will propose alternatives so that this system is scalable, so that it is prepared to support growth in data traffic and also has the possibility of continuously increasing the security levels of the system.

To motivate the discussion and justify our theoretical and experimental decisions throughout our work, the report will be divided as follows: We will begin by giving a brief introduction to the history of quantum mechanics, in such a way that we put the focus both on its philosophical and scientific bounds, to later take advantage of these conventions and implement quantum communications from a technological point of view. Then we will discuss how we could implement quantum communications as a solution to the security problem. Then the theory necessary to approach the problem from a quantum perspective will be reviewed.

In Chapter 2 the fundamentals of quantum mechanics, the necessary mathematics, and some relevant interferometric configurations will be reviewed. In addition, the different types of optical fibers will be reviewed and the concept of orbital angular momentum (OAM) will be introduced. This will be key to justify the design that we propose in this work. Finally, in chapter 2 the most relevant aspects of a photonic lantern, a central element in our proposal, will be reviewed. Chapter 3 presents a standard quantum key distribution (QKD) schemes, its advantages and disadvantages, and how it influenced our proposal, which is also explained and analyzed there.

In Chapter 4, we will show and explain the most relevant results when implementing our proposal. The difficulties that arose and their solutions are also presented.

In Chapter 5, where we will analyze in depth the relevant discussions that have arisen from our proposal, where possible future works are exposed, the capacity that this system has to be scaled and how compatible it is with current telecommunications network.

Finally, in the annex, the three papers published as a result of this work are presented.
1.1 A Paradigm Shift: A Brief History of Quantum Mechanics

Quantum mechanics tries to explain the behavior of objects on an atomic scale. Its foundations are capable of giving an interpretative and scientific framework to a large number of physical phenomena today. Quantum mechanics has been able to lay the foundation for science as we know it today, providing the ability to make experimental predictions with astonishing precision. However, some of the controversies that have arisen since its birth cannot be ignored until today. In this section, a brief review will be made of some key facts of scientific history that allowed quantum mechanics to be sustained and how it gave rise to numerous areas that have allowed the revolutionary technological environment in which we live as a society.

Eternal, indivisible, indestructible and homogeneous. Those were one of the main words that Democritus would use to describe those fundamental particles in charge of composing everything that could be observed. The idea of taking a piece of rock and dividing it over and over again would not be an infinite process, but there would come a point where we would find an element that was impossible to divide, an element that years later we were going to call "atom". The first conception about atoms was that they are in continuous movement and their characteristics vary depending on the compound analyzed, for example, the water atom would be different from the atoms that make up a metal.

It took thousands of years for a new idea to emerge about atomic structures, and it would be John Dalton in 1805 who would postulate that all atoms of an element are identical to each other, and each of these atoms is different from atoms of another element. These structures are solid and indivisible spheres and have a neutral charge [21]. After almost 100 years, J.J. Thomson discovered that atoms must have more associated charges (positive and negative charges), and would propose the famous "raisin pudding" model, where the atom is a positively charged sphere and electrons, whose charge is negative, are distributed inside [22].

In 1901, A long-standing problem (an anomaly) known as "black body radiation" was impossible to solve by traditional physics. Also known as the "ultraviolet catastrophe", this absolute mystery could not be elucidated by the brightest minds of that time, until Max Planck proposed a daring idea [23]: He argues in his article that the radiation of a black body is quantized, and it must also be a function of temperature, independent of the cavity wall material. These quantized packets have an associated energy, which is related to the radiation frequency "f" and the Planck's constant "h"

\[ E = fh \]  \hspace{1cm} (1.1)

Max Planck would never have imagined that his article would be the starting point of a storm of new scientific paradigms, which would allow the crossing of irreconcilable theories and new ways of understanding our own world. Along with this, a series of scientific facts was unleashed that would be the foundations of the known sciences today.
In 1905, The Annus Mirabilis, which owes its name to Albert Einstein’s remarkable and fantastic contributions to various areas of physics, would highlight the article that won him the Nobel Prize a few years later. Einstein was able to associate black body radiation with the behavior of "gas": By studying the small particles in the gas, a heuristic derivation of the quantized packets of light present in the radiation could be obtained. Then, using statistical mechanics, he provided an alternative explanation of Planck’s formula. According to this derivation, the absorption and emission of light must be quantified: A ray of light is not a wave that travels through space, but discrete energy packets (which would later be known as photons). This phenomenon will be known as the photoelectric effect [24].

In 1911, E. Rutherford proposed the "planetary model" of the atom [25], where a single nucleus composed of protons and neutrons is in the center of the atom. Around the nucleus, the electrons are orbiting. Its simplicity and brilliant analogy with the solar system has made this model still used in classrooms today, so that students have a friendly approach to physics.

1913 would be another key moment, when the danish Niels Bohr, Rutherford’s graduate student, proposed an atomic model absolutely contrary to common sense (from a classical perspective) [26,27]. The model proposed by Rutherford could not remain stable in time, since due to the movement of the electrons, these would inevitably end up collapsing in the nucleus. On the other hand, Bohr’s model explained the stability of matter in general: The electrons are in fixed circular orbits. The closer the electrons are to the nucleus, the energy levels are higher, otherwise we can speak of a low energy state. Each orbit has a certain amount of electrons and these can only be present in discrete energy levels determined by these orbits, that is, the electron cannot be in intermediate energy levels, and they will move between orbits only if they absorb or emit energy. The results of Bohr were able to explain the main laws of the hydrogen spectral lines. This work earned Bohr the 1922 Nobel Prize for Physics. However, In order to maintain the notion of transition from one orbit to another, Bohr was forced to regard the transition as ‘instantaneous’ (quantum jumps). Emerging quantum theory at that time, could only explain quantum jumps in a probabilistic way.

In 1923, Arthur H. Compton was formulating a quantum theory of X-ray scattering by light elements [28]. The Compton effect (in honor of his last name) discovered there is perhaps one of the most analyzed and studied effects in quantum physics along with the photoelectric effect. This study empirically demonstrated that photons coming from x-rays tend to behave like particles when they interact with matter. However, in 1924, Louis de Broglie [29,30] almost completely moved away from Newtonian influence. He postulated the wave nature of electrons and suggested that all matter has wave properties. The wavelength associated with a particle is related to the energy derived by Plank. These events were one of the first cornerstones of the concept of wave-particle duality that is fundamental to quantum mechanics.

In 1925, Werner Heisenberg, Max Born, and Pascual Jordan presented one of the first formalities to quantum mechanics known as matrix mechanics. Its fou-
lations were logically consistent with Bohr’s atomic model [31-35]. Here we have to deal with discrete finite bases which allows us to reduce a quantum mechanics problem to the addition and multiplication of vectors and matrices. Under this framework, vectors represent a quantum state and matrices generally represent quantum operators. The algebraic operation between a quantum operator and a quantum state would allow the description of observables. If we are acting with a Hermitian operator in a quantum state, this operation has a physical meaning (more details in 2.1.1). Those mathematical tools were presented to describe quantum mechanics from a discrete mathematics worldview.

Almost simultaneously, in 1926, Erwin Schrödinger [36,37] presented one of the fundamental bases for understanding quantum mechanics from a continuous (rather than discrete) mathematical perspective. It was also known as wave mechanics formulation. Schrödinger developed a differential wave equation as shown below.

\[ i\hbar \frac{\partial \psi(r,t)}{\partial t} = \frac{\hbar^2}{2m} \nabla^2 \psi(r,t) + V(r,t) \psi(r,t) \]  

(1.2)

Where \( \psi(r,t) \) represent the wave function of a particle (electron). One of the most revolutionary derivations of this equation is that we must assume that electrons are waves that permeate all of space. The equation allows us to determine both the changes in the wave function over time and the total energy of the system.

Surprisingly the matrix mechanics presented by Heisenberg, Born and Jordan and the physical interpretation of wave mechanics presented by Schrödinger are mathematically equivalent. However, the interpretation of this equation lacked content when trying to explain what the wave function really was. Among other reasons, the wave function could contain complex numbers, which implies that there is no real physical interpretation.

In 1926, Max Born [38,39] presented an idea that would change the scenario of quantum physics, by suggesting that the interpretation of the wave function should be linked to a probability amplitude, and where only the square of the magnitude of this function could deliver probabilistic interpretations associated with measurements made on an object described by that function. This result, which opened the door to interpreting the inherently random nature of subatomic particles (and consequently of the universe), led to Einstein’s famous letter to Max Born:

"...You believe in the God who plays dice, and I in complete law and order in a world that objectively exists, and which I, in a wildly speculative way, am trying to capture..."

In 1927, Heisenberg developed a concept known as the uncertainty principle [40]. Here it is stated that the exact position and the exact momentum of an object can never be known simultaneously. However, this is not due to our lack of knowledge of a particle or due to the lack of precision in the measurement devices, but responds to an even deeper principle: the uncertainty principle is a fundamental and universal limit on how much we can know about pairs of conjugate
1.1 A Paradigm Shift: A Brief History of Quantum Mechanics

quantities (more details at 2.1.1). If we consider the uncertainties of position $\Delta x$ and momentum $\Delta p$ of a particle (both variables do not commute), according to the uncertainty principle they are governed under the following condition:

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$ (1.3)

Where $\hbar$ represents Planck’s constant (seen at the beginning of this chapter) divided by $2\pi$. Here it is observed that by defining an arbitrarily small quantity, it immediately means an increase in the uncertainty of another variable to maintain the inequality. It was a point of no return to the greatest scientific and philosophical debates of the last century.

All the interpretations and results obtained up to that time were confronted at the Solvay conference in 1927, one of the most remembered physics lectures of all time. Three fundamental approaches to quantum theory were presented: Schrödinger’s wave mechanics, de Broglie’s pilot wave theory, and Born and Heisenberg’s matrix mechanics. This conference is also remembered for the intense debates carried out by Bohr and Einstein. [41].

After these debates, the "interpretations of quantum mechanics" would arise, which allowed the development of philosophical and scientific tools that gave way to a theoretical framework capable of interpreting the results obtained up to that moment.

One of the most accepted interpretations (the interpretation that will be adopted in our work) is the Copenhagen interpretation, which is generally attributed to Bohr’s idea of particle-wave complementarity, Born’s probability waves, and the Heisenberg’s uncertainty principle. (and some contributions from Schrödinger later). The interpretation says that a subatomic particle is described by a wave function, which obeys the Schrödinger equation. This wave propagates through space until it interacts with a measuring device, after that the original wave function, made up of a set of possible solutions, will collapse to a value within this set.

