

UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI FISICA ED ASTRONOMIA
“G. GALILEI”

STOCKHOLMS UNIVERSITET
FYSIKUM

CORSO DI LAUREA MAGISTRALE IN FISICA

Three-Users Secure Quantum Communication With Qutrits

Laureando:

Massimiliano SMANIA

Relatore:

Dr. Marco BAZZAN

Correlatore:

Prof. Mohamed BOURENNANE

ANNO ACCADEMICO 2014/2015

Contents

Introduction	v
1 Classical Foundations	1
1.1 Cryptography	1
1.1.1 One-time Pad - A Symmetric-key cypher	1
1.1.2 The RSA protocol - Computationally secure cryptography	2
1.2 Optics	4
1.2.1 Electromagnetic waves	4
1.2.2 Interference	5
1.2.3 Multiport Devices	7
2 The Quantum World	11
2.1 The Basics	11
2.1.1 Wave-Particle Duality	11
2.1.2 The Quantum State $ \Psi\rangle$	12
2.1.3 Superposition Principle	13
2.1.4 No-Cloning Theorem	13
2.2 Quantum Optics	14
2.2.1 EM Field: Analogy and Quantization	15
2.2.2 Photon Number State	16
2.2.3 Coherent States	17
2.2.4 Beam Splitter: from Number States to Single Photon Interferometry	19
2.3 Quantum Information	22
2.3.1 Qubits	23
2.3.2 Mutually Unbiased Bases	26
3 Quantum Cryptography	29
3.1 Quantum Key Distribution	29
3.1.1 BB84 Protocol	30
3.1.2 Security against eavesdropping	34

3.1.3	QKD with phase encoding - the Plug&Play configuration . . .	35
3.1.4	QKD with qutrits	38
3.2	Quantum Secret Sharing	39
3.2.1	QSS with qubits	40
3.2.2	QSS with qudits	41
4	The Experiment	47
4.1	Setup and Equipment	47
4.1.1	Passive Optical Components	50
4.1.2	Active Optical Components	53
4.1.3	Electronic Devices	55
4.1.4	LabVIEW Software	57
4.2	Three Users QSS with Qutrits - The Protocol	59
4.3	Results and Analysis	62
4.3.1	Phase Modulators Calibration	62
4.3.2	Qutrit Error Rates	63
5	Conclusions	69
5.1	Achievements	69
5.2	Future Improvements of the Setup	70
	Bibliography	72

Introduction

Quantum information certainly is one of the most promising interdisciplinary fields that take advantage of quantum mechanics.

By combining the principles of this theory with state of the art technology, it manages to break communication and information problems that cannot be solved with classical theories, and it achieves that in ultimately thrilling and appealing ways.

One of the fields where this theory turned out to be groundbreaking is cryptography, a subject that directly or indirectly interests specialists and non-specialists alike. In this research area, the photon is certainly the favorite quantum object to work with. We will see how quantum properties of light can make communication more secure - or may we say *unconditionally secure* - and effective. In particular, the cryptographic task of *key distribution* between two users and its “generalization” to many parties, called *secret sharing*, have been heavily studied after Bennett and Brassard proposed a protocol for secure key distribution employing single photon polarization in 1984 [1].

In the following years, many theoretical proposals and experimental realizations vastly stimulated the scientific community interest in this subjects.

Nowadays, quantum key distribution (QKD) with good rates over 200 kilometers of optical fiber has been achieved [2], and protocols for secure quantum secret sharing (QSS) with many parties over dozens of kilometers of fibers have been successfully carried out [3]. The general goal is to implement these schemes in the already extensively available fiber telecommunication network, in order to have a smoother transition from classical to quantum communication.

In the past decade, QKD systems have become commercially available, and successful secure quantum communication over real fiber telecommunication networks have been attained around the world.

All these experiments share a common feature: they use two dimensional quantum systems (called *qubits*) as information carriers. However, as higher dimensionality means denser coding¹ and looser security requirements [4], several research groups

¹To understand this, compare a big number written in base ten with the same number in binary system. Which one is longer?

have shown their interest in testing protocols in higher dimension, and consequently QKD protocols for more than two dimensions have been successfully implemented in the lab.

With regard to QSS, proposals with three dimensional systems - called *qutrits* in analogy with qubits - have obtained good experimental results [5]. However, they all suffer from the consequences of being based on entanglement, specifically they are not scalable with respect to the number of parties participating in the secret sharing, mainly because of two reasons; the first one is somehow technological, that is, entangled states with many particles are still hard to prepare in the lab. The second reason is related to detection efficiency and is more intrinsic: the proposed protocols require single photons detections from every user in an experiment run, thus detection efficiency decreases exponentially with the number of users.

Our work, realized at the KIKO group labs in Stockholm², consisted in realizing a proof-of-principle experiment that implemented a different and innovative protocol for qutrits QSS, proposed in [6], in a fiber interferometric setup. The main difference between this new scheme and the ones we have just mentioned is that this does not require entanglement, being instead based on one single photon per run, with information encoded in its phase. Our configuration is highly scalable because it needs only three detectors, therefore its detection efficiency is independent from the number of parties. This is, of course, of paramount importance in a secret sharing protocol.

After a brief recap of some classical features of cryptography and optics in the first chapter, we will move into the fascinating quantum world.

First of all, the basic ingredients that any work related to quantum cryptography needs will be presented in chapter 2, then we will discuss a bit more in detail about quantum cryptography in chapter 3, and in particular about QKD and QSS, finally presenting the protocol we implemented in a general and formal way at the end of the same chapter.

The last part, i.e. chapter 4, regards our experimental work. Results and comments will follow a description of the setup we built and a more specific explanation of the protocol.

²<http://kiko.fysik.su.se/>

Chapter 1

Classical Foundations

1.1 Cryptography

Every piece of information we share has a target, and whenever this information has any value we would like it to be acknowledged only by the designated receiver. In an ideal world writing “TOP SECRET” on top of the message would suffice but, unfortunately, that is usually not the case. This is why cryptography was invented thousands of years ago. The first form of cryptography simply consisted in writing down the “secret” message anywhere, since literacy was practically non-existent. Ancient Greeks used bizarre methods as tattooing the message on a slave’s shaved head and hide it under the grown hair [7], but also started adopting proper cryptographic protocols, as transposition and substitution cyphers. Even though these methods are still employed nowadays, mainly by first grade children, they are known to be easily breakable by means of frequency analysis. Many other protocols were invented during the Renaissance thanks to the general improvement of education standards and advances in science, however modern cryptographic methods can be easily divided in two groups: symmetric-key and asymmetric-key cyphers. The former group exploits the same key for encrypting and decrypting, while the latter needs two keys, usually a public one for encrypting and a private one for decrypting. Let’s see some examples.

1.1.1 One-time Pad - A Symmetric-key cypher

The One-time pad method, invented in 1882 by Frank Miller, is to this day the only (classical) method proved to be completely secure [8]. The encryption and decryption of any message is based on the bitwise exclusive OR (XOR) operation and the key should be at least as long as the message itself. We can see a practical example in Table 1.1. Provided that the key is random, never reused and secret,

Message	Y	E	S
Plain text ASCII	0 1 0 1 1 0 0 1	0 1 0 0 0 1 0 1	0 1 0 1 0 0 1 1
Secret digital key	0 1 1 1 0 0 1 1	0 1 1 0 1 0 0 1	0 1 1 0 0 1 0 0
Encrypted text ASCII	0 0 1 0 1 0 1 0	0 0 1 0 1 1 0 0	0 0 1 1 0 1 1 1
Secret digital key	0 1 1 1 0 0 1 1	0 1 1 0 1 0 0 1	0 1 1 0 0 1 0 0
Deciphered text ASCII	0 1 0 1 1 0 0 1	0 1 0 0 0 1 0 1	0 1 0 1 0 0 1 1
Message	Y	E	S

Table 1.1: Example of one-time pad. The message (written in ASCII code) is encrypted by XOR operation with the secret key. The key, once transmitted to the receiver, can be applied again to obtain the original message.

the cypher is totally unbreakable. The **only** information an adversary can gain from the key is the maximum length of the message. Unfortunately, the one-time pad method has some severe disadvantages: for it to be secure, the key must be *genuinely random*, a requirement not easily satisfied; but most of all, every time we send a message we need to generate a new (one-time) key at least as long as the message that has to be securely and wholly transmitted to the receiver. These are the reasons why this cryptographic method is usually discarded in favor of less - or differently - secure protocols. Let's have a look at the most famous one.

1.1.2 The RSA protocol - Computationally secure cryptography

With the blazing fast development of technology and telecommunications in the twentieth century, a fundamental problem concerning security arose: the key distribution part of any cyphering process for symmetric-key protocols is risky and very demanding. Diffie and Hellman managed to solve this problem in 1976, when they published the first public-key method (known as the Diffie-Hellman key exchange [9]) that successfully established a secret key over an authenticated *public* channel without prior secret-key sharing. One year later Ron Rivest, Adi Shamir and Leonard Adleman invented the famous RSA algorithm [10], which is still used today for both secret sharing and digital signature. The protocol has been upgraded many times since its first release to overcome potential weak spots, but we can understand the way it works just by looking at the original algorithm. Before starting, we should introduce **Alice** and **Bob**, two characters (not necessarily human) usually living at least one room apart and with plenty of secret stuff going on between them. They are the protagonists of every cryptographic protocol, either classical or quantum,

and they often have to deal with their technologically cutting edge and infinitely rich arch-enemy, **Eve** the eavesdropper, trying to work out their secrets 24/7. Now, back to the RSA protocol, let's pretend that Alice needs to send a secret encrypted message to Bob. This is how they could do it:

1) **Bob: keys generation**

- Chooses two *random* distinct prime numbers p and q of similar bit-length and calculates $n = p \cdot q$. The length of n is the key-length
- Computes the *totient* $\phi(n) = (p - 1)(q - 1)$
- Picks an integer $1 < e < \phi(n)$ such that e is *coprime* with $\phi(n)$
- Announces n and e on a public channel. (n, e) is the public key
- Calculates the private key exponent d by solving $d \cdot e = 1 \pmod{\phi(n)}$. (n, d) is the private key.

2) **Alice: message encryption**

- Converts the message M to an integer $0 < m < n$ using a padding protocol
- Encrypts the message by calculating the cypher-text $c = m^e \pmod{n}$
- Sends the cypher-text c over a *public* channel

3) **Bob: message decryption**

- Using the private key (n, d) , decrypts the message c calculating $m = c^d \pmod{n}$
- Recovers the plain-text message M applying the same padding protocol used by Bob.

We see that any eavesdropper trying to calculate d starting from the public key (n, e) will have to factorize n to find p and q . This is called the *factorization problem* and with the currently available algorithms it's solvable in exponential time. This means that breaking the RSA encryption takes a time which is exponential to the bit-length of n . Keys up to 768 bits have been broken [11], and modern RSA protocols use 1024 to 2048 bits keys. So this protocol is **not** completely secure. It is only computationally secure, in the sense that no available computational power could break it in any reasonable time. However, we cannot be sure that a new algorithm capable of solving the factorization problem in polynomial time has not been or will never be invented. Actually, Peter Shor has proved in 1994 [12] that a quantum computer could, using Shor's quantum algorithm, solve the factorization problem in polynomial time, therefore breaking RSA security. The world clearly needs a new kind of cryptography.

1.2 Optics

This work is based on quantum mechanics applied to optics. However, most of the experimental characterization of the various components used has been done in classical regime. The reason is that working in classical conditions is much easier than quantum (for example you can use oscilloscopes instead of the extremely delicate single photon detectors). This is possible because, as we will see later on, many optical objects and physical quantities behave in a very similar way in the two regimes. For example, whenever we consider interference we are interested in *intensities*, which are proportional to squared field amplitudes. Very similarly in the quantum formulation we would like to predict the number of photons (i.e. the *probability density functions*), which in turn is proportional to the squared modulus of the wave function. Therefore we give now a brief recap of classical optics, before moving on into the quantum world.

1.2.1 Electromagnetic waves

We all know that light is a wave, and of course we have - at least - heard about Maxwell's equations. Let's see how the first statement is derived from those legendary equations. If we have electric field \mathbf{E} , magnetic field \mathbf{B} , electric charge density ρ and electric current density \mathbf{j} , then the equations describing the fields evolution are

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\epsilon_0} \quad (1.1a)$$

$$\nabla \cdot \mathbf{B} = 0 \quad (1.1b)$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \quad (1.1c)$$

$$\nabla \times \mathbf{B} = \mu_0 \mathbf{j} - \frac{1}{c^2} \frac{\partial \mathbf{E}}{\partial t} . \quad (1.1d)$$

In vacuum, with no electric charge or current, the solutions to Maxwell equations are the electromagnetic waves. In fact, if we take the curl of eqs. (1.1c) and (1.1d) and use the vector identity

$$\nabla \times (\nabla \times \mathbf{F}) = \nabla(\nabla \cdot \mathbf{F}) - \nabla^2 \mathbf{F} \quad (1.2)$$

keeping in mind eqs. (1.1a) and (1.1b), we get

$$\left(\nabla^2 - \frac{1}{c^2} \frac{\partial^2}{\partial t^2} \right) \mathbf{E} = 0 \quad (1.3)$$

$$\left(\nabla^2 - \frac{1}{c^2} \frac{\partial^2}{\partial t^2} \right) \mathbf{B} = 0 \quad (1.4)$$

These are equations describing transverse waves propagating with velocity c and with $\mathbf{E} \perp \mathbf{B}$. The explicit solutions are

$$\mathbf{E} = \mathbf{E}_0 e^{i(\mathbf{k} \cdot \mathbf{r} - \omega t + \phi)} \quad (1.5)$$

$$\mathbf{B} = \mathbf{B}_0 e^{i(\mathbf{k} \cdot \mathbf{r} - \omega t + \phi)} \quad (1.6)$$

where $|\mathbf{E}_0|$ and $|\mathbf{B}_0|$ are the waves amplitudes, \mathbf{k} is the wave vector, ω the pulsation frequency and ϕ the optical phase. We should also remember that $c = \omega/k$. The previous calculations were done for EM waves traveling in vacuum, but the analysis is the same - short of some constants - for any dielectric medium. The main difference, which affected our work, is that the wave velocity in a material with relative permittivity ϵ_r becomes

$$v = \frac{c}{\sqrt{\epsilon_r}} = \frac{c}{n} \quad (1.7)$$

Another important property of EM waves is **polarization**. This is defined as the direction of the electric field and, considering that \mathbf{E} and \mathbf{B} lie on the plane perpendicular to \mathbf{k} , it can be of three different types:

- *linear polarization*: the direction of \mathbf{E} is constant
- *circular polarization*: \mathbf{E} rotates along a circle. This situation can be seen as two orthogonal linearly polarized waves with the same amplitude and $\frac{\pi}{2}$ phase difference
- *elliptical polarization*: this is the most general case, and we can depict it as two orthogonal linearly polarized waves with a phase difference that is neither 0 nor $\frac{\pi}{2}$.

It's usually extremely important to control the polarization when working on secure communication with single photons. In fact, in order to have high interference visibility, the light pulses should have equal amplitude and polarization. While amplitudes - or intensities - are easy enough to control, polarization is trickier. In fact, light pulses propagating in free space are not subjected to polarization changes, but there are other transparent materials that have different refractive indexes depending on the polarization of the traveling wave. This special property of such crystals is called *birefringence*. As we will see later on, standard communication fibers are strongly birefringent, and this has been one of the most delicate aspects of this work.

1.2.2 Interference

The main physical phenomenon behind the secret sharing achieved in this work is interference, so it is important to have a good understanding of the subject. The

principle of superposition states that whenever two light waves are located on the same spacial region, their amplitudes sum point by point. This is called interference, and we should mention that it happens only if the two waves have similar properties, namely polarization and frequency. Interference is called *constructive* when the phase difference between the two waves is an even multiple of π , while odd multiples will give *destructive* interference.

Many types of interferometers have been invented, depending on aim and application; We can see an example of a simple Mach-Zehnder interferometer on fibers in Fig. 1.1: a light pulse entering the interferometer from port A gets splitted by the fiber coupler (FC). The two halves go through arms 1 and 2 - or paths L_1 and L_2 - and recombine at the output C thanks to a second fiber coupler. We can do some calculations considering a simple case where only 50 : 50 couplers are used, with neither attenuation nor birefringence. To make the example slightly more interesting (and suitable to this thesis) let's consider an extra phase ϕ added to the pulse going through arm 1, achieved by using, for example, a commercial phase modulator. We should consider only the electrical field, as we know from Maxwell's equations that $|\mathbf{E}| \approx c|\mathbf{B}|$, so $I \approx |\mathbf{E}|^2$. The incoming light wave is then of the form of eq. (1.5). After the second coupler the two halves recombine and at point C we have

$$\begin{aligned} \mathbf{E}(C, t) &= \frac{\mathbf{E}_0}{2} e^{i(kL_1 - \omega t + \phi)} + \frac{\mathbf{E}_0}{2} e^{i(kL_2 - \omega t)} \\ &= \frac{\mathbf{E}_0}{2} e^{i(kL_1 - \omega t + \phi)} (1 + e^{i[k(L_2 - L_1) - \phi]}) \end{aligned} \quad (1.8)$$

We can find the light intensity at the output C, which is what we actually measure, by taking the squared average of eq. (1.8)

$$I(C) = \frac{|\mathbf{E}_0|^2}{2} (1 + \cos(k\Delta L - \phi)) \quad (1.9)$$

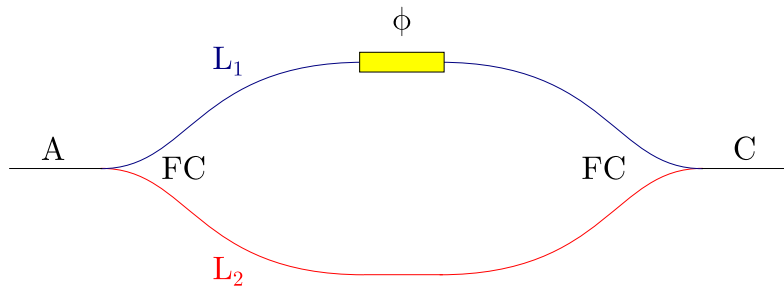


Figure 1.1: A simple Mach-Zehnder interferometer on fibers with input port A, a fiber coupler that splits the incoming light into two arms of length L_1 and L_2 , one of which includes a ϕ phase shift, another coupler that recombines the paths together into output port C.

It's now clear that we have maxima whenever the cosine argument is an even multiple of π , that is

$$\frac{\Delta L}{\lambda} - \frac{\phi}{2\pi} = m, \quad m \in \mathbb{Z} \quad (1.10)$$

while minima are related to odd multiples of π .

