



**UNIVERSIDAD DE CONCEPCIÓN  
DEPARTAMENTO DE FÍSICA**

---

**HIGH-DIMENSIONAL DECOY-STATE QUANTUM KEY  
DISTRIBUTION OVER 0.3 KM OF MULTICORE  
TELECOMMUNICATION OPTICAL FIBERS  
(DISTRIBUCIÓN CUÁNTICA DE CLAVE CON ESTADOS  
SEÑUELO EN ALTAS DIMENSIONES A TRAVÉS DE  
UNA FIBRA ÓPTICA MULTINÚCLEO)**

Tesis para optar al grado de  
Magister en Ciencias con mención en Física


**por**

**Nicolás Octavio Vera Paz**

**Director de Tesis: Dr. Gustavo Moreira Lima**

---

Universidad de Concepción  
Facultad de Ciencias Físicas y Matemáticas  
Departamento de Física  
Concepción, Chile.  
2016



Director de Tesis : Dr. Gustavo Moreira Lima  
Comisión : Dr. Guillermo Barreto Xavier  
Dr. Esteban Sepúlveda

*Dedicado a mis padres.*

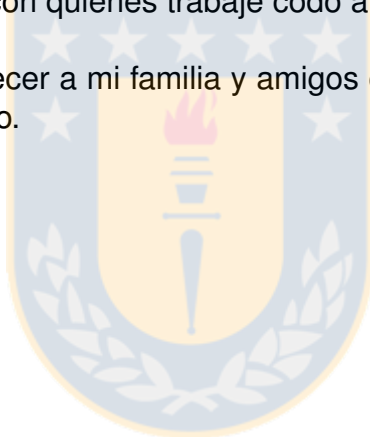


# Agradecimientos

Quisiera agradecer al doctor Gustavo Lima por su gran disposición como profesor guía durante mi maestría.

También quiero agradecer a todo el equipo de trabajo del Núcleo Milenio de óptica avanzada, en especial a Anna Przysiezna, Gustavo Cañas, Esteban Sepúlveda, Pablo Gonzalez, Santiago Gomez y Miguel Solís, quienes contribuyeron a mi formación científica y con quienes trabajé codo a codo.

Por último quiero agradecer a mi familia y amigos cercanos, ya que sin ellos nada de esto tendría sentido.



# Abstract

Multiplexing is a strategy to augment the transmission capacity of a communication system. It consists of combining multiple signals over the same data channel and it has been very successful in classical communications. However, the use of enhanced channels has only reached limited practicality in quantum communications (QC) as it requires the complex manipulation of quantum systems of higher dimensions. Considerable effort is being made towards QC using high-dimensional quantum systems encoded into the transverse momentum of single photons but, so far, no approach has been proven to be fully compatible with the existing telecommunication infrastructure. In this thesis, we overcome such a technological challenge and demonstrate a stable and secure high-dimensional decoy-state quantum key distribution session over a 0.3 km long multicore optical fiber. The high-dimensional quantum states are defined in terms of the multiple core modes available for the photon transmission over the fiber, and the decoy-state analysis demonstrates that the technique enables a positive secret key generation rate up to 25 km of fiber propagation. Finally, we show how our results build up towards a high-dimensional quantum network composed of free-space and fiber based links, through what we call the Multicore Fiber Mode Sorter, an interface device between multicore fibers and OAM free space modes of light.

# Resumen

El multiplexado es una estrategia para aumentar la capacidad de transmisión de un sistema de comunicación. Este consiste en combinar múltiples señales sobre el mismo canal de datos, y ha sido una estrategia muy exitosa en comunicaciones clásicas. Sin embargo, el uso de canales mejorados ha alcanzado una practicalidad limitada en comunicaciones cuánticas (QC). Esfuerzo considerable está siendo hecho en pos de usar sistemas cuánticos de altas dimensiones en QC, codificados en el momento transversal de fotones individuales pero hasta ahora, ningún método ha probado ser totalmente compatible con la infraestructura de telecomunicaciones existente. En esta tesis, superamos este desafío tecnológico y demostramos una sesión estable y segura de distribución cuántica de clave en altas dimensiones con estados señuelos a través de una fibra óptica multinúcleo de 0.3 km de longitud. Los estados de alta dimensionalidad están definidos en términos de los modos asociados a los núcleos disponibles para la transmisión del fotón en la fibra, y el análisis de los estados señuelo demuestra que nuestra técnica permite una generación positiva de clave a través de 25 km de fibra. Finalmente, mostramos nuestros resultados dirigidos hacia la creación de una red cuántica de alta dimensionalidad compuesta por conexiones de espacio libre y fibra, a través de lo que nosotros llamamos el Selector de Modos de fibra multinúcleo, un dispositivo-interfaz entre fibras multinúcleo y modos de espacio libre de momentum angular de la luz.

# Contents

<b>Agradecimientos</b>	<b>iv</b>
<b>Abstract</b>	<b>v</b>
<b>Resumen</b>	<b>vi</b>
<b>List of figures</b>	<b>ix</b>
<b>List of tables</b>	<b>x</b>
<b>Preface</b>	<b>1</b>
<b>1 High Dimensional Quantum Key Distribution</b>	<b>2</b>
1.1 Introduction . . . . .	2
1.2 Cryptography and quantum key distribution . . . . .	3
1.2.1 Mutually Unbiased Basis . . . . .	3
1.2.2 Fidelity of Quantum States . . . . .	4
1.2.3 Cryptography . . . . .	4
1.3 Sources, Photon Splitting attack and Decoy States . . . . .	6
<b>2 High dimensional QKD through Multicore fiber</b>	<b>10</b>
2.1 Optical Fibers and Multicore fibers . . . . .	10
2.2 Multi-Core Fiber Experiment . . . . .	12
2.3 Detection System Modelling . . . . .	13
2.3.1 Introduction . . . . .	13
2.3.2 Angular Spectrum and Fourier Plane Condition . . . . .	14
2.3.3 Multi-Core Fiber and Fourier Plane . . . . .	15
2.3.4 Loss and QBER estimation in the MCF Setup . . . . .	16
2.4 Results . . . . .	17
2.4.1 Single-photon source . . . . .	18
2.4.2 Alice state generation . . . . .	18
2.4.3 Bob state detection . . . . .	20
2.4.4 Fiber propagation, mean QKD state fidelity, referential frame control system . . . . .	20
2.4.5 Which-path information erasure . . . . .	21
2.4.6 Automated QKD session . . . . .	21
2.5 QKD results . . . . .	22

<b>3 Multicore fiber mode sorter</b>	<b>25</b>
3.1 Laguerre Gauss modes and Orbital Angular Momentum of Light . . . . .	25
3.2 Efficient Sorting of LMG . . . . .	27
3.2.1 Coordinate Transformations in Optics and Log-Polar Transformation .	27
3.2.2 Afocal System . . . . .	28
3.2.3 Mode Sorter . . . . .	29
3.3 Multicore Fiber Mode sorter . . . . .	29
3.3.1 Numerical Simulation . . . . .	31
<b>Conclusions</b>	<b>34</b>
<b>Conclusiones</b>	<b>35</b>
<b>Bibliography</b>	<b>36</b>





# List of Figures

1.1	BB84 protocol illustrated in a 2-D case. . . . .	6
1.2	Secret key rate for $d$ dimensional Hilbert spaces when considering a single-detector and a $d$ -detector scheme configuration. . . . .	9
2.1	Different kinds of optical fibers. . . . .	11
2.2	Experimental setup . . . . .	12
2.3	Bob detection system components . . . . .	13
2.4	A pinhole is added in the FP and a DM in the Image Plane of the MCF due to the first lens. . . . .	16
2.5	Intensity profile for a particular base states. . . . .	17
2.6	Mean QKD state fidelity. . . . .	19
2.7	Experimental QKD results. . . . .	23
3.1	Transversal intensity for LGM with different $l$ and $m$ . . . . .	26
3.3	Coordinate change basic scheme. . . . .	27
3.4	Collimation scheme . . . . .	29
3.5	Log-polar transformation. . . . .	30
3.6	MCF mode sorter. . . . .	31
3.7	Phase profiles for optical transformations . . . . .	32
3.8	Multifacet transformation . . . . .	33

# List of Tables

1.1	System parameters for estimation of the secret key generation probability as a function of transmission distance. . . . .	9
2.1	QBER vs. Loss table. . . . .	17
2.2	Measured parameters for the weak decoy + vacuum protocol. . . . .	24



# Preface

This thesis has been divided in three chapters for easier reading.

- **Chapter 1: High Dimensional Quantum Key Distribution.** This chapter reviews briefly concepts about quantum mechanics, cryptography and quantum key distribution. A mayor insight into Decoy States method is presented, which is an important part for the results of this thesis.
- **Chapter 2: High dimensional QKD through Multicore fiber.** This chapter shows the experimental setup proposed, and the main results of this thesis. It starts with an introduction about optical fibers, follows with the presentation of the experimental setup for High dimensional QKD through multicore fiber experiment, then shows the detection system modeling for characterization, and finishes with the presentation of experimental results.
- **Chapter 3: Multicore fiber mode sorter.** This last chapter shows the proposition and numerical simulation of the Multicore fiber mode sorter, a device thought for a flexible hybrid quantum network.

# Chapter 1

## High Dimensional Quantum Key Distribution

The purpose of this chapter is to introduce the reader into the state of the art and motivation of High Dimensional Quantum Key Distribution (HDQKD), as well to show some concepts and definitions about cryptography that will be helpful to the understanding of this thesis. Section 1.1 introduces the context and motivations in which this thesis develops, section 1.2 explains basics of cryptography and quantum key distribution (QKD), and section 1.3 takes a deep dive into the Decoy-state method, as it is an important part of this work. A result about the key generation rate in higher dimensions regarding the distance of communication is presented.

### 1.1 Introduction

In an age defined by several technological breakthroughs, we are aware that our privacy will be threatened by the likely development of quantum computers. Yet, we are confident that countermeasures will be created allowing post-quantum cryptography [1]. One possibility is the use of quantum-resistant classical cryptographic algorithms that provides a patch-safe solution for private communication to everyday internet users. Unfortunately, however, this method falls short while considered for sensitive documents of big corporations as classical signals can be copied and stored to be decrypted decades ahead. In this context, quantum cryptography emerges as a necessary and complementary alternative for modern global secure communications, since the certifiable security provided by this technique can not be compromised after the communication has been performed [2, 3, 4]. Thus, it provides the long-term privacy required in many cases.

Over the last decades we have witnessed the advances of telecommunication technologies by experiencing a huge increase on our capacity to send/download data. This has been vastly based on the development of new techniques to multiplex information in different degrees of freedom of light transmitted over an optical fiber, which have allowed their information capacity to be increased around tenfold every four years [5]. Analogously, in quantum communications, the use of high-dimensional quantum systems allows for more information to be transmitted between the communicating parties [6]. Fortunately, it turns

out that such complex quantum systems can be created by also exploring the degrees of freedom of faint light pulses (attenuated to the single-photon level), and therefore most of the multiplexing strategies developed for classical telecommunications are to some extent connected to the implementation of high-dimensional secure quantum communications. This hardware compatibility, considered together with the historical development of classical telecommunications that had to deal with an ever-growing internet traffic, shows that if quantum technologies are to emerge as an alternative solution for the post-quantum cryptography era, then it will rely on the use of high-dimensional quantum systems.

Even though experimental high-dimensional quantum cryptography is still at its infancy, secure communications based on the use of high-dimensional quantum systems encoded into the transverse momentum of single photons has been the subject of many recent experimental efforts [7, 8, 9, 10, 11], and theoretical analyses [6, 12, 13, 14, 15, 16, 17]. The motivation comes from the versatility provided by the fact that it can be used to define an infinite-dimensional Hilbert space in terms of the orbital angular momentum (OAM) of Laguerre-Gaussian single-photon modes [18], or also in terms of the number of linear transverse modes available for the photon transmission [19]. OAM encoded quantum systems are suitable for communication over free-space links due to its resilience against perturbation effects caused by atmospheric turbulence [20], while on the other hand, path encoded quantum states are suitable for communications systems based on waveguide integrated circuits [21]. However, all the implementations performed so far suffer of severe drawbacks. For instance, all of them have been limited to low bandwidth as the repetition rate lies at the range of kHz, and most important, no research proposed so far has accomplished a secure quantum communication session while propagating such quantum states over the already available telecommunication fiber based infrastructure, casting serious doubts about its viability for real world applications.

In this thesis is presented a work that represents a major step overcoming this last technological challenge by the demonstration of a secure high-dimensional quantum key distribution (HD-QKD) session between two parties communicating over a 0.3 km long telecommunication optical fiber, whose security is guaranteed by resorting to the decoy-state method. The new technique is built upon newly developed multicore optical fibers, now used in classical telecommunications for space-division multiplexing [5].

## 1.2 Cryptography and quantum key distribution

It is assumed that the reader is familiar with basic concepts of quantum mechanics. In this section we review some strictly necessary quantum mechanic concepts and cryptography definitions to understand the Bennet-Brassard (BB84) quantum key distribution protocol.

### 1.2.1 Mutually Unbiased Basis

Let  $\mathbb{H}$  be a  $d$ -dimensional space over  $\mathbb{C}$  with the usual vectorial product and the product induced norm. Let  $A$  and  $B$  be two hermitian operators in  $\mathbb{H}$ , with orthogonal unitary basis vectors  $\{|a_j\rangle\}$  and  $\{|b_j\rangle\}$  respectively. The basis are said to be Mutually Unbiased (MUBs) if

$$|\langle a_i | b \rangle| = \frac{1}{d}, \forall i, j \in \{1, \dots, d\} \quad (1.1)$$

When two basis are MUBs, a vector from one base is completely undetermined over projections in the other base [22]. For example, in a two dimensional case, as the polarization of a photon, given the base  $\{|H\rangle, |V\rangle\}$ , a MUB for this base is  $\{|+\pi/2\rangle, |-\pi/2\rangle\}$ , in this case, we can write a state from the first base in terms of the second one, say  $|H\rangle = \frac{1}{\sqrt{2}}(|+\pi/2\rangle + |-\pi/2\rangle)$ . It's clear that if we measure this vector over the second base, it will be undetermined over the two possible outputs,  $+\pi/2$  and  $-\pi/2$ . As we shall see, MUBs are central in QKD because of the indeterminacy propriety.