These historical events allowed the birth of a key concept known as quantum superposition: A quantum particle could be represented as a sum of two or more different states simultaneously. Each state can be modeled by an amplitude probability function, unless a measurement is performed..(more details in 2.1.1). This aspect will be key to understanding the motivation to develop quantum protocols to provide high levels of security.

In 1935, quantum mechanics had to overcome a major obstacle to its credibility, known as the EPR paradox in honor of Einstein, Podolsky, and Rosen [42]. The paradox in principle was a simple thought experiment that tried to show that quantum mechanics was not a complete theory and that our ignorance of subatomic systems leads us to interpret an apparent randomness of the results obtained in the measurement processes. It was simply the result of variables that had not yet been discovered or properly modeled, which were called hidden variables. EPR proposes the following experiment: Imagine two particles that interacted in the past and remain in a strongly correlated state. Two very distant observers, in such a way that the action of one does not affect the other, each receive one of these
particles. Then, if an observer measures the inertia (Momentum) of one of them, he knows what the inertia (Momentum) of the other is. On the other hand, if one observer measures the position, thanks to this strong quantum correlation, we can know the position of the other particle instantly. At this point, EPR argues that if the logic imposed by quantum mechanics is followed, where the properties of the particles are not defined until they are measured (we violate realism), then there is a contradiction when only one of the observers measures one of the particles, since the state of the other can be known immediately, even when it has not been measured. Furthermore, if we assume that the measure of one particle influences the other, then we would have to accept that there are influences traveling faster than the speed of light, since in principle it had been assumed that both observers were far enough away not to do it. Then, the locality principle is violated [42]. EPR argues that either it is accepted that the properties of the particles were defined a priori (realism), then quantum mechanics is an incomplete theory that contains hidden variables or accept that the lack of realism creates a paradox by having to assume that there are non-local influences faster than the speed of light. During the same period, Schrödinger would call these strong correlations "quantum entanglement" in his famous paper where he uses a paradox with a cat in a box to illustrate this phenomenon [43]. On the other hand, Einstein would call this phenomenon "spooky action at a distance."

Although the EPR paradox was a severe blow, much of the scientific community believed that it did not invalidate quantum mechanics. However, quantum mechanics would require polishing its formalism and its interpretations. It would not be until 1964 when John Bell would present a brilliant theory that would mark the fate of local realist theories and quantum mechanics [44]. Bell begins his analysis by assuming a local realistic theory (LRT) as proposed by EPR. Then, he establishes that entangled particles will be delivered to two entities far from each other (Alice and Bob). Bell presents an inequality composed of correlations produced by the measurements of both entities. This inequality is derived for EPR-Bohm setup which is equivalent to the original EPR argument but using the spin of two entangled particles. The distance between Alice and Bob is sufficient so that the measurement of one is not affected by the other. The measurements that Alice can perform uses an instrument that has two different settings (basis) and each setting has two possible binary values associated with the measurement (-1 and 1). The same happens with Bob and the selections of these settings are independent of each other. The scheme used is summarized in FIG. 1.1

Among several ways to show Bell’s theorem, the CHSH inequality, named by Clauser, Horne, Shinmony, and Holt, is a good alternative to present a generalization that applies to realizable experiments [45]. The inequality is shown below:

$$|E(A_1B_1) + E(A_1B_2)| + |E(A_2B_1) - E(A_2B_2)| \leq 2$$  \hspace{1cm} (1.4)

where $E(AB)$ represents the correlation between the measurements made by two devices configured in A and B respectively. This correlation is defined by:

$$E(AB) = P_{AB}(1,1) + P_{AB}(-1,-1) - P_{AB}(1,-1) - P_{AB}(-1,1)$$  \hspace{1cm} (1.5)
1.1 A Paradigm Shift: A Brief History of Quantum Mechanics

And $P_{AB}(x, y)$ is the probability of obtaining the result $x$ and $y$ when the devices in Alice and Bob are set in A and B respectively. The possible values of this equation are limited to very specific and defined values, as long as it is assumed that the predictions of the results are governed by realism and locality (initial hypothesis). At this point, quantum mechanics strikes back: For certain configurations of the measuring devices, the correlations in the equation mentioned above exceed the limit imposed by any local realist theory. Specifically, for certain configurations, we get the value $2\sqrt{2}$. This number can be found for certain values of electron spin or, for example, for certain values associated with the polarization of a single photon. So when measuring entangled particle correlations, Bell’s inequality is violated. The implications of this result have immense depth, since from here it is assumed that there is no local realist theory that contains hidden variables capable of reproducing all the predictions of quantum mechanics. And finally, given the initial conditions imposed by Bell (taken from EPR), in a quantum experiment we must reject "realism" or "locality": They depend on each other, but both cannot be valid at the same time if we want to explain quantum results.

John Bell had shown by his theorem that the predictions made by quantum mechanics were not merely philosophical, but were a completely different physical model that obeyed his own predictions. Furthermore, he marks a clear boundary for determining whether an experiment can be explained by hidden variables theory or its predictions can only be explained by quantum mechanics. Then, we can define the quantity $|E(A_1B_1) + E(A_1B_2)| + |E(A_2B_1) - E(A_2B_2)| = S$, whose value can be interpreted as shown Table 1.1.

This is a simple and powerful tool that allows to decide if an experiment is under the laws of classical or quantum mechanics, only by measuring correlations in the results.

These results were formidable (and still are) and many people was tempted to say that Quantum mechanics is a complete theory. Given the technological limitations, unexpected circumstances may appear in experiments involving Bell’s inequalities [46]. However, technological advances have made it possible to discard

![EPR-Bohm setup to derive Bell’s inequality](image)

Figure 1.1: EPR-Bohm setup to derive Bell’s inequality. Alice and Bob each randomly (and independently) choose between two settings ($A_1/A_2$ and $B_1/B_2$ respectively), to measure entangled particles coming from the source. After that, the correlations can be estimated.
Table 1.1: For those cases in which "S" is in the quantum regime, we will say that "we have a violation of the Bell inequality", understanding that in a classical regime, our value must be bounded by 2.

many of the doubts raised by some local realistic theories [47,48].

One of the first great achievements of the experimental world in proving Bell’s theorem, occurred when Aspect, Dalibard and Roger in 1982 [49], did the first Bell test using entangled photons, where the predictions of quantum mechanics were reaffirmed.

Undoubtedly, in this brief quantum history some interesting and important facts of the discussion have not been told, however, thanks to this historical journey it can be explained in detail that quantum mechanics has established itself as a scientific theory that can interpret and predict many physical phenomena with high precision. In addition to providing us with tools to understand all those contradictory characteristics of nature (at least as classical physics thought), it suggests, for example, that we should accept properties like superpositions, entanglement, and random behavior as intrinsic elements of nature. Since we have been able to establish from a historical, philosophical and scientific perspective that quantum mechanics would be the object that best explains and interprets the known universe, then the next question will be related to the advantages that can be obtained by understanding and accepting the elements and theories that make up the quantum world from a technological perspective.

1.2 Motivation: The Mix of Two Worlds

In the beginning, we have mentioned how the exponential growth of data traffic in telecommunications networks has motivated the development of optical communications, and many studies indicate that this trend will continue. The Internet, social media and online meetings would not have been possible without the optical fiber. Many technological leaps were necessary to increase the capacity in telecommunication systems, such as wavelength division multiplexing (WDM), time division multiplexing (TDM), optical amplifiers (EDFAs), and new types of optical fibers.

From the discussions presented in the previous section, it has been shown that some encryption tasks performed following the laws of quantum mechanics can have great advantages over classical systems (systems governed by classical physics) [12, 18-20]. In particular, we are interested in quantum key distribu-
Motivation: The Mix of Two Worlds

Quantum key distribution (QKD), a technique that can improve the security of data propagating over telecommunications networks [17,18]. In section (2.1.1) we will go into more detail about the meaning of what we understand by quantum state, the measurement processes and how their results can be interpreted. For now we will assume that the measurement on a individual quantum system, in our case a photon, can lead either to deterministic results with 100% certainty, or it can be a result which will be understood in a probabilistic framework. To exemplify this situation, we will resort to the concept of polarization, which can be represented as a vector. usually 6 elements are highlighted that form a set of bases to create any other arbitrary polarization [50], these are: horizontal, vertical, diagonal, antidiagonal, circular clockwise and circular anticlockwise polarization. In section (2.1.1) we will also see that a quantum state can be represented by vectors using the Dirac notation.

For now, we assume that the aforementioned polarizations can be represented by: $|H\rangle$, $|V\rangle$, $|+\rangle$, $|-\rangle$, $|R\rangle$ and $|L\rangle$ respectively. Additionally, there is an optical component called polarization beam splitter (PBS). A PBS has two inputs (we will only use one for our example) and two outputs. single-photons will be transmitted (output 1) or reflected (output 2) depending on their initial polarization.

![Behavior of the PBS](image)

Figure 1.2: Behavior of the PBS. If an incoming photon brings H polarization, it will be transmitted (click on detector 1 (D1). If an incoming photon with V polarization comes, it will be reflected (click D2) behavior.

$|H\rangle$ and $|V\rangle$, are two orthogonal elements in a Hilbert space of dimension two, therefore they form a basis for all other polarization states. As an example, one can form the other four polarization states mentioned above as follows:

$$|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$$
$$|-\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}$$
$$|R\rangle = \frac{|H\rangle + i|V\rangle}{\sqrt{2}}$$
$$|L\rangle = \frac{|H\rangle - i|V\rangle}{\sqrt{2}}$$

If an incoming photon carries one of these four polarization states and hits a PBS, now the probability of detecting that photon will be 50% at each detector,
as shown in the following figure:

Figure 1.3: If a photon has $|+\rangle, |-\rangle, |R\rangle$ or $|L\rangle$ polarization interacts with a PBS, it could be either transmitted (click D1) or reflected (click D2)

There is another optical component called half-wave plate (HWP) that allows the rotation of a state of polarization. By applying a rotation of $\pi/2$, one can transform from $|+\rangle (|-\rangle)$ to $|H\rangle (|V\rangle)$ and vice versa. When a photon passes through a PBS a deterministic or random measurement can be obtained, depending on the input polarization. Furthermore, if a half-wave plate is placed between an incoming photon and the PBS, the detection will be determined by this joint interaction. Therefore, we can consider the PBS and a HWP assembly as an adjustable measuring station with 2 different configurations: The first of them can measure with complete certainty a photon with vertical or horizontal polarization; the second configuration allows deterministic measurements of diagonal or antidiagonal polarization. Although this setup was explained to perform measurements of incoming photons, it can also be used to prepare a quantum state. This is achieved by considering a single photon source (they could have any polarization), then they go through a PBS that will transmit horizontally polarized photons and reflect vertically polarized ones. We choose those photons with horizontal polarization and discard those with vertical ones. They will pass through an HWP that can be adjusted to deterministically obtain photons with polarization $|H\rangle, |+\rangle, |V\rangle$ or $|-\rangle$. This is the principle of quantum communication systems where a QKD scheme is implemented. For this, two bases are needed in a two-dimensional Hilbert space. The first basis could be generated by $|H\rangle$ and $|V\rangle$, and the second by $|+\rangle$ and $|-\rangle$. These bases are mutually unbiased because if Alice prepares a state that belongs to one of the basis, then any possible result of the measurement with respect to the other basis (made by Bob) has the same probability, that is, there is a 50% probability if measured by D1 or D2 (for dimension "d" the probability is 1/d). The general scheme of a QKD system is shown below:

In a realistic system, the presence of a spy should always be assumed. So even when Alice and Bob have a key for encryption purposes, they cannot get their message across with total confidence. The key would have also been shared at some point and in this process, Eve can infiltrate the channel and obtain the key. The problem may be even greater if Eve infiltrates the channel, steals the key, and her presence is not noticed.