1.2.3 Multiport Devices

In the last paragraph we have seen a simple example of a two-arms interferometer. This work, however, is based on a three-arms interferometer; in order to build such a setup we need something slightly more complicated than a plain coupler. Any optical device with N inputs and N outputs is called a *multiport device*, and can be seen as a black box related to a transfer matrix which describes how any input state (e.g. an electrical field) is transformed into an output state. Once again we will consider only the case with neither attenuation nor birefringence. The latter approximation is allowed because we used only polarization maintaining fibers in the three interferometer arms with linearly polarized light (and polarization aligned to the fiber slow axis). Any birefringent optical element was placed exclusively in common paths, so that all interfering pulses would undergo the same changes, thus resulting in no relative effect. This will be much clearer later on once we present the optical setup in detail. The lossless approximation, however, is **never** strictly correct in practice. One of the 3x3 beam splitters (also called *tritters*) we used, for example, has coupling ratios (from input 1 to the outputs) of 36% : 27% : 36%, meaning that some light is “lost” inside the tritter. Anyway, as we are not interested in absolute intensities, but only in relative ones, we can consider this approximation legitimate as long as the coupling ratios for the different input-output configurations are approximately equal. In the lossless case the device is called *ideal* multiport splitter. Considering then an ideal splitter, energy conservation guarantees the unitarity of the transfer matrix, and if we consider tritters with equal coupling ratios for any input-output combination, we get the condition that each matrix entry should have the same absolute value. These conditions dramatically reduce the possible different matrices. We present here the 3x3 symmetric tritter case, as this is what we actually employed in the experiment. A candidate frequently adopted in literature [13][14] is the matrix

$$T = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{-i\frac{2\pi}{3}} & e^{i\frac{2\pi}{3}} \\ 1 & e^{i\frac{2\pi}{3}} & e^{-i\frac{2\pi}{3}} \end{pmatrix} \quad (1.11)$$

We can now use this matrix to predict the output intensities of a balanced ($L_1 = L_2 = L_3$ in Fig. 1.2) three-arms Mach-Zehnder interferometer similar to the one in

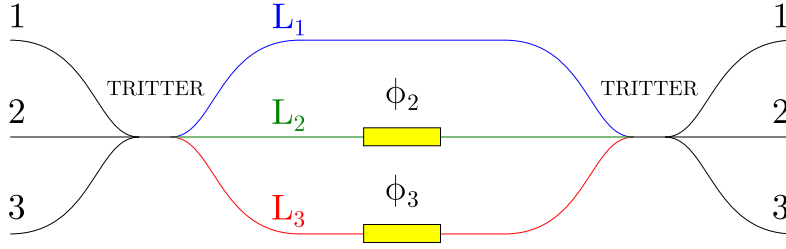


Figure 1.2: Mach-Zehnder three-arms fiber interferometer consisting of two 3x3 tritters and two phase modulators. Commercially available tritters introduce “by default” a $\frac{2\pi}{3}$ relative phase between any two of the three inputs (as we can see from Eq. (1.11)).

Fig. 1.2.

The full matrix of the whole tritter-phase modulators-tritter system is of course the matrix product of the three different elements, that is

$$TST = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{-i\frac{2\pi}{3}} & e^{i\frac{2\pi}{3}} \\ 1 & e^{i\frac{2\pi}{3}} & e^{-i\frac{2\pi}{3}} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\phi_2} & 0 \\ 0 & 0 & e^{i\phi_3} \end{pmatrix} \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{-i\frac{2\pi}{3}} & e^{i\frac{2\pi}{3}} \\ 1 & e^{i\frac{2\pi}{3}} & e^{-i\frac{2\pi}{3}} \end{pmatrix} \quad (1.12)$$

where the matrix S represents phase modulators in arms 2 and 3 that carry out phase shifts of respectively ϕ_2 and ϕ_3 angles. If we name the incoming electric field $\mathbf{E}^{\text{in}} \equiv (E_1^{\text{in}}, 0, 0)^1$ and the outgoing electric field $\mathbf{E}^{\text{out}} \equiv (E_1^{\text{out}}, E_2^{\text{out}}, E_3^{\text{out}})$, with the subscript index representing the input/output port as in Fig. 1.2, we can compute the output amplitudes simply by

$$\mathbf{E}^{\text{out}} = (TST)\mathbf{E}^{\text{in}} \quad (1.13)$$

As always we are interested in intensities, i.e. the squared modulus of electric fields, which can be found after some calculations to be

$$I_1 = \frac{(E_1^{\text{in}})^2}{9} \{3 + 2[\cos \phi_2 + \cos \phi_3 + \cos(\phi_2 - \phi_3)]\} \quad (1.14a)$$

$$I_2 = \frac{(E_1^{\text{in}})^2}{9} \left\{ 3 + 2 \left[\cos \left(\phi_2 - \frac{2\pi}{3} \right) + \cos \left(\phi_3 + \frac{2\pi}{3} \right) + \cos \left(\phi_2 - \phi_3 + \frac{2\pi}{3} \right) \right] \right\} \quad (1.14b)$$

$$I_3 = \frac{(E_1^{\text{in}})^2}{9} \left\{ 3 + 2 \left[\cos \left(\phi_2 + \frac{2\pi}{3} \right) + \cos \left(\phi_3 - \frac{2\pi}{3} \right) + \cos \left(\phi_2 - \phi_3 - \frac{2\pi}{3} \right) \right] \right\} \quad (1.14c)$$

We can notice from these equations that (relative) output intensities depend only on phase differences between distinct paths. Most importantly, whenever we have a

¹In our experiment, as happens in most of the same type, we are using only one input port of the tritter. In this example we are connecting the laser source to input 1.

maximum in one output (e.g. in port 1 for $(\phi_2, \phi_3) = (0, 0)$), the other two yield no light at all. We will see how this property translates into the quantum language of operators and probabilities, and how crucial it is for secret sharing.

Chapter 2

The Quantum World

2.1 The Basics

At the very beginning of the twentieth century Max Planck and Albert Einstein explained black-body radiation and the photoelectric effect with a very bold hypothesis: light can behave as if it was made of particles - later called photons - with discrete energy levels and momenta. Before the end of the twenties, quantum mechanics, or at least all its basic principles, had been pretty much laid out. However, no one could foresee how remarkably accurate its predictions were going to turn out in future experiments. One century later we are still looking for new ways to exploit the amazing consequences of this counterintuitive - often even illogical - theory. Quantum communication is one of the most straightforward yet potentially revolutionary application taking advantage of the quantum properties of reality, namely the wave-particle duality, the superposition principle and the no-cloning theorem. We will have a look at these special features of the theory in the next paragraphs.

2.1.1 Wave-Particle Duality

Black-body radiation and the photoelectric effect can both be explained assuming that light consists of particles - *photons* - with quantized energy, $E = h\nu$ per photon of frequency ν . h is of course the Planck constant, introduced in 1901 by Max Planck appositely to solve the black-body emission spectrum problem. But of course we know from our everyday experience that light also has wavelike properties, as diffraction and interference. The single most astonishing experiment showing this dual nature is the well-known *double slit experiment*, where single, isolated photons show interference patterns only if we are not aware of the paths they took, otherwise they simply behave as “classical” particles. Experiments showing interference fringes have been run not only with photons, but also with electrons, atoms and even much

bigger molecules exceeding 10000 amu [15]. In conclusion, not only light but matter too is inherently dual in nature, and in order to fully understand quantum mechanics and grasp the logic governing it we definitely need to abandon the classical notions of particles and waves, moving instead towards the idea of a **quantum particle**. This can be done introducing the quantum state - or wave function - ψ .

2.1.2 The Quantum State $|\Psi\rangle$ ¹

In any physical theory we characterize a system by its **state** and experimentally measurable quantities called **observables**. In the quantum mechanics formalism we identify a generic (pure) state by a vector in a Hilbert space, whose properties depend on the system it is linked to. We also refer to vectors in Hilbert spaces as wave functions, as these spaces are usually made up of complex functions. For example, the Hilbert space associated to position and momentum states of a single particle is the space of square-integrable (wave) functions L^2 . While states are linked to wave functions, observables are represented by self-adjoint linear operators acting on the state space. The possible states of a system (after a measurement) are the **eigenstates** of these operators, and the **eigenvalues** related to these eigenstates are the possible values of the observable associated with an operator.

Before a measurement, a system can be in a state $|\Psi\rangle$ which is a linear combination of pure states $|\Phi_i\rangle$, each with its own statistical weight factor c_i . We write this generic state as

$$|\Psi\rangle = \sum_i c_i |\Phi_i\rangle. \quad (2.1)$$

In the standard interpretation (a.k.a. *Copenhagen interpretation*) of quantum mechanics, whenever we measure an observable on a state the system **collapses** on an eigenstate of the measured observable and the measurement outcome is the eigenvalue related to that eigenstate.

Wave functions also give us the so called *transition probabilities*, which represent the probability for a system to collapse from a state $|\Psi_i\rangle$ to a state $|\Psi_j\rangle$ after a measurement. We can get these probabilities by calculating the squared absolute value of the inner product (defining the considered Hilbert space) between the two states

$$P(|\Psi_i\rangle \rightarrow |\Psi_j\rangle) = \|\langle\Psi_i|\Psi_j\rangle\|^2 \quad (2.2)$$

It is clear that if we write the initial state $|\Psi\rangle$ as in Eq. (2.1) including all possible final states in the sum, the transition probability to any state $|\Phi_i\rangle$ will simply be

$$\|\langle\Phi_i|\Psi\rangle\|^2 = |c_i|^2 \quad (2.3)$$

¹We are going to use the *bra-ket* notation throughout the whole thesis, taking for granted the reader's knowledge about it.

The *probabilistic nature* of quantum mechanics comes then from the measurement process. With regards to position measurements, we can think of quantum particles as waves that interact with each other by means of interference and superposition as long as we do not measure their location, at which point they immediately collapse in a position operator eigenstate (i.e. a precise location) and assume particle-like properties.

On a slightly more technical level, we can explain quantum interference by introducing the *superposition principle*.

2.1.3 Superposition Principle

The link between mathematical foundations - that give us Hilbert spaces and wave functions - and physics is the **Schrödinger equation**. Its most general form for a single non-relativistic particle is

$$\left[-\frac{\hbar^2}{2m}\nabla^2 + V(\mathbf{r}, t) \right] \Psi(\mathbf{r}, t) = i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r}, t) \quad (2.4)$$

where as usual m is the particle mass, $V(\mathbf{r}, t)$ the potential energy and $\Psi(\mathbf{r}, t)$ the particle wave function. Eq. (2.4) is a **linear** partial differential equation. In particular, its linearity implies that many (often in infinite number) wave functions $\Psi(\mathbf{r}, t)$ are solutions to the equation. The physical meaning of this statement is explained by the **superposition principle**: a quantum system exists in all its possible states (i.e. wave functions that solve its Schrödinger equation) simultaneously, but as soon as a measurement is performed on the system, it collapses in one of the possible eigenstates of the measured observable. It is crucial to understand that this uncertainty deriving from superposition is not something caused by our limited knowledge of the system that just goes away as soon as we perform a measurement. A quantum system before a measurement actually *is* in a superposition of different states. This is the reason why we can see interference patterns in the double slit experiment - or in this work - even when we are working with a *single photon*. Regarding Fig. 1.2, for example, due to a superposition of the states placing our photon in each of the three arms, we actually measure interference-like intensities in the three outputs, despite the photon being only one.

2.1.4 No-Cloning Theorem

The no-cloning theorem, first proved by Wootters and Zurek in 1982 [16], is the ultimate argument that makes quantum communication secure. There are different ways to prove it; we are going to give a simple demonstration for pure states in the following lines, but proofs exist for mixed states as well. Suppose we have two

quantum systems, A and B , with the same state space. System A is initially in the state $|\Psi\rangle_A$, **pure** but **unknown** to us, while system B is in the pure generic state $|0\rangle_B$. The whole point in copying is to have both systems in the state $|\Psi\rangle$ in the end. Slightly more precisely, we have a *composite system* initially in the state $|\Psi\rangle_A \otimes |0\rangle_B$, and we want some unitary cloning operator to transform this state to $|\Psi\rangle_A \otimes |\Psi\rangle_B$.

Suppose this operator exists, then it must be able to clone not only the initial state $|\Psi\rangle_A$, but also any other different initial state, for example $|\Phi\rangle_A$. In this case we have

$$\begin{aligned} U(|\Psi\rangle_A \otimes |0\rangle_B) &= |\Psi\rangle_A \otimes |\Psi\rangle_B \\ U(|\Phi\rangle_A \otimes |0\rangle_B) &= |\Phi\rangle_A \otimes |\Phi\rangle_B \end{aligned} \tag{2.5}$$

If we take the inner product of eqs. (2.5), we end up with the very restricting condition

$$\langle \Psi | \Phi \rangle = (\langle \Psi | \Phi \rangle)^2 \tag{2.6}$$

This is satisfied either if $|\Psi\rangle$ and $|\Phi\rangle$ are orthonormal or if $|\Psi\rangle = |\Phi\rangle$.

We have just proved that no unitary operator can clone *any* pure state. From the quantum communication security point of view, this means that if the exchanged information is encoded in non-orthogonal states (i.e. with different bases), an eavesdropper will not be able to clone a *single photon* state without knowing a priori the basis previously used for encoding.

Despite the no-cloning theorem, you can of course still make imperfect copies of any unknown state. Actually, it turns out [17] that the optimal universal cloning machine could reach, for a two-dimensional system, the surprising fidelity of $\sqrt{\frac{5}{6}}$.

2.2 Quantum Optics

In the previous chapters we have briefly discussed some aspects of classical optics and quantum mechanics. This section is the place where these two elements come together and create the extremely fascinating subject that is **quantum optics**.

How does classical optics become quantum? Not surprisingly, what we need is an analogy and a quantization method. We have seen in Sec. 1.2.1 that the EM field (which we will mostly be calling *light* as per “professional” bias) is an oscillatory phenomenon. The analogy is then of course between light and the harmonic oscillator. If we then quantize EM field oscillations, what we get is the amazing quantum optics!

We will start this section by explaining the basic ideas behind light quantization, and after showing the analogy with an harmonic oscillator, we will have a look at some interesting states of light that enhance its quantum nature.

2.2.1 EM Field: Analogy and Quantization

In Sec. 1.2.1 we mentioned Eqs. (1.5, 1.6) as possible solutions for Maxwell equations in vacuum. If we now suppose to confine the radiation field in a one-dimensional cavity along the z -axis limited by conductive walls at $z = 0$ and $z = L$, the fields must vanish at the boundaries. We further assume that the cavity is empty and that the electric field is polarized along the x -axis.

Single-mode fields satisfying these boundary conditions are [18]

$$\begin{aligned} E_x(z, t) &= \sqrt{\frac{2\omega^2}{\epsilon_0 V}} q(t) \sin(kz) \\ B_y(z, t) &= \sqrt{\frac{2\omega^2}{\epsilon_0 V}} \left(\frac{\mu_0 \epsilon_0}{k} \right) \dot{q}(t) \cos(kz) \end{aligned} \quad (2.7)$$

where ω is the mode frequency and k its wave number, $q(t)$ and $\dot{q}(t) = p(t)$ include time dependences of the solutions and have the dimension of length and velocity respectively. We will see that these quantities are the canonical position and momentum for a unit mass particle.

The Hamiltonian of this single-mode EM field is found by integrating the energy density over the whole cavity volume, that is

$$H = \frac{1}{2} \int dV \left[\epsilon_0 E_x^2(z, t) + \frac{1}{\mu_0} B_y^2(z, t) \right]. \quad (2.8)$$

Substituting Eqs. (2.7) into Eq. (2.8) we can easily find

$$H = \frac{1}{2} (p^2 + \omega^2 q^2) \quad (2.9)$$

which is clearly equivalent to a harmonic oscillator of unit mass.

We now enter the quantum formalism by substituting the canonical position and momentum variables with their corresponding quantum operators

$$\begin{aligned} q &\rightarrow \hat{q} \\ p &\rightarrow \hat{p} = -i\hbar \frac{\partial}{\partial q} \\ H &\rightarrow \hat{H} \end{aligned} \quad (2.10)$$

with the usual commutation relation

$$[\hat{q}, \hat{p}] = i\hbar. \quad (2.11)$$

At this point the two **ladder operators** are traditionally introduced. They are the *annihilation* operator \hat{a} , and its adjoint \hat{a}^\dagger , called the *creation* operator, defined as

$$\begin{aligned} \hat{a} &= \frac{1}{\sqrt{2\hbar\omega}} (\omega\hat{q} + i\hat{p}) \\ \hat{a}^\dagger &= \frac{1}{\sqrt{2\hbar\omega}} (\omega\hat{q} - i\hat{p}). \end{aligned} \quad (2.12)$$

From Eqs. (2.11, 2.12) their commutation relation turns out to be

$$[\hat{a}, \hat{a}^\dagger] = 1 . \quad (2.13)$$

Substituting Eqs. (2.12) into the operator version of Eq. (2.8), we can rewrite the Hamiltonian operator in terms of \hat{a} and \hat{a}^\dagger as

$$\hat{H} = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right) . \quad (2.14)$$

With the commutators

$$\begin{aligned} [\hat{H}, \hat{a}^\dagger] &= \hbar\omega \hat{a}^\dagger \\ [\hat{H}, \hat{a}] &= -\hbar\omega \hat{a} \end{aligned} \quad (2.15)$$

and remembering the Schrödinger equation

$$\hat{H}\Psi_n = E_n\Psi_n \quad (2.16)$$

we can find out how the ladder operators act on the eigenfunctions of \hat{H} . With some straightforward calculations we get

$$\hat{H}\hat{a}\Psi_n = (E_n - \hbar\omega)\hat{a}\Psi_n \quad (2.17a)$$

$$\hat{H}\hat{a}^\dagger\Psi_n = (E_n + \hbar\omega)\hat{a}^\dagger\Psi_n . \quad (2.17b)$$

Eqs. (2.17) show that the harmonic oscillator energy spectrum is discrete and its eigenenergies are equally spaced by $\hbar\omega$ steps. Furthermore, the creation operator \hat{a}^\dagger *raises* the energy by $\hbar\omega$ while the annihilation operator \hat{a} *lowers* it by the same amount.

Reassuming, the energy spectrum is

$$E_n = \left(n + \frac{1}{2} \right) \hbar\omega , \quad n \in \mathbb{N} \quad (2.18)$$

We will see in the next paragraph how we can interpret the ladder operators and the quantum number n in the EM field case.

2.2.2 Photon Number State

Whenever we are considering light, the quanta of energy our system contains (n in Eq. (2.18)) are called **photons**. We understand now why \hat{a} and \hat{a}^\dagger are named *annihilation* and *creation* operators: if we act on a state $|\Psi_n\rangle$ with \hat{a} , the system will lose an amount of energy equal to $\hbar\omega$, that is, the annihilation operator will remove a photon from the system. Of course the opposite happens with regards to

\hat{a}^\dagger . We can therefore write the wave functions solving the Schrödinger equation for the harmonic oscillator and the Schrödinger equation itself in the so-called *number state representation*:

$$\begin{aligned} |\Psi_n\rangle &\equiv |n\rangle \\ \hat{H}|n\rangle &= \hbar\omega \left(n + \frac{1}{2} \right) |n\rangle . \end{aligned} \quad (2.19)$$

Considering Eqs. (2.17) and after normalization, we can redefine ladder operators as

$$\begin{aligned} \hat{a}|n\rangle &= \sqrt{n}|n-1\rangle \\ \hat{a}^\dagger|n\rangle &= \sqrt{n+1}|n+1\rangle \end{aligned} \quad (2.20)$$

which imply

$$|n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle \quad (2.21)$$

where $|0\rangle$ is the ground (or vacuum) state. Eq. (2.21) also suggests that we may intuitively interpret the state $|n\rangle$ as a vacuum state where n photons have been created.