## 1.2.2 Fidelity of Quantum States

In order to measure performance of a real experiment involving quantum states, we need to define a way to compare two quantum states. For example, in a QKD protocol, due to imperfections in Alice's experimental setup or due to effects of the quantum channel over propagating states, the state  $|\psi'\rangle$  arriving to Bob may not be the same state  $|\psi\rangle$  that Alice wanted to prepare. A way to quantify the difference between two pure states is through the definition of the "Fidelity" between two states [22]. It is defined by

$$F(|\psi\rangle, |\psi'\rangle) = |\langle \psi' | \psi \rangle|^2. \quad (1.2)$$

Fidelity, as defined in 1.2 takes values between 0 and 1. For states that only differ in a global phase, the fidelity value is 1. For orthogonal states, it takes the value 0. It can be thought as how much a state is projected into another. Other more general definitions of fidelity involving density matrices are not considered here because our work doesn't involve quantum state tomography. We define the Quantum Bit Error rate (QBER) as the complement of fidelity.

$$QBER = 1 - F. \quad (1.3)$$

## 1.2.3 Cryptography

### One-time pad

In cryptography, One-time pad (OTP) is an encryption scheme where two communicating parties share a randomly generated key string [23]. One of the parties mixes a message with the key using an OR operation. This party send the encrypted message to the other party, which performs a XOR operation for message decryption. This scheme is theoretically secure against cracking under certain assumptions that are hard to justify. The problems with this scheme are:

- Authentication of communicating parties.
- True randomness in string generation.

- Key distribution

Authentication refers to the problem where the message is not authenticated by the scheme. An attacker, knowing the length of the key string, can implant a message different from the original one. The true randomness is the problem associated with the use of Pseudo-random number generation for string generation. New investigations aim for the certification of random numbers with the use of quantum mechanics. Key distribution is a mayor problem, and the principal subject of this work. The secure sharing of a secret string between the communicating parties is a non-trivial problem. Any way to share a secret key based in classical physics is in principle insecure, it just depends on the technological capacities of the hacker to crack the scheme and get the string. In quantum cryptography it is assumed that an eavesdropper interested in stealing the message has unlimited technological resources at his disposal. It is even assumed that he manufactured some of the equipment used by the communicating parties. Quantum Key Distribution presents a solution to this problem because it's security is guarantied by quantum mechanics, and in particular in the Non-Cloning theorem. In the following subsection a concise resume of a quantum key distribution protocol is shown.

### BB84 Protocol

The objective of a QKD protocol is to produce a shared secret random key between two parties that can be used to encrypt a message [24]. These two parties, that we shall call Alice and Bob, generate this key by the sharing of a qudit by means of a quantum channel. In the Bennet-Brassard protocol (BB84), extended to  $d$  dimensions, Alice prepares a *qudit* chosen randomly between a set of states belonging to two MUBs. Each state has a symbol asociated. She sends the state to Bob, and he chooses randomly between measuring over one of the two MUBs. After sharing some number of *qudits*, Alice broadcasts in a public channel the MUB she used for every qudit sent, and they discard their dit when the chosen MUBs were different. Later, Alice and Bob share small portions of generated key to compare the error rate. If there is someone (that we shall call Eve) trying to eavesdrop the quantum sharing in the channel, the No-Cloning theorem guaranties that the sates will not be the same, because Eve has to measure somehow the *qudit*, raising the error rate. If this error rate beats certain threshold, it means that necessarily Eve is trying to eavesdrop, so Alice and Bob will decide to not communicate the encrypted message.

Fig.1.1 illustrates the BB84 protocol for  $d = 2$ , like polarization encoding in photons. Since in real life implementations there are errors associated with the crafting of quantum states, fidelity of such states has to be taken into account, because for certain thresholds of quantum bit error rates (QBER) ( $QBER = 1 - F$ ) the security of a QKD protocol may be compromised because certain attack strategies performed by Eve become viable with increasing QBER. It turns out that for QKD protocols that use  $d > 2$ , security advantages arises with respect to this security threshold, making high dimensional QKD protocols more robust against Eve's attacks [6].

Classical post-processing techniques, as error correction and privacy amplification are used to remove errors and to make useless information owned by an eventual eavesdrop-

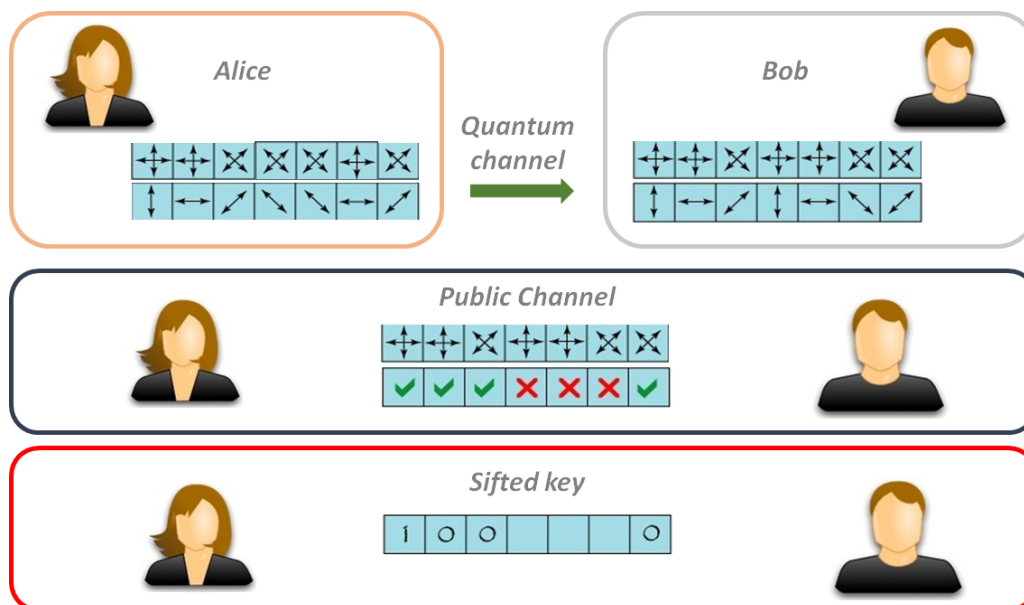


Figure 1.1: BB84 protocol illustrated in a 2-D case. Source: Own elaboration.

per [3]. In these processes, computational time is used as huge amounts of raw data are generated, and part of the string is consumed. As we will see in the next section, the key generation rate of a QKD protocol depends on these classical processes.

### 1.3 Sources, Photon Splitting attack and Decoy States

In QKD protocols as BB84, security against eavesdroppers is guaranteed when single photons are used in the communication protocol. In practice, there are not single photon sources available, only coherent-state sources where the probability of having  $\mu$  photons per pulse corresponds to Poissonian distribution,  $P(\mu) = \exp\langle n \rangle \frac{\langle n \rangle^\mu}{\mu!}$ , so that multiphoton pulses will be generated. Eve, for which we suppose technological superiority, can save duplicated photon without measuring them, and when Alice reveals the basis she used, Eve can measure her stolen photons in such bases, gaining information of the string. To overcome this problem, the QKD protocols have been implemented with  $\mu \ll 1$ , so the probability of generation of a pulse with two or more photons is very low, giving Eve only limited information about the key, proportional to the probability of multiphoton states.

When the transmission channel suffers high losses, a powerful kind of attack can be used by Eve: the Photon-Number Splitting Attack (PNSA), which can give Eve full string information exploiting the Poissonian distribution of generated photons. To describe it, we assume that Alice and Bob are performing a BB84 protocol, where Alice sends photons to Bob through a high loss channel with 90% losses, or with a yield  $\gamma = 10\%$ . Let's assume also that Bob's detector can't resolve number of photons detected. In this way, Bob expects detection only in 10% of the pulses sent by Alice. Let's also assume that Alice is using a coherent state source, with 90% probability of single photon per pulse and 10% of multiphoton pulse probability. Alice doesn't have knowledge about when she is sending single photons



or multiphotons. Eve intercepts the channel and blocks all the single photon pulses. When a multiphoton pulse is sent, she stores one photon and sends the other through a perfect channel without losses. Thus, Bob will detect in one each ten pulses, as expected. Then, when Alice publishes her used bases, Eve measures her photons, gaining full knowledge of the key and compromising the security of the QKD session. We can see that for this example, in order to have a secure session, the yield has to be greater than the probability of multiphoton pulses.

$$\gamma > p_{multi} \quad (1.4)$$

$p_{multi}$  is a measure for the quality of the source as a single photon generator. The problem is that for increasing loss (lower yield) a nearly perfect single photon source is needed.

A modification of the usual QKD protocols was proposed as a counter measure against the PNSA. The Decoy State method allows Alice and Bob to detect if a PNSA is taking place during the QKD session. The idea is the following: the PNSA implies that the yield of the multiphoton pulses is abnormally high compared to those with single photons. Alice intentionally, and randomly, sends decoy pulses that are multiphoton. Eve can not distinguish between signal multiphoton pulses and decoy multiphoton pulses, so both kind of pulses will have the same yield. After the session, Alice publishes which pulses were decoy, and Bob can analyze the yield of the decoy pulses respect to the signal ones.

For our purposes, we are interested in a Decoy State method for HD-QKD systems. We show how the secret key generation probability  $R$  (namely the probability of obtaining a secure bit for each transmitted pulse) of a HD-QKD system can be derived using the decoy-state approach [28, 25, 26]. Our analysis follows the method of Ref. [30], and modifications are performed when necessary for dealing with the high-dimensional case. We also show how the key rate is estimated as a function of the distance.

The secret key generation probability for a  $d$ -dimensional systems is given by [30, 35]

$$R \geq Q_0 \log_2 d + Q_1 [\log_2 d - H_d(e_1)] - Q_\mu H_d(E_\mu) f(E_\mu), \quad (1.5)$$

where  $Q_0$  and  $Q_1$  are the gains of the vacuum and single-photon states, respectively.  $Q_\mu$  is the overall gain (i.e. the probability of obtaining a detection when the signal state is sent),  $E_\mu$  is the overall error rate, while  $e_1$  is the error rate of the single-photon states.  $H_d(x) = -x \log_2 [x/(d-1)] - (1-x) \log_2 (1-x)$  is the  $d$ -dimensional modified Shannon entropy of the QBER [12];  $f(E_\mu)$  is the inefficiency of the error correction function. The secret key probability considers the use of the efficient BB84 protocol [29].

The values of  $Q_\mu$  and  $E_\mu$  are directly obtained from the experimental data when Alice sends signal pulses. On the other hand, the parameters associated to single-photon pulses ( $Q_1$  and  $e_1$ ), and vacuum ( $Q_0$ ), cannot be directly measured. They must be inferred through the use of an analytical or numerical approach based on the decoy-state technique [38]. A practical implementation consists on using only one weak (with average photon flux  $\nu < \mu$ ) and vacuum decoy states. Under this approach,  $Q_0$  can be directly estimated as  $Q_0 = e^{-\mu} Y_0$ , where  $Y_0$  is the measured yield of the vacuum states (i.e. the probability of detection mea-

sured when no photons are sent from Alice).

On the other hand, a lower bound  $Q_1^L$  on  $Q_1$ , and an upper bound  $e_1^U$  of  $e_1$ , can be written as [30]

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2} \left[ Q_v e^v - \frac{v^2}{\mu^2} Q_\mu e^\mu - \frac{\mu^2 - v^2}{\mu^2} Y_0 \right], \quad (1.6)$$

and

$$e_1^U = (E_v Q_v \mu e^v - \mu e_0 Y_0) / (v Q_1^L e^\mu), \quad (1.7)$$

with  $Q_v$  and  $E_v$  measured with the weak decoy state. These values are fed into Eq. (1.5) to calculate the experimental secret key rate.

The same method can be exploited to derive the expected key rate as a function of the channel length. In this case the values of  $Q_\mu$ ,  $Q_v$ ,  $E_\mu$  and  $E_v$  can be estimated by assuming the propagation in a lossy channel. When using a photon source modeled as an incoherent mixture of Fock states, given by the Poisson distribution  $P_n = \mu^n e^{-\mu} / n!$ , the overall gain and QBER values are computed through the summation over all possible states. Thus,  $Q_\mu = \sum_{n=0}^{\infty} Y_n P_n$  and  $E_\mu = (1/Q_\mu) \sum_{n=0}^{\infty} e_n Y_n P_n$ . In the above expression  $Y_n$  is the  $n$ -photon yield, defined as the probability of detection at Bob's station when Alice sends an  $n$ -photon Fock state and  $e_n$  is the corresponding error. The  $n$ -photon gain,  $Q_n = Y_n P_n$ , results from the product of the yield  $Y_n$  and the probability  $P_n$  of the state being produced by Alice.

In a lossy channel the expected value of  $Y_n$  is  $Y_n \approx Y_0 + \eta_n$ , where  $Y_0$  is the vacuum yield – related to the dark count probability of the SPD ( $P_{dark}$ ). The parameter  $\eta_n = 1 - (1 - \eta)^n$  is related to the overall efficiency  $\eta$  of the channel – given by the detector efficiency and the internal transmittance of Bob's apparatus. The link transmittance is given by  $10^{-\alpha L/10}$ , with the attenuation coefficient represented by  $\alpha$  [dB/km] and the transmission link length given by  $L$  [km]. The error associated to the  $n$ -photon states can be estimated to be  $e_n = (e_0 Y_0 + e_{opt} \eta_n) / Y_n$ , where  $e_{opt}$  is due to the optical misalignment of the detection system.

In a  $d$ -dimensional QKD system employing  $d$  outputs (one single-photon detector at each output), the yield of the vacuum states is  $Y_0 = 1 - (1 - P_{dark})^d$  which, for small values of  $P_{dark}$ , increases linearly with the dimension  $Y_0 \approx d P_{dark}$ . The QBER associated to vacuum states is  $e_0 = (d - 1) / d$ , corresponding to the probability of a random dark count to occur in an SPD which is not expected to fire when Alice and Bob's bases are matched.

With one single-photon detector in the  $d$ -dimensional case, the vacuum yield is independent of the dimension and limited to  $Y_0 = P_{dark}$ . On the other hand, some non-vacuum states sent by Alice will not be measured by Bob, even in the case of compatible bases between Alice and Bob, and the overall efficiency is reduced to  $\eta_n = [1 - (1 - \eta)^n] / d$ .

The expected values of  $Q_\mu$  and  $E_\mu$  and the parameters associated to single-photon events,  $Q_1$  and  $e_1$  for a given overall channel efficiency  $\eta$  and a  $d$ -dimensional QKD system, are summarized in Table 1.1 for both single and  $d$  detector cases. The curves for the secret key rate, as a function of the fiber length, shown on Fig. 1.2 are computed by feeding the values of table 1.1 into Eq. (1.5).