Quantum key distribution is a great alternative to mitigate these types of
1.2 Motivation: The Mix of Two Worlds

Eve
Quantum Channel
Alice
Bob
Classic Channel

Figure 1.4: A QKD scheme. Alice prepares a quantum state and sends it to Bob through a quantum channel (green line). In the channel, Eve may be the unwanted entity in the scheme that will try to intercept and decode the information shared by Alice and Bob. The classic channel is public and serves for Alice and Bob to share all bases with which they measured photons, to agree on the key that they will use to encode a message in the future.

problems, where the key that Alice and Bob will share is determined by trust in two laws of quantum nature: Inherently random behavior of quantum objects, and the quantum measurement process (quantum collapse). For example, the BB84 protocol consists of rely on quantum mechanics to increase the security levels of a communication system [18]. This type of technique can be implemented by using the polarization of individual photons as the degree of freedom.

The BB84 protocol can be summarized as follows: Alice must prepare a random bit sequence. Each bit will be encrypted onto the polarization of an individual photon. Alice must decide whether she will encrypt this photon by using either the rectangular basis (basis X) formed by 2 orthogonal elements $|H\rangle$ or $|V\rangle$ or she will choose the diagonal (basis Y) composed by the elements $|+\rangle$ or $|-\rangle$. The result of this is a photon that contains information (Qubit). Alice records the bases she used to prepare each qubit. The qubit string is sent through a quantum channel. Bob receives the string of qubits and will measure them by choosing his detection settings at random, completely independent of Alice’s preparation. A natural setup to measure(prepare) polarized single-photons is by using an HWP and a PBS. If Bob has selected the same setting that Alice prepared her state with, then Bob will definitely know Alice’s original bit values. Otherwise, the result will be fully random. Bob records the measurement values and the choice of bases during the process. Then Alice and Bob have the records of the bases used to prepare (measure) the qubits and also the (obtained) values. Alice and Bob will exchange the bases they used as public information though a classic channel, but not the bit values (values obtained after measurements). This aspect is important, because this protocol has been designed even when some of the information might be visible to Eve.

Once there is mutual knowledge about the choice of the bases, Alice and Bob will discard those measures where their basis choice did not coincide. Theoretically, due to the existence of two measurement bases, and that the measurement process is independent and random, the string will be reduced by approximately half. It is
very important to note that once a qubit has been measured, Alice and Bob now have classical information (bit). After this sifting process, they both have a key [18]

Alice and Bob will randomly choose a small part of this key and share it through a public channel. Then both compare the values of their bits. In the ideal case, Alice and Bob will not see any difference in their bits. In a practical scenario, the polarization can fluctuate when a photon is injected into an optical fiber due to birefringence. Therefore, there will be a small threshold of errors that can be characterized in advance. We can define the "quantum bit error rate" (QBER):

\[ QBER = \frac{N_{\text{errors}}}{N_{\text{total}}} = \frac{N_{\text{errors}}}{N_{\text{success}} + N_{\text{errors}}} \] (1.6)

Where \( N_{\text{errors}} \) and \( N_{\text{success}} \) is the number of incorrectly and correctly detected qubits respectively. The QBER value can be obtained by characterizing the intrinsic channel errors due to non-ideal conditions. If a BB84 protocol is running and a sudden increase in this value arise, there is a possibility that Eve is spying on the channel. The reason lies in the concepts reviewed in the previous chapter on the measurement process: If Eve intercepts the information Alice sends, Eve must irrevocably measure the photon. So Eve will only have 50\% of chance of sending the same prepared state to Bob. Once Bob reads the photon sent by Eve, the chances of hitting the state for Alice are even lower. After Alice and Bob exchange their bases, they will see that the QBER will have increased. Upon realizing this situation, Alice and Bob can assume Eve’s presence and wait until the channel is secured again. Just by taking one action, Eve is part of the complete system and her action will be revealed.

A valid thought would be to question Eve’s procedure: She could take a photon from Alice, clone it, and send the original to Bob. She measures the photon that has been cloned and Bob will do the same for the original. When the bases reconciliation process occurs, the errors do not increase. However, this would only be possible if we are working with classical bits. Working under the laws of quantum mechanics provides important advantages for this type of process: The no-cloning theorem states that it is impossible to create a identical copy of an arbitrary unknown quantum state (more details in 2.1.1). Therefore, Eve is forced to take action, collapse Alice’s prepared state and probably destroy it.

Even accepting that we are working in a quantum framework, there is another reasonable argument that can challenge the protocol: If the basis in which Alice prepares the photon coincides with the basis that Eve chooses to measure, Eve will be able with 100\% certainty to know the initial state, forward it to Bob and Eve is undetected. If the bases do not match, Eve only has a 50\% of predicting the outcome. This indicates that, in principle, Eve has only a 25\% chance of being discovered and evidently questions the protocol. However, Eve must perform this process for each Qubit of information that is sent, and only an small portion of errors will generate a dramatic change in the chances that Eve is not detected: If we now consider 2 qubits sent by Alice, Eve is forced to be lucky in both cases, that is,
1.2 Motivation: The Mix of Two Worlds

the chances of being discovered are now 50%. If we go up to 10 qubits, the odds increase to 94.4% and if we finally consider a session involving 20 qubits, then Alice and Bob have a 99.68% chance of discovering Eve. If we add to this that recently QKD experiments have been able to be carried out at speeds on the order of Kbits to Mbits, then Eve’s chances of success are radically reduced [51]. Thanks to the principles of quantum mechanics, Eve can obtain information only at the cost of introducing errors to the channel [18]. Once Alice and Bob have shared and correctly defined their key, they can use it to encrypt their messages with a high level of security.

This great advantage of encrypting messages employing the QKD technique has been demonstrated, which motivates the research and optimization of this type of systems. However, two problems arise: The first is that the polarization of a photon is not stable as it propagates through an optical fiber. And second, even in the presence of a stable system, it is not possible to encode a photon in dimensions greater than two. Theoretically, it has been shown that by encoding a photon in higher dimensions, one could access protocols that provide even more security, in addition to having more information per photon [51-53]. The challenges will be to find another degree of freedom where a photon can be encoded and that the proposed system is scalable in dimensionality. The system must be stable, present an alternative compatible with current systems and, above all, be capable of reliably propagating, transmitting and detecting quantum states.

Optical communications based on spatial division multiplexing (SDM) have been a topic of great interest today, due to the enormous benefits in increasing the capacity of the channels, increasing the bandwidths and increasing the speed of data transmission [51-54]. The idea of carrying out the multiplexing process is to generate different virtual channels on the same physical channel. Several studies have been conducted on "Multi-core-fiber" (MCFs), where different individual cores are in the same cladding [55]. We have chosen another option as a channel which is called "few-mode-fibers" (FMF) [51,56-58]. In a FMF, the core is slightly larger transversely than the core of a single-mode fiber. The different spatial modes that travel through the fiber are orthogonal and can be separated, so that each mode could correspond to a different channel. In our case, we are mainly developing a platform in quantum communications, so the central focus is not to have more channels, but to use each of N-modes traveling through the fiber to prepare a d-dimensional Qudit (more details in 2.2 and 2.3). In this way, the dimension will depend on the fiber used as a channel. The scalability will be given by technological factors that can be improved over time, unlike using polarization where the limit is given by the physical nature of the phenomenon. Finally, our proposal will use key ideas from phase coding schemes, time-bin schemes and recent technologies associated with spatial multiplexing. Towards the end of the work we will show that it has been possible to generate this platform for future quantum applications using the new generation of optical fibers and SDM technology. In addition, the system can be expanded to higher dimensions.
Is it not good to know what follows from what, even if it is not really necessary for all practical purposes (FAPP)? Suppose for example that quantum mechanics were found to resist precise formulation. Suppose that when formulation beyond FAPP is attempted, we find an unmoving finger obstinately pointing outside the subject, to the mind of the observer, to the Hindu scriptures, to God, or even only Gravitation? Would not that be very, very interesting?

- John Bell (Against ‘measurement’ (1990))

\(^1\text{FAPP is Bell’s disparaging abbreviation of *for all practical purposes.}\)
2.1 Fundamentals of Quantum Mechanics

Within the vast philosophical dispute of quantum mechanics, there is no total agreement as to its interpretations. However, one of the great achievements of quantum mechanics was to give physical interpretations to natural phenomena that until then had not been satisfactorily explained, both mathematically and philosophically. In particular, we are more interested in the discrete conceptions of these phenomena from matrices and vectors. In 1939, Paul Dirac would introduce the concept of "bra-ket" notation [59], where it is possible to represent a vector in $\mathbb{C}^N$ (a Hilbert space of dimension N). This notation is widely used and allows elegant representation of vector operations such as inner product, outer product and matrices acting as operators on vectors. In the following sections we will delve into some fundamental concepts of quantum mechanics from a mathematical perspective. Although the postulates and theorems necessary to address our proposal will be mentioned, rigorous proofs of all of them will not be presented. For more in-depth aspects and descriptions, please see the text by Nielsen and Chuang [60].

