UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia “Galileo Galilei”

Corso di Laurea Magistrale in Fisica

Security of Quantum Protocols certified by the dimension of the Hilbert space

Relatore:
Prof. Giuseppe Vallone

Correlatore:
Prof. Mohamed Bourennane

Laureando: Marco Avesani
Matricola: 1080014

Anno Accademico 2015/2016

Contents

Introduction

The security of exchanged data plays a central role in our modern and digitalized society. Every information sent through Internet can be, in principle, intercepted by an attacker, listening over our communication channel. In order to protect the transmitted data, these information are not sent in their plain-text form, but complex algorithm are used to encrypt them, so that only the legitimate parties can recover the original message. This cryptographic procedures are used for example every time we access to our home baking platform.

Despite the research behind these cryptographic algorithms is in constant development, and could provide really complex ways to encrypt data, the security of conventional cryptography is not absolute, since it's usually based on tasks that are hard to solve for our current technology. For example, the RSA, the most common public-key encryption system, is based on the difficulty for modern computers of factoring two big prime numbers. However, development of new mathematical tools or better hardware can, in principle, break these systems. Moreover, advances in the quantum information field, showed that such problems are not so hard to solve for a quantum computer.

In other words, classical cryptography cannot be a definitive solution for this problem.

The fairly new field of quantum information, instead, showed that using the properties of quantum mechanical systems, is possible to build an unbreakable secure communication protocol. This new quantum protocol is called Quantum Key Distribution (QKD), since can generate and distribute a pair of secure and identical keys between two users. The security of QKD doesn't relies, like the RSA, on hard to solve tasks but is directly linked to the physical properties of quantum system, for example single photons, and so is assured directly by the law of physics.

QKD has been successfully tested experimentally, both in free-space and in fiber, and projects of quantum networks are starting to appear.

Unfortunately, real-life implementations of QKD are usually afflicted by imperfections that are not considered in the theoretical models used to prove their security. This opens security flaws in the QKD, which can compromise the entire protocol.

For this reason, new QKD schemes that relax the assumption on the inner working of the employed devices are object of an intense research.

In this thesis we are going to explore one of these possible alternatives to "standard" QKD, that can provide an higher lever of security, called Semi-Devi-Independent (SDI).
We are going to see how some particular properties of the dimension of the Hilbert space, can be used in order to prove the secrecy of the communication. Moreover, the same theoretical background can be used also for the generation and certification of true randomness in a quantum random number generator.
In this work, realized with the KIKO group at Stockholm University, we have performed a proof-of-principle experiment over standard telecommunication optical fiber, aimed to show the feasibility of Semi-Device-Independent protocols.
The encouraging results we have obtained, show that the realization of SDI protocols ,for both QKD and Random Number Generation, is already possible with current technology, making these protocols a valid alternative to the less secure "standard" quantum protocols implemented until now.

CHAPTER 1

Introduction to Quantum Information

1.1 Quantum Information's basic block: the Qubit

In information theory and in computer science the basic building block is the bit. This is a mathematical construct, a boolean variable, that can assume only one of two possible values and can be implemented in any physical two state system. For example, it can be implemented in the position of a mechanical or electronic switch, in two different voltage levels, in the intensity, wavelength or polarization of light, two direction of magnetization of a ferromagnetic material and a numerous of others incredible ways.

All the modern society relies on the concept of bit: electronic, computation, digital communication are just an example of the applications that are possible thanks to this concept. The main characteristic of the bit is the mutual exclusivity of the values it can assume: in any moment the value of the bit is either 1 or 0.

When one is dealing with quantum mechanical system, however, a way richer phenomenology is possible.