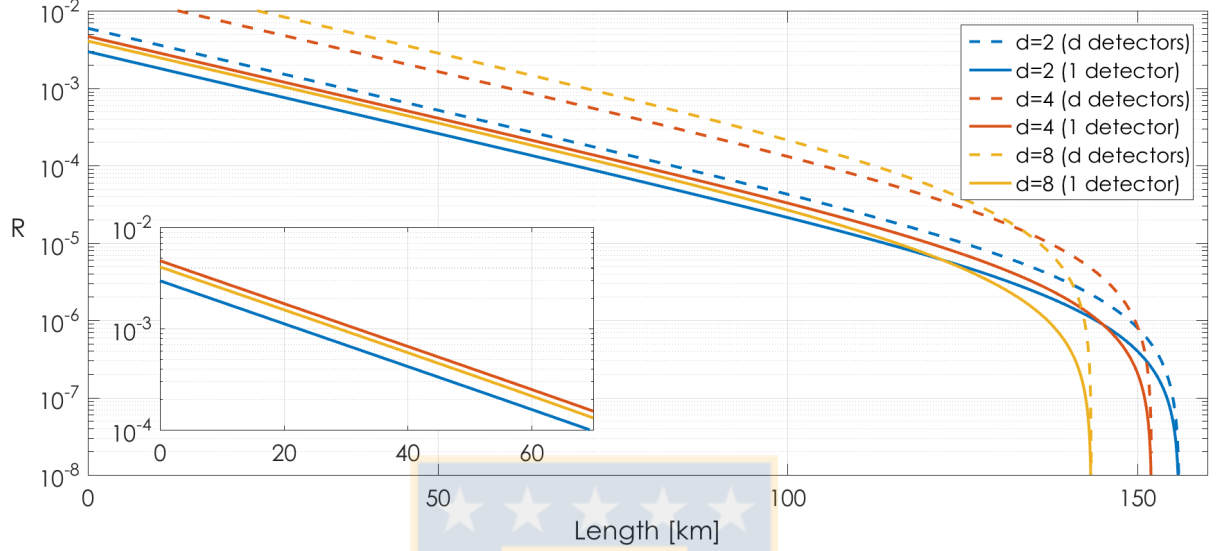


Figure 1.2: **Secret key rate for  $d$  dimensional Hilbert spaces when considering a single-detector and a  $d$ -detector scheme configuration.** Here we perform secret key rate simulations considering the infinite decoy case, while using as input parameters the data from [36]. In the  $d$ -detector case, as expected, the rate increases for shorter distances and the cut-off point in the secret rate vs. distance curve occurs for shorter distances, as  $d$  increases. In the single-detector case, the probability of correctly projecting the transmitted state onto itself decreases linearly with  $d$ , while the information gain per transmitted photon only increases with  $O(\log(d))$ . Thus, the case of  $d = 8$  always generates a lower secret key rate when compared to  $d = 4$ . Nonetheless, as shown on the inset, our implementation (i.e. the  $d = 4$  case) is capable of beating  $d = 2$  case. Source: Own elaboration.

	$Q_\mu$	$E_\mu$	$Q_1$	$e_1$
$d$ detectors	$Y_0 + 1 - e^{-\mu\eta}$	$\frac{e_0 Y_0 + e_{opt}(1 - e^{-\mu\eta})}{Y_0 + 1 - e^{-\mu\eta}}$	$(Y_0 + \eta)\mu e^{-\mu}$	$\frac{e_0 Y_0 + e_{opt}\eta}{Y_0 + \eta}$
Single detector	$Y_0 + \frac{1 - e^{-\mu\eta}}{d}$	$\frac{e_0 Y_0 d + e_{opt}(1 - e^{-\mu\eta})}{Y_0 d + 1 - e^{-\mu\eta}}$	$(Y_0 + \frac{\eta}{d})\mu e^{-\mu}$	$\frac{e_0 Y_0 d + e_{opt}\eta}{Y_0 d + \eta}$

Table 1.1: System parameters for estimation of the secret key generation probability as a function of transmission distance. Source: Own elaboration.

# Chapter 2

## High dimensional QKD through Multicore fiber

In reference [9] a 16-dimensional quantum key distribution session was demonstrated, experimentally, but one problem with that work was that the quantum link was a really short free space channel (30cm). The scheme presented there suffers from large diffraction through propagation, restraining the length of the communication channel to the order of meters. For any serious QKD protocol, it's necessary to have a sufficiently long channel to communicate remote parties. One solution for this is the use of optical fibers, that can transport photons with low loss by long distances, but the use of dimensions larger than two have never been demonstrated. New designs in fibers, in particular the new multi-core fibers, offer promising high dimensional quantum channels for QKD. In this chapter we review some aspects of optical fibers and the advantages of multicore fibers, and we show the setup and results for the experiment for Quantum Key Distribution based in multi-core fiber (MCF). These results represent the main purpose of this thesis.

### 2.1 Optical Fibers and Multicore fibers

An optical fiber is an electromagnetic waveguide with circular cross-section. It is constituted by an inner transparent dielectric core surrounded by a cladding made with a lower refractive index dielectric material. Under ray optics, it can be understood as if light propagating inside the core is kept inside by the total internal reflection phenomena. Optical fibers can be thought as cavities, where the electric field can oscillate in different propagation modes. In this sense, there exist Single Mode Fibers (SMF) that support only the gaussian mode of propagation, and Multimode Fibers (MMF) that support multiple propagation modes. SMF are preferred for communication since they preserve spatial coherence over long distances. Multiplexing information in a single SMF is possible by the use of the different degrees of freedom of a photon. Wavelength, phase, time and polarization multiplexing have been used to increase exponentially the amount of data that can be sent by a single SMF [51]. New multi-core fibers allow a new way of path multiplexing by offering various cores inside a single cladding. Fig.2.1 shows different kinds of SMF and MMF, in single core single mode fiber (SCSMF) and MCF configurations.












Number of modes	Single-core	Multi-core		
		Uncoupled-type	Coupled-type	
Single	SMF 	Homogeneous/Heterogeneous  		LMA fiber 
Few	FMF 	Few-mode MCF 	Hybrid structure 	Strongly/Weakly coupled 
Multi	MMF 	Multi-mode MCF 		LMA fiber 

Figure 2.1: **Different kinds of optical fibers.** Source: Kunimasa Saitoh and Shoichiro Matsuo, MCF for large capacity transmission, *Nanophotonics* 2013; 2(5 to 6): 441.

In SMF exist an evanescent wave outside the fiber core. In single mode MCF this can be a problem because this evanescent wave can leak from a core into other cores, so it is important to design a MCF with good spacing between the cores in the cladding. In [51], a characterization of this leakage was done. There are fibers where the coupling between cores is intentional, as in the Large mode Area fibers [Fig 2.1].

There are interferometry-based communication protocols that have been attempted in a SMF scheme. A laser beam is separated into two SMF, and reunited again for interference in a Mach-Zehnder like scheme. Such system suffers strong decoherence because mechanical and thermal fluctuations between the two SMF. MCF present a solution to this particular problem because all the paths of the interferometer are within the same cladding so the fluctuations are the same for all paths, giving the system an intrinsic resistance against thermal and mechanical fluctuations. As we show later, there is still a slow phase drift that has to be taken into account.

## 2.2 Multi-Core Fiber Experiment

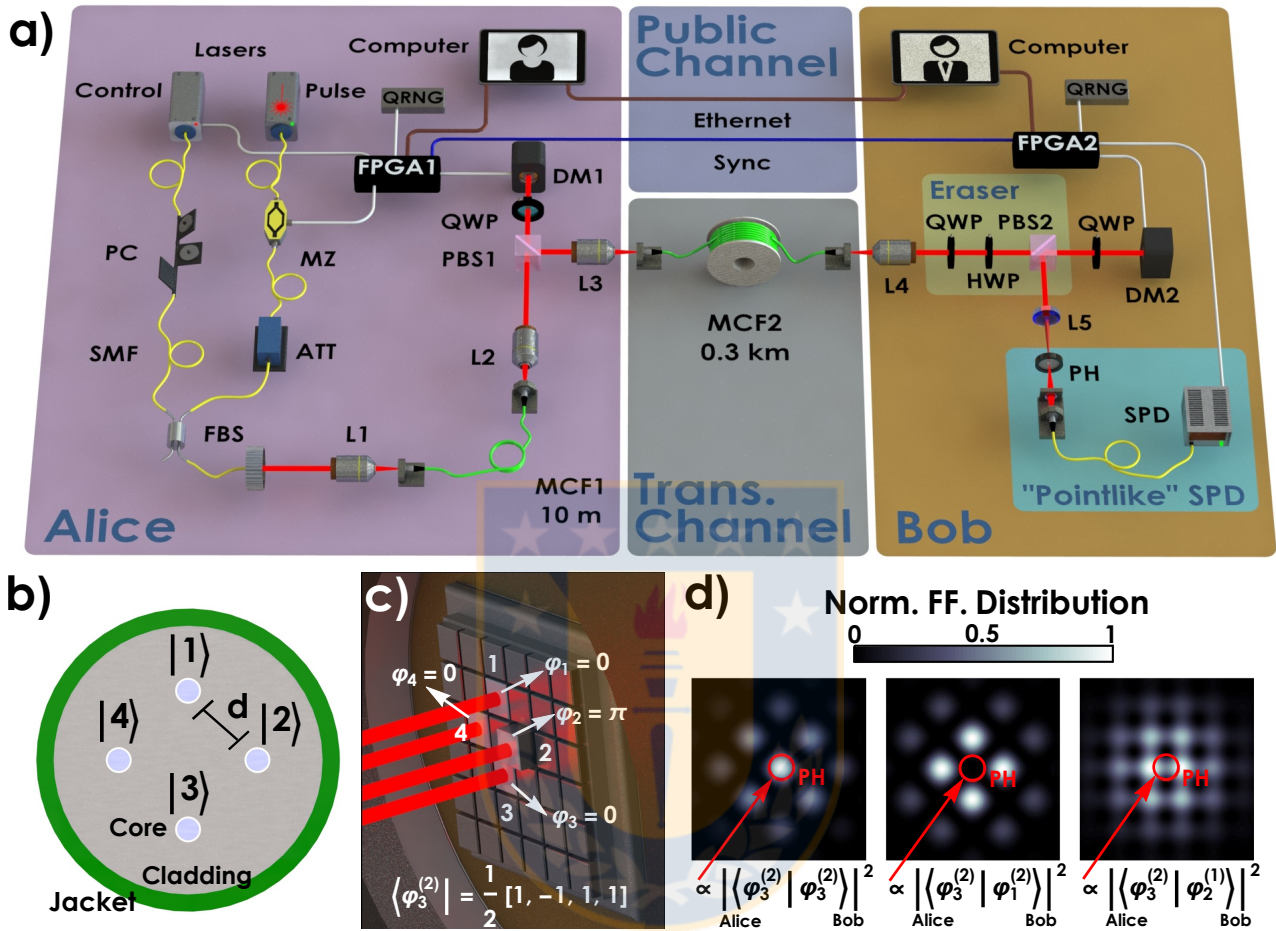


Figure 2.2: **Experimental setup.** Source: Own elaboration.

Fig.2.2 show the experimental setup we built for MCF study. a) In our scheme Alice employs a source of weak coherent states to encode the 4-dimensional BB84 QKD states using a deformable mirror (DM1). The single photons are sent to Bob through a 0.3 km long four-core multicore fiber. Bob employs a quantum eraser to get rid of any possible polarization-mode coupling during fiber propagation. He then uses an identical deformable mirror to Alice's (DM2) and a "pointlike" SPD, to implement his measurements. The QKD protocol is automatically executed using two FPGA electronic modules, fed with QRNGs. Finally each FPGA sends its results to a computer, which are used to determine the session's QBER. A control laser is used to periodically check whether Alice and Bob's referential frames are aligned, and the FPGAs also command this control procedure. b) Schematic of the multi-core fiber's cross-section. c) The deformable mirror is composed of a  $6 \times 6$  mirror matrix (Boston micromachines). The light coming from each core from the MCF is mapped to an individual mirror. As an example, cores  $|1\rangle$ ,  $|3\rangle$  and  $|4\rangle$  have a relative phase of 0 applied, while  $|2\rangle$  has a  $\pi$  relative phase-shift. d) Simulation of the FF distribution, with the pinhole area indicated by the red circle. The first case shows when Bob's projection is performed on the same state as the one Alice sent, both using the same MUB. It displays constructive

interference through the pinhole. In the second case the pattern shows a situation where an orthogonal projection is used within the same MUB, leading to destructive interference and no detection. The final case happens when any projection is made using a different MUB within respect to Alice's. Then there is a 25% probability that the photon will be detected. ATT: Adjustable optical attenuator; DM: Deformable mirror; FBS: Fiber beamsplitter; HWP: Half-wave plate; L: Objective lens; MCF: Multicore fiber; MZ: Mach-Zehnder amplitude modulator; PBS: Polarizing beamsplitter; PH: Pinhole; QRNG: Quantum random number generator; QWP: Quarter-wave plate; SPD: Single-photon detector; SMF: Single-mode fiber.

## 2.3 Detection System Modelling

### 2.3.1 Introduction

In optics experiments, the detection system (DS) has to be fully characterized. A full theoretical description of the DS is necessary in order to achieve a correct analysis of the data given by the experiment. Here we analyse the DS (Bob) of the high-dimensional quantum key distribution using Multi-Core fiber (HD-MCF) experiment. Fig.2.3 shows of what consist the DS of Bob, who is receiving prepared quantum states codified in the phase of different paths of a photon.

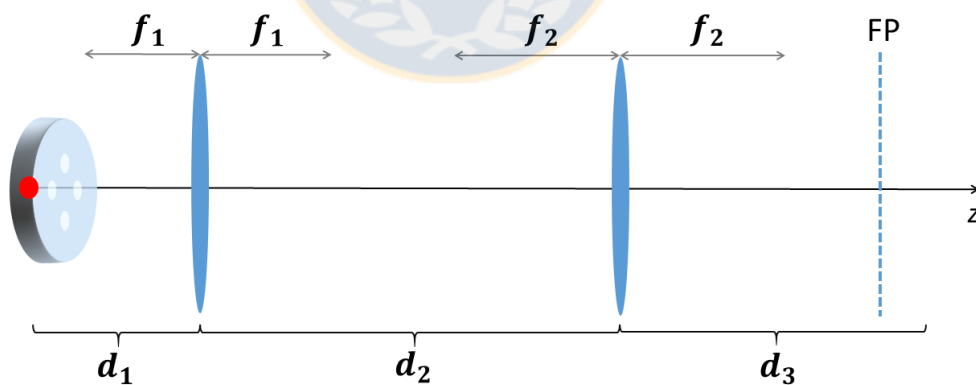


Figure 2.3: **Bob detection system components.** A two lenses system is depicted. The lens L1 forms an image of the object over the Deformable Mirror (DM) and the second lens performs a Fourier Transform of the object over a Fourier Plane (FP) at the unknown distance  $d_3$ . Source: Own elaboration.