2.1.1 Linear Algebra for Quantum Mechanics

In a Hilbert space of dimension "d", that is, a complex space that accepts the inner product operation, a vector can represent a quantum state. The quantum state is associated with a physical property of an object. Sometimes these intrinsic properties of the object are also referred to as "degree of freedom" (DOF). In quantum communication, we will use those DOFs to encode information in an individual quantum system in order to create a Qubit. For example, polarization is one of many different degrees of freedom that we can use. However, information can also be encoded using frequency, time-phase, spatial mode distribution, among many
To implement a quantum protocol, it is highly desirable to have elements that can form a basis in an $d$-dimension in Hilbert space, for the preparation and measurement of states after propagation. As we saw in the previous chapter, the BB84 protocol requires at least two mutually unbiased bases [61].

A vector representing a quantum state will be written as $|\psi\rangle$, which is called "ket $\psi$". Furthermore, any quantum state can be represented by a superposition of two or more orthogonal quantum states as follows:

$$|\psi\rangle = \frac{1}{N} \sum_{j=1}^{N} \alpha_j |j\rangle$$ (2.1)

where $N$ represents the dimension of the quantum state, $\alpha_j$ represents a complex number and $|j\rangle$ are orthogonal elements forming a basis of dimension $N$. We will call the dual vector "bra" $\langle \psi |$ which is the transposed complex conjugate of $|\psi\rangle$. A quantum state $|\psi\rangle$ is valid if the following condition is fulfilled:

$$\langle \psi |\psi \rangle = 1$$ (2.2)

Equation 2.2 has been written using Dirac’s notation. The alternative notation would be $\langle \psi | \cdot |\psi \rangle = 1$ (For simplicity and concordance, we will use the notation shown in 2.2 which follows the spirit of the Dirac notation). The quantum state must necessarily be normalized (hence the importance of the normalization constant $\frac{1}{N}$ shown in 2.1). Furthermore:

$$\sum_{j=1}^{N} |\alpha_j|^2 = 1$$ (2.3)

The previous equations allow modeling the **quantum superposition**, the fundamental characteristic of quantum mechanics that allows a state to be in a linear combination of multiple elements until the moment of being measured, where the state will collapse into a particular state depending on the measuring device such. In other words, an individual quantum system can exist simultaneously in multiple states, unless the measurement operation is performed (as we will see later).

Since we are working in a Hilbert space of dimension $N$, we accept the existence of the inner product between two different states. Suppose we have two states called $|\psi_1\rangle$ and $|\psi_2\rangle$, then the inner product is given by:

$$\langle \psi_1 |\psi_2 \rangle = \langle \psi_2 |\psi_1 \rangle$$ (2.4)

The value 0 is reached when both vectors are orthogonal and 1 when they are parallel. An operator is a square matrix $A$ of dimension $N$ generally associated with measurement processes and measured values. We can also model rotations and observables. Those types of matrices have a complex conjugate element denoted as $A^*$. The transpose of a matrix $A$ is $A^T$ and we can define an hermitian operator $A$ if $A = A^T$. Finally, the hermitian conjugate is $A^\dagger \equiv (A^T)^*$. Finally We can define an unitary operator if $AA^\dagger = A^\dagger A = I$.
2.1 Fundamentals of Quantum Mechanics

From a mathematical frame of reference, we say that an operator $A$ is acting on a state $|\psi_1\rangle$ if the following operation is performed:

$$A|\psi_1\rangle = |\psi_2\rangle$$ (2.5)

one interpretation from a physical point of view of eq. (2.5) could be the measurement of a quantum object represented by the wave function $|\psi_1\rangle$ (quantum state). It could also be a rotation or any other transformation on $|\psi_1\rangle$. The object $|\psi_2\rangle$ is the result obtained after operating on $|\psi_1\rangle$.

The phase factor is a complex number with norm equal to one. It is usually represented in its general form as $e^{i\phi}$. When this factor multiplies to a ket (bra), it has no physical meaning, in fact, any state can ignore a phase factor such that $e^{i\phi}|\psi\rangle = |\psi\rangle$. When this factor is multiplied by a quantum state, that factor can be called a global phase. A global phase does not change the inner product:

$$e^{-i\phi}\langle\psi|\cdot e^{i\phi}|\psi\rangle = e^{0}\langle\psi|\cdot|\psi\rangle = \langle\psi|\cdot|\psi\rangle$$ (2.6)

However, when there is a quantum superposition, there may be relative phases which only manifest themselves in some components of the wave function. For example, we consider the case of antidiagonal polarization:

$$|\psi\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} = \frac{|H\rangle + e^{i\pi}|V\rangle}{\sqrt{2}}$$ (2.7)

The antidiagonal state is a superposition of 2 orthogonal states. Then, relative phases cannot be ignored. We will also see that this relative phase plays an important role in calculating the probability of predicting the results of a measurement.

As we saw in section (1.1) Max Born was the one who made an exceptional contribution to the field of quantum mechanics by giving a probabilistic interpretation of the wave function proposed by Schrödinger. Born postulates that the square of the amplitude of this function is equal to the probability density of the state [39].

Suppose an arbitrary quantum state in dimension 2, where the two orthogonal elements that form this state are horizontal and vertical polarization, then the state $|\psi_1\rangle$ can be written as:

$$|\psi_1\rangle = \alpha_1|H\rangle + \alpha_2|V\rangle$$ (2.8)

if this qubit is sent to a PBS, there will be a probability that this state will be measured either on the transmitted path or on the reflected path. The probability of each event is given by the square of the module of the complex number multiplying $|H\rangle$ or $|V\rangle$.

Furthermore, any element of the complex number space fulfills the property that when multiplied by its complex conjugate, the result is exactly the square of the norm (modulus) of the same element. Given the interpretation of quantum mechanics, this result will be the probability density distribution of the quantum state:

$$|\langle\psi_1|\psi_1\rangle|^2 = (\alpha_1^*|H\rangle + \alpha_2^*|V\rangle) \cdot (\alpha_1|H\rangle + \alpha_2|V\rangle) = |\alpha_1|^2 + |\alpha_2|^2 = 1$$ (2.9)
The probability that the initial state becomes the horizontal (vertical) state is $|\alpha_1|^2$ ($|\alpha_2|^2$). After measurement, the original state irrevocably becomes the measured state.

Following a probabilistic construction, given the wave function $|\psi_1\rangle$, the probability of obtaining the result $|\psi_2\rangle$ when the measurement is made over $|\psi_1\rangle$ is:

$$|\langle \psi_2 | \psi_1 \rangle|^2 = |(\alpha_{21}^* \langle H | + \alpha_{22}^* \langle V |) \cdot (\alpha_{11} | H \rangle + \alpha_{12} | V \rangle)|^2$$

(2.10)

Given the eq (2.10), it is possible to estimate the probability of measuring each of the states used in the BB84 protocol given one of the possible prepared states as follows:

$$|\langle H | H \rangle|^2 = |\langle V | V \rangle|^2 = |\langle + | + \rangle|^2 = |\langle - | - \rangle|^2 = 1$$

(2.11)

$$|\langle H | V \rangle|^2 = |\langle V | H \rangle|^2 = |\langle + | - \rangle|^2 = |\langle - | + \rangle|^2 = 0$$

(2.12)

$$|\langle H | + \rangle|^2 = |\langle V | + \rangle|^2 = |\langle H | - \rangle|^2 = |\langle V | - \rangle|^2 = \frac{1}{2}$$

(2.13)

This is a way of showing that the diagonal and rectangular bases are MUB. Finally, we will introduce the concept of a tensor product between 2 qubits as:

$$|\psi_1\rangle \otimes |\psi_2\rangle$$

(2.14)

The result of this operation represents the joint state produced by $|\psi_1\rangle$ and $|\psi_2\rangle$. The initial states that were in a space of dimension $N$ and $M$ respectively, will generate an element in the complex space of dimension $N \times M$. In general, the Kronecker product is a generalization of the tensor product with respect to a standard choice of bases and will generally be used for this type of operations [60].

2.1.2 Postulates and theorems of Quantum Mechanics

A postulate is a statement that is assumed to be true without the need for proof. The postulates are also known as axioms and are fundamental in the elaboration of theorems and the lemmas. Quantum mechanics is made up of a set of postulates that must be accepted to support the experimental and philosophical interpretations of its results. The postulates presented below produce the necessary frame of reference to generate all the fundamental quantum theory that connects the experimental results, the mathematical support and the philosophical explanations.

**Postulate 1:** An isolated physical system is a complex space with inner product (Hilbert space) known as the state space of the system. The system is completely described by its state vector (Wave function) which is a unit vector in the state space of the system (from here, it is possible to model a quantum object from a vector).
2.1 Fundamentals of Quantum Mechanics

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time $t_1$ is related to the state $|\psi'\rangle$ of the system at time $t_2$ by a unitary operator $U$:

$$|\psi'\rangle = U|\psi\rangle$$ (2.15)

In a more refined version, if one wishes to describe the evolution of a quantum state in continuous time, one must resort to the Schrödinger equation. It is important to note that the wave function described by the first two postulates is in a closed system. However, when this particle interacts with the outside, it can be measured by an experimenter, which leads us to the third axiom.

Postulate 3: Any quantum measurement can be described by a set $M_m$ of measurement operators (matrices). The index $m$ refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result $m$ occurs is given by

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$ (2.16)

After measurement, the state will collapse into the following state:

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$ (2.17)

The set of quantum operators must satisfy the completeness equation in order to give a probabilistic interpretation, that is:

$$I = \sum_m M_m^\dagger M_m$$ (2.18)

In this way, the fact is expressed that the sum of all the probability of all the possible measurements carried out by the measuring device will add up to 1

$$1 = \sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle$$ (2.19)

An observable is a property of a physical system that can be determined ("observed"). In particular, the action of a Hermitian operator acting on a quantum state can be associated with the observables obtained by an experimental measurement.

Postulate 4: The state space of a composite physical system made up of two or more quantum objects is represented by the tensor product of the objects

Given the mathematical foundations and postulates mentioned in the previous section, we can state 3 theorems that will be useful in future calculations (for more depth and proof of the theorems, see Nielsen and Chuang [60]):
**Theorem 1 (Uncertainty Principle):** If we suppose $A$ and $B$ are two Hermitian operators. We can also define the commutator as $[A,B] \overset{\text{def}}{=} AB - BA$. We then have:

$$\Delta(A)\Delta(B) \leq \frac{1}{2}|E([A,B])|$$  \hspace{1cm} (2.20)

**Theorem 2 (Indistinguishability):** Non-orthogonal states cannot be reliably distinguished.

**Theorem 3 (No-Cloning Theorem):** It is impossible to make an exact copy of an unknown quantum state.

Given the postulates and theorems, it is possible to claim the advantages of quantum communications, for example, by the BB84 protocol. It is also shown that the observation of any quantum object will be determined by the interaction between a measuring device and said object. Theorem 3 is a key aspect to increase the confidence levels of the QKD protocols since Eve has no possibility to clone a state and forward it to Bob.