In fact is possible to build the quantum version of bit, the qubit, using a two level quantum mechanical system. Unlike the bit, quantum mechanics tell us is that the qubit can be in a linear *superposition* of $|0\rangle$ and $|1\rangle$, the two possible outcomes of a measure. Thus the most general state the system can assume can be written as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.1}$$

The state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states and form an orthonormal basis for this vector space. However, like the bit, the outcomes of a measure performed on the qubit can be only one of the two state that compose the computational basis and this, in the case of a state in the form given by Eq 1.1, happens with probability α^2 for $|0\rangle$ and β^2 for for $|1\rangle$. The normalization condition for probabilities implies that $|\alpha|^2 + |\beta|^2 = 1$, and so $|\psi\rangle$ is a vector of unitary length. With the above condition, Equation 1.1 can be written as:

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \tag{1.2}$$

where η is a global phase, carrying no information about the state, since physical states are described by ray vectors on a Hilbert space. This reformulation is useful because permits to express the state of a qubit in function of two angles, θ and ϕ representing a point on the surface of a 3 dimensional sphere, called the Bloch sphere. This graphical representation is extremely useful when one is working with qubit but unfortunately is not possible to easily generalize it for dimension bigger than 2.

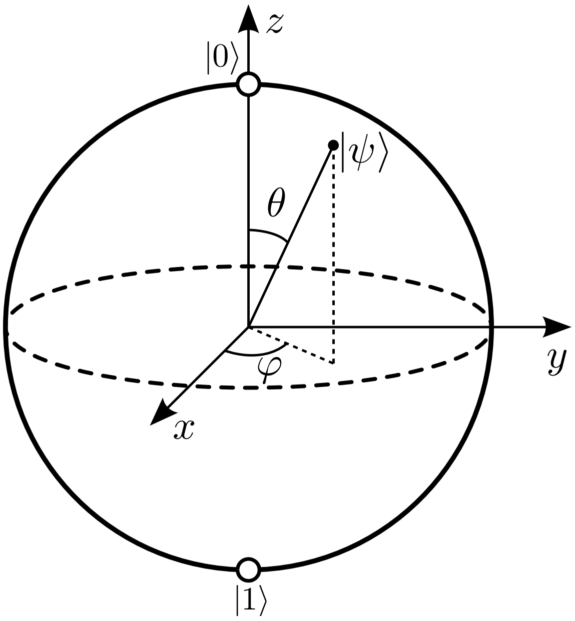


Figure 1.1: *Representation of the Bloch sphere*

This representation is useful to catch a fundamental difference between the bit and the qubit. While the bit can assume only two different and discrete values, the qubit can represent an infinite continuous set of states, spanning all over the surface of the sphere: this means that infinite information can be represented by the qubit. However, whenever we try to access to the information, by measuring it, we change the state of the qubit, making its state to collapse into one of the eigenstate. So, at first sight the qubit could seem useless. How can we use the qubit as a resource if we destroy its fundamental property in the moment we are reading it?
The answer is that, even if we can't access the qubit, we can perform unitary operations on it preserving *all* the information it contains. This is the power of quantum computation. Moreover the qubit is quantum mechanical system, and must obey to the laws of quantum mechanics that, as we are going to see, forbids or provides an advantage on some tasks performed on the qubit, respect the classical predictions.
But how we can realize a qubit in practice?
As already said any quantum two level system can be used as a qubit: the states of an electron in an atom, the nuclear spin in a uniform magnetic field, the polarization of a photon are just few

examples of the physical realizations of a qubit system. One of the most widely used implementation is based on single photon's polarization: here $|0\rangle$ and $|1\rangle$ can be the horizontal and vertical polarization of the photon.