Here we are interested in obtaining at which distance  $d_3$  from the second lens forms the Fourier Plane (FP). At this plane, the Fourier Transform of the input object (the MCF) is

obtained, and represents the Far Field (FF) or Interference plane. After obtaining this plane, we model the loss due to a pinhole placed in the FF, and we do an estimation of the minimum Quantum Bit Error Rate (QBER) achievable with this system.

### 2.3.2 Angular Spectrum and Fourier Plane Condition

A complete description of the system can be achieved by the Angular Spectrum of Light [37]. The following equations the propagations and the transmissions through all the components of the set-up shown in Fig.2.3.

$$\hat{E}_{iL_1}(\vec{q}'', z_1) = \hat{E}_0(\vec{q}'') e^{-i\frac{q''^2}{2k} z_1}, \quad (2.1)$$

$$\hat{E}_{T_1} = \int \hat{E}_{iL_1}(\vec{q}'', z_1) T_{L_1}(\vec{q}'' - \vec{q}'), \quad (2.2)$$

$$\hat{E}_{iL_2}(\vec{q}', z_2) = \hat{E}_0 e^{-i\frac{q'^2}{2k} (z_2 - z_1)}, \quad (2.3)$$

$$\hat{E}_{T_2} = \int \hat{E}_{iL_2}(\vec{q}', z_2) T_{L_2}(\vec{q}' - \vec{q}), \quad (2.4)$$

$$\hat{E}(\vec{q}, z_1) = \hat{E}_0 e^{-i\frac{q^2}{2k} (z_3 - z_2)}, \quad (2.5)$$

Where  $\hat{E}_0$  is the Fourier Transform of the  $E_0$  object complex field. Here we consider  $z_1 = d_1$ ,  $z_2 = d_1 + d_2$  and  $z_3 = d_1 + d_2 + d_3$ . The resulting complex electric field at an arbitrary plane in  $z_3$  is given by

$$E(\vec{x}, z_3) \propto \int \int e^{i\frac{q^2}{2k} (f_2 - \frac{f_2^2}{\alpha} - (z_3 - z_2))} \hat{E}_0(\vec{q}'') \times e^{i\frac{q''^2}{2k} (f_1 - \frac{f_1^2}{\alpha} - z_1)} e^{i(\vec{x} - \frac{1}{k\alpha} f_1 f_2 \vec{q}'')} \vec{q} d\vec{q} d\vec{q}'' \quad (2.6)$$

Where  $\alpha = f_1 + f_2 - (z_2 - z_1)$ . The Fourier Plane condition is given by making zero the exponent of the  $q$  dependent Gaussian factor in Eq.2.6 In this way, the  $q$  Fourier transform results in a Dirac Delta, and the resulting electric field at the plane found by the condition is proportional to the Fourier Transform of the object  $E_0$ .

$$E(\vec{x}, z_3) \propto \hat{E}_0(\vec{q}'') e^{i\frac{q''^2}{2k} (f_1 - \frac{f_1^2}{\alpha} - z_1)} \quad (2.7)$$

The Dirac Delta gives the spacing of the Fourier Plane.

$$\vec{q}'' = \frac{k\alpha}{f_1 f_2} \vec{x} \quad (2.8)$$



### 2.3.3 Multi-Core Fiber and Fourier Plane

For our purposes, the object in Eq.2.7 will be the MCF. It can be modelled as the sum of four the four Gaussian beams coming out from each of the four cores.

$$U(r) = U_T(\rho) + U_R(\rho) + U_B(\rho) + U_L(\rho), \quad (2.9)$$

where, for instance,

$$U_T(r) = C(z) e^{\frac{\rho}{w^2(z)}} e^{-ikz} e^{-i\frac{k\rho_T^2}{2R(z)}} e^{-i\zeta(z)}, \quad (2.10)$$

with  $\rho_T = x^2 + (y - c_T)^2$ . Analogous for other cores. The Fourier transform for each core is given by

$$\mathfrak{S}\{U_T\} = e^{-\frac{1}{4\beta}(q_x^2 + q_y^2)} e^{-ic_T q_y}, \quad (2.11)$$

$$\mathfrak{S}\{U_R\} = e^{-\frac{1}{4\beta}(q_x^2 + q_y^2)} e^{-ic_R q_x}, \quad (2.12)$$

$$\mathfrak{S}\{U_B\} = e^{-\frac{1}{4\beta}(q_x^2 + q_y^2)} e^{ic_B q_y}, \quad (2.13)$$

$$\mathfrak{S}\{U_L\} = e^{-\frac{1}{4\beta}(q_x^2 + q_y^2)} e^{ic_L q_x}, \quad (2.14)$$

$$(2.15)$$

Fourier transforms conserve Gaussians, and each Gaussian is centred with respect to the optical axis. In the Fourier plane, it's impossible to know from which core the detected photon arrived. When the fields are present at the same time, they will interfere.

$$U(q) = \frac{\pi}{\beta} e^{-\frac{1}{4\beta}(q_x^2 + q_y^2)} (e^{ic_B q_y} e^{-i\phi_B} + e^{-ic_B q_y} e^{-i\phi_T} + e^{ic_B q_x} e^{-i\phi_L} + e^{-ic_B q_x} e^{-i\phi_R}), \quad (2.16)$$

where we have introduced the relative phases  $\phi_T$ ,  $\phi_R$ ,  $\phi_B$  and  $\phi_L$  between the cores. These relative phases determine the *qubit* that will be measured in the detection setup. The intensity is given by

$$I = 2 \frac{\pi^2}{\beta^2} C^2(z) e^{-\frac{1}{4\beta}(q_x^2 + q_y^2)} (2 + \cos(2c q_y + \phi_T - \phi_B) + \cos(2c q_x + \phi_R - \phi_L) + \cos(c(q_x + q_y) + \phi_T - \phi_L) + \cos(c(q_x + q_y) + \phi_R - \phi_B) + \cos(c(q_x - q_y) + \phi_R - \phi_T) + \cos(c(q_x - q_y) + \phi_B - \phi_L)). \quad (2.17)$$

### 2.3.4 Loss and QBER estimation in the MCF Setup

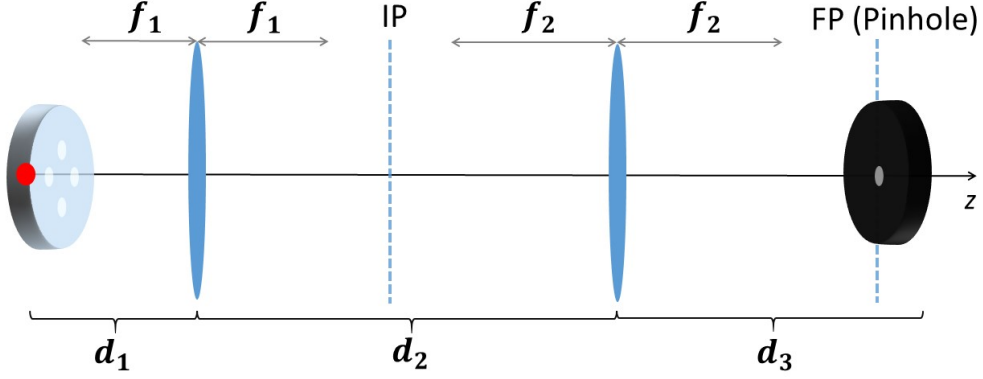


Figure 2.4: A pinhole is added in the FP and a DM in the Image Plane of the MCF due to the first lens. Source: Own elaboration.

In order to characterize the DS, we consider the situation of Fig.2.4, where a pinhole is added in the center of the Fourier Plane of the DS, and a Deformable Mirror (DM) is added in the image plane of the MCF due to the first lens. The DM-Pinhole system does a projective measurement over the photon arriving from the MCF. Lets consider the path photon basis  $\{|1\rangle, |2\rangle, |3\rangle, |4\rangle\}$ , where each basis state corresponds to a photon coming out from a particular core. We can write another basis in terms of the previous one.

$$\begin{aligned}
 |\phi_1\rangle &= |1\rangle + |2\rangle + |3\rangle + |4\rangle, \\
 |\phi_2\rangle &= |1\rangle + e^{-i\pi}|2\rangle + |3\rangle + e^{-i\pi}|4\rangle, \\
 |\phi_3\rangle &= |1\rangle + |2\rangle + e^{-i\pi}|3\rangle + e^{-i\pi}|4\rangle, \\
 |\phi_4\rangle &= |1\rangle + e^{-i\pi}|2\rangle + e^{-i\pi}|3\rangle + |4\rangle.
 \end{aligned}
 \tag{2.18}$$

$$\tag{2.19}$$

The DM mirror puts the relative phases between the nucleus states. Fig.2.5 shows the intensity in the FP according to Eq.2.17 for each state with the parameters specified in caption. The pinhole light is coupled to the detector. It is important to know how much light the pinhole is blocking for constructive interference, and how much is passing for destructive interference. This has a direct impact on the QBER achievable by the system. Depending on the experiment, one has to find the best QBER-Loss compromise. Table 2.1 shows the QBER-Loss compromise for various pinhole diameters, where we simulated the pinhole as a circle function multiplied element to element with the matrix corresponding to Eq.2.17, and where we used a wavelength  $\lambda = 1550\text{nm}$ ,  $W_0 = 8\mu\text{m}$  (core field diameter),  $f_1 = 18\text{mm}$ ,

PH diameter ( $\mu m$ )	Loss (dB)	QBER (%)
25	-19.19	2.3
50	-13.57	8.8
75	-10.58	18.8
100	-8.82	30.7

Table 2.1: For lower loss, we have worse QBER because of the leaking of destructive modes into the pinhole. Source: Own elaboration.

$f_2 = 77.2mm$ ,  $d_1 = 19.75mm$ , and  $d_2 = 430mm$ . For this configuration, the distance from the second lens to the Fourier Plane is  $d_3 = 95mm$ .

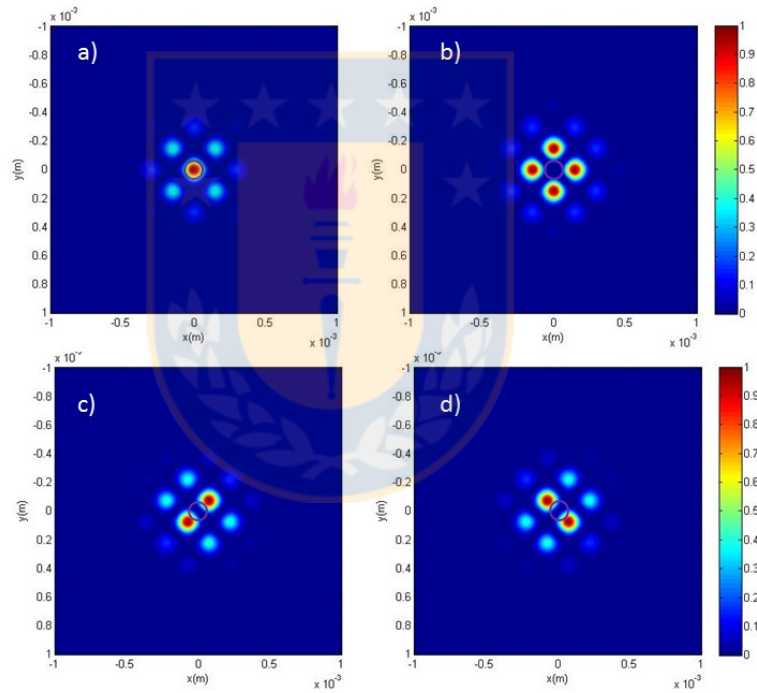


Figure 2.5: Intensity profile for a particular base states. Source: Own elaboration.

## 2.4 Results

In this section a complete description of the experimental setup is shown, including details of the electronics and experimental parameters. The main experimental results about the QKD session using the Decoy-States method are shown, as well as secondary results regarding the phase drifts in the fiber and the control system implemented to compensate the drifts in real time.

### 2.4.1 Single-photon source

In our work we employ a heavily attenuated telecom distributed feedback laser, whose emission wavelength is 1546.32 nm, as our source of weak coherent states [Fig. 2.2(a)]. The laser operates in continuous wave (CW) mode and is externally modulated by a Mach-Zehnder electro-optical modulator (MZ), generating 500 ps wide optical pulses. A calibrated optical attenuator (ATT) is used to set the desired average photon number per pulse,  $\mu$ , at Alice's output. Distinct QKD sessions have been implemented in our work, but the highest average photon number per pulsed adopted was  $\mu = 0.27$ . In this case, the probability of having non-null pulses, i.e., of having pulses containing at least one photon is  $P(\mu = 0.27 | n \geq 1) = 23.7\%$ . Pulses containing only one photon are the vast majority of the non-null pulses generated ( $\sim 90\%$ ). The repetition frequency for the optical pulses is limited to 1 kHz due to restrictions on the preparation (measurement) of Alice (Bob) quantum states, as explained below. Last, note that since the period between consecutive pulses (1 ms) is much longer than the coherence time of the laser ( $\sim 0.1\mu\text{s}$ ), there is no need to employ active phase randomization of the pulses, avoiding potential security loopholes [48].

### 2.4.2 Alice state generation

The probabilistically generated single photons are then used at Alice's site to encode the required high-dimensional quantum states for the QKD session. For this purpose the attenuated pulses are initially coupled into a 10 m long Fibercore multicore fiber (MCF1), composed of four single-mode cores, by means of a  $10\times$  objective lens (L1) [See Fig. 2.2(a)-(b)]. The core mode field diameter is  $8.5\mu\text{m}$  and the cores are separated by a distance  $d = 36.25\mu\text{m}$  to ensure that cross-talk effects are negligible. The input face of the fiber is positioned slightly out of the lens focal plane such that all cores of the fiber are equally illuminated. Thus, the probability amplitudes for the photon transmission by each core are equally weighted. Contrary to standard fiber arrays, the cores of multicore fibers lie within the same cladding, ensuring that random phase-fluctuations induced by thermal and mechanical stress are strongly suppressed. Therefore, the state of the single photons transmitted over the MCF1 can be written as a coherent superposition given by  $|\Psi\rangle = \frac{1}{2}\sum_1^4 e^{i\phi_l}|l\rangle$ , where  $|l\rangle$  denotes the state of the photon transmitted by the  $l$ th transverse core mode, and  $\phi_l$  is the relative phase acquired during the propagation over the  $l$ th core. This is the fiducial state which is then used to prepare the required states for the 4-dimensional BB84 QKD session.