From now on, we can deepen our proposal. As we have reiterated in previous sections, the use of polarization is an excellent starting point to exemplify and implement in QKD systems, however this technique has two major drawbacks: polarization is not stable while propagating in optical fibers and it is not possible to scale these types of systems to higher dimensions either.

Our scheme uses a combination of encodings related to the information contained in the "optical path" (and the relative phase) and the spatial mode encoding. State preparation using these techniques is based primarily on assuming the coherent superposition of quantum states, and the measurement process is based on determining interference patterns of individual photons. One of the most famous physics experiments is Thomas Young’s double-slit experiment [62] which shows that atomic scale particles have wave behavior when they do not interact with a measurement. Although the interference of two rays of light from the same source produces an interference pattern, in the quantum world we work with single photons that produce an interferometric pattern determined by the configuration of the system and the wave function of the same photon. That is, a photon will interact with all the probability amplitudes that model the possible observables at the output of the system. A setup capable of measuring the interference pattern is called an interferometer. There are many types of them, but we are particularly interested in the Mach-Zehnder interferometer. In the following sections we briefly explain its operation and its possible applications in quantum communications.

### 2.1.3 Mach-Zehnder Interferometer

The Mach-Zehnder interferometer (MZI) is an optical arrangement that consists of an initial stage of dividing a ray of light from the same source into two rays with equal amplitude. The rays will go their separate ways and eventually recombine into an optical component. There will be two possible outputs in the system, which will be evaluated by measuring the optical intensity. The intensity will be conditioned by the relative phase between the two rays that occurs when
both are recombined. If since the initial division of the beam, both components have traveled the same distance within the interferometer, have the same optical intensity and the same polarization when recombining, in an ideal environment one will always find the maximum power in one of its outputs and the minimum in the other. If we observe another scenario, it is due to the existence of a relative phase between both beams, which was acquired during propagation and which has conditioned the interference. this relative phase can be such that the maximum intensity will now be measured at the output where it was previously minimum.

\[
\psi = a + i e^{i \phi} b
\]

\[
a = \frac{D_1 + i D_2}{\sqrt{2}}
\]

\[
b = \frac{i D_1 + D_2}{\sqrt{2}}
\]

Figure 2.1: Fig a) represents the standard model of a BS with two F inlets and two outlets. Fig b) represents the result of the interaction of a photon represented by its wave function decomposing into two possible paths \(|a\rangle\) or \(|b\rangle\). Fig c) represents the action produced by a relative phase applied in one of the paths within an interferometer. Fig d) represents an MZI with a phase modulator in one of its paths and two possible outputs. After recombination, objects \(|a\rangle\) and \(|b\rangle\) transform into a superposition related to \(|D_1\rangle\) and \(|D_2\rangle\) (detector 1 and 2) where the photon will be detected.

In the case of an MZI used for quantum applications, the shape of the interference pattern will be given by the probability amplitude of the wave function of an individual photon. A central element to build an MZI is the Beam Splitter (BS), whose main function is to divide an incoming beam of light into two rays with a defined amplitude. In this case, the BS is 50:50, that is, it will generate two rays at its outputs with the same intensity and corresponding to half the original intensity. (For this type of analysis we will study each component in an ideal way and without introducing losses). A BS can also have two inputs and two outputs, which can be modeled using classical physics. In (Fig 2.1 a), E1 and E2 are two possible light beams entering the BS. E3 and E4 represent the outgoing rays. If we inject light from E1 (E2), then E4 and E3 will represent transmitted (reflected) and reflected (transmitted) light respectively.

However, when it comes to a single photon, we can no longer talk about the
division of a photon, but about the interaction of a quantum operator and an incoming wave function.

In order to model our initial quantum state, we will define a function capable of containing information about which pathway the photon will choose to enter the interferometer. Since the state is arbitrary, it can be modeled by:

$$|\psi\rangle = \alpha |1\rangle + \beta |2\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

(2.21)

It is clear that $|1\rangle$ and $|2\rangle$ represent the possible orthogonal paths where the photon could be. $\alpha$ and $\beta$ must fulfill the normalization condition and the square of its modulus represents the probability of the photon to choose one path or another. For our purposes, we will force the incoming photon to pass through port 1, then $\alpha = 1$ and $\beta = 0$. Our BS can be modeled using a Hermitian operator as follows:

$$BS = \frac{1}{\sqrt{2}} \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}$$

(2.22)

The action of this operator in the prepared quantum state will be the result of the following operation:

$$BS|\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

(2.23)

This is shown in Fig 2.1 b) where $i$ represents the reflection produced by the BS and both components have the same probability amplitude. The MZI shown in Fig. 2.1.d) is the complete version of this system, consisting of two BSs, two mirrors in each path, which only add a global phase to the entire system, so that their action can in principle be ignored. A phase modulator placed in one of the arms provides a relative phase between paths. In the final recombination, both paths are defined by the detectors where the single-photon will be measured.

The mathematical justification is as follows: the initial state becomes a superposition of two paths as shown in eq 2.23. The action of the phase modulator is observed in a single component:

$$|\psi\rangle \rightarrow \frac{|a\rangle + ie^{i\phi}|b\rangle}{\sqrt{2}}$$

(2.24)

Where $\phi$ is the value of the relative phase. In the final recombination, both paths interact with the final BS, which can be expressed as follows:

$$|a\rangle \rightarrow \frac{|D_1\rangle + i|D_2\rangle}{\sqrt{2}}$$

(2.25)

$$|b\rangle \rightarrow \frac{i|D_1\rangle + |D_2\rangle}{\sqrt{2}}$$

(2.26)

We can replace the values obtained from (2.25) and (2.26) into (2.24)
2.2 Spatial Modes in an Optical Fiber

\[ |\psi\rangle = \frac{1}{2} \left[ (1 - e^{i\phi})|D_1\rangle + (1 + e^{i\phi})|D_2\rangle \right] \]  
(2.27)

Equation (2.25) represents the wave function that models the behavior of the MZI, where the probability of measuring the states \(|D_1\rangle\) and \(|D_2\rangle\) is given by the relative phase. We can then write the probability that a single-photon is detected at either output of the MZI:

\[ |\langle D_1|\psi\rangle|^2 = \sin^2 \left( \frac{\phi}{2} \right) \]  
(2.28)

\[ |\langle D_2|\psi\rangle|^2 = \cos^2 \left( \frac{\phi}{2} \right) \]  
(2.29)

For most \(\phi\) values the output will be random, however, in the set \(\phi = \{0, \pi\}\) it is possible to know with complete certainty where the photon will appear.

2.2 Spatial Modes in an Optical Fiber

Traditional optical fiber channels (single-mode fibers) are designed to support only the fundamental Gaussian mode of propagation, which is not useful for encoding qubits by using spatial modes of propagation. Although multi-mode fibers support various spatial modes, we need complex electronic and optoelectronic systems to control and reconstruct the original phase wavefront after propagation. Since the advent of spatial division multiplexing (SDM) technologies, new optical fibers were developed to increase the reach of these systems. Among them, the few-mode fiber (FMF) used in our experiments stands out. In this subsection we will briefly discuss the concept of spatial modes given by the solution of the Maxwell equations in an optical fiber. Furthermore some types of optical fiber that support these propagation modes and particularly, we will define the concept of orbital angular momentum (OAM), a highly desired object in optical communications and also in quantum communications for encoding information.

2.2.1 From Maxwell Equations to Linearly Polarized modes

Between 1862 and 1865, James Clerk Maxwell published a set of equations that related the dependence between the magnetic field and the electric field. Among Maxwell’s equations is Gauss’s law (eq 2.30), which describes how charges affect the electric field and defines that the electric field decays quadratically with distance. He also defines that in nature magnetic monopoles do not exist naturally and the magnetic field must always close on itself (eq 2.31). Faraday’s law is also presented (eq 2.32), which says that if the magnetic field changes in time, a spatial change of the electric field will also be observed. Finally there is Ampere’s law (eq 2.33) that says that an electric field changing in time or charges moving, activate a magnetic field that closes on itself. the four equations are defined as follows:

\[ \nabla \cdot \vec{E} = \frac{\rho}{\epsilon_0} \]  
(2.30)
\[ \nabla \cdot \vec{B} = 0 \quad (2.31) \]
\[ \nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t} \quad (2.32) \]
\[ \nabla \times \vec{B} = \mu_0 \vec{J} + \mu_0 \epsilon_0 \frac{\partial \vec{E}}{\partial t} \quad (2.33) \]

From the combination of Maxwell’s equations, it is possible to obtain the wave equation in Cartesian coordinates. In particular, we are interested in solving the wave equation in an optical fiber, which has a well-known cylindrical structure and boundary conditions. The wave function in an optical fiber is then defined by:

\[ \frac{\partial^2 E}{\partial \rho^2} + \frac{1}{\rho} \frac{\partial E}{\partial \rho} + \frac{1}{\rho^2} \frac{\partial^2 E}{\partial \phi^2} + \left( (\eta_{eff} K_0^2) - \beta^2 \right) E = 0 \quad (2.34) \]

Where \( \rho \) and \( \phi_0 \) are the usual cylindrical coordinates. \( K_0 \) is the wave number defined as \( K_0 = \frac{2\pi}{\lambda} \), \( \eta_{eff} \) is the refractive index of optical fiber and \( \beta \) is the phase propagation constant. In order to solve the wave equation in optical fibers, the method of separation of variables for partial differential equations is used, where we consider a weakly guidance model for optical fibers. This general solution is shown below:

\[ E_z(\rho, \phi, r, \lambda) = A(\lambda) F(\rho) e^{i \phi} e^{-i \beta z} \quad (2.35) \]

\( A(\lambda) \) is a function that represent the amplitude, \( z \) is the direction of propagation. \( F(\rho) \) is a function that will define the shape of the solutions of the differential equation. When (eq 2.34) is solved using (eq 2.35), \( F(\rho) \) can be found where the Bessel equations of the first \( J_l(\rho) \) and second \( K_l(\rho) \) kind are obtained naturally. The term \( l \) is the order of the Bessel equation that represents a family of solutions as shown below:

The functions \( J_l(\rho) \) are solutions associated with the propagation of waves through the radial distance \( a \) in an optical fiber and \( K_l(\rho) \) to the cladding. In this way \( F(\rho) \) will be defined as a piecewise function:

\[ F(\rho) = \begin{cases} 
C_1 J_l(\frac{u}{a}) & \rho \leq a \\
C_2 K_l(\frac{w}{a}) & \rho > a
\end{cases} \quad (2.36) \]