Finally, we should notice that if we act on the state $|n\rangle$ with the operator $\hat{a}^\dagger\hat{a}$, we get

$$\hat{a}^\dagger\hat{a}|n\rangle = \sqrt{n}\hat{a}^\dagger|n-1\rangle = n|n\rangle . \quad (2.22)$$

$\hat{a}^\dagger\hat{a}$ is indeed called **number operator**. Number states are eigenstates of the number operator \hat{n} as we can see from Eq. (2.22).

We will understand later how important this operator actually is for secure quantum communication. Nevertheless, number states are *not* a good description of physical field states generated, for example, by a laser. It is actually possible to show [18] that number and phase are complementary observables, so that number states have uniform (i.e. *random*) phase distribution, which is certainly not the case for coherent light coming from a laser source.

It is suitable then to introduce a different class of states, conveniently called *coherent states*, which better describes “real” coherent light sources.

2.2.3 Coherent States

We have noticed in the previous section that number states contain a definite number of photons and are thus characterized by completely random phases. On the contrary, *coherent states* do not have a fixed number of photons nor a precise phase. Actually, the product of uncertainties in amplitude and phase for coherent states is the minimum allowed by the Heisenberg’s *uncertainty principle* [19].

There are different ways of introducing coherent states; here we are going to do it by taking advantage of their most fundamental difference from number states, that is, they are eigenstates of the annihilation operator. Thus, they must satisfy the relation

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \quad (2.23)$$

where α is a complex number as \hat{a} is *not* Hermitian.

Thanks to number states completeness we may expand any state $|\alpha\rangle$ as

$$|\alpha\rangle = \sum_{n=0}^{\infty} c_n |n\rangle, \quad (2.24)$$

acting with \hat{a} on each term we get

$$\sum_{n=0}^{\infty} c_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} c_n |n\rangle \quad (2.25)$$

and comparing coefficients recursively we can easily calculate

$$c_n = \frac{\alpha^n}{\sqrt{n!}} c_0. \quad (2.26)$$

From the normalization condition we find $c_0 = \exp(-|\alpha|^2/2)$, thus the final expression for a coherent state becomes

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (2.27)$$

We can understand something more about coherent states by carrying out some simple calculations. For example, from Eq. (2.23) and its conjugate we can compute the expectation value of the number operator

$$\bar{n} = \langle \alpha | \hat{n} | \alpha \rangle = \langle \alpha | \alpha^* \alpha | \alpha \rangle = |\alpha|^2. \quad (2.28)$$

We can therefore regard α as a complex number whose modulus is proportional to the electric field amplitude and thus the squared modulus to the field intensity.

The variance of the photon number is found to be [20]

$$(\Delta n)^2 = \langle \alpha | (\hat{n} - \bar{n})^2 | \alpha \rangle = \bar{n}, \quad (2.29)$$

which shows that coherent states have poissonian photon number distribution.

Finally, we can calculate the probability for a coherent state to contain n photons as

$$P(n) = |\langle n | \alpha \rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} = e^{-\bar{n}} \left(\frac{\bar{n}^n}{n!} \right) \quad (2.30)$$

which clearly proves the Poisson distribution hypotheses.

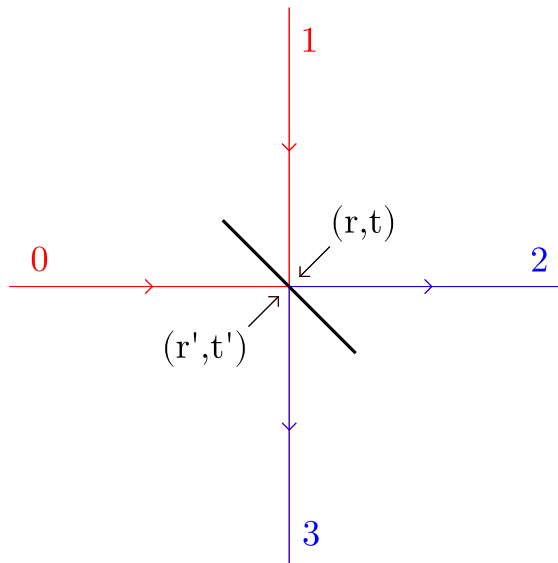


Figure 2.1: 2x2 beam splitter with input ports (0,1) and output ports (2,3). Reflectance and transmittance are shown according to eq. (2.31).

2.2.4 Beam Splitter: from Number States to Single Photon Interferometry

We have seen in sec. 1.2.2 how classical interference can easily be explained by means of a wave-like description of light. At some point we had also hinted at the similarity between interferometric results in the classical and quantum cases. However, in order to fully understand single photon interferometry and see how the quantum states we have just introduced are actually exploited in this field, we should give a quantum mechanical description of a single photon interferometer.

The building block of most interferometers is the **beam splitter**. In this work 3x3 beam splitters (called **tritters**, with three input and three output ports) have been used. We should however look at the simpler 2x2 case first, and then upgrade the result to the slightly more complicated 3x3 device.

Let us suppose we have a 2x2 beam splitter as the one in Fig. 2.1. First of all we should notice that even if we are using only one input port, it is absolutely *necessary* to consider both inputs in the quantum treatment, otherwise contradictions would raise² (for example ladder operators commutation relations would not be preserved). This is one of the many occasions in which vacuum turns out to be a proper quantum state that needs to be considered.

That being made clear, we write ports with subscripts (using numbers as Fig. 2.1), so that \hat{a}_i and \hat{a}_i^\dagger will be respectively the annihilation and creation operators for port i . If we take r and t as the complex reflectance and transmittance of the beam

²For an example with calculations, see section 6.2 in [18]

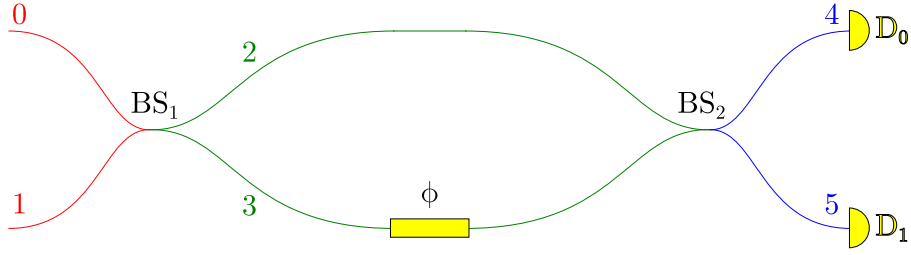


Figure 2.2: Fiber Mach-Zehnder interferometer with input ports (0, 1), a 2x2 beam splitter (also known as *fiber coupler*) working in accordance to eqs. (2.33), two arms one of which includes a ϕ phase shift, another 2x2 coupler that recombines the pulses into output ports (4, 5), connected respectively to detectors D_0 and D_1 . Detection probabilities for this setup are derived in eqs. (2.38) and (2.39).

splitter, the device transformations for the ladder operators are

$$\begin{aligned}\hat{a}_2 &= r\hat{a}_1 + t'\hat{a}_0 \\ \hat{a}_3 &= t\hat{a}_1 + r'\hat{a}_0 .\end{aligned}\tag{2.31}$$

Furthermore, because of energy conservation the following relations must be satisfied

$$\begin{aligned}|r| &= |r'| \\ |t| &= |t'| \\ |r|^2 + |t|^2 &= 1 \\ r^*t' + r't^* &= 0 \\ r^*t + r't'^* &= 0 .\end{aligned}\tag{2.32}$$

We now introduce some typical hypothesis about the beam splitter: we choose to describe a 50:50 splitter which introduces a $\frac{\pi}{2}$ phase shift in the reflected pulse. This type of device is made of a single dielectric layer.

Considering this choice and eqs. 2.32, eqs. 2.31 become

$$\begin{aligned}\hat{a}_2 &= \frac{1}{\sqrt{2}}(i\hat{a}_1 + \hat{a}_0) \\ \hat{a}_3 &= \frac{1}{\sqrt{2}}(\hat{a}_1 + i\hat{a}_0) .\end{aligned}\tag{2.33}$$

We may see now how we can easily apply this formalism to a simple interferometric fiber system as in fig. 2.2. The Mach-Zehnder interferometer consists of two 2x2 50:50 beam splitters and a phase modulator in one of the two arms. We may write any input state in photon number representation as $|m\rangle_i|n\rangle_j$, meaning that we have m photons in mode (or path) i and n in mode j .

Let us consider the input state $|\psi\rangle_{in} = |0\rangle_0|1\rangle_1$ that is, a single photon entering the interferometer from port 1. Taking into account eqs. 2.33 and their conjugates

and the obvious fact that an input vacuum state transforms into an output vacuum state, we can compute the system state after the first beam splitter

$$\hat{a}_1^\dagger |0\rangle_0 |0\rangle_1 = |0\rangle_0 |1\rangle_1 \quad (2.34)$$

$$\begin{array}{c} \downarrow BS_1 \\ \hat{a}_1^\dagger |0\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}} \left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger \right) |0\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}} \left(i|1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3 \right) . \end{array} \quad (2.35)$$

It should be noticed that the state coming out from the first splitter is *entangled*. It is indeed a superposition of the photon being in mode 2 or 3, with probabilities equal to $\frac{1}{2}$.

Because of the phase modulator PM , the state with the photon in mode 3 will be phase shifted by an angle ϕ

$$\frac{1}{\sqrt{2}} \left(i|1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3 \right) \xrightarrow{PM} \frac{1}{\sqrt{2}} \left(i|1\rangle_2 |0\rangle_3 + e^{i\phi} |0\rangle_2 |1\rangle_3 \right) \quad (2.36)$$

With very similar calculations we can now compute the final state after the second beam splitter

$$\begin{array}{c} \frac{1}{\sqrt{2}} \left(i|1\rangle_2 |0\rangle_3 + e^{i\phi} |0\rangle_2 |1\rangle_3 \right) \\ \downarrow BS_2 \\ \frac{1}{2} \left[i \left(e^{i\phi} + 1 \right) |1\rangle_4 |0\rangle_5 + \left(e^{i\phi} - 1 \right) |0\rangle_4 |1\rangle_5 \right] = |\psi\rangle_{out} . \end{array} \quad (2.37)$$

The probability that detector 0 (D_0 in fig. 2.2) clicks corresponds to the probability for the system to be found in the state $|1\rangle_4 |0\rangle_5$, that is

$$P(D_0) = \left| \langle \langle 1|_4 \langle 0|_5 | \psi \rangle_{out} \right|^2 = \frac{1}{2} (1 + \cos \phi) , \quad (2.38)$$

while, on the other hand

$$P(D_1) = \left| \langle \langle 0|_4 \langle 1|_5 | \psi \rangle_{out} \right|^2 = \frac{1}{2} (1 - \cos \phi) . \quad (2.39)$$

The $\cos \phi$ dependences clearly show the interference process going on in the system. We should point out that the result we have just obtained is completely analogous to the one we had previously got to in the classical formalism (see eq. 1.9). Except that this time we have taken account of the fact that photons are indivisible, by using photon number states.

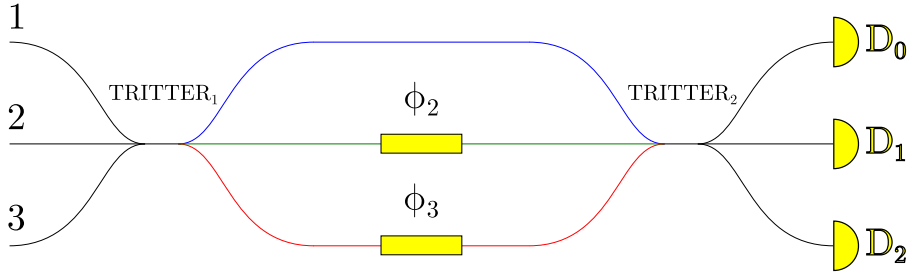


Figure 2.3: Mach-Zehnder three-arms fiber interferometer consisting of two 3x3 tritters and two phase modulators. Phase differences dependent probabilities for the three detectors are reported in eqs. (2.40).

We mentioned in the beginning of this section that we would have explained how the 2x2 beam splitter results change when we have different beam splitters; in particular, we should show the 3x3 unbiased beam splitter case, as this is the type of multiport device used in this thesis work.

Consistently with what we have just seen, there is no need to carry out the calculations one more time, as the result we obtain using creation and annihilation operators for the tritter is the same as the classical scenario described by eqs. 1.14. The only difference of course is that in the single photon case we may interpret intensities as probabilities, and $(E_1^{in})^2 = 1$ (remembering that $|\mathbf{E}|^2 = \bar{n}$).

All these things considered, the final probabilities for a single photon 3-arms interferometer as in fig. 2.3 are

$$P(D_0) = \frac{1}{9} \{3 + 2 [\cos \phi_2 + \cos \phi_3 + \cos(\phi_2 - \phi_3)]\} \quad (2.40a)$$

$$P(D_1) = \frac{1}{9} \left\{ 3 + 2 \left[\cos \left(\phi_2 - \frac{2\pi}{3} \right) + \cos \left(\phi_3 + \frac{2\pi}{3} \right) + \cos \left(\phi_2 - \phi_3 + \frac{2\pi}{3} \right) \right] \right\} \quad (2.40b)$$

$$P(D_2) = \frac{1}{9} \left\{ 3 + 2 \left[\cos \left(\phi_2 + \frac{2\pi}{3} \right) + \cos \left(\phi_3 - \frac{2\pi}{3} \right) + \cos \left(\phi_2 - \phi_3 - \frac{2\pi}{3} \right) \right] \right\} . \quad (2.40c)$$

2.3 Quantum Information

“Information is physical” are the famous first words of a 1996 Landauer’s paper [21]. Even disregarding the underlying physics the author was referring to in this powerful sentence, one can easily agree. *Any* piece of information is carried - or encoded - in some physical way. Everyday examples are electrical pulses or magnetic states in computers, protein sequences in genetics, light pulses in fiber communication. These and every other “commercially” available system work within the boundaries of classical physics, at least in the information treatment part.

At the beginning of this chapter we mentioned how quantum physics managed, in the first decade of the last century, to overcome some key problems that classical physics was suffering from. But the new theory didn't just solve those problems, it also turned out to be a groundbreaking step forward in physics and basically everything else. A question naturally comes up then: why don't we apply quantum physics and its amazing consequences to information processing and computation? As it always happens, it took a genius to come up with the right question. Richard Feynman introduced the idea of a quantum computer in 1982 [22] and since then a lot of progress has been made both theoretically and experimentally towards that goal. Many benefits of a quantum computer over a classical one have already been proved, and they all include the idea of **efficiency**. What do we mean by efficiency? In information science, problems are divided in complexity classes; two significant examples are

- **Polynomial complexity class (P)**: the number of computer operations required to solve these problems scales as a polynomial power of the problem size (i.e. *bits*)
- **Non-polynomial complexity class (NP)**: the number of operations increases with size faster than any polynomial function.

An example of a task that turns out to belong to the NP class in classical computing (it's dependence with size is actually **exponential**) has already been introduced in sec. 1.1.2, when we considered prime numbers factorization. This task cannot be solved efficiently by classical computers, while it can in the quantum computing realm (where it belongs to P-class problems). In fact, prime numbers factorization is only one of the tasks that can be carried out more efficiently by quantum computers. Apart from computing, there are other areas where quantum physics show its superiority over classical models. One of them is of course *cryptology*. Later in this section we will talk about it, but in order to do it we are going to need some basic notions about quantum information.

2.3.1 Qubits

We all know the *bit*, the basic unit of classical information. It can be defined as a two-valued variable, which can be 0 or 1, or equivalently *false* or *true*. This logical value is usually implemented in computers as on/off voltages or "up/down" magnetization states.

By analogy, quantum information is built upon the **qubit** (short for *quantum bit*). A qubit *can* be in one of the two logical states $|0\rangle$ or $|1\rangle$ (as we are talking about quantum states, we are going to use the *bra-ket* notation as usual), but this is not

the whole story. $|0\rangle$ and $|1\rangle$ are the two states constituting the *computational basis* ($\langle i|j\rangle = \delta_{i,j}$) of a two-dimensional Hilbert space related to our quantum system. As we know, a quantum system can be in any **superposition** of the basis states; therefore, the generic qubit state can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.41)$$

where as usual $|\alpha|^2 + |\beta|^2 = 1$. A qubit state can thus be interpreted as a unit vector in a two-dimensional complex (Hilbert) space, exactly as any two-dimensional quantum system.

However, the main difference between classical and quantum bits comes out in the measurement process. As a bit is either 0 or 1, whenever we perform a measurement on it we will get exactly its state as a result. On the contrary, a measurement on a qubit (in the computational basis) in the state (2.41) will return $|0\rangle$ - or more precisely its related eigenvalue - with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. This *probabilistic nature* inherent in qubits may seem destabilizing at first, but it actually is a huge resource to build a whole new way of communicating and computing.

Now that we introduced the abstract concept of qubit, we should spend some words on how to physically realize it. Any quantum system with two easily distinguishable states, orthogonal to each other, can act as a qubit. Common examples are: photon polarization (horizontal/vertical or left/right), electron spin (up/down) or even atomic energy levels (ground/first excited), provided that they are sufficiently decoupled from the other levels. As an example, we consider a linearly polarized photon, with horizontal and vertical polarization states acting as our computational basis, such that for example

$$\begin{aligned} |0\rangle &\equiv |H\rangle \equiv \text{Horizontal} \\ |1\rangle &\equiv |V\rangle \equiv \text{Vertical} . \end{aligned} \quad (2.42)$$

These polarization states are easily understood by looking at fig. 2.4. Now suppose, for example, that we happen to measure a diagonally (i.e. $|+\rangle$ - see fig. 2.4) polarized photon. We can write this state in the computational basis as

$$|+\rangle = \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle) . \quad (2.43)$$

At this point we can easily understand that a measurement in our chosen computational basis is going to return either H or V randomly, as $|\alpha|^2$ and $|\beta|^2$ in eq. (2.41) are both equal to $1/2$.

Now you may be wondering why we should use qubits if any measure - that is, all we can acknowledge - is going to return only one of two values just as in the classical

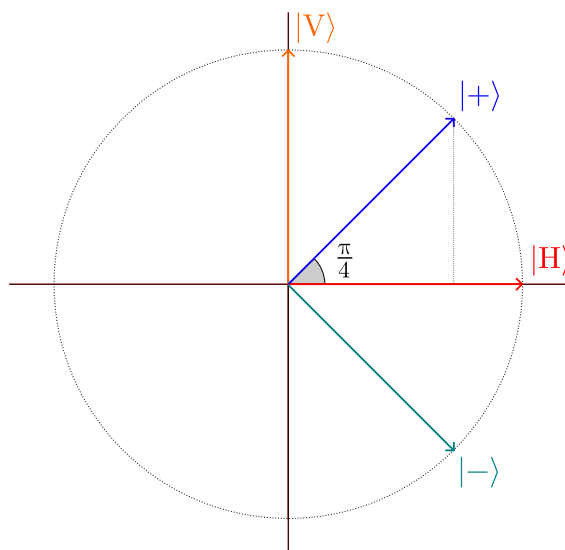


Figure 2.4: Linear polarizations space for a photon. Every point on the dashed circle is a linear polarization state, and may be written as a linear combination of one of the two bases $\oplus = \{|H\rangle, |V\rangle\}$ and $\otimes = \{|+\rangle, |-\rangle\}$. In this drawing we can also clearly see the non orthogonality of the two bases.

bit case. The point is that any different linear combination (i.e. **superposition**) of basis states carries different information; in our example, any linear polarization (and they are infinitely many) is a different state, therefore we can in principle store an infinite amount of information in a qubit state. Of course whenever we perform a measurement in any basis, the system will collapse to an eigenstate of that basis, and there goes our information! But we should notice that thanks to unitarity evolution, all the information stored in the superposition is somehow preserved. Furthermore, if we have more than one qubit, the number of states our system may be in increases exponentially with the number of qubits, thus making the amount of information huge very soon³.