The 4-dimensional BB84 QKD session requires that Alice and Bob prepare eight states spanning two MUBs. These states will be denoted by  $|\varphi_i^{(j)}\rangle$ , where  $i = 1, 2, 3, 4$  refers to the  $i$ th state of the  $j$ th MUB, with  $j = 1, 2$ . The states of the first MUB are defined by:  $\langle\varphi_1^{(1)}| = \frac{1}{2}[1, 1, 1, 1]$ ,  $\langle\varphi_2^{(1)}| = \frac{1}{2}[1, -1, 1, -1]$ ,  $\langle\varphi_3^{(1)}| = \frac{1}{2}[1, 1, -1, -1]$  and  $\langle\varphi_4^{(1)}| = \frac{1}{2}[1, -1, -1, 1]$ . The second MUB states are:  $\langle\varphi_1^{(2)}| = \frac{1}{2}[1, 1, 1, -1]$ ,  $\langle\varphi_2^{(2)}| = \frac{1}{2}[1, 1, -1, 1]$ ,  $\langle\varphi_3^{(2)}| = \frac{1}{2}[1, -1, 1, 1]$  and  $\langle\varphi_4^{(2)}| = \frac{1}{2}[-1, 1, 1, 1]$ . The states are expressed in the basis of the four fiber core modes indicated in Fig. 2.2(b). Alice state preparation is done by imaging the output face of the MCF1 onto a deformable mirror (DM1) by means of a second  $10\times$  objective lens (L2). The  $10\times$  magnification factor is intentionally chosen such that the image of each core is formed at different mirrors belonging to the DM1, as shown schematically in Fig. 2.2(c). Each mirror

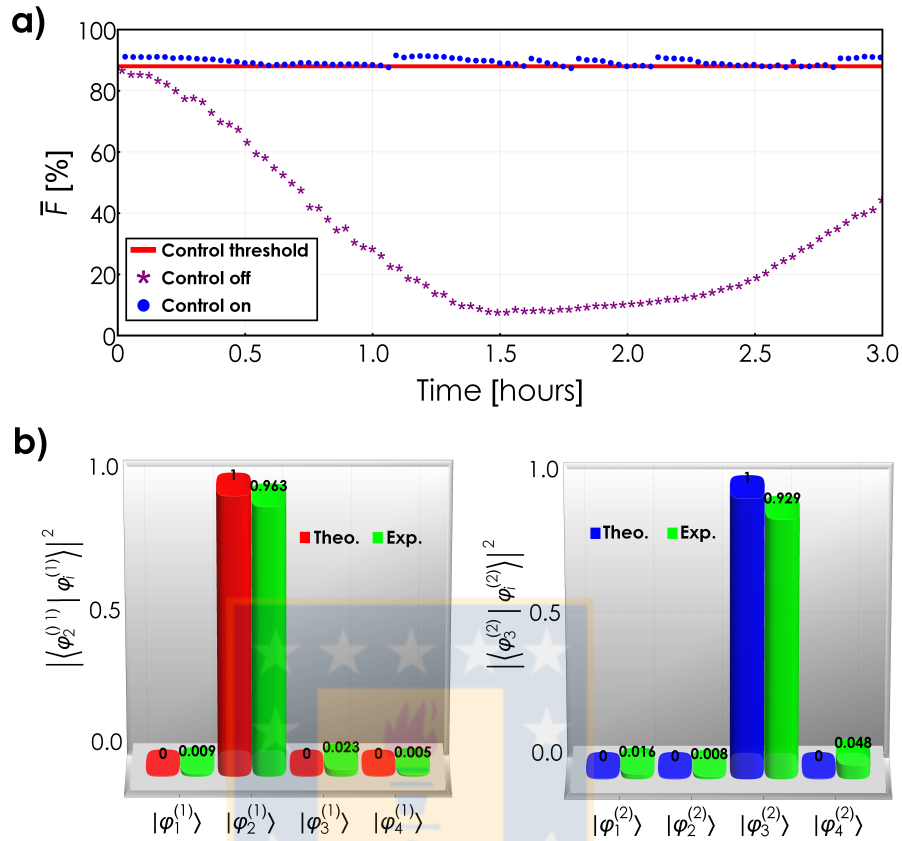


Figure 2.6: **Mean QKD state fidelity.** a) We show the mean QKD state fidelity, averaged over all the eight 4-dimensional BB84 states transmitted through the 0.3 km long multicore fiber. In the case with the control off, the fidelity slowly degrades as a function of time due to the misalignment of Alice and Bob's shared referential frame. With the control turned on, the fidelity is always above the chosen threshold, thus enabling stable QKD sessions. b) Two examples of measured fidelities after 1.08 hours, for the states  $|\varphi_2^{(1)}\rangle$  and  $|\varphi_3^{(2)}\rangle$ . Theoretical and experimentally measured fidelities are shown. Source: own elaboration

longitudinal position can be set individually. By defining different offset positions for the four mirrors, the residual phases  $\phi_l$  are compensated and the first state  $|\varphi_1^{(1)}\rangle$  prepared. The other QKD states are generated by calibrating in respect to the other longitudinal position of each mirror that corresponds to a relative phase-shift  $\varphi_l = \pi$ , also schematically shown in Fig. 2.2(c).

The single photons are then coupled back to a similar but 0.3 km long multicore fiber (MCF2) [resorting to a third  $10\times$  objective lens (L3)], comprising the transmission channel to Bob's station. Finally it is important to note that during Alice's preparation stage, polarizing optics are used to ensure that there is no coupling/entanglement between the polarization and the modes available for the photon transmission [See Fig. 2.2(a)]. Thus, ensuring that there is no state information from Alice's available in the polarization degree of freedom of the photons sent to Bob, which could be exploited by an eavesdropper.

### 2.4.3 Bob state detection

After the photon is transmitted through the MCF2 fiber it is detected at Bob's station for state analysis. Bob's detection scheme is similar to the one used by Alice. The output face of the MCF2 is magnified at a second deformable mirror (DM2) with a  $10\times$  objective lens (L4), and the relative-phase of each core is addressed individually by four independent mirrors. To define a common shared referential frame between the communicating parties, like in fiber-based polarization QKD schemes, Bob first defines the offset positions of the four mirrors for the post-selection of the state  $|\varphi_1^{(1)}\rangle$ , when Alice is also sending such state. Thus, compensating residual phase-shifts  $\phi'_l$  acquired over the MCF2 propagation. By placing a "pointlike" single-photon detector at the DM2's far-field (FF) plane, and properly adjusting the mirrors longitudinal positions to set phase-shifts equal to  $\pi$ , Bob can post-select for detection any state  $|\varphi_i^{(j)}\rangle$  required for the 4-dimensional BB84 QKD session. In our case the "pointlike" single-photon detector is composed of a pinhole (PH) fixed at the center of the FF plane of a lens L5 ( $f_{L5} = 7.5$  cm), a single-mode fiber, and an InGaAs avalanche single-photon detector (SPD) [See Fig. 2.2(a)]. The probability that a photon is detected at the center of the FF plane,  $C_s$ , is proportional to the overlap between the generated and the post-selected states [See details at [9, 49]]. At Fig. 2.2(d) we show three examples of the FF distribution, which arise from the phase modulations used by Alice and Bob to prepare and measure the states indicated below each figure. The red circle indicates the area of the employed pinhole. One can see that  $C_s \propto |\langle \varphi_i^{(j)} | \varphi_{i'}^{(j')} \rangle_{Bob}|^2$ , also with  $i' = 1, 2, 3, 4$  and  $j' = 1, 2$ . Note that the pinhole diameter defines the overall quality of Bob's measurement, which in turn defines the losses and the lowest achievable QBER as we show in Table 2.1. In our case we adopted the second configuration since lower error rates are preferable over losses for secret key bit generation rate. Last, the use of one single-photon detector configuration for the 4-dimensional QKD is discussed on the Methods section.

### 2.4.4 Fiber propagation, mean QKD state fidelity, referential frame control system

The fact that the cores of multicore fibers lie within the same cladding make them intrinsically robust against random-phase fluctuations, as thermal and mechanical perturbations act globally over the core modes. Nonetheless for long multicore fibers, like the MCF2 used as our transmission channel, slowly time varying phase-drifts can still be observed. This effect deteriorates the referential frame shared by Alice and Bob, resulting in a mean QKD state fidelity ( $\bar{F} \equiv 1 - QBER$ ) that decreases over time as the error rate increases. The typical behavior observed for  $\bar{F}$  is shown with the purple star-dotted curve into Fig. 2.6(a). This renders HD-QKD over long/installed multicore fibers not practical if not properly addressed. To overcome this problem we developed a custom control system. It checks the referential frame of Alice and Bob stations over given time intervals of 30 s and the control routine is initialized if the QBER surpasses a defined threshold value. During the control procedure the QKD session, which will be explained next, is interrupted. The control system is composed of a laser that is multiplexed into the multicore fibers, together with the attenuated pulses, and two field programmable gate arrays (FPGA1 and FPGA2) electronic modules that are used to actively control both deformable mirrors of the setup [See Fig. 2.2(a)]. Based on a

custom designed closed-loop maximum-power-point-tracking algorithm, the control system varies the offset positions of all the active mirrors used on the QKD session until the recorded QBER is back to a value below our defined threshold of 12%. Then, it is turned off and the QKD session restarts. Note that the control laser operates only during the referential frame control session, otherwise the security of our QKD session would be compromised. The resulting effect of the control system is shown into Fig. 2.6(a) with a blue dotted curve. One can see that it allows the stabilisation of the shared referential frame, critical for long-term QKD sessions. In Fig. 2.6(b) we show the fidelity measurement for the states  $|\varphi_2^{(1)}\rangle$  and  $|\varphi_3^{(2)}\rangle$  at 1.08 hours of test. The mean QKD state fidelity is  $\bar{F}_{1.08} = (92.05 \pm 0.03)\%$  and the corresponding fidelity for each state is  $(96.31 \pm 0.03)\%$  and  $(92.93 \pm 0.03)\%$ , respectively.

### 2.4.5 Which-path information erasure

Before the QKD session is implemented, it is also important to consider that polarization drifts may occur over long multicore fibers. That is, different core modes can be associated to different polarization modes at the end of light propagation over the fiber. This would be a consequence of asymmetries of the transverse shape of the core modes arising from imperfections during the fabrication process, which may generate polarization mode dispersion with different intensities for each core. In this case, the polarization degree of freedom will partially mark the single-photon propagation path over the fiber, which in turn compromises the state coherence if the polarization is not also properly addressed by Bob. Fortunately, this effect can be fully compensated with the use of polarisation filters. In our case, the polarization-based distinguishability of the core modes was almost constant over time as our multicore fiber was protected inside the laboratory. Then, we used quarter-waveplates (QWP), half-waveplates (HWP) and polarizing beamsplitters (PBS) to erase the which-path information [See Fig. 2.2(a)]. The overall loss at the eraser stage was of only 1.2 dB. Note, however, that for installed multicore fibers active polarisation controls based on liquid crystals displays can be used.

### 2.4.6 Automated QKD session

The 4-dimensional BB84 QKD session is also implemented by the two field programmable gate array electronic units. FPGA1, belonging to Alice, generates a 1 kHz synchronisation signal which is shared with Bob's FPGA2. After each sync pulse, FPGA1 reads a random number generated by a idQuantique Quantis quantum random number generator (QRNG), number that will determine the state that will be created at DM1. After DM1 is set for generating a particular state, the attenuated optical pulse is generated by the MZ modulator, and the state is codified into the probabilistic generated photon, which is sent to Bob through the 250 mt MCF. Simultaneous to Alice's state choice, Bob reads it's own QRNG to choose a state to project the incoming photon, and sets the DM2 according to this choice. A delayed version of the synchronisation pulse is fed in the gated-mode SPD, with the gate width adjusted to 0.85 ns. FPGA2 then checks whether there was a detection in the SPD for that particular sync pulse. Both FPGAs record in each measurement round, the chosen MUB and the corresponding state and whether a single-photon was detected. The FPGAs compare the detected strings after basis reconciliation to calculate the QBER.

## 2.5 QKD results

The secret key generation rate ( $R$ ) as a function of the dimension  $d$  is given by (see section 1.3)

$$R \geq Q_0 \log_2 d + Q_1 [\log_2 d - H_d(e_1)] - Q_\mu H_d(E_\mu) f(E_\mu), \quad (2.20)$$

where  $Q_0$  and  $Q_1$  are the gains of the vacuum and single photon states, respectively.  $Q_\mu$  is the experimentally measured gain for an average  $\mu$  photon number.  $H_d(x) = -x \log_2 [x/(d-1)] - (1-x) \log_2 (1-x)$  is the  $d$ -dimension modified Shannon entropy of the QBER, which considers that the error can randomly occur in any of the  $d-1$  detectors [12].  $e_1$  is the single-photon error rate,  $E_\mu$  is the measured overall quantum bit error rate (QBER), and  $f(E_\mu)$  is the inefficiency of the error correction function. We have employed  $f(E_\mu) = 1.05$  [50] since reported error rates in typical HD-QKD experiments, including ours, hover around 10% [9, 11]. The secret key probability considers the use of the efficient BB84 protocol [29], while an additional factor  $1/d$  is required if all bases were employed with equal probability.

We first performed a long term automated measurement to demonstrate the stability achieved in our experiment by performing a BB84 QKD session over the 0.3 km of multicore fiber, while employing an average photon number per pulse  $\mu = 0.27$ . The results are shown in Fig. 2.7(a), where we have an average of 44.5 detections per hour, with an average QBER of 10.25%. The results clearly show that the control system is able to minimize phase drifts during the run, while keeping a QBER considerably lower than the security thresholds. The thresholds are 18.93% and 25% for collective and individual attacks, respectively [6].

Based on this measured mean 10.25% QBER over the entire session, and with ( $\eta_{SPD} = 6.09\%$  and  $\eta_{Bob} = 24.5$  dB,  $\alpha = 0.4$  transmission coefficient for our Fibercore multicore fiber and an estimated optical misalignment of  $e_{opt} = (9.64 \pm 0.98)\%$ , we estimated the key rate as a function of distance by optimizing over  $\mu$  and assuming the infinite decoy case (see section 1.3). The result is represented by the red curve in Fig. 2.7(b), which gives an upper bound for the key generation rate in our system.