Having defined the radial field function, we introduce the concept of normalized frequency \( V \), which is a dimensionless value widely used to design various types of optical fiber, as will be seen in the next chapter. The variables \( u \) and \( w \) are related to the normalized frequency \( V \) as follows:

\[ V = \frac{2\pi a}{\lambda} \sqrt{n_1^2 - n_2^2} = \sqrt{u^2 - w^2} \quad (2.37) \]
where $n_1$ and $n_2$ is the refractive index of the core and cladding respectively. In order to determine the values of $u$ and $w$ that are a solution to the wave equation, the eigenvalue equation must be solved:

$$\frac{J_{l+1}(ua)}{uJ_l(ua)} = \frac{K_{l+1}(wa)}{wK_l(wa)}$$  \hspace{1cm} (2.38)

This equation composed of two components (The Right Side Equation (RSE) and the Left Side Equation (LSE)), where the common method to find solutions is to graph the RSE and LSE and find the points where they intersect. Each of these solutions are known as modes. The modes will have associated an effective refractive index and their own constant of propagation, as shown by the following expression:

$$\eta_{eff}(\lambda, m) = \frac{\beta_m \lambda}{2\pi}$$  \hspace{1cm} (2.39)

$m$ is an integer that is associated with the set of solutions obtained for a particular value of $l$. We are interested in linearly polarized (LP) modes which are a particular type of modes that propagate in a weak guiding medium and have negligible electromagnetic field components in the direction of propagation [63-69]. Although LP modes are approximations of exact modes, nevertheless, they have been widely used since they all predict the characteristics of exact modes with high precision [63, 66, 70 - 72]. By convention they are labeled as $LP_{lm}$, where $m$ and $l$ are the values seen above which can be excited with experimental techniques. Like exact modes, LP modes represent the electromagnetic field distribution of an electromagnetic wave in a waveguide. Extensive experiments and simulations have been performed to determine the shapes of these distributions. In addition, the fundamental characteristics have been studied to predict what conditions are necessary for the existence of these modes [63-65, 73-79]. We are intentionally
interested in 3 of them, starting with the fundamental mode (Gaussian) or usually called $LP_{01}$ mode. Then there are two cases of degenerate LP modes labeled $LP_{11a}$ and $LP_{11b}$, whose propagation constants are equal to each other and smaller than that of the Gaussian mode. The shape of the 3 modes is shown below:

![Theoretical Spatial Intensity Profiles](image)

![Theoretical Phase Profiles](image)

Figure 2.3: Each column represents the spatial intensity distribution and the phase profile for each mode. For the case of the Gaussian mode there are no discontinuities in the distribution and the phase front is equal to zero. For the case of both degenerate modes, two lobes of equal intensity are observed with a maximum value in their centers. Both lobes are in counter-phase, which is represented by the color blue and red. Both modes are rotated in both phase and intensity distribution.

By varying the physical parameters of an optical fiber, one can preferentially exit certain LP modes. The next chapter highlights those features and we show one of the initial justifications for our project.

### 2.2.2 Types of Optical Fibers

From a purely physical point of view, an optical fiber is a waveguide designed to propagate light. It is manufactured from two sections known as core and cladding which have different refractive indices, with the core index having the highest value. However, the difference between both indices is such that it allows us to analyze the behavior of a wave propagating under the conditions of "weak guidance" as we saw in the previous section. In (eq 2.37) the normalized frequency was presented to solve the propagation equations and to determine the radial intensity distributions. This parameter is essential to estimate the number of modes that an optical fiber can support. The value of $V$ will depend on the central wavelength of the light propagating in a waveguide ($\lambda$). Furthermore, it is directly proportional to the radius of the guide ($a$). These refractive indices can be classified into two types: The step-index which represents an abrupt change in the refractive index from the
2.2 Spatial Modes in an Optical Fiber

Cladding towards the core. In Fig. 2.4 it is represented with dotted lines. On the other hand, the graduated index represents a smoother transition. In optical communications it is desirable to have a gradual index because this reduces modal dispersion over long distances.

![Diagram of optical fibers](image)

Figure 2.4: Different cross-sectional profiles of optical fibers (top) and their respective refractive indices (bottom).

The normalized frequency and the various interpretations of its value have been studied extensively [80,81]. For our experimental approach, we will say that a fiber is single-mode (only propagate gaussian mode) if $V < 2.405$. Otherwise, it must be assumed that the fiber carries more than one spatial propagation mode. If the radius increases, it is trivial to observe that the number of propagated modes will also increase. For 1550nm, the typical core radius of a single-mode fiber is 9um. A multi-mode fiber is designed with larger radius that can be around 50um or more. The number of modes that can be transported by a multi-mode fiber are proportional to $V^2$. By reducing the radius close enough to a single-mode profile, it is possible to have fewer modes, which are easier to manipulate and control. The few-mode fiber used in our proposal has a radius of 11um and for 1550nm it is capable of supporting 3 LP modes: $LP_{01}$, $LP_{11a}$ and $LP_{11b}$. It can be shown that these modes are orthogonal to each other. This opens up a series of experimental possibilities, among which the use of each LP mode as a communication channel independent of the rest stands out. As for quantum communications, radial intensity distributions must be reinterpreted in terms of physical meaning. In the context of quantum mechanics, they are probability distributions, where the single-photon is more likely to be in those places where the intensity levels are highest. For example, a photon propagating with a Gaussian spatial distribution is very likely to be in the center of the optical fiber, and
that probability decreases as we get closer to the cladding. For both LP11 modes, there are two main regions where the single-photon is most likely to be found. This analysis can provide elements to construct a three-dimensional Hilbert space if we consider each LP mode that propagates in the FMF as the orthogonal elements that form a basis [58, 82, 83]. It is also possible to have a two-dimensional system if the propagation of only two elements are considered and the third is suppressed by experimental techniques.

2.2.3 Orbital Angular Momentum (OAM)

Electromagnetic waves have an angular momentum related to the phenomena of rotation of the electromagnetic field of light. A single photon whose phase and wave fronts have a helical behavior will carry an orbital angular momentum (OAM). OAM is an electromagnetic mode and has a singularity in the center of its radial distribution, which is derived from its helical azimuth phase around the optical axis. In 1992, Allen et al. [84] showed for the first time that a photon could have a spiral structure with a well-defined OAM value. Like the spin of an electron, OAM of light is quantized, however, OAM can take any quantized value represented by an integer \( l \), which is the OAM order. Usually this type of mode is written as \( OAM_{\pm l} \). The term \( \pm l \) will indicate the direction of rotation (clockwise or anticlockwise). The following figure shows 3 different OAM structures:

![Figure 2.5: Three electromagnetic waves carrying OAM. All are observed under the same time and with the same amplitude. As \( l \) increases, the number of turns will increase, therefore its phase profile will change faster.](image)

The creation, propagation and detection of qudits has been desired over the years, but the natural bounds of the degrees of freedom of individual quantum systems have been a difficult challenge. Since (in principle) the OAM of light offers unlimited expansion to high-dimensionality, it has become a natural selection towards the new generation of encoding techniques [85-101]. Several ways of preparing OAM states have been studied, such as the use of spatial light modulators [102] or q-plates [52]. This has paved the way for many applications such as in biophysics [91,103,104], astronomy [105] and metrology [106]. However, when quantum communication employs such bulk optical components, integration with
current optical networks is difficult as they operate at speeds much lower than required. That is why a different way is needed to prepare and detect this type of spatial propagation modes that overcome to technological barrier.

2.3 The Photonic Lantern: A Cornerstone

The photonic lantern (PL) is multiplexer/demultiplexer device for mode division multiplexing (SDM). It has been broadly used in numerous optical communication experiments [85, 86, 107-116] in order to increase the channel capacity. The PL has one few-mode-fiber at the output, and \( N \) independent single-mode fibers at the input. The PL can map each one of the input Gaussian modes into a higher LP-mode on the FMF. In our case, we use a 3-mode photonic lantern.

We have labeled the 3 inputs ports from 1 to 3. We can inject a beam of light through port 1 and the PL will map this Gaussian mode \((LP_{01})\) into another Gaussian mode at the output. If we now send light to port 2 (port 3) we will have the \( LP_{11a} \) (\( LP_{11b} \)) mode on the FMF output. This device is made of an adiabatic taper that provides a low transition from the input single-mode fibers to the FMF, in such a way to transform the proper LP mode at the output. Mapping occurs by a matching process between the effective refractive indices of the conical region and the incoming spatial modes. The final spatial modes will be given by the interaction of the supermodes in the internal structure of PL. These results can be obtained experimentally with components made of optical fiber that are fully commercially available. (Figure 2.6) shows a PL schematic:

![Commercial mode-selective photonic lantern (Phoenix Photonics 3PLS-GI-15). It allows that the spatial modes supported by our FMF being propagated together.](image)

We can assign each LP mode as a basis element of the 3-dimensional state. Furthermore, we can only use 2 LP modes as orthogonal elements to create a two-dimensional Hilbert space by using 2 ports of the PL. One of the great advantages of creating coherent superpositions using LP modes is that under certain experi-
mental manipulations it is possible to create the desired OAM modes. To achieve this, 2 PL inputs must be connected to the same light source, in order to ensure a coherent superposition on the FMF output. It has been studied in simulations and in experimental demonstrations that OAM modes can be created from the linear combination of even and odd spatial modes of propagation [72, 86, 95] as follows:

\[
OAM_{\pm l} = LP_{11}^{(even)} \pm i \cdot LP_{11}^{(odd)}
\]  

(2.40)

Regarding to the previous equation, ”±” represents the direction of rotation of the OAM mode and \(i\) represents a relative phase of \(\pi/2\) between both components. This result is key in our proposal, since the \(LP_{11a}\) and \(LP_{11b}\) modes have even and odd symmetry respectively. Furthermore the relative phase can be achieved by experimental manipulation.

So far, we have seen the advantages quantum systems can have if they decide to incorporate SDM technologies, in addition to the potential they have for future scaling. The next chapter briefly explains two proposed schemes for the distribution of quantum states over long distances (Phase encoding and Time-bin encoding) and then looks at how we integrate these SDM technologies inspired by the key ideas of these schemes.
I feel very much like Dirac: the idea of a personal God is foreign to me. But we ought to remember that religion uses language in quite a different way from science. The language of religion is more closely related to the language of poetry than to the language of science. True, we are inclined to think that science deals with information about objective facts, and poetry with subjective feelings. Hence we conclude that if religion does indeed deal with objective truths, it ought to adopt the same criteria of truth as science. But I myself find the division of the world into an objective and a subjective side much too arbitrary. The fact that religions through the ages have spoken in images, parables, and paradoxes means simply that there are no other ways of grasping the reality to which they refer. But that does not mean that it is not a genuine reality. And splitting this reality into an objective and a subjective side won't get us very far.