We mentioned some of the simplest ways to physically realize a qubit. Slightly more creatively, we will see that a two dimensional system can easily be built using phase differences of light pulses. This is indeed the way our secret sharing protocol works.

Before getting there, however, we need to “upgrade” the qubit to a higher level. We have seen that qubits are two-dimensional entities, but what about higher dimensional systems?

We can in general define a d -dimensional quantum information system as a *qudit*. Given a computational basis $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ for the qudit Hilbert space, we

³For a very comprehensive and entertaining introduction to the charms of quantum computation, look no further than [23].

can, in analogy with eq. (2.41), write any pure state $|\psi\rangle$ as superposition of the basis states

$$|\psi\rangle = \sum_{i=0}^{d-1} c_i |i\rangle \quad (2.44)$$

where as usual any measurement in the computational basis will return i (that is the eigenvalue of the state $|i\rangle$) with probability $|c_i|^2$.

Of course working with higher dimensional systems has the advantage of carrying more information with the same number of quantum systems. Nevertheless, while in principle nothing forbids us from doing quantum communication with high dimensional qudits, things can get quite complicated on the experimental side. Instabilities and ridiculously low generation rates (especially in the entanglement-based protocols) may actually nullify the advantages the additional dimensions grant.

Getting back to our work, we dealt with the 3-dimensional version of qudits, called **qutrits**. We will get into a more detailed explanation of the advantages of this choice over qubits once we have the required knowledge.

Finally, we will now go through a short mathematical digression which may seem a bit out of place, but it is actually of paramount importance for quantum communication security.

2.3.2 Mutually Unbiased Bases

Granted that we can express any state in a Hilbert space as a linear combination of vectors making up a basis for that space, we move now one level higher in our discussion about quantum information. Hilbert spaces can have many different bases, therefore making our life more complicated, apparently. But this is *exactly* what makes quantum communication **secure**. Imagine Alice preparing a secret state in one of many bases and sending it to Bob. Eve, the mean eavesdropper, would like to know the state Alice sent, so she intercepts and measures it. But hang on, there is a problem! In which one of the many possible bases is she going to perform her measurement? If she picks the right one she will get the correct result, but even if Alice and Bob choose to implement only two bases, she is going to get a wrong - or at least not “deterministic” - result half of the times. We will discuss about these security issues later, but we can sense some crucial doubts here: is there a best choice for Alice and Bob when it comes to choose bases? And if there is, how can they get to know them? Well, the latter question is way over the level of this dissertation (and it actually is currently an open theoretical problem), but we can still answer the former and show some results.

The answer of course is yes, and the solution for our overcautious friends is using Mutually Unbiased Bases (MUBs). They are defined in the following way:

consider a quantum system linked to an N -dimensional Hilbert space; two bases $\{|e_0\rangle, |e_1\rangle, \dots, |e_{N-1}\rangle\}$ and $\{|f_0\rangle, |f_1\rangle, \dots, |f_{N-1}\rangle\}$ for this space are *mutually unbiased* if and only if

$$|\langle e_i | f_j \rangle|^2 = \frac{1}{N} \quad \forall 0 \leq i, j \leq N - 1. \quad (2.45)$$

Condition (2.45) can be interpreted in many ways. For sure it means that the overlap between states belonging to MUBs is constant and independent of the states considered. From a more “practical” point of view, it guarantees that if we prepare a state in one basis and measure it in any other which is unbiased to the first one, every outcome is *equally likely*. That is, **no information** can be obtained about a state if the measurement is performed in the wrong basis.

The existence of a complete set of MUBs in any dimension is an open question. It has been proved that complete sets of $N + 1$ MUBs exist, first in prime dimensions [24] and later in any power of prime dimensions [25]. But there is no general rule for all remaining dimensions. For example dimension 6 has been and currently is heavily studied, with strong conjectures suggesting the existence of only three MUBs [26].

However, the two and three-dimensional cases are well known and characterized, and we report them here as examples.

- Two dimensions - **Qubit MUBs**

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad B_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad B_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \quad (2.46)$$

where every matrix B_i is a basis, and columns are basis vectors. We may notice that B_1 is the computational basis, with $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. If we consider photon polarization with definitions (2.42), then we can easily see that these three MUBs correspond respectively to horizontal/vertical, diagonal/antidiagonal and left/right circular polarization states.

- Three dimensions - **Qutrit MUBs**

$$\begin{aligned} M_1 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & M_2 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \\ M_3 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{pmatrix} & M_4 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega^2 & \omega^2 \\ \omega^2 & 1 & \omega^2 \\ \omega^2 & \omega^2 & 1 \end{pmatrix} \end{aligned} \quad (2.47)$$

with $\omega = e^{\frac{i2\pi}{3}}$.

It is clear that these definitions satisfy condition (2.45). For example, naming vectors in *bra-ket* notation as $|M_i(j)\rangle$ with $j = 0, 1, 2$ indicating the matrix column, we can calculate the squared inner product of a vector from M_2 with one from M_3 :

$$\begin{aligned} |\langle M_2(2)|M_3(2)\rangle|^2 &= \frac{1}{9} \left| \begin{pmatrix} 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} \omega \\ 1 \\ \omega \end{pmatrix} \right|^2 = \frac{1}{9} |\omega + \omega^2 + \omega^2|^2 = \\ &= \frac{1}{9} \left| e^{\frac{i2\pi}{3}} + 2e^{\frac{i4\pi}{3}} \right|^2 = \frac{1}{9} \left| -\frac{3}{2} + i\frac{\sqrt{3}}{2} \right|^2 = \frac{1}{3}. \end{aligned} \quad (2.48)$$

We will see how the protocol we used for quantum communication takes advantage of three dimensional MUBs and their unique properties.

At this point we are ready to introduce the subject which this experimental work has focused on, that is quantum cryptography.

Chapter 3

Quantum Cryptography

3.1 Quantum Key Distribution

Quantum cryptography is the extremely fascinating field that studies innovative ways to solve classical cryptographic problems by using special features uniquely possessed by quantum mechanical systems. Its applications range from military security to card games [27]. This experimental work focused on the so-called *quantum secret sharing* (QSS) problem, which will be introduced in the following of this chapter. Indeed we shall first concentrate on the most studied and developed problem in the quantum cryptography field, that is *quantum key distribution* (QKD). We will see that QSS has many similarities with QKD, and can almost be interpreted as a generalization to many users.

We mentioned in sec. 1.1.2 that commercial - but also military - cryptographic protocols are currently based on public-key cyphers, and we pointed out in an almost arrogant way that these methods are not secure. Well, quantum mechanics not only offers an **unconditionally** secure way to encrypt private information, but it also allows us to do it through a public (i.e. **not protected**) channel. Let us explain this. The main weakness of any classical cypher is the secret key exchange: when Alice sends her decrypting key to Bob, for example by e-mail or phone, she has no way to be sure that Eve has not intercepted the transmission and is not aware of the key, unless maybe if she personally delivers it to Bob. But suppose that Bob is the US president and Alice is his best secret agent acting undercover somewhere in a very hostile country. How can they possibly meet? All it takes for them to solve this problem is some hundred-thousands of dollars worth of optical equipment - which is surely no problem for them - and a good fiber optical network. Apart from this unlikely (or maybe not that much) scenario, the crucial point is that quantum cryptography is not focused on the encryption part of a secure communication, but rather on the key distribution process. Once Alice has sent her secret

key to Bob by means of a secure QKD protocol, they can use for example a one-time pad method, which has been proved to be unbreakable (see sec. 1.1.1 and [8]), to encrypt their messages, and be comfortably positive about their shared secrets.

But how does QKD works precisely, and why is it unconditionally secure?

While classical cryptography needs very special (and often expensive) precautions to make sure that no eavesdropper is intercepting the secret key, thus keeping the communication channel secure, QKD offers a failsafe way to know easily when someone is listening to our communications, therefore letting us exchange information through public channels while being sure that no one is listening.

What basically happens is that Alice sends a key to Bob through a public unprotected channel, and if this is intercepted by Eve then quantum mechanics assures us that Alice and Bob get to know it, thus discarding the key and creating a new one. As soon as they manage to have a shared secret key, they can encrypt and decrypt messages.

On a slightly more physical level, what prevents Eve from eavesdropping without being unmasked is the fact that any measurement on a quantum state affects the state itself, i.e. it projects the state on the basis the measurement is performed in, thus resulting in the system being in a state belonging to that basis, not necessarily the same as before the measurement (see sec. 2.1.2). Technically, Alice and Bob are sure that Eve cannot copy a state without modifying it thanks to the **no-cloning theorem** we proved in sec. 2.1.4. Of course this is true provided that there is only one copy of the system transmitted between the users. We will get into more details on the security of QKD later.

We should point out that there are two basic types of QKD, one involving **entangled** particles and the other using **single** particles. While the former may be more fascinating from a fundamental point of view, here we are going to present only single particle schemes, as these are incredibly simpler to understand and implement, and far more common in the field. Moreover, we will discuss exclusively photon based QKD, which is basically the only type deeply studied and implemented.

We will now introduce an extremely simple protocol for QKD from which most of the currently realized systems are developed. It is based on qubits encoded in photon polarization.

3.1.1 BB84 Protocol

Early proposals to exploit quantum mechanics in order to establish secure cryptography date back to the early '70s, when Stephen Wiesner submitted his “*Conjugate Coding*” paper to the *IEEE Transactions on Information Theory*, unfortunately only to see it rejected. It took some more years and lots of discussions between that

same physicist and two of his friends, Charles Bennett and Gilles Brassard, before the first protocol for QKD was invented and published¹ in 1984 [1].

The original scheme was based on photon polarization encoding, and this is how we are going to present it as it is the simplest way to understand the principles behind it.

The protocol uses qubits encoded in two MUBs, for example we choose the horizontal/vertical and the diagonal/anti-diagonal bases, that is matrices B_1 and B_2 in eq. (2.46). Looking at the notation we used in fig. 2.4, we can rename vectors in a more convenient way using Dirac's notation

$$\begin{aligned} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &\equiv |H\rangle & \begin{pmatrix} 0 \\ 1 \end{pmatrix} &\equiv |V\rangle \\ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} &\equiv \frac{|H\rangle + |V\rangle}{\sqrt{2}} \equiv |+\rangle & \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} &\equiv \frac{|H\rangle - |V\rangle}{\sqrt{2}} \equiv |-\rangle. \end{aligned} \quad (3.1)$$

From these definitions, and from the fact that we are using MUBs, it is clear that states belonging to different bases are not orthogonal to each other. We will see that this is exactly where the security comes from.

Anyway, back to the protocol, Alice and Bob want to establish a binary key, so they need to agree on each vector representing either “0” or “1” for example as in tab. 3.1.

		<i>basis</i>	
		\oplus : horizontal/vertical	\otimes : diagonal/anti-diagonal
<i>bit</i>	0	$ H\rangle$	$ +\rangle$
	1	$ V\rangle$	$ -\rangle$

Table 3.1: Given the two mutually unbiased bases used in the protocol, one vector from each basis represents either 0 or 1.

At this point, having established a public quantum channel (e.g. optical fiber or free space) and a public classical channel, as phone or email, Alice and Bob are ready to take the following steps:

1. Alice **randomly** generates a bit and **randomly** chooses one of the two bases. The randomness of these choices is of course crucial if she wants her data to be unpredictable. Depending on the outcomes, she prepares a photon in the

¹It actually took a meeting in the pool of a Caribbean posh hotel, by the beach in San Juan, as Brassard himself explains in a very entertaining paper on the history of quantum cryptography [28].

correct polarization state according to tab. 3.1, and she sends it to Bob through the quantum channel after registering its polarization and time of departure. So, for example, if she randomly generated $(1, \oplus)$, she will send a vertically polarized photon (i.e. $|V\rangle$).

2. Bob receives the photon and, unaware of the basis Alice encoded it in, he randomly picks either \oplus or \otimes and performs a measurement in that basis. The outcome will be unconditionally correct (save for experimental errors or **eavesdropping**) if he happens to choose the same basis as Alice, otherwise thanks to the defining property (2.45) of MUBs the outcome will be random. He finally registers time of arrival, measurement basis and outcome.
3. After having checked that traveling times are constant (and possibly make sense too), Alice and Bob share through the classical channel their basis choices: they discard every run in which they picked different bases, and keep the rest. This process will result in them having strings of bits which will be in average half the number of runs, as Bob will randomly choose the wrong basis half of the times. During this process only the basis choices are revealed, while the vector choices and measurements (i.e. the bit values) are kept secret.
4. Bob and Alice now perform a security check on the sifted key: they share a statistically relevant amount of bits and compare their values; if no eavesdropping happened (and the experimental setup was perfect) the shared bits will be totally identical and the two friends can be sure that Eve has no information about the key. On the contrary, if there are errors in the sample then they can argue that Eve has probably gained some information, in which case they just discard the key and run the whole process again from the first step, possibly on a different quantum channel.
5. If the key generation was successful, they can apply for example a one-time pad method to encrypt their message with the key they have just established, and share it through the classical channel, being confident that Eve does not possess the key to decrypt it.

We can see a practical example of a key generation process following the BB84 protocol in tab. 3.2.

This protocol is extremely simple and easy to implement in a lab. However, we should mention some common sources of errors affecting any real QKD implementation:

- **Random deletion of photons:** this source of errors and problems affects every implementation. It frequently happens that while Alice has sent a pho-

Alice	bit	0	0	1	0	1	1	1	0	1
	basis	\oplus	\otimes	\otimes	\otimes	\oplus	\otimes	\oplus	\oplus	\otimes
	state	$ H\rangle$	$ +\rangle$	$ -\rangle$	$ +\rangle$	$ V\rangle$	$ -\rangle$	$ V\rangle$	$ +\rangle$	$ -\rangle$
Bob	basis	\oplus	\oplus	\otimes	\oplus	\oplus	\otimes	\otimes	\oplus	\oplus
	outcome	0	1	1	0	1	1	0	0	1
basis check		✓	×	✓	×	✓	✓	×	✓	×
sifted key		0		1		1	1		0	
error check?		yes		no		yes	no		no	
secure key				1		1	1		0	

Table 3.2: Secure key generation with BB84 protocol. In this case there has been no eavesdropping.

ton, Bob registers no click in any detector, as if the photon had never left the source. This may be caused by absorption or scattering by the setup, or by detection efficiencies. Depending on the specific configuration, the attenuation from the single photon source to the detectors may be of many dozens of decibels, and detection efficiency usually goes from 10% to 70% with commercially available photodetectors. These factors however, while considerably reducing the key generation rate, are innocuous from the security point of view, as Alice will simply discard any run which Bob has not measured.

- **Birefringence and noisy quantum channel:** this is a serious problem for protocols using polarization, as standard commercial fibers are birefringent, thus they introduce changes in the polarization during the photon transmission. This is why most protocols nowadays use phase encoding for which birefringence is not a big problem. We shall see anyway, that these other type of implementations suffer from interferometric instabilities and require other countermeasures.
- **Detector dark counts:** this problem is caused by thermal detections in photodiodes. Every time a photon gets lost in the transmission, it is still possible for Bob to register a click in a random detector because of the thermal excitations inside the photocathode. This problem becomes really important for low-efficiency detectors and highly attenuating setups, and even more if gated biased photodetectors are used, as in our case. The solution is to reduce the attenuation as much as possible and find a good compromise between dark counts and efficiency.

All the aforementioned problems may be solved by using error correction algorithms,

whose final effect is a reduction of the key length, or equivalently, of the generation rate.

But what about security against external threats? Let's see how Eve could use her infinite budget to hack this - and actually almost any other - QKD protocol.

3.1.2 Security against eavesdropping

Many different types of attacks have been invented and subsequently neutralized during the years, thanks to the unstoppable creative power of scientists. We have said more than once that QKD is a priori unbreakable because of the fundamental principles of quantum mechanics (and thus nature which seems to adapt pretty well to this theory) that lead to the no-cloning theorem. Unfortunately, theories are always approximations of real-world experiments, or rather their ideal counterparts. In fact, even if Eve cannot attack the principles of quantum mechanics, she can surely exploit any technological and experimental weakness in Alice's and Bob's setups. For this reason when we introduced Eve in sec. 1.1.2, we said that she has access to any feasible technology - and then some - to be bought with unlimited money.

We should say from the beginning that this work has not taken care of all the countermeasures against the technological attacks we are now going to present, as they usually consist in some additional equipment or error correction algorithm, and this work has been focused mainly on a proof-of-principle of the proposed protocol. Nonetheless, it is important to have an idea of the problems any real-world QKD implementation has to face.

- **Intercept and resend:** this is the simplest type of attack Eve can perform. She basically cuts the transmission line halfway between Alice and Bob and measures the state. She then sends to Bob a new system in the same state she got from the measurement. As she is not aware of which basis the state she receives is encoded in, she will choose the wrong basis 50% of the times, in which cases if Bob measures the state in the same basis Alice encoded it in, he will get the state wrong in half the runs. The total error introduced by Eve is then in average $50\% \times 50\% = 25\%$. This attack can be easily detected in the error checking part of the protocol (step number 4). Actually, Eve could use better bases for the attack and get help from others (in a so-called coherent attack). It has been proved that the minimum error introduced by the optimal cloning attack to a QKD protocol is 11% in the qubit case and 15.95% if qutrits are used [4]. If Alice and Bob obtain an error rate lower than these thresholds, they are sure that no such attack has been performed.

- **Photon number splitting:** in real QKD implementations weak pulsed lasers attenuated much below the single photon level are used. Usually average intensities as low as 0.1 photons per pulse are used, but as the photon number distribution is Poissonian (see sec. 2.2.3), there is always a small probability that more than one photon is sent in one pulse. If Alice sends two photons, Eve can split them, keeping one in a quantum memory and sending the other to Bob, and then measure it after the bases announcement. There are many countermeasures against this attack. The best solution would certainly be to use a true single photon source. Even though modern implementations of these sources still have low generation rates, experiments have been run with them [29], thus setting high expectations for their future use. The best solution is employing *decoy states*, which consist in randomly sending pulses with a different average number of photon. Successful realizations of these protocols have been attained [30][3].
- **Man-in-the-middle:** this is a weakness that QKD shares with any other cryptographic protocol. In fact, nothing guarantees to Alice that the person she thinks is Bob actually is...Eve! The solution to this problem requires the step of *identity verification*, for which well-known classical procedures exist and can be applied. However, they all require a previously shared secret key, for which it may be necessary for Alice and Bob to meet face to face *untantum* before starting their secret sharing.

Finally, we should say that other attacks exploiting particular configurations have been carried out, but they can all usually be solved by means of some setup modifications or improvement.

In conclusion, the BB84 protocol looks extremely useful and well-built for QKD, but it has one major flaw in its polarization implementation, that is the birefringence problem we discussed above. A possible, and actually almost universally accepted, solution is to use instead an interferometric setup with phase encoding.

3.1.3 QKD with phase encoding - the Plug&Play configuration

In order to implement a real-world QKD system, we need it to work over long distances. For example, we can think of running a protocol over telecommunication optical fibers, which means over a hundred of kilometers between “repeaters”. These commercial fibers are not polarization maintaining and due to environmental changes they are strongly - and randomly - birefringent. Thus polarization is not the way to go in the real-world scenario.