We also calculated the rate as a function of the fiber length by using the well known, and practical, vacuum + weak decoy protocol [30]. It consists of two weak decoy states (of which one is the vacuum) and a stronger signal state. Based on our experimental setup characteristics, we fix the weak decoy mean photon number per pulse to  $\nu = 0.1$  (a compromise between optimizing the key rate and the estimation of  $e_1$  and  $Q_1$ ) and optimize the mean photon number  $\mu$  of the signal state to obtain the secret key rate. The result is given by the blue curve in Fig. 2.7(b). This clearly shows we can generate positive secret key rates up to 25 km of multicore fiber when using a realistic decoy protocol with standard components and single-photon detectors. To demonstrate it, we performed the key exchange section while employing the value of  $\mu = 0.2$  for the signal at the distance of 0.3 km, and the decoy states ( $\nu = 0.1$  and vacuum). We finally obtain a secret key generation rate per pulse of  $(4.31 \pm 1.19) \times 10^{-6}$ , plotted as the black dot in Fig. 2.7(b). Table 2.2 displays the measured parameters that are used to calculate the key rate at the distance of 0.3 km. (see section 1.3 for details). Our calculation returns a lower bound for the single-



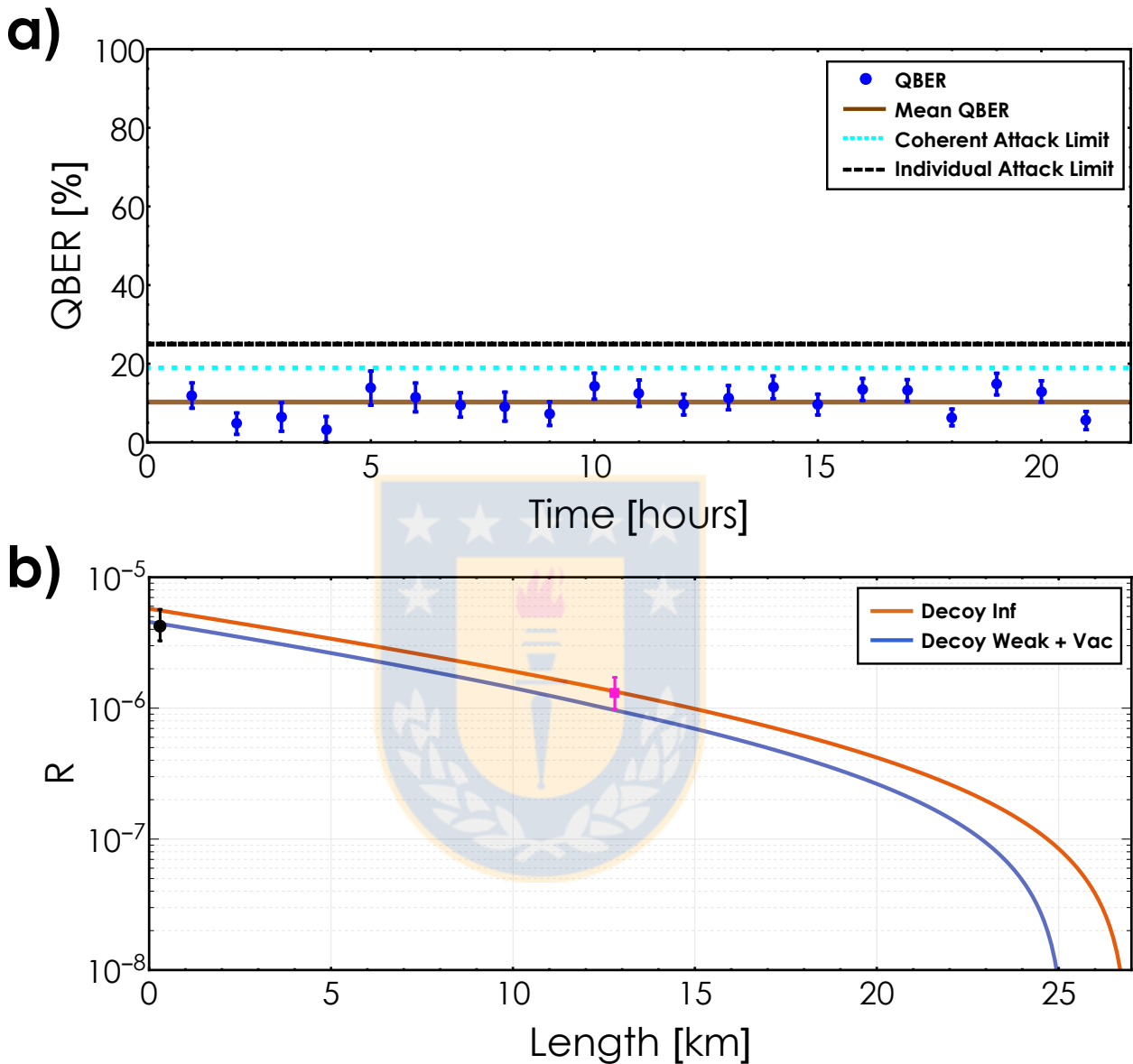


Figure 2.7: **Experimental QKD results.** a) Quantum bit error rate (QBER), as a function of time, with each data point indicating the average over the past hour. The brown line shows the average measured QBER of 10.25% in a HD-QKD session with  $\mu = 0.27$ . The dashed black and cyan lines denote the theoretical upper bounds to achieve positive key rate for  $d = 4$ , while considering individual (25%) and coherent (18.93%) attacks, respectively. b) Secret key generation rate (R) as a function of distance, while considering the upper bound case of infinite decoys (red curve) and the practical weak decoy + vacuum protocol (blue curve). The two data points correspond to the actual key generation rate for the QKD experimental runs performed (see text for details), for the weak decoy + vacuum (black circle) and infinite decoy (magenta square) cases. Error bars correspond to propagated errors arising from the Poissonian detection statistics. Source: Own elaboration

Signal ( $\mu$ )	Weak ( $\nu$ )	Vacuum
$Q_\mu = (9.31 \pm 0.63) \times 10^{-6}$	$Q_\nu = (4.89 \pm 0.30) \times 10^{-6}$	$Y_0 = (2.06 \pm 0.23) \times 10^{-7}$
$E_\mu = (10.8 \pm 1.4)\%$	$E_\nu = (9.0 \pm 1.3)\%$	$E_0 = (71.1 \pm 3.4)\%$

Table 2.2: **Measured parameters for the weak decoy + vacuum protocol.** Experimental results used to obtain the secret key generation rate at a distance of 0.3 km, when using the weak decoy + vacuum protocol. Source: Own elaboration

photon gain  $Q_1^L = (6.96 \pm 1.30) \times 10^{-6}$  and an upper bound of the single-photon error rate  $e_1^U = (7.53 \pm 2.20)\%$ .

Lastly we performed a new HD-QKD run with an extra 5 dB optical attenuator placed before the detector to simulate a total transmission distance of 12.8 kms (as our multicore fiber is specified to have an attenuation coefficient of 0.4 dB/km), assuming an infinite number of decoy states. The goal is to demonstrate an upper bound for the rate at a longer distance. This was executed over a continuous period of 45.3 hours, with an average QBER of  $9.80 \pm 1.69\%$ , with a secret key generation rate per pulse of  $(1.30 \pm 0.36) \times 10^{-6}$  (shown as the magenta square in Fig. 2.7b).



# Chapter 3

## Multicore fiber mode sorter

Another alternative for high dimensional quantum communication is based on free-space propagating OAM LG modes of light, which span a theoretically infinite discrete Hilbert space. Long distance OAM free-space classical communication have been demonstrated, suggesting the feasibility of practical quantum communications based on OAM through free-space [31]. In this chapter device to create a flexible hybrid high-dimensional network is presented, which can be used to interconnect multicore fiber based ground stations to OAM based free-space optical links. In this way, Alice would be able to communicate with Bob even when there is no line-of-sight between them, and also no deployed multicore fibers connecting them. For this purpose, she would encode information into high-dimensional OAM quantum states, send them through a free-space link, and at an intermediate station (sharing a line-of-sight with Alice) connected to the multicore optical network, Alice's states would be feed-forward to Bob's station. Our device is a modified version of a previously reported OAM mode sorter, which is capable of mapping different OAM modes into distinct transverse propagation modes [27]. The proposed modification relies on an extra new transformation that maps the already separated modes into the typical core mode configuration of multicore fibers. This scheme provides high phase stability and efficient coupling.

In section 3.1 we present a review of Laguerre Gauss modes, a OAM carrying type of modes. In section 3.2 the theory behind the efficient separation of modes is presented. In section 3.3 we show the main results associated with what we call the "Multicore Fiber Mode Sorter" (MCFMS).

### 3.1 Laguerre Gauss modes and Orbital Angular Momentum of Light

In the study of gaussian beams, one solves the paraxial Helmholtz Equation for the complex envelope of a complex field

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)A - j2k\frac{\partial A}{\partial z} = 0, \quad (3.1)$$

Eq.3.1 has different sets of solutions that can be different for the coordinate system that

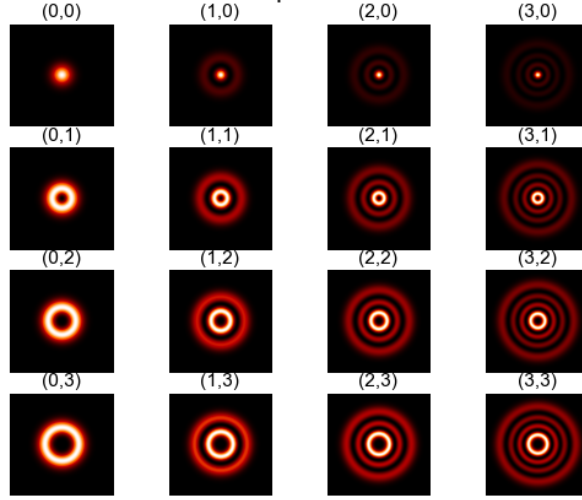


Figure 3.1: Transversal intensity for LGM with different  $l$  and  $m$ . For  $l \neq 0$ , the mode has a central singularity.  $m + 1$  corresponds to the number of rings. Source: [http://pendientedemigracion.ucm.es/info/aocg/python/optica/modulos\\_optica/modulo\\_fuentesXY/index.html](http://pendientedemigracion.ucm.es/info/aocg/python/optica/modulos_optica/modulo_fuentesXY/index.html)

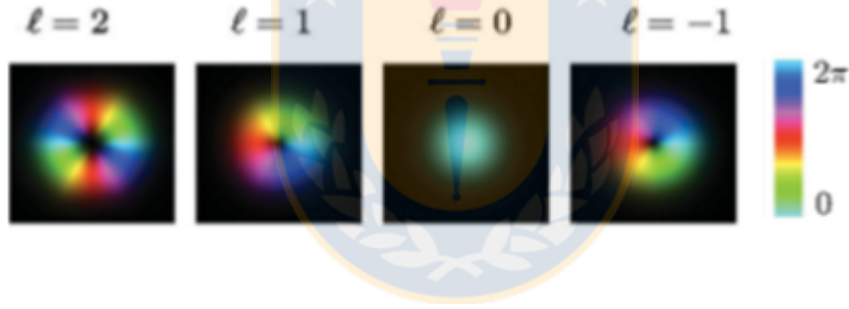


Figure 3.2: Phase gradient for different LG modes. Source: [27]

we are using. For example, in cartesian coordinates, the solutions are the Hermite Gauss modes; in elliptic coordinates, we have the Ince-Gaussian modes, and in the cylindrical coordinates  $(\rho, \phi, z)$ , the solutions are the Laguerre Gauss modes. The complex amplitude for a pure LGM is

$$\begin{aligned}
 U_{l,m} = & A_{l,m} \left[ \frac{W_0}{W(z)} \right] \left( \frac{\rho}{W(z)} \right) \mathbb{L}_m^l \left( \frac{2\rho^2}{W^2(z)} \right) \exp \left( -\frac{\rho^2}{W^2(z)} \right) \\
 & \times \exp \left[ -jkz - jk \frac{\rho^2}{2R(z)} + j(l+2m+1)\zeta(z) \right] \exp(-jkl),
 \end{aligned} \tag{3.2}$$

Where  $W_0$  is the beam waist,  $W(z) = W_0 \sqrt{1 + \left( \frac{z}{z_R} \right)^2}$  is the beam radius (with  $z_R$  corresponding to the Rayleigh range),  $\zeta(z) = \arctan\left(\frac{z}{z_R}\right)$  is the Gouy phase, and  $\mathbb{L}_m^l$  are the associated Laguerre polynomials. Fig.3.1 shows the transverse intensity profile for different  $l$

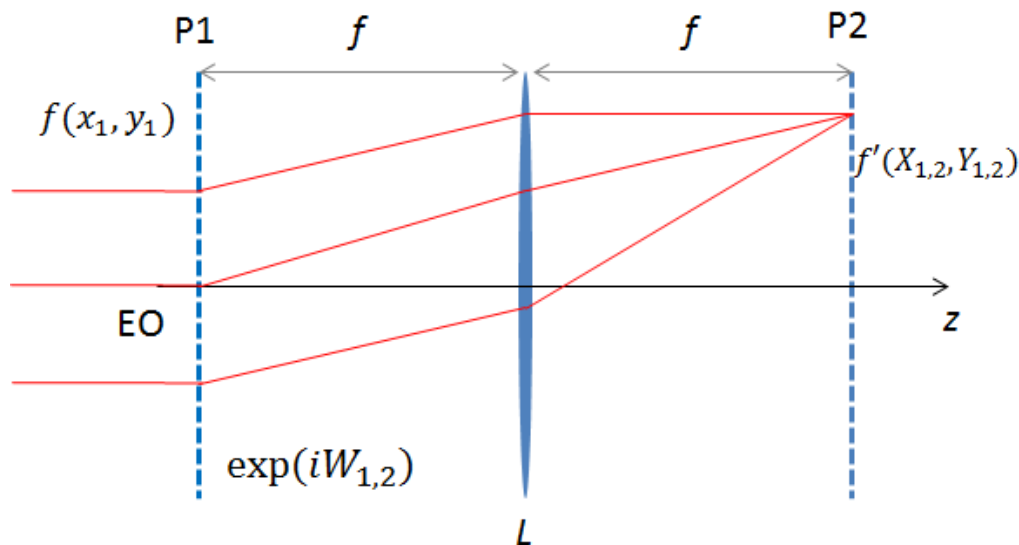


Figure 3.3: Coordinate change basic scheme. A colimated wavefront goes under a unitary transformation, and a thin lens applies a Fourier transform. Source: Own elaboration.

and  $m$ . The last exponential in Eq.3.2 corresponds to a circular phase, which depends on  $l$ . Given an  $l$ , the OAM for a single photon in a LGM is  $J = \hbar l$ . For convenience, we will refer to the  $l$  number as the OAM of the mode. Fig.3.2 shows the circular phase for different OAMs.

## 3.2 Efficient Sorting of LMG

From Fig.3.1 it can be seen that the distinction between LGM from their intensity is tricky; first of all, we can't distinguish between  $U_{l,m}$  and  $U_{-l,m}$ , because they only differ in the direction of the circular phase, and it's not much better for other cases; for  $l = 3$ , the ring radius is similar to  $l = 2$ , making it very difficult for a detection system of any kind to distinguish between them. It's necessary to have a method for clear distinction between modes for experimental realization, and this can be achieved by means of the circular phase.