- Niels Bohr (Solvay Conference of 1927)
3.1 Quantum Communication Systems Over Optical Fibers

Select an individual quantum system, encode it by experimental manipulation, propagate it over long distances, and decode it to interpret the message sent. These are the basics for understanding quantum communications in general. We have reviewed in previous chapters that working with single-photons is a great advantage for the use of QKD protocols and optical fibers is positioned as the preferred quantum channel.

At least two channels are needed to complete the QKD process. On the one hand, the authentication, error correction, sifting and privacy amplification processes are carried out through the classic channel. Electronic systems are needed for the control and synchronization of the qubits and the subsequent comparison of keys. This stage happens after the processing of the quantum information delivered by the physical layer, therefore it works at the level of bits, which are the results of the measurements of qubits distributed by a quantum channel.

Once Alice and Bob have gone through the entire key authentication process and determine that a communication can be made without suspecting that they are being spied on, then optical communication can use the shared keys to provide information between both users with all benefits that this technology implies, such as high bandwidth and high data transmission capacity (application layer through the optical network).

The physical layer, in which we are mainly interested, consists of 3 sub-blocks: first, the block associated with the "control system", which, as explained above, consists of representing all the electronic technologies necessary to carry active control of the opto-electronic systems used for QKD, also for synchronization be-
between detectors and light sources, post-processing of individual photons, among other functions. The "QRNG" (quantum random number generator) block is another key aspect of this stage, as good design allows both Alice and Bob to have true independence when choosing the bases to prepare or measure quantum states. Furthermore, the use of a generator based on the principles of quantum nature allows a number of advantages over classic random number generators.

(Figure 3.1) illustrates the 3 design stages to establish a QKD process and the subsequent transfer of encrypted information by using a secure key. Therefore, transmitting individual photons through the quantum channel with minimal distortions and with great reliability is a crucial task in any QKD system, and the design of the optical platform should be the cornerstone of the whole process.

![Diagram of QKD system](image)

Figure 3.1: Illustrates the three design stages of a QKD system. Alice’s and Bob’s physical layers are connected by a quantum channel, which in our case is an FMF. The physical layer is related to the hardware of the quantum channel and all the necessary conditions that ensure the reliable propagation of qubits are defined. The second layer is the one in charge of key extraction. This occurs after Bob has performed the measurement process. Alice and Bob transmit their bases over a classic channel, compare their measured results, correct errors, define their keys, and determine whether or not there is a spy on the channel. Once there is security in the encryption, Alice and Bob can send information through the optical network, which corresponds to the third layer. In our work, we have focused on the optical platform which is essential for the future performance of a QKD protocol.

A natural selection for quantum communication is to use the relative phase between two possible optical paths that a single photon could take. Following the same idea of a Mach-Zehnder interferometer, we can extend its two physical paths
3.1 Quantum Communication Systems Over Optical Fibers

separately to implement the well-known phase encoding technique (This scheme and its experimental details are explained in more detail in Paper I and Paper III at the end of this document, however an overview is provided below).

We can divide the scheme into three entities, where two of them are Alice and Bob and the third is the channel. Figure 3.2 represent the phase coding scheme:

Figure 3.2: Phase encoding scheme made of optical fibers. The qubits are encrypted by a relative phase between both paths that is represented by the phase angle $\phi_A$ and $\phi_B$ provided by the phase modulators placed on Alice and Bob respectively. In practical cases, this phase can undergo changes due to the birefringence of the optical fiber, experimental imperfections, environmental disturbances, among other factors. This makes this system more difficult to stabilize if the single-mode fiber link gets longer.

Alice consists of a Single-Photon Source (SPS) connected to a beam splitter (FC: Fiber Coupler), where the quantum superposition formed by the 2 probability amplitude functions associated with two different paths that the incoming single-photon can take is created. Alice applies a relative phase between both paths equal to $\phi_A$, whose values are uniformly distributed in the discrete set $\phi_A = [0, \pi/2, \pi, 3\pi/2]$. Experimentally it is done through an optical phase modulator located in one of her paths. Before entering the channel, the encoded qubit is represented by the wave function on the left side of the Figure 3.2 on Alice’s side. The quantum state propagates through a channel consisting of two different single-mode fibers. At the end of the channel, Bob applies another relative phase $\phi_B = [0, \pi/2, \pi, 3\pi/2]$ to the incoming quantum state. The wave function, just before making the projection on the beam splitter on Bob’s side is represented by the wave function on the right side of the Figure 3.2 on Bob’s side. The probability of measuring a photon on one detector or another will be given by the
Methods

phase difference applied by Alice and Bob (eq. 2.27). The phase difference will
determine whether Bob's measurement is deterministic or totally random in the
same way as an MZI. Whichever path a single-photon takes, it will arrive to Bob
in the same time slot.

The main drawback of this scheme occurs in practical cases, since the phase
added by Alice can undergo changes due to the birefringence of the optical fiber, ex-
perimental imperfections, environmental disturbances, among other factors. This
makes this system more difficult to stabilize if the single-mode fiber link gets longer.
Furthermore, two optical fibers paths are required, so it may be impractical for
real applications.

Time-bin encoding system arise as a solution to these problems. This scheme is
shown and explained in (Fig. 1.b) of Paper III. Now there are two small unbalanced
MZI, one on Alice's side and the other on Bob's side. In this way a superposition of
paths is created where its elements are defined as "early" and "late", in reference
to the probability that the photon could take those paths. Figure 3.3 represent
how Alice encrypts a qubit using an unbalanced MZI:

\[ |\psi\rangle = |e\rangle + i e^{i \phi_A} |l\rangle \]

Figure 3.3: A single-photon source (SPS) is connected to a FC in such a way
as to generate a superposition of paths following the idea of the phase encoding
scheme. However, this interferometer is unbalanced, which implies that there will
be a short path (|e\rangle) and a long path (|l\rangle). After the second FC, both bins leave
Alice in a coherent quantum superposition as shown by the equation in the upper
right corner. Using this technique, both components of the wave function can
current in a single single-mode optical fiber, unlike the phase coding scheme where
two separate fibers are needed.

When both bins are recombined in Alice's output FC, they will travel together
through a single single-mode optical fiber at different times. Bob will make the
projection of the quantum state sent by Alice on his final FC and we will have 3
time slots that represent the three possible arrivals for all combinations. Figure
3.4 represent the full time-bin encoding scheme.
Time-bin encoding provides numerous advantages over the previous system, for example, it is much easier to stabilize two short interferometers, in addition, a single-optical fiber is needed as a channel. However, after the final measurement, a post-selection process is required, since if the photon decides to take both short paths or both long paths, then there is no interference, since both events can be distinguishable. However, in the central beam it is impossible to determine with complete certainty whether the photon has decided to travel the short path in Alice and the long path in Bob or vice versa. This makes the event indistinguishable and interference can be observed in Bob. After post-selection, the system follows the rules of the phase encoding scheme. However, the main trade-off is that we must discard 50% of the information. Post-selection losses are even more drastic if we scale to high-dimensions by a factor of \((d - 1)/d\).

In summary, time-bin encoding system is a practical solution for QKD systems. On the other hand, the theoretical solution provided by the phase coding scheme avoids the problem of post-selection, however it is not practical in real situations.

In the next section we will present our proposal, which is inspired by the advantages of both systems explained above, we also introduce the central ideas that allow making this scheme a scalable system.
3.2 Our Proposal: A Few-Mode-Fiber Platform for Quantum Communication

Our proposal and its experimental details are explained in more detail in paper II and paper III at the end of this document, however an overview is provided below.

The system has two short interferometers (one on Alice and the other on Bob), just like the time-bin scheme. However, both interferometers are not unbalanced. In this scheme the superposition of paths is created as in the traditional phase coding scheme, nevertheless both probability amplitude functions arrive in a photonic lantern (PL) rather than at a FC. Depending on which port of the PL is excited with light (photon), one can map from a Gaussian mode into a high-order one. Since there is a superposition of paths at the input of the lantern, then the mapping will be from a qubit with path information into a qubit carrying spatial mode information. The PL has a few-mode-fiber at the output capable of supporting 3 spatial modes of propagation. Furthermore, this scheme consists of only one optical fiber as a channel (Like the time-bin scheme), but instead of having a single-mode fiber, we have a few-mode fiber capable of supporting the 3 spatial modes of propagation. The following figure summarizes the above:

\[
\psi = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\phi_A} |1\rangle) \\
|0\rangle \rightarrow |LP_{11a}\rangle \\
|1\rangle \rightarrow |LP_{11b}\rangle \\
\]

Figure 3.5: Our proposal borrows a key concept from the robust time-bin configuration: Two short interferometers interconnected through a (single) few-mode fiber. Photons traveling through paths \(|0\rangle\) and \(|1\rangle\) are mapped into orthogonal optical modes supported by the fiber using a photonic lantern. Since the local interferometers are now symmetrical, these photons will arrive in the same time bin and no temporal postselection is needed.

In (fig. 3.2) we have used ports 2 and 3 of the PL, where the spatial modes \(LP_{11a}\) and \(LP_{11b}\) are excited. We do this on purpose, as coherent superposition...
of these modes can generate $OAM_{\pm 1}$ modes if Alice applies the relative phases $\phi_1 = \pi/2$ or $\phi_2 = 3\pi/2$. Since both spatial modes are orthogonal, they themselves generate a basis in two-dimensional Hilbert space. Traditional QKD protocols need at least 2 MUB, therefore Alice can create another two-dimensional base by applying the values $\phi_3 = 0$ or $\phi_4 = \pi$.