1.2 No-cloning theorem

Quantum mechanics, from the beginning, caused a sort of shock and surprise, mining the fundamental conception of how nature was believed to work. Many predictions were in contrast with the common sense, so used to the macroscopic world ruled by the laws of classical physics. One of this strange effects predicted by quantum mechanics, that is of absolute importance in quantum information theory and cryptography, is linked to the action of copy. Copy of information is performed everyday: fax, photocopiers, scanners but also copies on CD, DVD or USB-keys. All of these actions are so normal in our classical world that the hypothesis that copy is forbidden in the quantum world seems absurd. Quantum mechanics however states that is impossible to create a perfect quantum cloning machine and the formalization of this idea is enclosed in the No-cloning theorem [1].
Suppose we have a quantum system A in a pure state $|\psi\rangle_A$ that belongs to a generic Hilbert space $\mathscr{H}$. Now if we want to copy that state, what we need is another system B described by a pure state $|e\rangle_B$ that belongs to the same Hilbert space $\mathscr{H}$. The initial state of this composite system can be described by

$$|\psi\rangle_A \otimes |e\rangle_B \tag{1.3}$$

The operation of copy can be represented by an unitary operator U such that:

$$U(|\psi\rangle_A \otimes |e\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B \;\; \forall\psi \tag{1.4}$$

Since it must be valid for all ψ we can require that:

$$\begin{aligned} U(|\psi\rangle_A \otimes |e\rangle_B) &= |\psi\rangle_A \otimes |\psi\rangle_B \\ U(|\phi\rangle_A \otimes |e\rangle_B) &= |\phi\rangle_A \otimes |\phi\rangle_B \end{aligned} \tag{1.5}$$

Taking the inner product of the two equations and remembering that U must preserve this operation we have:

$$\langle\phi|\psi\rangle = |\langle\phi|\psi\rangle|^2 \tag{1.6}$$

which is satisfied only in the case $|\psi\rangle = |\phi\rangle$ or for $|\psi\rangle$ orthogonal to $|\phi\rangle$.
These few lines are describing a stunning and central feature of quantum systems: a quantum cloning machine that can clone an unknown arbitrary quantum system can't be built. However, if we relax the requests and we admit also imperfect copies, an universal quantum machine is possible and can reach a fidelity $\mathscr{F} = 5/6$ [2]. This is the key point that assures security in many quantum cryptography protocols: if information is encoded in a single quantum system, and this system is transmitted, this cannot be copied without introducing errors, thus revealing the presence of a possible eavesdropper.

1.3 Local realism, entanglement and Bell inequalities

In the previous sections we saw how Quantum Mechanics describes effects that are in contrast with our common sense and our expectation. But quantum mechanics attacked even deeper aspects that were thought to belong to nature: reality and locality.
Reality states that the physical properties of objects exist in a defined state independently on the observation. This is clearly true for classic physics but it can't be said for QM, since QM give us the probability to measure a certain state and, moreover, predicts that the value of two non-commuting operators cannot be simultaneously determined. Locality, on the other end, states that two space-like separated events must be independent. Again QM predicts that a system of entangled particles can share correlations that are non-local, apparently violating the principle of locality. Historically these two principles were thought so fundamental, that was a common opinion believe that law of physics had to obey to both: any complete physical theory must be consistent with local realism. For sure this was the opinion of Einstein, Podolsky and Rosen which in 1935 published a ground-breaking article [3], where they showed that, if both reality and locality principles are assumed, quantum mechanics must be incomplete and that some "hidden variables" must be included in the theory in order to make it complete.
But is this hidden-variable model just another reformulation of quantum mechanics or it can be tested in some way? The answer to this question was given in 1964 by Jhon Bell in [4]. In his remarkable work he showed that any local hidden variable theory has a bound on the correlation experienced on space-like separated particles, and this bound can be calculated and tested experimentally. This limitation can be express in the form of an inequality: the expectation value of some observables of the two particle must be below a certain threshold in the case of a local hidden variable theory. If experiments are performed, and value higher of this bound are obtained, this means that nature cannot be described by such set of theories.
After few years experiments started to tests Bell's predictions, starting with the one by Freedman in 1972 [5], and then by Aspect in 1981,1982 [6] [7]. The reported results were well beyond the bound predicted by local hidden variable theories, and in good agreement with the one predicted by quantum mechanics. The conclusion was that nature is not-local or not-realistic, or both. Unfortunately experiments performed suffered problems of experimental design or set-up that affect the validity of the experimental finding. These problems are often referred to as "loopholes".
Despite being an old problem, is really challenging to design and realize a loophole-free Bell test and until now no-one could perform such experiment, closing once for all the question. However, recently, three experiments [8] [9] [10] claimed to have performed a loophole free Bell test and, if the results will be confirmed, these test will be of crucial importance for both foundations of quantum mechanics and for application in the quantum information field.