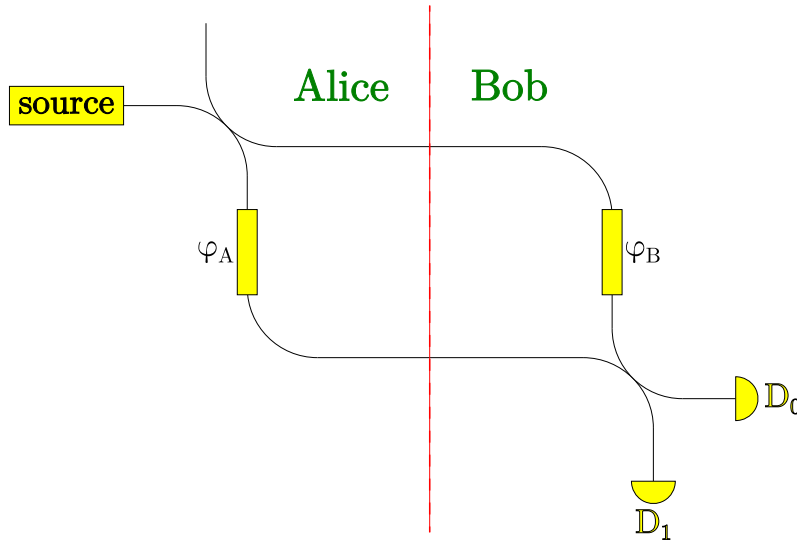


Figure 3.1: Qubit QKD interferometric setup with phase encoding (φ_A, φ_B). The *source* is either truly single photon or an attenuated pulsed laser.

A good solution is a somehow slightly different realization of the BB84 protocol, with **interferometry** and **phase encoding** instead of polarization states. Suppose Alice and Bob use an interferometric setup as in fig. 3.1. We know from sec. 2.2.4 that the measurement outcome depends on the relative phase between the two arms pulses, namely $\phi = |\varphi_A - \varphi_B|$ in our figure. But then we can easily establish two MUBs and perform the BB84 protocol just as in the polarization case. For example we can take the angles $\{0, \pi\}$ as one basis and $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ as the other. Whenever Alice and Bob both choose the same basis the total phase difference ϕ will be a multiple of π , thus giving a click in a definite detector with probability 100%, otherwise $\phi = \frac{\pi}{2}$ or $\phi = \frac{3\pi}{2}$, thus giving random detections as we can see from eqs. (2.38) and (2.39), just as in the polarization case when Bob measures in the wrong basis. Actually, exactly as in that case, Bob only needs to choose the basis, that is, choose between angles 0 and $\frac{\pi}{2}$. You can find all the possible cases in tab. 3.3, where we supposed that detector 0 and 1 correspond respectively to bit values 0 and 1.

This version of the BB84 protocol is definitely the most common in the QKD

Alice's bit	0	0	1	1	0	0	1	1
φ_A	0	0	π	π	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{3\pi}{2}$	$\frac{3\pi}{2}$
φ_B	0	$\frac{\pi}{2}$	0	$\frac{\pi}{2}$	0	$\frac{\pi}{2}$	0	$\frac{\pi}{2}$
$\phi = \varphi_A - \varphi_B $	0	$\frac{\pi}{2}$	π	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	$\frac{3\pi}{2}$	π
Bob's outcome	0	random	1	random	random	0	random	1

Table 3.3: BB84 protocol with phase encoding. The MUBs are $\{0, \pi\}$ and $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$.

move on to the very similar qutrits case.

3.1.4 QKD with qutrits

Knowing how the BB84 protocol works in the easiest case, we can now describe an “upgraded” version of the same type of protocol for the three dimensional case, that is for **qutrits**. This upgrade has two main advantages over the standard qubit version

- **Denser coding:** of course having three possible outcomes from every measurement is better than two. To understand why, just compare any big number written in binary system with the same number in base three!
- **Enhanced security:** this cannot be so easily understood. The main point is “how good” Eve can clone a generic state used in the protocol. It turns out that an *optimal cloning machine* gets worse with increasing dimensions [4], and as we have already mentioned in sec. 3.1.2, the upper boundary for qutrits error rate (QTER) is 15.95% for coherent attacks (where Eve keeps many photons in memory and measure them at the same time), while it is 11% for qubits.

An other potential advantage is the possibility to use more MUBs, as their number increases for higher dimensions, at least for power of prime ones (see sec. 2.3.2). This of course makes Eve’s life harder, as she has to guess between more basis, but it also decreases the number of bits that pass the key-sifting part, as Bob will measure in the right basis less often too, thus causing lower generation rates.

Anyway, QKD for qutrits works very similarly to the qubits case. Photon polarization cannot be used this time, since polarization state space is two dimensional, but phase encoding can instead be adopted. The generalization of the BB84 protocol to three dimensions consists in the two users working with two of the three dimensional MUBs in eq. (2.47). In analogy with fig. 3.1, the simplest setup they can use is reported in fig. 3.3.

Choosing for example vector $|M_2(1)\rangle = \begin{pmatrix} 1 & \omega & \omega^2 \end{pmatrix}^T$ means adding phases $\varphi_1 = \omega = e^{\frac{i2\pi}{3}}$ to the pulse in arm 1 and $\varphi_2 = \omega^2 = e^{\frac{i4\pi}{3}}$ to the pulse in arm 2. As we can see from eqs. (2.40), the final probability to have a click in one detector will be unitary if Alice and Bob chose the same basis, otherwise detection will be random. We should comment again that a setup as in fig. 3.3 is quite inconvenient because of interferometric instabilities. Unfortunately, no automatically balanced interferometer can be built for the three dimensional case (as there must be three different paths), but there are much better configurations than this, as we will see for example when we explain our own setup.

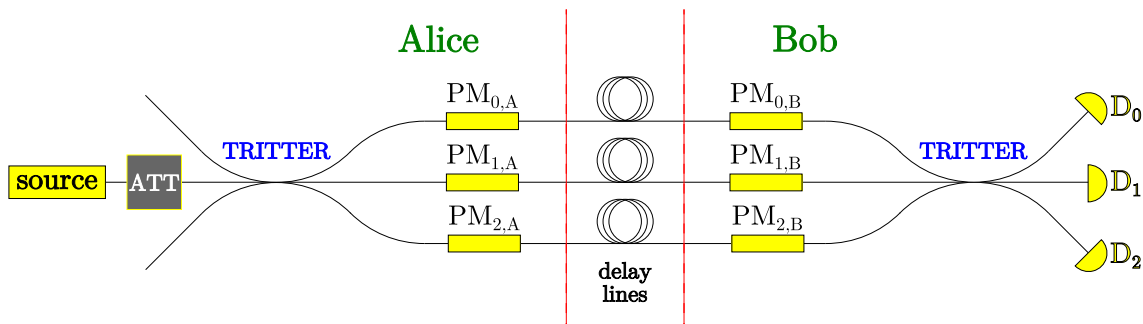


Figure 3.3: Qutrit QKD setup. The interferometer must be carefully balanced in order to have good visibilities. For this reason (and because it needs **three** fiber channels between Alice and Bob) this is not the best setup, however it is useful to understand the basics of qutrit QKD.

3.2 Quantum Secret Sharing

In this case, a somewhat classical example is: suppose there is a group of high commanders in a very belligerent country that is in charge of an extremely powerful nuclear arsenal (hopefully it won't ring any bell). Now, what happens if one of these men one day feels particularly irritated and decides to launch a missile against some opposite group/organization? For sure the launch will need at least a password from each commander (here is an example of secret sharing), but then how can we be sure that this lunatic had not intercepted all the other's passwords during the initial distribution process and kept them hidden knowing that a bad day would have eventually come?

Secret sharing protocols aim at solving these kind of problems by splitting a secret among different users, in such a way that one or more of them (but not all of course) cannot reconstruct it without the collaboration of the others.

There are classical solutions for these issues, but as you may guess they all require some secure communications between users, therefore being susceptible to eavesdropping attacks. But wait a minute! We **know** that quantum communication can do that! This problem is somewhat similar to the key distribution problem then, except that in this case there usually is a distributor splitting the secret and giving one part to each of many users, and this distributor has to take care not only of any external eavesdropper, but also of one or more possible traitors inside the sharing group.

Contrary to the QKD case, the first papers reporting QSS protocols exploited entanglement [32, 33]. Nevertheless, QSS was successfully carried out later using only one particle with interferometry and phase encoding [34, 3]. All these experiments have been realized with qubits. After an initial explanation of the two dimensional phase encoding case, we will present the protocol for qudits we used and our particular

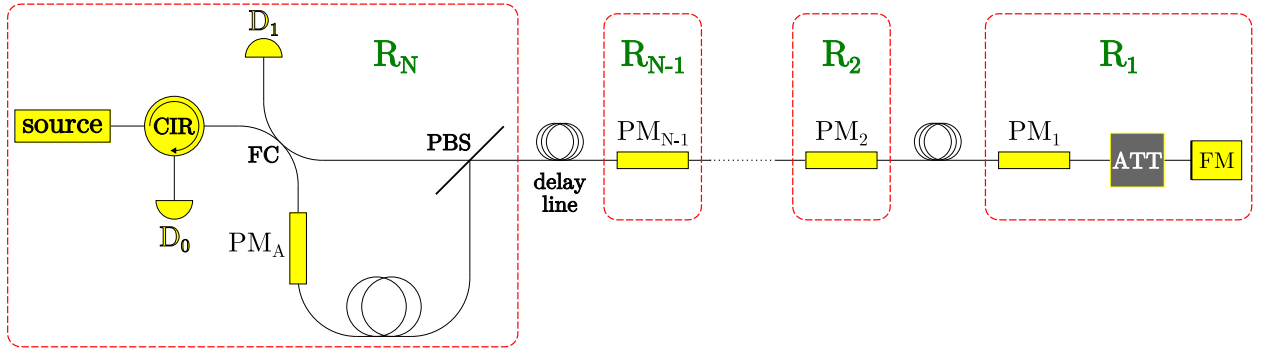


Figure 3.4: Plug&Play QSS setup using qubits. In this example there are R_N parties.

implementation.

3.2.1 QSS with qubits

The QSS method for N users we are going to present is based on the BB84 protocol we have seen in sec. 3.1.1. Our exposition will basically report the protocol introduced in ref. [3], as per the setup in fig. 3.4.

1. As in the BB84 protocol, a qubit is initially prepared in the state

$$|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \quad (3.2)$$

by the first user R_1 ².

2. Each user R_n from R_1 to R_{N-1} acts sequentially on the received qubit with the unitary operator

$$\hat{U}(\varphi_n) = |0\rangle\langle 0| + e^{i\varphi_n}|1\rangle\langle 1| \quad (3.3)$$

where φ_n is one of four angles divided in the two mutually unbiased bases $\{0, \pi\}$ and $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$. Sounds familiar? These are exactly the same setting applied to the same qubits of the BB84 QKD protocol described in sec. 3.1.1. And precisely as in that case,

3. R_N chooses only the basis, that is he picks either $\varphi_n = 0$ or $\varphi_n = \frac{\pi}{2}$. The qubit will finally be in the state

$$|\psi_N\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\sum_{n=1}^N \varphi_n} |1\rangle \right) \quad (3.4)$$

²Actually in a Plug&Play setup as in fig. 3.4 and [3], R_N both prepares *and* measure the qubit. However, nothing changes in the mathematical and physical properties of the protocol.

In the end he measures the qubit in the $\otimes = \{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ basis. Again, very similarly to the BB84 case, the probabilities of the outcomes will be

$$\begin{aligned} \frac{1}{4} |\langle + | \psi_N \rangle|^2 &= P(D_0) = \frac{1}{2} \left(1 + \cos \sum_{n=1}^N \varphi_n\right) \\ \frac{1}{4} |\langle - | \psi_N \rangle|^2 &= P(D_1) = \frac{1}{2} \left(1 - \cos \sum_{n=1}^N \varphi_n\right). \end{aligned} \tag{3.5}$$

as per eqs. (2.38) and (2.39).

4. The parties reveal in reverse order the bases they used on a public channel. From this information they know which runs gave a unitary probability for one detector and zero for the other (we call these *deterministic* runs) and which returned random results. These second type of runs get at this point discarded, and in average half of the measurements will remain (as in the key-sifting part of BB84).

Whenever the run is deterministic, $N - 1$ users can calculate the remaining party's phase by sharing their own setting among each other, thus achieving the goal of secret sharing.

We should point out that the reverse order in the basis revealing part is due to security reason, so that any cheating from user R_n may become harmless.

Finally we would like to mention a crucial advantage of the single particle protocols over the entanglement ones, that is *scalability*. In fact, suppose we have ten users: if Alice wants to run an entanglement-based QSS protocol, she needs to generate ten entangled systems for every run and perform at least ten measurements at the same time. This is gonna result in a ridiculously low generation rate, if any at all. If you also consider the imperfect (euphemistically speaking) detection efficiency η , the rate will decrease as η^N because every user adds his own detectors. In the single particle version instead, adding users simply means having higher attenuation, which is not such a big problem, and can in principle be solved with better equipment. Moreover, the number of detectors is constant, and such is detection efficiency.

We will now present a more general protocol for higher dimensional QSS.

3.2.2 QSS with qudits

QSS has been experimentally achieved both with entanglement-based [33] and single particle [34, 3] protocols. However, these implementations employed qubits. Using higher dimensional systems gives the same advantages we talked about in the

QKD case (see sec. 3.1.4), namely **denser coding** and **higher security boundaries**. It is interesting then to explore the possibility of higher dimensionality for QSS methods. Therefore, we are now going to present a generic protocol valid for any prime number dimension except for two, which we have already explained in the previous section anyway. This scheme has been proposed in [6], and this work is part of its experimental realization.

First, we need to introduce few mathematical objects, some new and others simply written in a more convenient notation.

As you may guess at this point, the protocol is going to use MUBs. We can write every basis as $\{|s_l^j\rangle\}$, where $j = 0, \dots, d-1$ ³ specifies the basis and $l = 0, \dots, d-1$ labels the vector in basis j . We can then remind the MUBs defining condition rewritten in a slightly more precise way than eq. (2.45), that is

$$\left| \langle s_l^j | s_{l'}^{j'} \rangle \right|^2 = \frac{1}{d} (1 - \delta_{j,j'}) + \delta_{j,j'} \delta_{l,l'} , \quad (3.6)$$

while all the d MUBs vectors can be written as

$$|s_l^j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(l+jk)} |k\rangle \quad (3.7)$$

where $\omega = e^{\frac{i2\pi}{d}}$. This definition is consistent with eq. (2.47).

Now we introduce two new unitary operators whose combined actions on any MUB vector $|s_l^j\rangle$ can return any other vector $|s_{l'}^{j'}\rangle$ in the MUBs set, and no other vector outside this set.

The first operator is

$$\hat{X}_d = \sum_{m=0}^{d-1} \omega^m |m\rangle \langle m| , \quad (3.8)$$

and by applying it on a generic vector in our set we get

$$\begin{aligned} \hat{X}_d |s_l^j\rangle &= \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \omega^m |m\rangle \langle m| \sum_{k=0}^{d-1} \omega^{k(l+jk)} |k\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k((l+1)+jk)} |k\rangle = |s_{l+1}^j\rangle . \end{aligned} \quad (3.9)$$

We have shown that the action of \hat{X}_d is to increase the vector index, thus by applying it several times to any state we can get any other state in the same MUB.

³It is worth noticing that we are using only d MUBs, even though we know (see sec. 2.3.2) that in prime d dimensions we have $d+1$ MUBs. This happens because the computational basis is of no use in this protocol.

The second operator as you may guess will change the basis, that is index j . We define it as

$$\hat{Y}_d = \sum_{m=0}^{d-1} \omega^{m^2} |m\rangle \langle m| \quad (3.10)$$

and its action is

$$\begin{aligned} \hat{Y}_d |s_l^j\rangle &= \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \omega^{m^2} |m\rangle \langle m| \sum_{k=0}^{d-1} \omega^{k(l+jk)} |k\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(l+(j+1)k)} |k\rangle = |s_l^{j+1}\rangle. \end{aligned} \quad (3.11)$$

As we anticipated, \hat{Y}_d increases the basis index j , and its multiple application will give us any basis in the MUBs set.

Therefore, we see that we can easily map $|s_l^j\rangle$ into any other vector $|s_{l'}^{j'}\rangle$ just by combining the actions of these two operators elevated to some powers, while being sure that we will obtain no vector outside our set.

We are now ready to present the protocol, which involves N users that act sequentially on the same qudit system.

1. R_1 , the *distributor*, prepares the qudit system in the initial state

$$|\psi_0\rangle = |s_0^0\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle. \quad (3.12)$$

2. Sequentially, every user R_n with $n = 1, \dots, N - 1$ generates two independent random numbers $x_n, y_n \in \{0, \dots, d - 1\}$, acts on the received qudit with the transformation

$$\hat{X}_d^{x_n} \hat{Y}_d^{y_n} |\psi_{n-1}\rangle = |\psi_n\rangle \quad (3.13)$$

and finally forward the obtained qudit to the next party, that is R_{n+1} .

3. The last user, R_N , applies $\hat{X}_d^{x_N} \hat{Y}_d^{y_N}$, getting the final state

$$|\psi_N\rangle = \prod_{n=1}^N \hat{X}_d^{x_n} \hat{Y}_d^{y_n} |\psi_0\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{\sum_{n=1}^N (kx_n + k^2 y_n)} |k\rangle. \quad (3.14)$$

He then performs a measurement in the basis $\{|s_l^0\rangle\}$, and announces on a public channel the outcome $a \in \{0, \dots, d - 1\}$, which at this point none of the parties knows if it is deterministic or random.

4. All the users R_2, \dots, R_{N-1} , *in random order*, announce their y_n . R_1 and R_N do it after everyone else, again in random order. This is important for security reasons.

5. Here comes the usual *key-sifting* part: if and only if the condition

$$\sum_{n=1}^N y_n = 0 \pmod{d} \quad (3.15)$$

is satisfied, then the final state $|\psi_N\rangle$ was an eigenstate of the measurement operator, that is, $|\psi_N\rangle \in \{|s_l^0\rangle\}$. The run is then valid and equation

$$\sum_{n=1}^N x_n = a \pmod{d} \quad (3.16)$$

produces the shared secret, that is the set $\{x_n\}$. This happens averagely in $\frac{1}{d}$ of the runs. If, instead, condition (3.15) is not satisfied, the run is discarded.

6. As in every other protocol we have analyzed, all users announce on the public channel a statistically relevant part of their choices for x_n , in order to check inconsistencies with eq. (3.16).

We can at this point define a *qudit error rate* (QDER) as

$$QDER = \frac{C_w}{C_r + C_w} = \frac{C_w}{C_{TOT}} \quad (3.17)$$

where C_r is the number of valid runs which produced detections in the right output (i.e. eq. (3.16) is satisfied as expected), C_w the ones that violated eq. (3.16), by causing detections in a wrong output, and C_{TOT} is obviously the total amount of valid runs. This definition represents the error rate in the communication, and is commonly used in literature [5].

Back to the protocol, if the error rate is below the security threshold, than the shared secret is secure and at least $N - 1$ parties need to collaborate in order to solve eq. (3.16), thus finding out the remaining user's choice of x_n and reconstructing the whole secret $\{x_n\}$.