The system is very versatile, as it could work with other combinations of the PL instead of ports 2 and 3, for example, port 1 combined with either port 2 or 3. For any arbitrary combination we choose, by selecting appropriate relative phases, we can always find at least 2 MUBs for each combination. Below are the spatial profiles that can be created:

\[
|\psi\rangle = \frac{1}{\sqrt{2}} (|LP_{11a}\rangle + e^{i\phi_A}|LP_{11b}\rangle)
\]

\[
|\psi'\rangle = \frac{1}{\sqrt{2}} (|LP_{01}\rangle + e^{i\phi_A}|LP_{11a}\rangle)
\]

\[
|\psi''\rangle = \frac{1}{\sqrt{2}} (|LP_{01}\rangle + e^{i\phi_A}|LP_{11b}\rangle)
\]

\[
\phi_A = 0 \quad \phi_A = \frac{\pi}{2} \quad \phi_A = \pi \quad \phi_A = \frac{3\pi}{2}
\]

Figure 3.6: The 3 possible quantum superpositions by using different combinations of the 3 LP modes. Each row (green blocks) shows the mathematical representation of each state that can be prepared. The spatial modal distribution will depend on the phase $\theta_A$ applied by Alice. The values $\phi_A = [0, \pi/2, \pi, 3\pi/2]$ are arbitrarily chosen to be able to build 2 MUBs for each PL port combination. It is observed that OAM modes can be achieved if the combinations between $LP_{11a}$ and $LP_{11b}$ are used.

Once the state is propagated through the channel, Bob uses a PL as a demultiplexer mapping the high order spatial modes into an superposition with path information. Bob then applies another relative phase $\theta_B$ to the incoming superposition. The two bins where the photon could be arrive at the FC at the same time. Bob can perform a projective measurement of the wave function of the system in the same way as an MZ interferometer. We can notice that the post-selection process is no longer necessary. (Fig 3.7) shows the mapping performed by Bob.

Experimental details about the proposal are detailed in the three articles at-
44 Methods

Few-Mode Fibre Link

\[ \psi = \frac{1}{\sqrt{2}} (|LP_{11a}\rangle + e^{i\phi_B}|LP_{11b}\rangle) \]

\[ \psi = \frac{1}{\sqrt{2}} (|0\rangle + e^{i(\phi_A - \phi_B)}|1\rangle) \]

Spatial Mode Information  Mapping  Path Information

Figure 3.7: After mapping the coherent superposition through the lantern’s adiabatic region, Bob applies another relative phase \( \phi_B \) that allows him to choose between the two required measurement bases. The measurement procedure is concluded with both paths superposed at the 50:50 FC. Quantum state detection is done by two single photon detectors placed on each outcome.

Paper I explains our proposal as a few-mode fiber MZ interferometer using classical light (from a telecom laser diode). Here we show that an interference pattern can be measured by continuously changing the relative phase "\( \phi \)" between paths. Both outputs are proportional to \( \sin^2 \left( \frac{\phi}{2} \right) \) and \( \cos^2 \left( \frac{\phi}{2} \right) \) as we expected.

In these experiments we were able to work in two configurations: back-to-back (direct connection between photonic lantern) and using 100 m of single-mode fiber as a channel. The average visibilities between the two exits were 90.2% and 88.5% respectively. Since the system shows very little degradation after propagation and we can visualize the shape of the modal distributions using a CCD camera, we can demonstrate the feasibility of realizing QKD with the proposed configuration.

In paper II, we tested two different combinations using different ports on the PL. Here we have been able to demonstrate that it is possible to generate, transmit and detect OAM modes in an all-fiber platform, thus avoiding complex mode multiplexers and sorters based on bulk optics. On this occasion we have used 500 m of few-mode fiber instead of 100 m as shown in paper I, we have also tested the stability of the interferometer through the Fourier transform, as shown in Fig. 1. b) of the paper II. We have focused at 0 Hz because environmental phase drift behavior is generally characterized by low-frequency components. Since there is no significant changes of the central peak , we conclude that the environmental phase drift is negligible when adding an additional 500 m.
3.2 Our Proposal: A Few-Mode-Fiber Platform for Quantum Communication

Both Paper I and Paper II try to demonstrate from different perspectives that the platform is feasible to perform QKD. However, so far we have only worked with classical light. Following this line, in Paper III we have now replaced the classical light with a single photon source made from a laser and a variable optical attenuator. Fig.2, Fig.3 and Fig.4 of Paper III effectively show that the proposal has a high potential to be used as a platform for quantum communications (experimental details are in Paper III).

The time-bin configuration has intrinsic losses due to post-selection and these increase as we scale in the dimension in which we encode our qubit. Currently our proposal operates in a bi-dimensional Hilbert space, however we can increase the dimensionality of our schematic by using a PL with more ports and by using multiport beam splitters, to create the quantum superposition on Alice and the projection on Bob. To do this, we must use more spatial modes that propagate through the channel, which also implies using an FMF capable of transporting as many modes as required. From this point, it is possible to create a set of bases that allow QKD in high dimensions. Despite the above, the ideal would be to continue exploiting the advantages of having OAM spatial modes to encode information. That is why we use a combination of odd and even LP-modes, as presented in equation (Eq 2.40). For this, it is enough to have a PL capable of mapping these modes and to have a phase modulator on each path before the PL.

In summary, we have been able to test by using spatial division multiplexing to phase encode photons propagating through a few-mode fiber as a proof of principle for QKD protocols. This offers new possibilities for quantum information, for example, we ensure compatibility with next-generation optical networks and we are exploiting the advantages of using OAM. Finally, as far as we know, this is the first proposal of an all in-fiber generation and detection of OAM photonic states.
I think that when we know that we actually do live in uncertainty, then we ought to admit it; it is of great value to realize that we do not know the answers to different questions. This attitude of mind - this attitude of uncertainty - is vital to the scientist, and it is this attitude of mind which the student must first acquire.

- Richard P. Feynman (No Ordinary Genius: The Illustrated Richard Feynman, edited by Christopher Sykes, p. 239, 1994)
Conclusions

4.1 Discussions

Through our proposal we have contributed two major innovations: Removing intrinsic losses in widely used time-bin quantum communication systems, as well as the creation and detection of OAM photonic qubits with an all-fiber platform, where the novel elements are the photonic lanterns and few-mode fibers. Those results pave new paths for various applications of quantum and photonic information.

All the components used to develop the platform are commercially available, which is an advantage in at least two aspects: Replicating the results obtained in this work by various groups around the world, and the possibility of coupling this system to current optical networks.

The propagation losses in the optical fiber are an element to consider if this system has as its final goal to be coupled to the current optical networks. So are the insertion losses that are present in all the optical components involved. According to the manufacturer, the attenuation coefficient of our FMF is comparable to that of commercial single-mode fiber $\alpha = 0.22\text{dB/km}$ at 1550 nm. We have measured a total loss of 1.2 dB for the 500 m used which include two homemade APC / APC connectors that introduce 0.5 dB of loss each. In various QKD protocols, a QBER of 11% is the limit to ensure secure key generation. We currently have less than 6% of QBER and without any active control system. If we only consider the loss as a limiting factor, and with the same components that we are using, then we should have an additional loss of 3.85 dB until we reach a QBER of 11%. This corresponds to an additional FMF length of about 17 km.

By measuring the interference curves of a single-photon, we can test the applicability for quantum communication, where the experimental curves are presented
Conclusions

in Paper III. Furthermore, we have employed two mutually unbiased bases used in BB84, the OAM modes being orthogonal elements of those bases. The creation of these bases is achieved by applying a relative phase in Alice and Bob. The results for the transmitted and projected states are shown in Fig. 4 of paper III. For both consecutive and 500 m cases, the average probability for the main diagonal is $0.951 \pm 0.024$ and $0.9425 \pm 0.024$ respectively.

Our results show that we can successfully send and detect the four required states in BB84 over 500m from FMF. The reason we refer to BB84 is because it is the simplest and most widely used quantum communication protocol. In the light of the results, we have shown that this protocol could acquire technical advantages if it is implemented in our platform, our proposal could be the backbone for a full QKD implementation. As indicated in (Figure 3.1), it only remains to implement the key extraction layer, which can be achieved from the synchronization of 2 FPGAs (one in Alice and the other in Bob). In addition, we can further increase the viability of our platform by applying active modal correction techniques.

Crosstalk is a key parameter to ensure proper qubit propagation. we have obtained an extinction rate of -14.6 dB and -16.2 dB by measuring the power input in ports 1 and 2 of the first PL respectively for the opposite inputs ($|0\rangle$ and $|1\rangle$ ) of the second PL. We have used manual polarization controller to compensate for mode coupling during propagation in order to optimize mode (de) multiplexing in Alice (Bob) PL.

Single-mode fiber QKD experiments commonly run over several tens of kilometers, and also they are employed by using time-bin, polarization, or frequency encoding. QKD experiments with spatially encoded quantum states are more recent and therefore have been carried out at shorter distances. Specifically with FMF and spatial states, we are only aware of two other experiments: in [117], The OAM modes are sent over a 1 km few-mode fiber. They employ spatial light modulators to generate and detect OAM modes. This implies using a bulk optical element which carries the disadvantages seen above. in [118], Here OAM modes at 850 nm were transmitted over 250 m of telecom SMF-28 fiber (working as a few-mode fiber at 850 nm). Bulk optics elements are used to detect and generate the OAM states as well. In light of the results, the 500 m distance is competitive with the state of the art, as we do not use complex bulk optics to create and detect quantum states.

Other types of fiber could be used that support multiple spatial modes, however few-mode fibers provide intermodal phase stability because the modes propagate through the same cladding.

In the supplemental material of Paper III we show our theoretical proposal for a high-dimensional setup based on few-mode fibers and photonic lanterns, pointing to a clear direction for future research.

BB84 was used as an example to argue in favor of our proposal, but in principle other protocols could also be implemented, such a prepare-and-measure semi-device independent protocols. We strongly believe that these results will have a significant and imminent impact in areas such as long-distance quantum communication, photonic circuits, fundamental physics experiments, high-dimensional quantum information, and as a tool to increase the capacity of optical networks.
4.2 Future work

So far the platform has shown convincing results that allow for a number of future works. This work is a starting point to a line of investigation towards spatial quantum communications through few-mode fibers: Longer fibers as a channel, the use of more LP-modes to create/detect high-dimension qudits, the use of active modal coupling compensation, the implementation of a QKD session, and testing other protocols as semi-device independent are now possible as line of research. From here we can run a full QKD session, for example, using decoy states and rigorous security analysis.

This system can be scaled to higher dimensions by using multi-port beam splitters (MBS) and Lantern with more inputs. This by itself is another line of future research, since MBS for quantum communications applications have not yet been widely studied.


Bibliography


Kumar, M., Quantum: Einstein, Bohr, and the great debate about the nature of reality. (2011).


A. Sit et al., High-dimensional intracity quantum cryptography with structured photons, Optica 4, 1006-1010 (2017).


Bibliography


[97] Huang, H et al., 100 Tbit/s free-space data link using orbital angular momentum mode division multiplexing combined with wavelength division multiplexing, Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), (2013).


Papers

The papers associated with this thesis have been removed for copyright reasons. For more details about these see:

https://doi.org/10.3384/9789179293260