### 3.2.1 Coordinate Transformations in Optics and Log-Polar Transformation

It's possible to generate coordinate transformations over wavefronts. In reference [32] it is demonstrated that for the system described in Fig.3.3, given a coordinate transformation  $x_2 = X_{1,2}(x_1, y_1), y_2 = Y_{1,2}(x_1, y_1)$  (where  $(x_1, y_1)$  are the first plane coordinates), the unitary phase transformation  $W_{1,2}(x_1, y_1)$  can be obtained resolving the following equations system.

$$\begin{aligned}\frac{\partial W_{1,2}(x_1, y_1)}{\partial x_1} &= X_{1,2}(x_1, y_1) \frac{k}{f_L} \\ \frac{\partial W_{1,2}(x_1, y_1)}{\partial y_1} &= Y_{1,2}(x_1, y_1) \frac{k}{f_L},\end{aligned}\quad (3.3)$$

For the solution to exist, it must satisfy the following condition.

$$\frac{\partial X_{1,2}(x_1, y_1)}{\partial y_1} = \frac{\partial Y_{1,2}(x_1, y_1)}{\partial x_1}. \quad (3.4)$$

Because of Eq.3.4, not every coordinate transformation is possible. For example, the Polar Transformation  $X_{1,2} = \sqrt{x_1^2 + y_1^2}$ ,  $Y_{1,2} = \arctan\left(\frac{y_1}{x_1}\right)$  does not satisfy the condition. On the other hand, the Log-Polar coordinate transformation, defined as

$$\begin{aligned}u &= X_{1,2}(x_1, y_1) = -a \log\left(\sqrt{\frac{x_1^2 + y_1^2}{b}}\right) \\ v &= Y_{1,2}(x_1, y_1) = a \arctan(y_1/x_1),\end{aligned}\quad (3.5)$$

satisfies Eq.3.4. Here,  $a = \frac{d}{2\pi}$ , where  $d$  is the length of the angular coordinate mapped on the output space, and  $b$  is an arbitrary constant. Solving Eq.3.3 for the Log-Polar transformation, one finds the phase imprint.

$$W_{1,2} = \frac{2\pi a}{\lambda f_1} \left[ y_1 \arctan\left(\frac{y_1}{x_1}\right) - x_1 \ln\left(\frac{\sqrt{x_1^2 + y_1^2}}{b} + x_1\right) \right]. \quad (3.6)$$

### 3.2.2 Afocal System

The output in an optical coordinate transformation is not collimated. For experimental flexibility, it is convenient to have a collimated output and a both-way operation. This can be achieved by considering a second unitary phase transformation in the output plane (OP)(Fig.3.4). Given a coordinate transformation  $x_1 = X_{1,2}(x_2, y_2)$ ,  $y_1 = Y_{1,2}(x_2, y_2)$  with its associated phase imprint  $W_{1,2}(x_1, y_1)$ , the second phase imprint is obtained by resolving

$$\frac{\partial W_{2,1}(u, v)}{\partial u} = X_{2,1}(u, v) \frac{k}{f_L} \quad (3.7)$$

$$\frac{\partial W_{2,1}(u, v)}{\partial v} = Y_{2,1}(u, v) \frac{k}{f_L}, \quad (3.8)$$

where  $x_1 = X_{2,1}(x_2, y_2)$ ,  $y_1 = Y_{2,1}(x_2, y_2)$  is the inverse coordinate transformation of Eq.3.3. For the Log-Polar transformation, one finds that the inverse phase imprint is given by

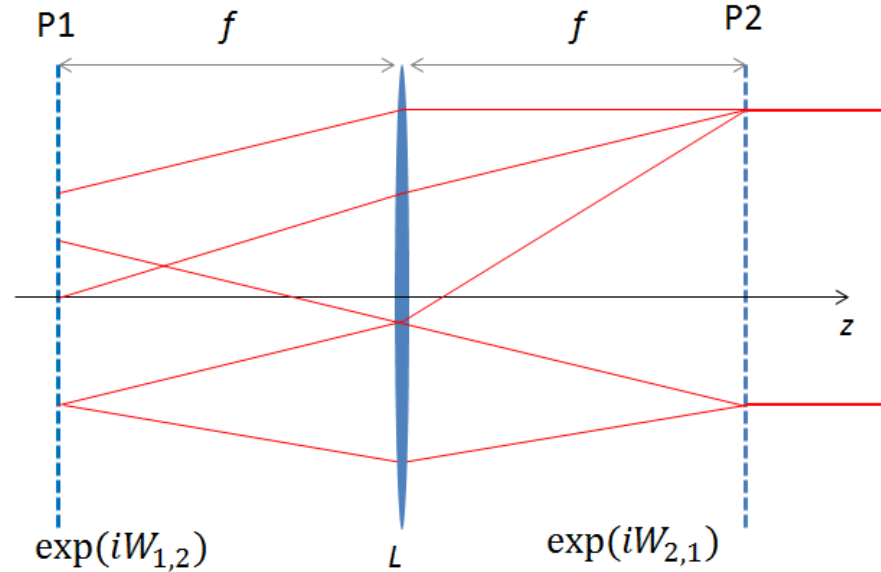


Figure 3.4: Inverse transformation scheme for collimated output. Source: Own elaboration.

$$W_{2,1} = -\frac{2\pi ab}{\lambda f_1} \exp\left(-\frac{x_2}{a}\right) \cos\left(\frac{y_2}{a}\right), \quad (3.9)$$

where  $a$  and  $b$  have the same values that in Eq.3.6

### 3.2.3 Mode Sorter

For our mode sorting system, we will use a Log-Polar transformation to map the circular phase gradient of the LGM into a lineal phase gradient, as show in Fig.3.5. The resulting wavefront is then focused by a positive lens, focusing each phase gradient in a different transversal position of the Far Field according to the formula

$$t_l = \frac{\lambda f}{d} l, \quad (3.10)$$

where  $\lambda$  is the wavelenght of the LGM,  $f$  is the focus of the positive lens, and  $l$  is the OAM of the LGM. Due to the unique transverse position assigned for every OAM, they can be distinguished just by placing a detector for every OAM in the output plane. This system, composed of the two unitary transformations and the lenses, is what we are going to call the "Mode Sorter".

## 3.3 Multicore Fiber Mode sorter

Here we present a method for coupling each OAM into a Multi-Core fiber. Based on the mode sorter shown previously, we use another coordinate transformation to couple each OAM (already transformed into a transversal position) into each fiber core. In our case,

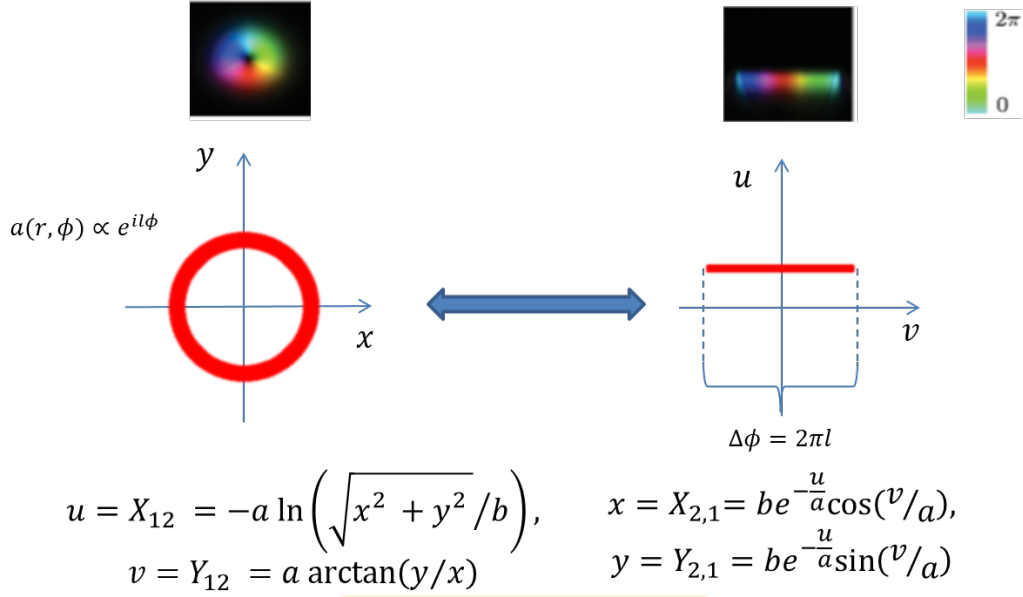


Figure 3.5: Visualization of Log Polar transformation in intensity and phase. Source: Own elaboration.

where the MCF has 4 cores, we can only couple 4 OAM into the fiber. The idea is that by means of a coordinate transformation, each transversal momentum (corresponding to a specific OAM) can be mapped in a new disposition that fits the fiber cores. For this, we propose a new coordinate transformation defined by

$$\begin{aligned} u &= w \cos(a_1 x_3) \\ v &= w \sin(a_1 x_3), \end{aligned} \quad (3.11)$$

where  $w$  is a scaling factor,  $a_1$  is the parameter that has to be adjusted depending on the coupling conditions and  $\{x_3, y_3\}$  correspond to the coordinates of the mode sorter exit plane. We will refer to Eq.3.11 as the Pseudo Polar transformation (PP). The PP maps each transversal position into the circular array of fiber cores. We can configure the transformation for coupling  $N$  OAMs into  $N$  cores disposed circularly. For Eq.3.11, the phase imprint obtained solving Eq.3.3 is

$$W_{1,2} = \frac{2\pi w}{\lambda f_3} x_3 \sin(a_1 y_3), \quad (3.12)$$

but we will use a modified phase imprint with added correction parameters.

$$\Phi_3 = \frac{2\pi w}{\lambda f_3} (s x_3 - \zeta) \sin(a_1 (y_3 - \beta)), \quad (3.13)$$



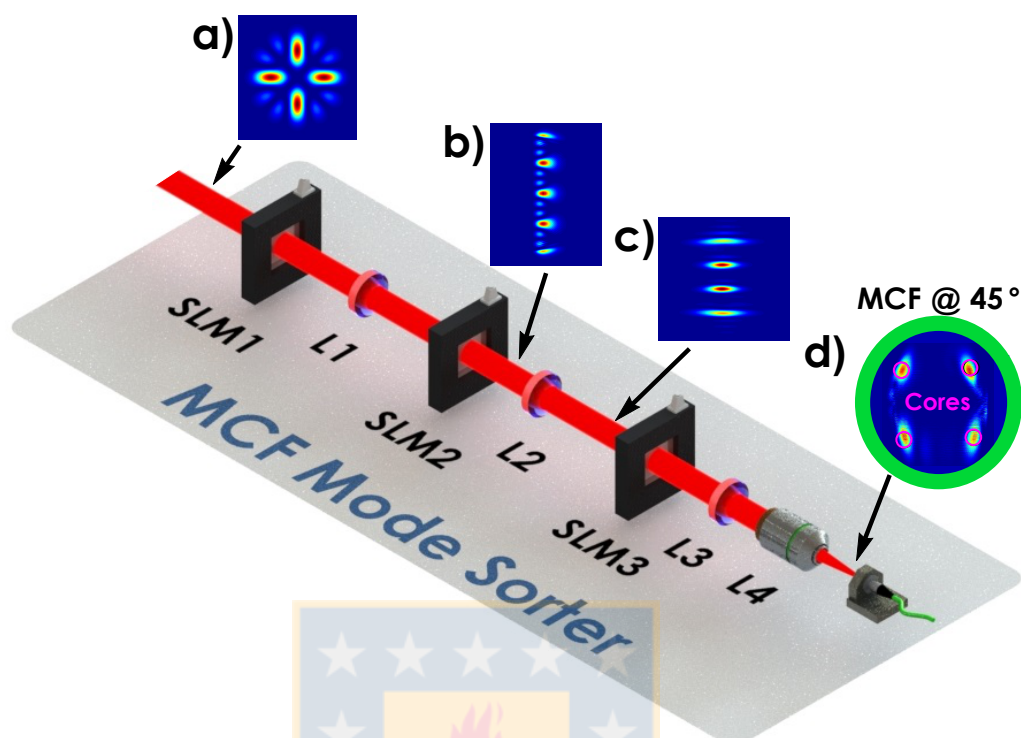


Figure 3.6: **MCF mode sorter**. Proposed scheme of a mode sorter that maps OAM Laguerre-Gauss (LG) modes to transverse propagation modes (and vice-versa) compatible with the core geometry of a multicore fiber. The device is based on the use of spatial light modulators (SLM) and lenses to implement coordinate transformations. a) Input superposition of four OAM LG modes defined by the azimuthal index  $l \in \{-6, -2, 2, 6\}$ . Then in b) and c), different transformations are applied separating the LG modes into different transverse modes (see main text for details). Finally in d), the mode sorting procedure is completed, with each OAM LG mode being coupled into a different core. An overall coupling efficiency of 40% is attainable, while cross-talk mode coupling is negligible  $< 0.15\%$ . Source: Own elaboration.

### 3.3.1 Numerical Simulation

The proposed MCF mode sorter scheme is shown in Fig. 3.6. To demonstrate its viability by numerical simulations, we consider (without loss of generalization) that an equally weighed superposition of four Laguerre-Gauss modes defined by the azimuthal index  $l \in \{-6, -2, 2, 6\}$  is sent through the MCF mode sorter [See Fig. 3.6(a)].

The first spatial light modulator (SLM1) and a thin lens (L1) are used to perform a log-polar optical coordinate transformation by using the phase modulation  $\Phi_1 = \frac{2\pi a}{\lambda f_1} [y_1 \arctan(y_1/x_1) - x_1 \ln(\sqrt{x_1^2 + y_1^2}/b + x_1)]$  at the SLM1.

The second SLM2 imprints the phase  $\Phi_2 = -\frac{2\pi ab}{\lambda f_1} \exp(-\frac{x_2}{a}) \cos(\frac{y_2}{a})$  to implement a required phase correction. The resulting transverse profile is given in Fig. 3.6(b).