We should point out once more that the single particle has the advantage of being highly **scalable** with respects to the entanglement version, because of course it doesn't require any entangled-particles generation and the number of detectors is constantly d , thus making detection (in)efficiency independent of the number of users.

Security of the protocol

We can basically have two different types of attacks:

- **Intercept and resend:** this is the same threat we have explained in sec. 3.1.2 for the QKD case. Exactly as in that protocol, if the QDER calculated in step

6 is lower than a secure threshold value, than the parties can safely assume that this attack has not been performed, or was not successful. We should point out again that higher dimensions have more relaxed security conditions [4].

The other attacks we described for QKD (namely photon number splitting and man-in-the-middle) have the same consequences and solutions in QSS.

- **Cheating parties:** this security threat is characteristic of secret sharing schemes. Suppose one of the users would like to cheat and gain some information on other users' choices of x_n . A potentially dangerous way to do this could be by storing the state he receives from the previous user in a quantum memory and send instead one of two entangled qudits, while keeping the other [35]. If in step 4 every other user announces his y_n *before* our cheater, then he could gain some information without being detected, such that by collaborating with other cheating users, a subset of less than $N - 1$ parties could reconstruct the whole secret.

Unfortunately for the cheater, the random way users announce their y_n prevents this possibility.

Security is instead not guaranteed if more than one cheater collaborate. However even in this case the probability for a successful attack can be made arbitrarily small by running the protocol more times. For example, it can be shown [6] that in the worst case scenario where there are $N - 2$ collaborating cheaters, 35 valid runs give a successful attack probability of 0.001 for $N = 11$.

We will see in the following chapter how this protocol has been experimentally applied to a three dimensional case, therefore proving that it could be implemented in order to achieve secret sharing.

Chapter 4

The Experiment

4.1 Setup and Equipment

In sec. 3.2.2 we have presented, theoretically, a protocol for an innovative approach to secret sharing, for any number of parties and in d dimensions (with d any prime number different from two). This chapter will discuss our experimental implementation of a three dimensional (i.e. *qutrits*) version of that proposed scheme: it will be shown that, save for some (reasonable) technical limitations, the system produces the expected results with error rates that are well below the security thresholds.

The technical problems mentioned above are due to the particular experimental realization of the setup, and will likely be solvable by future developments.

We start this chapter by presenting the experimental setup we built, pictured in fig. 4.1. It is a **three arms Mach-Zehnder-like interferometric system** completely realized with optical **fibers**. The core of this configuration are two 3x3 fiber splitters (usually called **tritters**). Along the tritters arms and in every user's station (see fig. 4.1), relative phases can be actively controlled by lithium niobate electro-optic phase modulators (PMs) driven by pulse generators. Thus, we can precisely govern the interference pattern at the setup outputs. The whole system is handled by computer software written in LabVIEW code. The configuration is Plug&Play-like (see sec. 3.1.3), in the sense that there is a mirror after the tritter system that reflects light back to the single photon detectors. This way, by a precise timings combination (see fig. 4.2), the pulses going through the long and short arms "exchange" paths in the way back, while the middle pulse travels through the medium arm twice. The main advantage is that, since there is no known way to build a true Plug&Play three-arms interferometer, at least two of them - i.e. the long and short ones - are automatically balanced, limiting the "manual" balancing to the medium arm only. Other standard fiber components employed are a circulator,

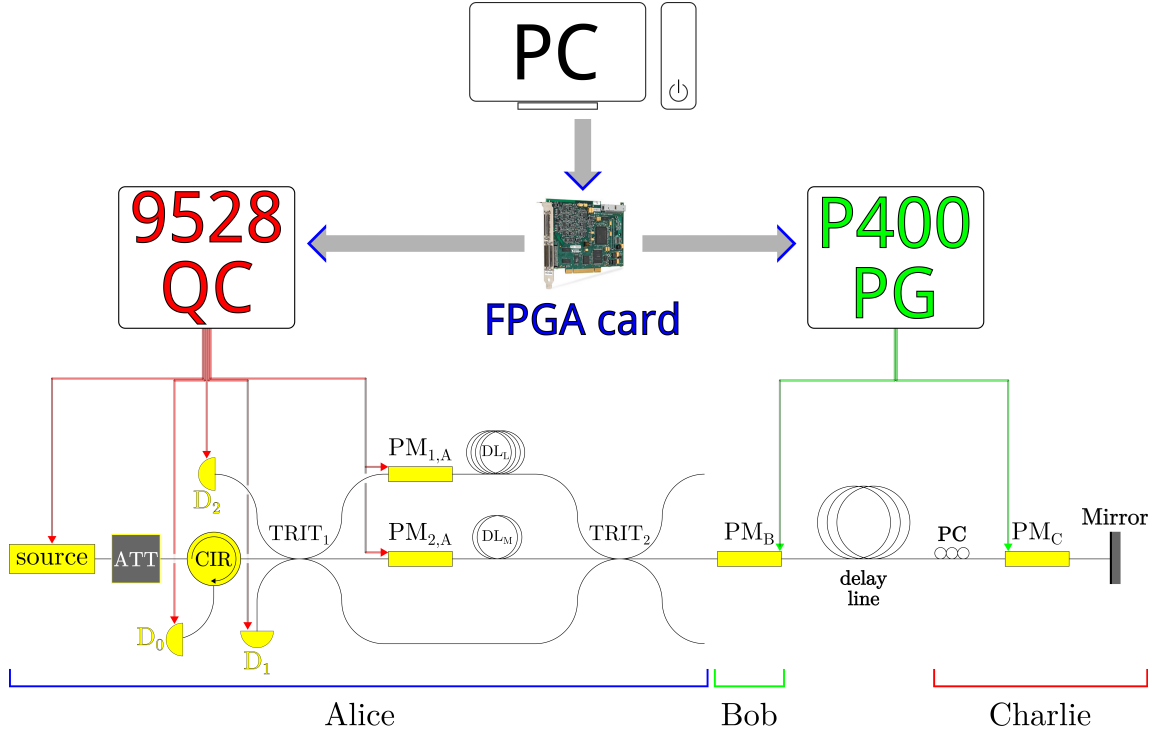


Figure 4.1: Setup used in this work. The components are: digital attenuator (ATT), circulator (CIR), two tritters (TRIT_1 and TRIT_2), phase modulators (PM), long and middle arms delays (respectively DL_L and DL_M), polarization controller (PC), Quantum Composer pulse generator (QC), P400 pulse generator (P400) and three single photon detectors D_0 , D_1 and D_2 .

a polarization controller and of course fiber connectors. The photon source is a 1550 nm externally triggered diode laser strongly attenuated to single photon level by a variable attenuator.

All the fibers except for a long delay line and the mirror are polarization maintaining, and only polarization maintaining arms of the tritters have been used.

We will now proceed with a more detailed walk through of the setup and a short description of the main components. In the following section we will describe the protocol presented in sec. 3.2.2 adapted to our configuration, and from a more experimental point of view.

After the desired transformations are set in the LabVIEW software, the PC sends them to an FPGA card, that triggers the Quantum Composer pulse generator (QC) and the P400 pulse generator (P400). The FPGA card also sets clock and frequency of every run. The QC then triggers the laser source. The pulse gets attenuated by the digital attenuator (ATT) enough to have 0.1 photons per pulse right after Charlie's station, and goes through the circulator (CIR) and to the first tritter (TRIT_1), where it is splitted in three. The pulse in the short (S) arm is our

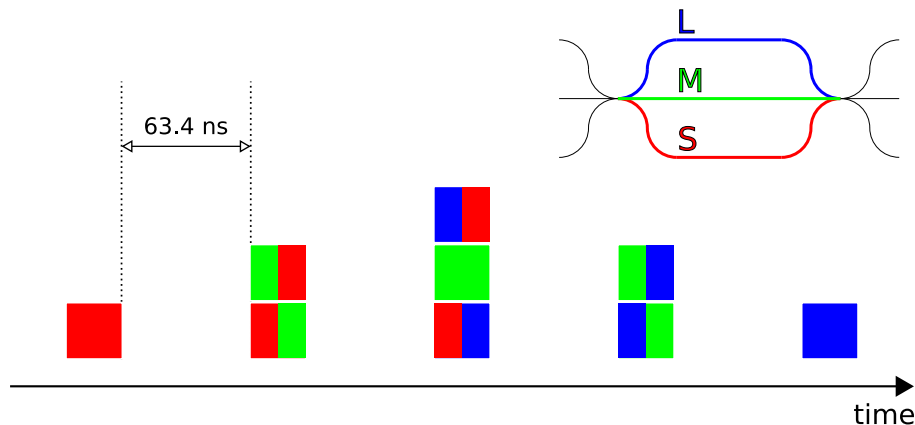


Figure 4.2: Pulses order at the interferometer output. Every square is a pulse, and its colors encode the arms the pulse has gone through, where red=short, green=medium and blue=long. For example, the square ■ represents a pulse that has traveled through the long arm in the way in and the short arm in the way out. Only the middle (composite) pulse is of our interest, since it contains the whole qutrit.

$|0\rangle$, the one in the medium (M) arm is $|1\rangle$ and in the long (L) arm we have $|2\rangle$. Delays DL_L and DL_M are respectively equal to (63.40 ± 0.05) ns and (126.75 ± 0.05) ns.

After the second tritter ($TRIT_2$) the three pulses go through the long single mode delay line ((244.02 ± 0.05) ns) which changes their polarization from horizontal to elliptical. Since the phase modulators (PM) have an horizontal polarizer at the output, a polarization controller (PC) after the long delay line changes polarizations back to horizontal, and the pulses get to the mirror and reflected. During the whole way to the mirror, all the PMs are off.

After the reflection, modulation starts: the FPGA card triggers the P400 that drives Charlie's PM first and then Bob's PM, according to the parameters we set in the software and at the perfect timing for every pulse. Each one of them is then splitted in three again by $TRIT_2$ and at this point the QC drives the voltages in Alice's PMs. The three pulses arrive at $TRIT_1$ at the same time and interfere. The QC now triggers the gated detectors that send a TTL pulse for every detection to the FPGA card that counts them.

It is worth noting that since the three pulses arriving at $TRIT_2$ on the way back get splitted in three again, in the end we will have **five** composite pulses coming out of the interferometer, as in fig. 4.2.

This "almost-Plug&Play" configuration has one main advantage over a Mach-Zehnder like setup, which would have an exact copy of Alice's tritter system at Charlie's station to make the pulses interfere: in our setup we only need $DL_L = 2DL_M$ in order to balance the interferometer. An other tritter system would need

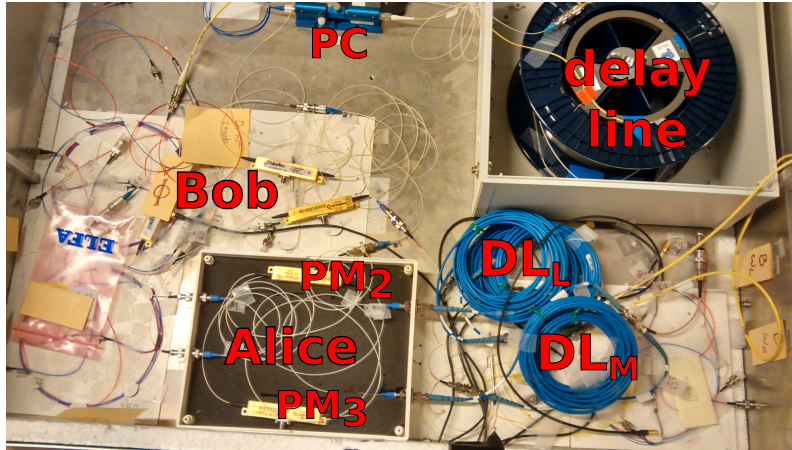


Figure 4.3: Photo of the setup in an early stage. For acronyms explanation see fig. 4.1

two more delay lines exactly identical (up to 1 cm - or 0.05 ns) to DL_L and DL_M .

In fig. 4.3 we reported a photo of the experimental setup during its realization.

4.1.1 Passive Optical Components

Optical Fibers

While most commercial and industrial fibers are *multimode* (MMF), in the quantum optics research field another type is more interesting, i.e. *single mode fibers* (SMF). These have a much thinner core (see fig. 4.4), and allow only one guided mode for signals having a wavelength close to the operational design (i.e. 1550 nm in our case).

A big problem with using fibers in the lab is silica **birefringence**. In fact, every

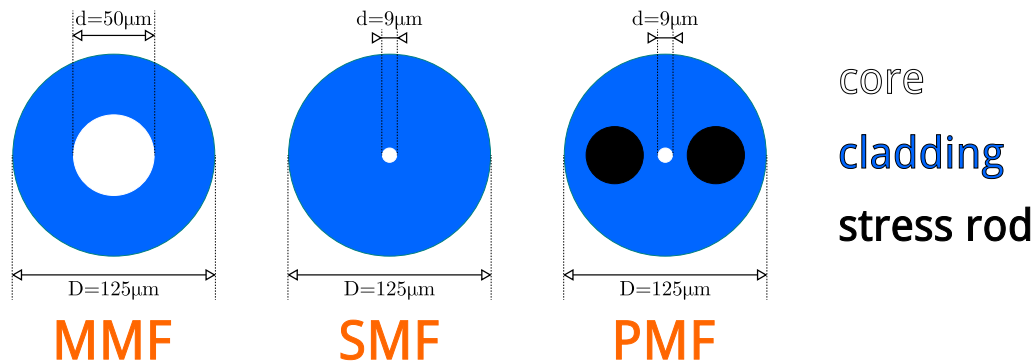


Figure 4.4: Longitudinal sections of different types of commercial fibers. The pictured PMF is called *Panda configuration* PMF, and it is the one we used throughout the whole setup.

fiber has fast and slow axes, and since their alignment depends on the stress induced on the core, polarization cannot be practically controlled. To solve this problem, a special kind of SMF has been invented, that is *polarization maintaining fiber* (PMF). PMFs have carefully localized defects (in the form of plastic rods aligned with the fiber cylindrical axis) in the cladding that cause strong stresses to the core, thus making external disturbances mainly negligible (see fig. 4.4). However, PMFs really preserve polarization only along the slow axis, therefore we need to align them carefully every time we make connections. More or less precise “mating sleeves” can help us doing this, but of course this problem will affect our interferometric visibility.

In our setup, we used only polarization maintaining 1550 nm fibers, except for the long delay line between Charlie and Bob and the mirror, which are normal SMFs (of course 1550 nm). Their polarization changes are canceled by a polarization controller on the way to the mirror and by Bob’s and Charlie’s horizontal polarizers at their PMs output on the way back.

Finally, we should say that modern SMFs have an average attenuation of 0.25 db/km, that is, intensities are halved every 12 kilometers. However in our setup, which falls way short of a kilometer, this attenuation is utterly negligible - also compared to basically every other component.

Circulator

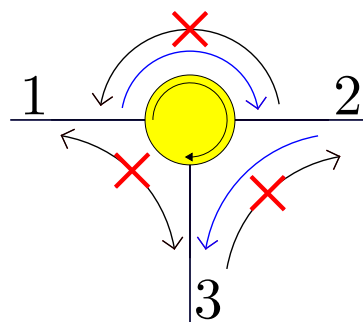


Figure 4.5: Fiber optics circulator.

An optical circulator (see fig. 4.5) is a three-ports device that directs light incoming from port i to port $i + 1$, while having very high attenuation rates (as high as an isolator, i.e. around 40 db) along the opposite way. For this reason, it is a non-reciprocal optical component, and is widely used in telecommunications.

In our setup, we used a polarization maintaining circulator from THORLABS (model CIR1550PM) with insertion loss equal to 0.9 db and 40 db isolation.

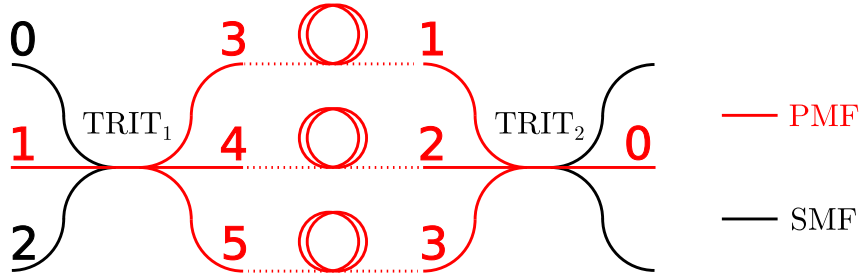


Figure 4.6: The two tritters used in the setup have 4 PM and 2 SM ports. Using them as in the picture allows us to have a PM qutrits source and measuring station.

Three-ports fiber couplers - Tritters

These couplers are a key component in our setup, as they materially create the qutrits and are responsible for the interference. They are basically made of three fiber cores fused together along a short distance, thus coupling EM fields from/into different ports. Due to energy conservation they introduce a $e^{\frac{i2\pi}{3}}$ relative phase shift between the outputs, as we have seen in sec. 1.2.3.

While those calculations referred to ideal tritters, i.e. with equal coupling efficiencies among the different ports and no insertion loss, real devices are slightly different, mainly in the latter condition. In particular we have used two tritters, again from THORLABS, with 4 PM ports and 2 SM ports each, as you can see in fig. 4.6.

Measured coupling ratios for the two tritters and the used ports (referring to fig. 4.6) are reported in each tritter data sheet. We list them in tab. 4.1.

Tritter	Input \rightarrow Output	Ratio
TRIT ₁	0 \rightarrow 3	33.39%
	0 \rightarrow 4	41.46%
	0 \rightarrow 5	25.15%
	1 \rightarrow 3	42.64%
	1 \rightarrow 4	23.33%
	1 \rightarrow 5	34.03%
	2 \rightarrow 3	25.65%
	2 \rightarrow 4	34.52%
	2 \rightarrow 5	39.83%
TRIT ₂	0 \rightarrow 1	36.54%
	0 \rightarrow 2	27.34%
	0 \rightarrow 3	36.12%

Table 4.1: Coupling ratios for the two employed tritters.

Of course these small differences in the ratios affect interference visibility and error rates, as equal intensities would be required to have good interferometric results. Unfortunately, the only way to fix this problem would be to have tritters with equal coupling ratios between every input-output pair. On the other hand, uniform insertion loss is not a problem in our case, since we need to attenuate the laser pulses anyway.

Polarization Controller

Having the same polarization is a crucial requirement for different light pulses to interfere. In our setup this is not a problem since every photon, on its way back to Alice's tritter system, goes through Bob's PM, inside which there is a horizontal polarizer that simply kills the vertical component, so that only horizontally polarized light interferes in TRIT₁¹

However for this reason, if photons arriving at these polarizers are vertically (or close to vertically) polarized, they will be almost completely deleted by them, and as the setup is already attenuating a lot by itself, we would like to avoid this. This is why we put a polarization controller next to the long SMF, which is by far the most polarization-changing object in our experiment.

The particular PC we adopted is from OZ Optics (model HFPC-11-1550-S-9/125-SCSC), and it consists of a short fiber length (0.39 ns) on which you can easily apply stress from any angle along its longitudinal section. These PCs are specifically built to make elliptically polarized light, coming from a SMF, linearly polarized in order to inject it into PMFs.

Mirror

We employed an extremely simple retroreflector from THORLABS (model P1-SMF28ER-P01-1) with one meter (5.07 ns) SMF tail. It has a minimum reflectance of 97.5%.