1.3.1 CHSH Inequality

The original inequality derived by Bell, was really hard to test experimentally since it required perfect (anti)correlated particles. A generalization of that inequality was derived in 1974 by Clauser, Horne, Shimony and Holt where the authors proposed the experiment needed to test their inequality [11]. Suppose to have two space-like separated parties, Alice and Bob, each of them receives a particle and on this particle they can measure a property. The outcome $A(x), B(y)$ on

Alice's and Bob's side respectively, depends on the settings they used and we assume that the outcomes can only be ± 1. One practical example could be the polarization of photons: if Alice and Bob receive one photon each, they can measure polarization of the photons and the setting in this case is the base they use to perform the measurement. Limiting to the case where only 2 settings are employed we have $x = \{a, a'\}$ and $y = \{b, b'\}$.
If we now assume that there is a local hidden variable λ that describes the system, then A and B must be function of this hidden variable yielding $A(x, \lambda)$, $B(y, \lambda)$. Finally, if the theory is local, since Alice and Bob are space-like separated, $A(x, \lambda)$ must be independent from $B(y, \lambda)$. Thus we can write the correlations between the two measurements as:

$$C_{AB}(x, y) = \int_\Lambda A(x, \lambda) B(y, \lambda) \rho(\lambda) d\lambda \tag{1.7}$$

where $\rho(\lambda)$ is the probability density function associated to the hidden variable λ. Considering another setting for Bob and using the fact that the measures take only ± 1 values:

$$\begin{aligned} |C_{AB}(a, b) - C_{AB}(a, b')| &= \left| \int_\Lambda \left(A(a, \lambda) B(b, \lambda) - A(a, \lambda) B(b', \lambda) \right) \rho(\lambda) d\lambda \right| \\ &\leq \int_\Lambda \left| \left(A(a, \lambda) B(b, \lambda) - A(a, \lambda) B(b', \lambda) \right) \right| \rho(\lambda) d\lambda \\ &\leq \int_\Lambda |A(a, \lambda) B(b, \lambda)| \left(1 - B(b', \lambda) B(b, \lambda) \right) \rho(\lambda) d\lambda \\ &\leq 1 - \int_\Lambda \left(B(b', \lambda) B(b, \lambda) \right) \rho(\lambda) d\lambda \end{aligned} \tag{1.8}$$

We can choose now another setting a' such that

$$C_{AB}(a', b') = 1 - \delta \qquad \text{with } \; 0 \leq \delta \leq 1 \tag{1.9}$$

This parameter is introduced to relax the condition of perfect correlation in the original paper by Bell.
Now we can divide Λ into two regions

$$\Lambda^\pm = \{\lambda | A(a, \lambda) = \pm B(b, \lambda)\} \tag{1.10}$$

Using 1.9 we can write:

$$\int_\Lambda A(a', \lambda) B(b, \lambda) \rho(\lambda) d\lambda = \int_{\Lambda^+} A(a', \lambda) B(b, \lambda) \rho(\lambda) d\lambda + \int_{\Lambda^-} A(a', \lambda) B(b, \lambda) \rho(\lambda) d\lambda = 1 - \delta \tag{1.11}$$

then using 1.10

$$\int_{\Lambda^+} A(a', \lambda)^2 \rho(\lambda) d\lambda - \int_{\Lambda^-} A(a', \lambda)^2 \rho(\lambda) d\lambda = 1 - \delta \tag{1.12}$$