The second lens (L2) performs the mode separation exploiting the different phase gradients of each OAM mode [Fig. 3.6(c)]. The last components SLM3 and L3 perform a new

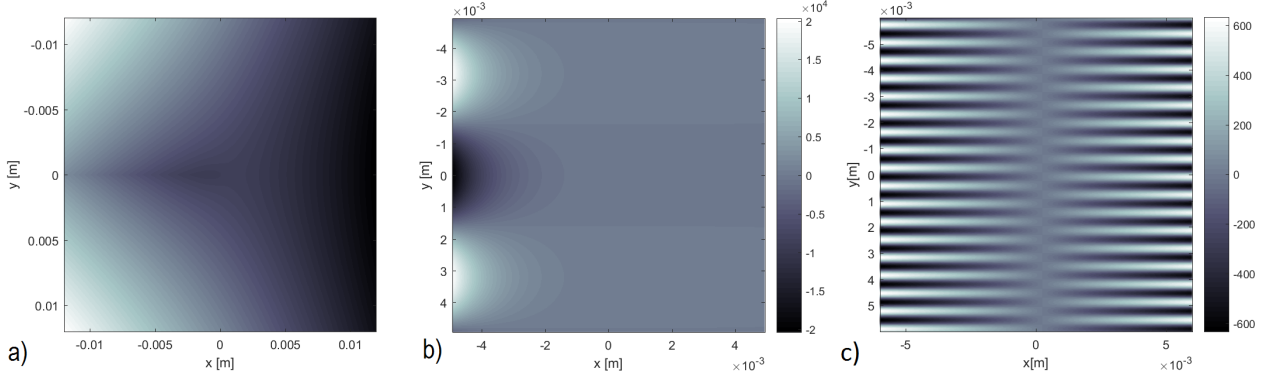


Figure 3.7: [

Phase profiles for the log-polar and pseudo-polar transformations.]Phase profiles for the log-polar and pseudo-polar transformations. Source: Own elaboration.

transformation, that maps the linearly distributed modes to a configuration typical of multicore fibers (rotated by  $45^\circ$ ). The phase necessary for this new transformation is  $\Phi_3 = \frac{2\pi w}{\lambda f_3}(sx_3 - \zeta) \sin(a_1(y_3 - \beta))$ , where we have added correction parameters  $s$ ,  $\zeta$  and  $\beta$  for fine grain adjustment [32]. In our numerical simulation we used focal lengths  $f_1 = 180$  mm,  $f_2 = 180$  mm and  $f_3 = 12$  mm, the wavelength  $\lambda = 1550$  nm, and a beam waist  $w_0 = 3200$   $\mu\text{m}$ . The other parameters are:  $a = 0.001$ ,  $b = 0.007$ ,  $c = 1.2$  m,  $s = 0.8$ ,  $\zeta = 300$  nm.  $a_1 = \gamma\pi d / [(l_4 + l_3)\lambda f_2]$  is the condition for fiber core matching, with the parameters  $\gamma = 0.975$ ,  $d = 2w_0$ ,  $\beta = b_1\lambda l_3/d$ ,  $b_1 = 1.5$  m, where  $l_4$ ,  $l_3$  are the highest and the second azimuthal indexes  $l$ . Note that this transformation can be applied to other OAM mode superpositions.

After being transmitted by a final  $20\times$  objective (L4), the light is coupled into the multicore fiber as it is shown in Fig. 3.6(d). To couple the light into the fiber we additionally have to rescale the image. We have made it 20 times smaller and additionally rescaled in  $y$  direction with ratio 0.32. The average coupling efficiency is 40%, and cross-talk effects are negligible  $< 0.15\%$ . That is, each OAM mode couples efficiently to a different core of the multicore fiber and the introduced error rate is negligible.

Figure 3.7 shows the phase profiles corresponding to each unitary transformation.

### Alternative Transformation

The former transformation has the disadvantage that the mapping has to be rescaled in the  $y$  direction. In physical terms, this implies using a pair of cylindrical lenses, adding more components and raising the complexity of the setup. There is an alternative transformation that we refer at the *multifacet* transformation, which consists in dividing the input plane into small facet, each of one is mapped onto arbitrary facets in the output plane, by means of phase ramps [52]. For our scheme, with the coordinate transformation setup proposed, each facet unitary phase transformation at the input plane is defined by

$$\phi_3 = \frac{2\pi a}{\lambda f_3} \left( \frac{x_3^2 + y_3^2}{2} + c_x x_3 + c_y y_3 \right) \quad (3.14)$$

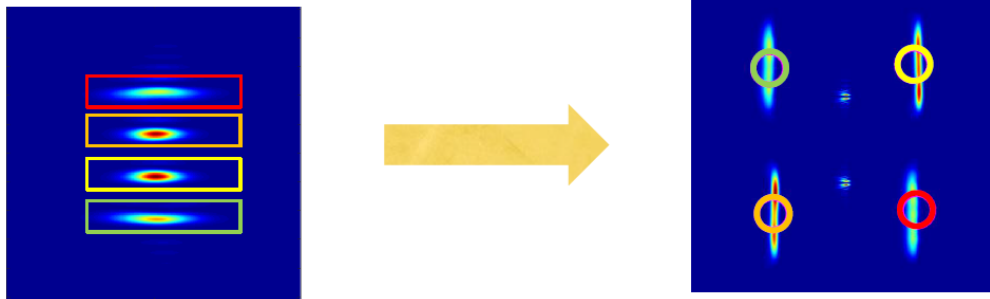


Figure 3.8: Multifacet transformation applied to the multicore fiber mode sorter. Each color represents the correspondence between the transverse modes and the fiber cores. Source: Own elaboration.

Where  $c_x$  and  $c_y$  corresponds to the arbitrary parameters for facets mapping. With this approach we achieve a coupling efficiency of 35% without the need of re scaling spaces, thus, simplifying the coupling system when comparing with the former transformation.



# Conclusions

Quantum key distribution has been the most successful protocol of quantum communication, with many different demonstrations performed across several distinct scenarios. The interest on QKD is only expected to grow more given the recent developments aiming at the construction of a quantum computer and the demonstration of metropolitan QKD networks [3]. Inline with standard communication systems some experiments have focused on increasing the transmission rate, which is arguably a major Achilles heel of QKD.

Considerable effort is being made to increase QC's information content by using the transverse spatial profile of a single-photon [7, 8, 9, 10, 11]. However, no approach so far has been proven to be fully compatible with a secure QKD session over the infrastructure already developed for classical telecommunications. In this work we show, for the first time, that stable and secure high-dimensional quantum communication is feasible over long-distance optical fibers. In our work 4-dimensional quantum states are encoded onto the linear-transverse momentum of single-photons and successfully transmitted over 0.3 km of a telecommunication multicore fiber. We demonstrated a fully automated and secure HD-QKD session by resorting to the decoy-state method. Our results set the stage for future implementations of high-dimensional quantum communication over the telecommunication infrastructure, constituting an important block of tomorrow's quantum internet. Our technique is also compatible with high-speed QKD links over long distances since, on the one hand, spatial light modulators with MHz repetition frequencies have been recently developed [33], while on the other hand the use of highly efficient superconducting detectors will greatly increase the maximum achievable distance [34]. Finally, it is shown that our work paves the way towards a high-dimensional quantum network composed of interconnected free-space and optical fiber links.

# Conclusiones

La distribución cuántica de clave ha sido el protocolo de comunicación cuántica más exitoso, con muchas demostraciones diferentes en escenarios distintos. Se espera que el interés en QKD crezca dados los desarrollos recientes que apuntan a la construcción de un computador cuántico y la demostración de redes metropolitanas de QKD [3]. En la misma línea de los sistemas de comunicación estándar algunos experimentos han sido enfocados en incrementar la tasa de transmisión, la cual es el mayor talón de Aquiles de la distribución de clave cuántica

Esfuerzo considerable está siendo hecho en incrementar el contenido de información en QC usando el perfil espacial transversal de fotones individuales [7, 8, 9, 10, 11]. Sin embargo, ningún acercamiento hasta ahora ha probado ser totalmente compatible con una sesión segura de QKD sobre la infraestructura ya desarrollada para telecomunicaciones clásicas. En este trabajo demostramos por primera vez, que una comunicación cuántica de alta dimensionalidad, segura y estable, es lograble a través de fibras ópticas en largas distancias. En nuestro trabajo, estados 4-dimensionales son codificados sobre el momento transversal lineal de fotones individuales y son transmitidos exitosamente a través de 0.3 km de fibra óptica multinúcleo. Hemos demostrado una sesión de HD-QKD totalmente automática y segura basada en estados señuelo. Nuestro resultado senta un precedente para futuras implementaciones de comunicaciones cuánticas de altas dimensiones sobre infraestructuras de telecomunicación, constituyendo un bloque importante para la internet cuántica del mañana. Nuestra técnica es también compatible con conexiones QKD de alta velocidad en largas distancias dado que, por un lado, moduladores espaciales con frecuencias de repetición de Mhz han sido recientemente desarrollados [33], mientras que por otro lado, el uso de detectores superconductores de alta eficiencia incrementarán en gran medida la máxima distancia alcanzable [34]. Finalmente, es mostrado que nuestro trabajo pavimentará las vías hacia una red cuántica de altas dimensiones compuesta de conexiones de espacio libre y fibra óptica.

# Bibliography

- [1] Bernstein, D., J., Buchmann, J. & Dahmen, E. (Editors). Post-quantum cryptography. Springer (Berlin) 2009.
- [2] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
- [3] Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon* **8**, 595 (2014).
- [4] Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *arXiv:1606.05853* (2016).
- [5] Richardson, D. J., Fini, J. M. & Nelson, L. E. Space-division multiplexing in optical fibres. *Nat. Photon.* **7** 354 (2013).
- [6] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using  $d$ -level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
- [7] Walborn, S. P., Lemelle, D. S., Almeida, M. P. & Souto Ribeiro, P. H. Quantum key distribution with higher-order alphabets using spatially encoded qudits. *Phys. Rev. Lett.* **96**, 090501 (2006).
- [8] Ali-Kahn, I., Broadbent, C. J. & Howell, J. C. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.* **98**, 060503 (2007).
- [9] Etcheverry, S. & et al. Quantum key distribution session with 16-dimensional photonic states *Sci. Rep.* **3**, 2316 (2013).
- [10] Mafu, M. & et al. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).
- [11] Mirhosseini, M. et al. High-dimensional quantum cryptography with twisted light. *New. J. Phys.* **17**, 033033 (2015).
- [12] Sheridan, L. & Scarani V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 030301 (2010).
- [13] Bunandar, D., Zhang, Z., Shapiro, J. H. & Englund, D. R. Practical high-dimensional quantum key distribution with decoy states. *Phys. Rev. A*, 022336 (2015).

- [14] Bao, H., Bao, W., Wang, Y., Chun, Z. & Chen, R. Practical high-dimensional quantum key distribution with decoy states. *J. Phys. A: Math. Theor.* **49** 205301 (2016).
- [15] Bao, H. & et al. Detector-decoy high-dimensional quantum key distribution. *Opt. Express* **24**, 22159 (2016).
- [16] Niu, M. Y., Xu, F., Furrer, F. & Shapiro, J. H. Finite-key analysis for time-energy high-dimensional quantum key distribution. *arXiv:1606.08394* (2016).
- [17] Brádler, K., Mirhosseini, M., Fickler, R., Broadbent, A. & Boyd, R. W. Finite-key security analysis for multilevel quantum key distribution. *New J. Phys.* **18**, 073030 (2016).
- [18] Leach, J., Padgett, M. J., Barnett, S. M., Franke Arnold, S. & Courtial, J. *Phys. Rev. Lett.* **88**, 257901 (2002).
- [19] Neves, L. et al. Generation of Entangled States of Qudits using Twin Photons. *Phys. Rev. Lett.* **94**, 100501 (2005).
- [20] Rodenburg, B. & et al. Influence of atmospheric turbulence on states of light carrying orbital angular momentum. *Opt. Lett.* **37**, 3735 (2012).
- [21] Ciampini, M. A. & et al. Path-polarization hyperentangled and cluster states of photons on a chip. *Light: Science & Applications* **5** e16064 (2016).
- [22] M. A. Nielsen & I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).
- [23] Wikipedia, One-time pad. In *Wikipedia, The Free Encyclopedia*, 2016. [https://en.wikipedia.org/wiki/One-time\\_pad](https://en.wikipedia.org/wiki/One-time_pad)
- [24] Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings Of The IEEE International Conference On Computers, Systems And Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
- [25] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
- [26] Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
- [27] Berkhout, G. C. G., Lavery, M. P. J., Courtial, J., Beijersbergen M. W. & Padgett, M. P. Efficient Sorting of Orbital Angular Momentum States of Light. *Phys. Rev. Lett.* **105**, 153601 (2010).
- [28] Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
- [29] Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and proof of its unconditional security. *J. Cryptol.* **18**, 133 (2005).
- [30] Ma, X., Qi, B., Zhao Y. & Lo H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).

- [31] Krenn, M., Fickler, R., Fink, M., Handsteiner, J., Malik, M., Scheidl, T., Ursin, R. & Zeilinger, A. Communication with spatially modulated light through turbulent air across vienna. *New Journal of Physics*. 16(11), 113028 (2014).
- [32] Hossack, W. J., Darling, A. M. & Dahdouh, A. Coordinate transformations with multiple computer-generated optical elements. *Journal Of Modern Optics*. 34, 1235-1250 (1987).
- [33] Qiu, C., Chen, J., Xia, Y. & Xu, Q. Active dielectric antenna on chip for spatial light modulation. *Sci. Rep.* **2**, 855 (2012).
- [34] Marsilli, F. & et al. Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7**, 210 (2013).
- [35] Lim, C. C. W., Curty, M., Walenta, N., Xu F. & Zbinden H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89** 022307 (2014).
- [36] Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84**, 3762 (2004).
- [37] Joseph W. Goodman, *Introduction to Fourier Optics*. Roberts & Company Publishers (2005).
- [38] Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052333 (2014).
- [39] Ding., X. et al. On-Demand Single Photons with High Extraction Efficiency and Near-Unity Indistinguishability from a Resonantly Driven Quantum Dot in a Micropillar. *Phys. Rev. Lett.* **116**, 020401 (2016).
- [40] Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51**, 1863 (1995).
- [41] Zhao, Y., Qi, B., Ma, X., Lo, H.-K. & Qian, L. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* **96**, 070502 (2006).
- [42] Peng, C.-Z. et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* **98**, 010505 (2007).
- [43] Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **16**, 18790 (2008).
- [44] Liu, Y. et al. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express* **18**, 8587 (2010).
- [45] Ferreira da Silva, T. et al. Proof-of-principle demonstration of measurement- device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).



- [46] Liu, Y. et al. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
- [47] Tang, Z. et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
- [48] Zhao, Y., Qi, Bi. & Lo, H.-K. Experimental quantum key distribution with active phase randomization. *Appl. Phys. Lett.* **90**, 044106 (2007).
- [49] Lima, G. et al. Experimental quantum tomography of photonic qudits via mutually unbiased basis. *Opt. Express* **19**, 3542 (2011).
- [50] Elkouss, D., Martinez-Mateo, J. & Martin, V. Information Reconciliation for Quantum Key Distribution. *Quant. Inf. Comp.* **11**, 0226 (2011).
- [51] Dynes, J. F. and others Quantum key distribution over multicore fiber *Opt. Express.* **24**, 15 13089 (2016).
- [52] David Mendlovic and Haldun M. Ozaktas Optical-coordinate transformation methods and optical-interconnection architectures *Applied Opt.* **32**, 26 5119 (1993).