4.1.2 Active Optical Components

Laser Source

As we said before, the ideal case scenario in quantum communication would be to use true single photon sources, which are still being researched. In the meantime, the common solution is to use pulsed weak lasers attenuated well below the single photon level.

¹Actually, DL_L and DL_M are made of many fibers, therefore several connectors can somehow slightly alter the horizontal polarization, again affecting visibilities and error rates.

In our work, we have employed a source which has actually been designed appositely for this task: it is a 1550 nm laser diode (model ID300) made by ID Quantique (one of the few firms that industrially produces QKD systems), externally triggered, that generates 1 mW pulses with FWHM $\simeq 500$ ns, and can be triggered at up to 500 MHz. In our experiment we have used two different trigger frequencies: a slower one, 3 kHz, for manual calibration of the interferometer (we will talk about its phase drifting in a while), and a faster frequency, equal to 70 kHz, for the communication. This limited frequency is due to the relatively slow FPGA card, which has long rise times for digital outputs, approximately 200 ns.

Light coming out from the laser is horizontally polarized, that is, aligned to the slow axis.

Attenuator

As we said before, a coherent light source as a laser can approximate a single photon source if its emissions are strongly attenuated.

In that situation, the photon number distribution is Poissonian (see sec. 2.2.3), that is the probability for a pulse with \bar{n} photons averagely to contain n of them is

$$P(n) = e^{-\bar{n}} \left(\frac{\bar{n}^n}{n!} \right) . \quad (4.1)$$

In our case we chose to attenuate until we had $\bar{n} = 0.1$ (which is the usual choice in the field) at the position in the setup where security against eavesdropping is needed, that is after Charlie's PM in the way back, after reflection and Charlie's modulation. At this intensity level we have the following probabilities

$$\begin{aligned} P_{\bar{n}=0.1}(0) &= 0.905 \\ P_{\bar{n}=0.1}(1) &= 0.090 \\ P_{\bar{n}=0.1}(n > 1) &= 0.005 , \end{aligned} \quad (4.2)$$

i.e. approximately one every ten pulses contains a single photon and around 5% of these have more than one. It is now very clear why this attenuated laser source is a big limitation for secure communication systems.

In our case, we have employed a digital variable attenuator from OZ Optics (model DA-100-SC-1550-9/125-P-50). It has -1.6 dB insertion loss, 2.11 ns insertion delay and can attenuate an additional 0.00 dB to -60.00 dB in 0.01 dB steps with ± 0.03 dB accuracy.

Depending on small changes in the setup, we set attenuation values from ranging from -18.00 to -22.00 dB. As the desired intensity level is clearly too low to be measured with any power meter or oscilloscope, to set the right values we measured

attenuations from different parts of the setup separately and we checked final intensities at the single photon detectors, considering that they have 20% detection efficiencies. However, since in this work we were not aiming for the best generation rate possible, we considered the $\bar{n} = 0.1$ level as an upper bound, so that experiments were run even if we were slightly below this intensity.

Phase Modulators

In our case, modulating the phase of a photon roughly means changing its velocity while keeping the same path lengths. This can be done by modifying the medium refractive index, which is easily obtained in materials exhibiting the electro-optic effect, as lithium niobate. This effect consists in the (linear in the lithium niobate case) dependence of the refractive index on the strength of the local electric field. Therefore, if we put a parallel plates capacitor along the propagating direction, its field will be proportional to the potential we apply, thus the angular modulation is proportional to the voltage. We can clearly see this dependence in the calibration plot in fig. 4.9.

The PM we used are made by JDSU (model APE PM-150-005) in lithium niobate, and they all have the same calibration. They work with DC voltages at up to 500 MHz repetition rates, and have 3.5 dB insertion loss and PMFs of different lengths. Since the phase modulation is polarization dependent, they all include a horizontal polarizer (aligned to the PMF slow axis).

We should say at this point that Bob's and Charlie's stations actually include two PMs each because of timing reasons. However, nothing changes by imagining every pair as a single PM.

4.1.3 Electronic Devices

FPGA Card

Communication between the controlling software and the experimental hardware is carried out by a Field Programmable Gate Array board. This is an integrated circuit that can be programmed after manufacturing via computer. Our card is the PCI-7833R, sold by National Instruments and whose FPGA circuit is manufactured by Xilinx. It has 8 analog inputs, 8 analog outputs and 96 digital input/outputs, and an internal clock working at 40 MHz and multiples, depending on the gate programming required.

We used an 80 MHz clock, which means that the best time resolution our software can have is $\frac{1}{80} = 12.5$ ns. This, together with the fact that the analog outputs are relatively slow (around 1 μ s rise time) and have low currents, is the reason why we

used “standard” pulse generators to trigger laser and detectors and to drive the PMs (that have high input impedance).

Quantum Composers delay pulse generator

The 9528 Digital Delay Pulse Generator manufactured by Quantum Composers is an 8 channels voltage generator that can provide standard digital and variable analog voltages with a time resolution of 250 ps and 200 ps jitter. It can be externally triggered and can operate at up to 20 MHz.

We triggered the 9528 with the FPGA card and we employed four channels to (digitally) trigger laser and detectors, and two channels to drive Alice’s PMs with analog voltages.

While this pulse generator has plenty of options, its major drawback is the rise time of the analog output signals, which is around 100 ns. Since qutrits created by Alice are made of three 63.4 ns apart pulses, this pulse generator is clearly not an option for the sequential modulation that Bob and Charlie are doing. Besides, the 9528 is two channels short of what we need for these users. These are the reasons why we used two additional pulse generators.

P400 delay pulse generator

The Highland Technology P400 delay and pulse generator is an extremely precise 4-channels device that can produce digital and analog voltages at 10 MHz with a jitter of only 25 ns. Widths and delays are adjustable for every output with 1 ps resolution and voltages can be set from -5.0 to 11.8 V. The most astonishing feature is the analog output rising time, which is equal to 2 ns from 0 to 11.8 V, thus making it the ideal candidate for sequentially modulating qutrit pulses at Bob’s and Charlie’s stations.

For timing reasons, we employed two P400s, one to perform ω phase shifts and the other for ω^2 . They were both triggered by the FPGA card.

Single Photon Detectors

The technologically most advanced devices employed in this experiment are the three PGA-600 single photon detectors manufactured by Princeton Lightwave. Since silicon photodetectors are insensitive in this wavelength region, the PGA-600 include an InGaAs diode. But this alone is not enough to detect 1550 nm single photons: the diodes are also biased above their breakdown voltages for a very short period - 1 ns - every time the detector is triggered and a photon is expected. This technique allows the device to reach 20% detection efficiency, but also causes so called *dark counts*,

which are fake detections due to avalanches started by the diode carriers. By cooling down the detectors to 218 K dark counts are extremely reduced (below $5 \cdot 10^{-5}$ per trigger), but considering the fact that we have one photon leaving Charlie's station every ten triggers and all the following attenuation, even a low number of dark counts can considerably affect the final error rate, as we will quantitatively see in the following section.

Our three photodetectors are externally triggered by the Quantum Composer and every time a detection happens, they send a TTL pulse to the FPGA card that stores it for the analysis.

4.1.4 LabVIEW Software

In order to easily and automatically control most of the parameters in the experiment, We have written some software in LabVIEW code. This programming language makes communication between computer and instruments way easier than other more generic coding languages, since many devices drivers can be downloaded from the web and used more or less right away. However, the price for this simplicity is flexibility, as usual: the available functions and methods that can be implemented are predetermined and not infinite, and a software often needs some serious upgrading every time the setup - or the analysis - is changed. Besides, as code optimization is automatically carried out by the compiler, it can sometimes be far from perfect. Still, a good LabVIEW software can easily take care of everything, from the (pseudo) random numbers generation to the QTER calculation. To give an idea of how this language really is easy to use, suffice it to know that the whole software controlling the experiment has been written in something more than a month, starting from no knowledge of the code whatsoever.

Since timing requirements are way too strict for a common operating system (Windows and Unix have approximately 1 ms time resolutions), the input and output settings cannot be controlled by the workstation in real time. This is why the software is divided in two main programs that we may call *host-software* (HS) and *FPGA-software* (FS). The main difference as you may guess is that the HS runs in the computer, while the FS is run by the FPGA card. Slightly less roughly, they work in the following way:

1. After the user has set the desired parameters in the graphical interface of the HS, this part sends them to the FS through a FIFO (First-In-First-Out) memory buffer. Due to this buffer limited resources, the settings for a maximum of 70000 runs (i.e. 70000 laser and detectors triggers) can be stored each time.
2. The FS runs the experiment and gets from the FPGA card inputs the signals

from the detectors, storing them in an internal register.

3. After the 70000 runs are finished, the FS returns to the HS the raw data, which can now be securely stored in the computer memory.

Steps 1 – 3 are called a *loop*.

4. New loops are carried out as many times as the user has initially set. Once all of them have been executed, the HS performs the analysis required to calculate the QTER, plus some other significant results.

In fig. 4.7 we can have a look at the HS graphical interface.


<p>"Real" EXP</p>  <p>Controlled Case EXP</p>		<p>Deterministic Runs 0</p> <p>Random Runs 0</p> <p>Det/Random 0</p> <p>Generation Ratio 0E+0</p>
<p>Runs/loop 70000</p>	<p>Loops 1</p>	<p>Total 0</p>
<p>OFF</p>		<p>Write to file D:\Mas...\test.lvm</p>
<p>Max number of runs/loop → FIFOs depth 70000</p> <p>SLOW Gate [Ticks] 25000</p> <p>FAST Gate [Ticks] 6000</p>	<p>TRIGGER</p> <p>QC delay [Ticks] 0 QC ON time [Ticks] 0 Oscilloscope delay 0 Osc trig ON [Ticks] 0</p>	
<p>Alice PM</p> <p>Alice's Case 0</p> <p>C-Zero [Volts] 0 D-Zero [Volts] 0 C-setting [Volts] 0 D-setting [Volts] 0</p>	<p>B&C PM</p> <p>B&C Case 0</p> <p>Bob delay [Ticks] 2546 2-3 peaks delay [Ticks] 3 B<-->C delay [Ticks] 384</p>	<p>TRIT 0</p> <p>QTER</p> <p>0 - CIR_Counts 0 1 - APD1_Counts Correct Meas. 0 2 - APD2_Counts Wrong Meas. 0</p>

Figure 4.7: Graphical interface of the controlling software.

4.2 Three Users QSS with Qutrits - The Protocol

Knowing something more about the setup, we can now specify the protocol presented in sec. 3.2.2 for this experimental configuration.

For stability reasons, we have used three dimensional systems (**qutrits**), i.e. the lowest possible dimensionality the qudits protocol allows. Moreover, we realized our proof-of-principle for three parties, just enough to have secret sharing.

First of all, let's analyze how our choices change the general formalism.

• Three dimensional systems - qutrits

- Using qutrits implies adopting MUBs for three dimensions, for example matrices M_2 , M_3 and M_4 in eq. (2.47), since M_1 cannot be used for interferometric setups.
- From eqs. (3.8) and (3.10) we find for three dimensions

$$\hat{X}_3 = \sum_{m=0}^2 \omega^m |m\rangle\langle m| = |0\rangle\langle 0| + \omega|1\rangle\langle 1| + \omega^2|2\rangle\langle 2| \quad (4.3)$$

for the “vector changing” operator, and

$$\hat{Y}_3 = \sum_{m=0}^2 \omega^{m^2} |m\rangle\langle m| = |0\rangle\langle 0| + \omega|1\rangle\langle 1| + \omega^4|2\rangle\langle 2| \quad (4.4)$$

for the “basis changing” operator.

- In the key-sifting part (step 5 in the qudits protocol in sec. 3.2.2), the condition for a valid run in eq. (3.15) becomes

$$\sum_{n=1}^N y_n = 0 \pmod{3}. \quad (4.5)$$

- $\mathbf{y}_n = \{\mathbf{0}, \mathbf{1}\} \quad \forall n = \{1, \dots, N\}$. This of course reduces the number of possible (x, y) pairs every party can apply, from nine to six. From a more practical point of view, the main consequence is a smaller fraction of valid runs, from $\frac{1}{3}$ to $\frac{1}{4}$, since there are less possibilities to satisfy condition (4.5), thus resulting in a slightly lower generation rate.

You may be wondering what the reason for this apparently pointless limitation is! Everything will be clearer as soon as we will have explained what “applying (x, y) ” practically means, but for now suffice it to know that more (x, y) pairs possibilities means more (classical!) computational resources needed by the controlling software, and this increase is exponential in the number of pairs. This experiment being a proof of concept, we are more interested in the physics,

that is showing the validity of the protocol which in principle is not changed by this limitation, than having high generation rates, rather a technological issue.

- **Three parties:** considering the previous choice, the consequence of having three users is that the condition for a run to be valid becomes

$$\sum_{n=1}^N y_n \in \{0, 3\} \quad (4.6)$$

that is, either all parties have $y = 0$ or they all have $y = 1$.

We can now present step-by-step the scheme we used in our experiment, in a more explicit and experimental way than in sec. 3.2.2.

The exposition will refer to our setup, shown in fig. 4.1.

1. Alice, who plays the role of the *distributor*, **prepares** a qutrit in the initial state

$$|\psi_0\rangle = \frac{1}{\sqrt{3}} (|0\rangle + |1\rangle + |2\rangle) \quad (4.7)$$

2. Charlie, Bob and Alice generate each the two independent random numbers $x_i \in \{0, 1, 2\}$ and $y_i \in \{0, 1\}$ where $i = C, B, A$ stands for the user's name initial. Then, sequentially and in $C \rightarrow B \rightarrow A$ order, they act with the operator $\hat{X}_3^{x_i} \hat{Y}_3^{y_i}$. To understand better how these operators action practically works, we can start by writing down explicitly all the possible combinations for each party, since there are only six of them:

$$\begin{aligned} (x, y) = (0, 0) &= \hat{X}_3^0 \hat{Y}_3^0 = \mathbb{1}_3 \mathbb{1}_3 = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| \\ (1, 0) &= \hat{X}_3^1 \hat{Y}_3^0 = |0\rangle\langle 0| + \omega|1\rangle\langle 1| + \omega^2|2\rangle\langle 2| \\ (2, 0) &= \hat{X}_3^2 \hat{Y}_3^0 = |0\rangle\langle 0| + \omega^2|1\rangle\langle 1| + \omega|2\rangle\langle 2| \\ (0, 1) &= \hat{X}_3^0 \hat{Y}_3^1 = |0\rangle\langle 0| + \omega|1\rangle\langle 1| + \omega|2\rangle\langle 2| \\ (1, 1) &= \hat{X}_3^1 \hat{Y}_3^1 = \omega|0\rangle\langle 0| + |1\rangle\langle 1| + \omega|2\rangle\langle 2| \\ (2, 1) &= \hat{X}_3^2 \hat{Y}_3^1 = \omega|0\rangle\langle 0| + \omega|1\rangle\langle 1| + |2\rangle\langle 2| \end{aligned} \quad (4.8)$$

with $\omega = e^{\frac{i2\pi}{3}}$. Since the three computational states ($|0\rangle, |1\rangle, |2\rangle$) are separated in time (see the next section for more details), every user can actually perform the phase shifts on every one of them separately and sequentially. For example, suppose Charlie generated the pair (1, 0); he will

- (a) do nothing to the first ($|0\rangle$) pulse
- (b) apply an $\omega = e^{\frac{i2\pi}{3}}$ phase shift to the second ($|1\rangle$)

(c) apply an $\omega^2 = e^{\frac{i4\pi}{3}}$ phase shift to the third ($|2\rangle$).

How to phase shift these light pulses? What you need to do is either change the path length or change the refractive index of the medium. Of course the best (and the only practically feasible in fibers) way to do it is the latter, and we achieved it with commercial phase modulators, as we described in sec. 4.1.2.

3. After all three parties have applied their own transformations, Alice obtains the final state

$$|\psi_f\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^2 \omega^{\sum_{i=C,B,A} (kx_i + k^2 y_i)} |k\rangle \quad (4.9)$$

on which she **performs a measurement** in basis M_2 , that is explicitly

$$M_2 = \left\{ \begin{array}{l} \frac{1}{\sqrt{3}} (|0\rangle + |1\rangle + |2\rangle), \\ \frac{1}{\sqrt{3}} (|0\rangle + \omega|1\rangle + \omega^2|2\rangle), \\ \frac{1}{\sqrt{3}} (|0\rangle + \omega^2|1\rangle + \omega|2\rangle) \end{array} \right\}, \quad (4.10)$$

with the tritter on the left in fig. 4.1 (TRIT_1)², getting the outcome $a \in \{0, 1, 2\}$.

4. Now Alice should announce the outcome publicly, then the three parties would randomly disclose some of their y_i and the non-valid runs would be discarded. But since this experiment is a proof of principle, we physicists working in the lab need to know everything in advance, in order to prove the principle indeed! So, at this point there are two possibilities:

(a) Condition

$$\sum_{i=C,B,A} y_i \in \{0, 3\} \quad (4.11)$$

is satisfied and the run is *valid*. Then if the measurement result is actually the same as predicted by equation

$$\sum_{i=C,B,A} x_i = a \pmod{3}, \quad (4.12)$$

we label the run as *correct*, otherwise as *wrong*.

(b) Equation (4.11) is *not* satisfied. The outcome is then *random*, and we label it that way.

²For a precise description of how a tritter works, see sec. 1.2.3 and [13]

5. We rerun the experiment many times from step 1 to step 4 with the **same** $(\mathbf{x}_i, \mathbf{y}_i)$ **settings** for every party. If case (a) in the previous step was true, then we should have only valid runs, and we can proceed on calculating the *qutrit error rate* as

$$QTER = \frac{[\textit{wrong runs}]}{[\textit{valid runs}]} = \frac{[\textit{wrong runs}]}{[\textit{correct runs}] + [\textit{wrong runs}]} . \quad (4.13)$$

Otherwise, if case (b) was true, we have only *random* runs, and we can just check if probabilities are actually uniformly $\frac{1}{3}$ for every detector by comparing outcome counts.

6. Whenever we set transformations that produce valid runs, if the obtained QTER is below 15.95% (see [4]), it means that the experiment was successful, i.e. **we could detect any eavesdropping while doing secret sharing** with this setup and protocol.

After a brief discussion of the most important devices used throughout the experiment, we will proceed with results presentation and some comments.

4.3 Results and Analysis

4.3.1 Phase Modulators Calibration

The first measurements we performed was the PMs calibration. To take these measurements we employed a very simple Plug&Play setup, as in fig. 4.8. This setup, completely polarization maintaining, is extremely stable (as we have said in sec. 3.1.3), thus making for an ideal calibration benchmark.

The measurements confirmed our expectation that all our PMs are identical. For this reason, we will report only one calibration. The results, taken using a LeCroy WaveMaster 8300A oscilloscope, are plotted in fig. 4.9.

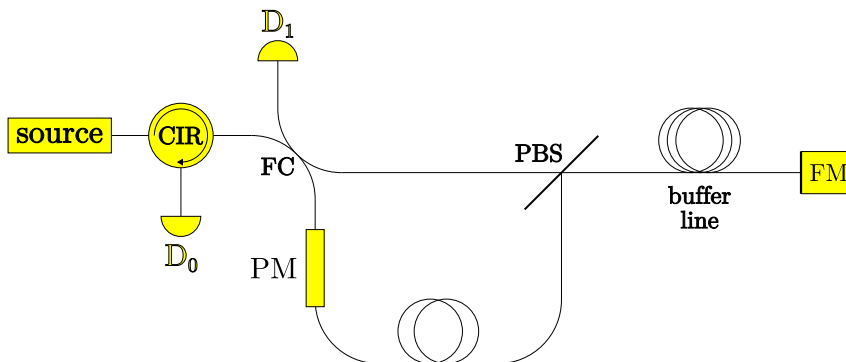


Figure 4.8: Plug&Play setup used for PMs calibration.