Using that $A(x, \lambda) = \pm 1$ and the normalization on $\rho(\lambda)$ we have:

$$1 - 2 \int_{\Lambda^-} \rho(\lambda) d\lambda = 1 - \delta \tag{1.13}$$

$$\int_{\Lambda^-} \rho(\lambda) d\lambda = \frac{1}{2} \delta \tag{1.14}$$

We can now rearrange the second term in Eq 1.8:

$$\int_{\Lambda}\left(B(b',\lambda)B(b,\lambda)\right)\rho(\lambda)d\lambda = \int_{\Lambda^+} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda - \int_{\Lambda^-} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda \tag{1.15}$$

$$= \int_{\Lambda^+} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda + \int_{\Lambda^-} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda \tag{1.16}$$

$$-2\int_{\Lambda^-} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda \tag{1.17}$$

$$= \int_{\Lambda} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda - 2\int_{\Lambda^-} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda \tag{1.18}$$

$$\geq \int_{\Lambda} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda - 2\int_{\Lambda^-} |A(a',\lambda)B(b,\lambda)|\rho(\lambda)d\lambda \tag{1.19}$$

$$= \int_{\Lambda} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda - 2\int_{\Lambda^-} \rho(\lambda)d\lambda \tag{1.20}$$

$$= C_{AB}(a',b) - \delta \tag{1.21}$$

Substituting into the original equation we have:

$$|C_{AB}(a,b) - C_{AB}(a,b')| = 1 - C_{AB}(a',b) - \delta = 2 - C_{AB}(a',b) + (1-\delta) \tag{1.22}$$

$$= 2 - C_{AB}(a',b) - C_{AB}(a',b') \tag{1.23}$$

and finally obtaining

$$\left|C_{AB}(a,b) + C_{AB}(a,b') + C_{AB}(a',b) - C_{AB}(a',b')\right| \leq 2 \tag{1.24}$$

which is the usual form for the CHSH inequality. We can see that for the CHSH inequality the bound for LHV theories is 2: any measured value above 2 would be a proof that the two particles testes are experiencing correlations not explainable by a LHV theory, and so, in contrast with local realism.

1.3.2 Quantum mechanics predictions

In Eq 1.24 we saw that the bound in the CHSH inequality for local hidden variable theories is 2, but which are the predictions of quantum mechanics? In the case of quantum mechanics we don't assume to have hidden variables, so the correlations $C_{AB}(a,b) = \langle A(a)B(b)\rangle$ are given by the expectation values of the measure operators on the wavefunction describing the two particles state. Thus we ca rewrite the CHSH inequality in the form:

$$\left|\langle A(a)B(b)\rangle + \langle A(a')B(b)\rangle + \langle A(a)B(b')\rangle - \langle A(a')B(b')\rangle\right| \leq B_{QM} \tag{1.25}$$

In the case Alice and Bob shares a maximally entangled state , for example $|\psi^-\rangle = \frac{1}{2}(|1\rangle|-1\rangle - |-1\rangle|1\rangle)$ where $|\pm 1\rangle$ are the eigenstates of σ_x, they can choose their settings such that

$$A(a) = \sigma_x \otimes I \tag{1.26}$$

$$A(a') = \sigma_z \otimes I$$

$$B(b) = I \otimes -\frac{\sigma_x + \sigma_z}{\sqrt{2}}$$

$$B(b') = I \otimes \frac{\sigma_x - \sigma_z}{\sqrt{2}} \tag{1.27}$$

For these value of the settings we obtain:

$$\langle A(a)B(b)\rangle = \langle A(a')B(b)\rangle = \langle A(a)B(b')\rangle = -\langle A(a')B(b')\rangle = \cos\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} \tag{1.28}$$

This value coincides with the upper bound for the CHSH inequality predicted by quantum mechanics, $B_{QM} = 2\sqrt{2}$. A rigorous proof has been proposed by Tsirelson and for this reason is called Tsirelson's bound [12]. This higher bound means that quantum mechanics violates the CHSH bound for local hidden variable theory and so QM is not compatible with the principle of local realism. For the sake of completeness is notable that a general theory subject only to the no-signalling condition has an upper bound of 4.