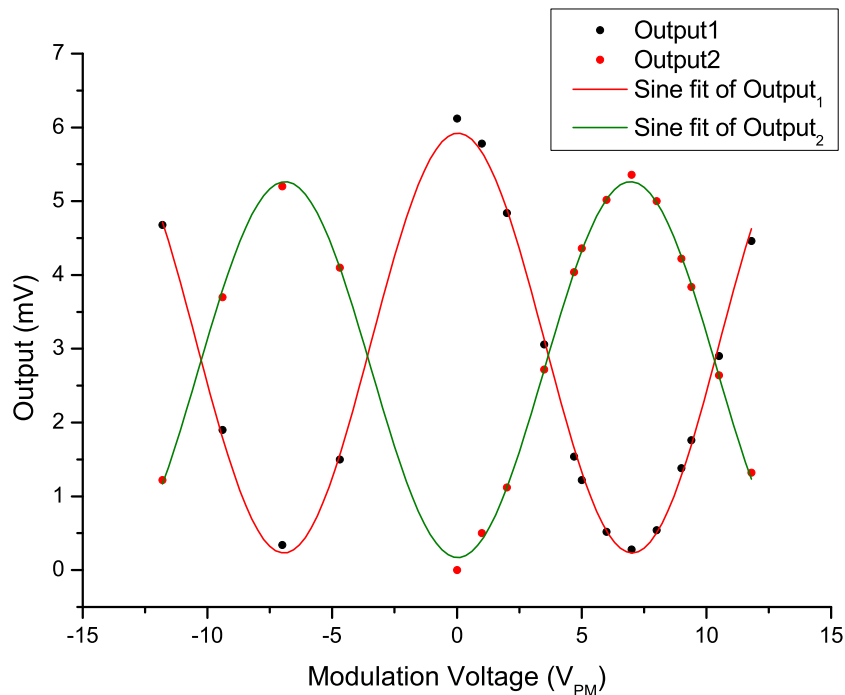


Figure 4.9: Amplitude vs. modulation voltage plot for one of the PMs. The angular phase shift is clearly linear in the voltage. Sinusoidal fitting curves are also plotted.

From the sinusoidal fitting, we obtained the period of the phase shifting in volts, which is equal to (13.97 ± 0.07) V. Therefore, the voltages needed to perform the ω and ω^2 phase shifts are

$$\begin{aligned} \varphi_{\omega} = \frac{2\pi}{3} &\rightarrow \Delta V_{\omega} = (4.66 \pm 0.02) \text{ V} \\ \varphi_{\omega^2} = \frac{4\pi}{3} &\rightarrow \Delta V_{\omega^2} = (9.31 \pm 0.05) \text{ V} . \end{aligned} \quad (4.14)$$

It is worth pointing out that these voltages uncertainties produce angular errors, in the phase shifts, that are fractions of a degree. These quantities are absolutely negligible compared to the errors introduced by all the factors we are going to describe in a moment, thus they will simply be neglected.

4.3.2 Qutrit Error Rates

There are $(3 \cdot 2)^3 = 216$ possible (x_i, y_i) pairs combinations for three parties. We report in tab. 4.2 some results which, as you will see, are quite similar among each other. In the table, a is the expected measurement outcome, $C_{i=0,1,2}$ are counts in detector i , QTER are calculated with the formula in eq. (4.13), and generation rates (R) are simply ratios between total counts and total running time.

Every measurement consisted in 10 loops with 70000 runs each, and lasted 30

(x_A, y_A)	(x_B, y_B)	(x_C, y_C)	a	C_0	C_1	C_2	QTER	R[trits/s]
(0, 0)	(0, 0)	(1, 0)	1	15	243	15	10.99%	9.1
(0, 0)	(0, 0)	(2, 0)	2	14	15	246	10.58%	9.2
(0, 0)	(1, 0)	(0, 0)	1	10	182	10	9.90%	6.7
(0, 0)	(1, 0)	(1, 0)	2	7	14	190	9.95%	7.0
(0, 0)	(1, 0)	(2, 0)	0	232	19	5	9.37%	8.5
(0, 0)	(2, 0)	(0, 0)	2	9	16	233	9.69%	8.6
(0, 0)	(2, 0)	(1, 0)	0	292	13	23	10.98%	10.9
(0, 0)	(2, 0)	(2, 0)	1	14	228	12	10.24%	8.5
(0, 1)	(0, 1)	(0, 1)	0	228	3	23	10.24%	8.5
(0, 1)	(0, 1)	(1, 1)	2	15	11	231	10.12%	8.6
(0, 1)	(0, 1)	(2, 1)	1	14	270	19	10.89%	10.1
(0, 1)	(1, 1)	(0, 1)	2	14	13	239	10.15%	8.9
(0, 1)	(1, 1)	(1, 1)	1	8	204	16	10.53%	7.6
(0, 1)	(1, 1)	(2, 1)	0	225	20	6	10.36%	8.4
(0, 1)	(2, 1)	(0, 1)	1	15	239	13	10.49%	8.9
(0, 1)	(2, 1)	(1, 1)	0	220	7	19	10.57%	8.2
(0, 1)	(0, 0)	(1, 1)	random	54	57	40	—	—
(0, 1)	(0, 0)	(0, 1)	random	40	49	67	—	—
(0, 1)	(1, 1)	(1, 0)	random	44	45	66	—	—
(0, 0)	(1, 1)	(0, 1)	random	61	61	72	—	—

Table 4.2: Some measurement results. QTER is not defined if the expected measurement outcome is random, and the generation rate is clearly zero in that case, since in a real secret sharing application all these runs would be discarded.

seconds³ (see sec. 4.1.4).

From the measurements reported here it is clear that not only that the protocol presented in sec. 4.2 works, but also that **real secret sharing tasks with this setup are possible**, since no measured QTER reaches the 15.95% security threshold [4], and actually they all are **below 11%**. These results are similar to those in entanglement-based qutrits experiments [5]. In the next paragraphs we will comment the data and try to understand what the reasons could be for our QTER to deviate from the ideal 0%.

³We have said before that the laser trigger frequency was 70 kHz. This stands correct, but due to computer elaboration time, there is a small time gap (of around two seconds) between loops, thus lowering the average frequency of a measurement.

Phase Drift

The main experimental problem any interferometer presents is a never stopping phase drift. This causes the interference pattern to move without any apparent external cause.

However, we need to consider that the light wavelength is - in our case - 1550 nm, and few nanometers changes in the paths length differences can be noticed with bare eyes in the interference pattern.

The main reasons for these small length changes are temperature fluctuations and mechanical stresses (as vibrations). Necessary countermeasures, adopted throughout the whole experiment, consist in putting the whole tritter system inside an aluminum box thermally shielded with Styrofoam, and placing this box on a stable optical table. These expedients allowed, some 20 minutes after the box closure, to have a more stable system.

During measuring sessions, it took the system around 10 minutes to make a full 2π phase shift due to this drift. Now, to evaluate the consequences of this systematic error on the QTER, we can think of it as a change in the relative phase (i.e. angle) between the three arms. Considering that every measurement lasted 30 seconds, 10 minutes for a 2π phase shift correspond to an 18° change during one measurement. If we put this value in eqs. (2.40) and calculate the probabilities, we get a QTER of approximately 2.2%.

While a bit roughly, this clearly labels this “natural” phase drift as the main systematic contribution to our error, thus making it the most eminent problem to solve in the future. Actually, good solutions have already been found and partially implemented [36], but need to be upgraded and optimized for every particular case. They basically consist in a PID (proportional-integral-derivative) controller that automatically adjusts the voltage in PMs to keep the system stable. Precisely this adjustment leads us to the next problem.

Calibration

Because of the above-mentioned phase drift intrinsic to the system, there was a necessary procedure to do before every measurement that can be called *calibration*. This consists in changing the phases until, without any additional transformation, we had a maximum of interference in detector 0 and minima in the other two. We set this situation as our “no modulation” starting point, and run the protocol once thereafter. Since both phases and voltages are relative, nothing changes in the formalism, and measurements of course confirmed this. However, due to the drift, this calibration process cannot take too long, thus it is not perfect. To make it faster, we reduced the attenuation in order to see higher count differences, since

probabilities don't change between classical and quantum regime anyway (compare eqs. (1.14) and (2.40)). Still, due to intensity fluctuations the maxima and minima could be found with a limited precision, also because the intensity curve derivative is zero at these points. To quantitatively evaluate this calibration error, we can consider the fact that during this process, we could not distinguish a maximum (or minimum) up to a voltage variation of $\pm 0.5V$, that correspond to $\simeq \pm 13^\circ$. This is another a systematic error that affects our interferometric visibility. To quantify it we can, as before, calculate the QTER given by the probabilities in eqs. (2.40) with this angular shift. We get a contribution to our QTER equal to 1.1%.

Therefore, this is an other relevant issue in the experiment. It can be partially solved by using a PID circuit as we mentioned in the previous paragraph, but the underlying cause, which is those intensity fluctuations, is intrinsic to any fiber system and is probably due to mechanical stresses and temperature fluctuations that slightly change the single mode fiber birefringence, thus changing the polarization arriving at the polarizers inside the PMs. These fluctuations are also the reason behind the slightly different generation rates in tab. 4.2.

Dark Counts

In sec. 4.1.3, when we described single photon detectors, we mentioned that they suffer from so-called dark counts, that are basically counts without photons, due to the above breakdown threshold bias. These counts represent a systematic error, and are independent of any laser. We measured their probability by running 50 loops (i.e. $50 \cdot 70000 = 3.5 \cdot 10^6$ runs) with the laser off, and we obtained 1 count per loop, that is approximately $1.4 \cdot 10^{-5}$ dark counts per trigger. This is in agreement with what is written in the data sheets of our detectors (whose values range from $1.3 \cdot 10^{-5}$ to $1.8 \cdot 10^{-5}$).

Considering again a typical case of 200–10–10 counts and QTER= 9%, subtracting dark counts would give us 199 – 9 – 9 counts and QTER= 8.29%, that is 0.7% less. In conclusion, this is an important issue too. However, this problem cannot be solved without using different types of single photon detectors, which are still not commercially available. Nonetheless, we should consider that dark counts are constant and independent of the working frequency, thus setting it higher, or simply reducing the setup attenuation rate, would lower their weight in the final result.

Interfering Polarizations and Intensities

Finally, two problems regarding the tritter may affect our interference quality. In order to have perfect patterns, interfering light pulses must have the same polarization and same intensities. With regards to polarization, we should point out

that there are many fiber connectors in both the medium and long arms. These connectors, as we said before, may easily have small misalignments from the PMF axis, thus leading to small polarization changes due to birefringence. This problem can be solved by substituting all these sequential fibers with a single one of the needed length.

On the other hand, intensities differences are caused by the slightly unequal coupling ratios between tritters inputs and outputs (see tab. 4.1). To solve this, we would need to use perfectly balanced tritters, which are hardly possible to find.

Chapter 5

Conclusions

5.1 Achievements

In this work, we have carried out a proof-of-principle experiment that has shown the possibility to achieve secret sharing tasks with qutrits and a single photon, with phase encoding, for the first time to our knowledge.

Our optical interferometric setup is entirely based on fibers, in order to make that possibility more realistically implementable with current fiber telecommunication networks.

In addition, this thesis work included extensive LabVIEW programming. The written software not only run the experiment while setting many protocol parameters, but also carried out most of the data analysis, as errors and rates calculation.

We have obtained secret sharing with error rates below 11%, that is quite far from the maximum security bound of 15.95%, and comparable to results found in literature [5]. This definitively proves that our setup can be employed for secure secret sharing tasks.

Above all, however, our protocol has some crucial advantages over other realizations based on entanglement. For example, with our setup we can easily extend our configuration to as many parties as we want, at the only price of signal attenuation, while in the entangled version more users means entangled states with more particles, whose generation is still an experimentally researched issue. On the other hand, the single particle scheme shows a definitive superiority in detection efficiency. In fact, as we mentioned before, entanglement-based protocols need three detectors per user (at least with three dimensional systems), and for a run to be considered valid every one of them needs to detect a photon with one of his three detectors (that is, perform a measurement and get any outcome). Supposing now that these detectors have an efficiency equal to η (where $\eta \sim 20\%$ in the best case scenario), then this probability scales as η^N , where N is the number of parties.

In our single particle scheme instead, only one user (Alice in our experiment) performs the measurements, thus the abovementioned probability is always proportional to η , independently of the number of parties. This makes our protocol extremely more scalable compared to the other proposals.

Finally, beside secret sharing, other security problems can be experimentally addressed with this same setup, for example the Byzantine Agreement and the Communication Complexity protocols. Therefore, many good results can be achieved with this configuration.

5.2 Future Improvements of the Setup

The fact that this experiment turned out to be successful represents a new place where to start from in order to achieve real secure QSS. Indeed, at the time of this writing, an upgraded version of the setup with a long delay between Alice and Bob is being realized and characterized.

However, to fulfill our dream of unconditionally secure secrets in everyday life, some improvements are still needed, as we have seen in chapter 4.

First of all, many kilometers of fibers would separate each user from the others, thus a far better phase stability control is needed. PID softwares could be a good solution to this problem.

Another great limitation that this experiment shared with every other in the quantum communication field is the photon source. In fact, our results indicate secure communication only if we suppose to have had exclusively single photons modulated in every run. To avert this security breach, we lowered the intensity to very low values, much below the single level. This of course highly limit the generation rate, thus giving more weight to the dark counts problem.

Talking about generation rates leads us to the discussion of a main part of our work, that is LabVIEW coding. While it proved to be very simple, powerful and reliable, this programming environment has also imposed some serious constraints on the experiment. For example, its low time resolution has made us use the P400 pulse generators to drive Bob's and Charlie's phase modulators, while Alice's ones had to be controlled by the much slower 9528 Quantum Composer pulse generator, thus lowering the maximum working frequency. Apart from code optimization, an integrated circuit specifically realized for the experiment, or at least less generic than an FPGA card, would probably result in much higher performances.

Another constraint to the generation rate which is shared among all quantum communication protocols is the detecting efficiency. InGaAs avalanche diodes are the best commercially available single photon detectors in the 1550 nm wavelength

region, nevertheless they have a very big drawback in the relatively low 20% efficiency. Groups all around the world have been studying and realizing prototypes of a new type of superconducting single photon detectors, that can reach outstandingly high efficiencies for these wavelengths, even more than 90%, while working at above-GHz frequencies [37].

Last but not least, it should be reminded that secret sharing and QKD protocols at some point all require, in general, random numbers generation, and that this needs to be genuinely random to make the communication secure. In our experiment we generated these numbers with pseudo random codes in the computer, while a real QSS implementation would need for example a quantum random number generator.

Hopefully, in a near future, this work will help in making secure quantum communication the standard way to exchange sensitive information, thus taking the amazing world of quantum mechanics one step closer to non-specialists curious enough to learn it.

Bibliography

- [1] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Proc. of IEEE Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.
- [2] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.*, 113:190501, Nov 2014.
- [3] Jan Bogdanski, Nima Rafiei, and Mohamed Bourennane. Experimental quantum secret sharing using telecommunication fiber. *Physical Review A*, 78(6), 2008.
- [4] Nicolas Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(12), 2002.
- [5] A. Vaziri G. Weihs A. Zeilinger S. Grblacher, T. Jennewein. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8, 2006.
- [6] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane. Quantum secret sharing with a single d -level system. *In preparation*, November 2014.
- [7] David Kahn. *The Codebreakers*. Macmillan.
- [8] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656?715, 1949.
- [9] Martin Hellman Whitfield Diffie. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22:644?654, Nov. 1976.
- [10] Ronald L. Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120?126, 1978.

- [11] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thom, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit rsa modulus. Cryptology ePrint Archive, Report 2010/006, 2010. <http://eprint.iacr.org/>.
- [12] Peter Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Symposium on Foundations of Computer Science*, 1994.
- [13] H. Weinfurter A. Zeilinger G. Weihs, M. Reck. All-fiber three-path mach-zehnder interferometer. 21:302, 1996.
- [14] R.G. Priest. Analysis of fiber interferometer utilizing 3 x 3 fiber coupler. *Microwave Theory and Techniques, IEEE Transactions on*, 30(10):1589–1591, Oct 1982.
- [15] Sandra Eibenberger, Stefan Gerlich, Markus Arndt, Marcel Mayor, and Jens Tuxen. Matter-wave interference of particles selected from a molecular library with masses exceeding 10 000 amu. *Phys. Chem. Chem. Phys.*, 15:14696–14700, 2013.
- [16] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, oct 1982.
- [17] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844–1852, Sep 1996.
- [18] C. Gerry and P. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.
- [19] D.F. Walls and G.J. Milburn. *Quantum Optics*. Springer, 2008.
- [20] M. Fox. *Quantum Optics: An Introduction*. Oxford Master Series in Physics. OUP Oxford, 2006.
- [21] Rolf Landauer. The physical nature of information. *Physics Letters A*, 217(4):188–193.
- [22] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982.
- [23] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

- [24] I D Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241, 1981.
- [25] William K Wootters and Brian D Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363 – 381, 1989.
- [26] Daniel McNulty and Stefan Weigert. On the impossibility to extend triples of mutually unbiased product bases in dimension six. *International Journal of Quantum Information*, 10(05), 2012.
- [27] Sadiq Muhammad, Armin Tavakoli, Maciej Kurant, Marcin Pawłowski, Marek Żukowski, and Mohamed Bourennane. Quantum bidding in bridge. *Phys. Rev. X*, 4:021047, Jun 2014.
- [28] Gilles Brassard. Brief history of quantum cryptography: A personal perspective. In *Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Workshop*, pages 19–23. IEEE.
- [29] P M Intallura, M B Ward, O Z Karimov, Z L Yuan, P See, P Atkinson, D A Ritchie, and A J Shields. Quantum communication using single photons from a semiconductor quantum dot emitting at a telecommunication wavelength. *Journal of Optics A: Pure and Applied Optics*, 11(5):054005, 2009.
- [30] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.
- [31] D Stucki, N Gisin, O Guinnard, G Ribordy, and H Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, 4(1):41, 2002.
- [32] Mark Hillery, Vladimr Bužek, and Andr Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829, 1999.
- [33] W. Tittel, H. Zbinden, and N. Gisin. Experimental demonstration of quantum secret sharing. 63(4), 2001.
- [34] Christian Schmid, Pavel Trojek, Mohamed Bourennane, Christian Kurtsiefer, Marek Żukowski, and Harald Weinfurter. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.*, 95:230505, Dec 2005.
- [35] Su-Juan Qin, Fei Gao, Qiao-Yan Wen, and Fu-Chen Zhu. Cryptanalysis of the hillery-bužek-berthiaume quantum secret-sharing protocol. *Phys. Rev. A*, 76:062324, Dec 2007.

- [36] Philipp Cörlin. Developing and utilizing a controller to stabilize the phases in a fiber based qutrit interferometer, 2011.
- [37] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, 7(3):210–214, 2013.