Anyway there is still a way to reconcile QM and LHV theories which is called: superdeterminism. Superdeteminism attacks directly one of the assumption of Bell's theorem: the free will. In a Bell test is assumed that the types of measurements performed at each detector can be chosen independently of each other and of the hidden variable being measured. In other words is the experimenter "free will" that chooses the settings for each round of the experiment. Superdeterminism instead states that there is no randomness in nature and everything is just evolving in time, following the law of a deterministic physics. In this sense, also the choice of the settings of the experimenter are already determined before they happen, in fact there is not even a choice, the settings used are just the ones that had to be used. Since the chosen measurements can be determined in advance, the results at one detector can be affected by the type of measurement done at the other without breaking the local realism.

1.4 Quantum optics: the toolbox for quantum information experiments

Light has played historically a central role in the fundamental tests of quantum mechanics. Because of the easiness of optical setups compared to the particle-based ones, photonic experiments in the last four decades, and still now, could give answer to important questions about the foundations of quantum mechanics. The invention of the laser first, and single photon detectors after, opened an entire world of possibilities to experimenters who wanted to work with single quantum systems.
In the next section some of the commonly used optic components will be presented from a quantum optic view and then the functioning of a single photon interferometer ,widely used in this thesis, will be described.

1.4.1 Beamsplitters

The beamsplitter, presented in Fig. 1.2, is a multi-port device used to combine or split light coming or exiting the ports. Classically the action of a such device can be described with two complex parameters, t and r, the trasmissivity and the reflcetivity. If light enters from one port, the incoming complex amplitude of electric field E_1 is partially transmitted to one port, $E_2 = tE_1$ while the other is reflected to the second port $E_3 = rE_1$. If the device is lossless, the conservation of energy requires $|t|^2 + |r|^2 = 1$. This description holds for classic electromagnetism, but how can be explained the action of these devices when a single photon is sent through?
To treat the beamsplitter quantum mechanically one can try to substitute the complex amplitude

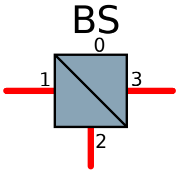


Figure 1.2: *Action of a beam splitter*

E_i with annihilation operators a_i. However, unlike the classical case, both the input port must be considered, otherwise the commutation relations for creation and annihilation operators are not preserved.[13]. The reason is that we must also consider the vacuum component. In this way the relations between the operators can be written as:

$$a_2 = t' a_0 + r a_1 \qquad a_3 = r' a_0 + t a_1 \tag{1.29}$$

Imposing the conservation of energy we have $|r|^2 = |r'|^2$, $|t|^2 = |t'|^2$, $|r|^2 + |t|^2 = 1$ and $r^* t' + r' t^* = r^* t + r t'^* = 0$ and we have to remember that, in the dielectric beamsplitter, the reflected component has its phase shifted by $\pi \backslash 2$. Combining everything together we can write:

$$a_2 = |t| a_0 + i(1-|t|) a_1 \qquad a_3 = i(1-|t|) a_0 + |t| a_1 \tag{1.30}$$

that can be simplified for a 50:50 beamsplitter to:

$$a_2 = \frac{1}{\sqrt{2}}(a_0 + i a_1) \qquad a_3 = \frac{1}{\sqrt{2}}(i a_0 + a_1) \tag{1.31}$$

Let's now consider what happens when a single photon enters in the port 1 of the beamsplitter. The state is described by:

$$|0\rangle_0 |1\rangle_1 = a_1^\dagger |0\rangle_0 |0\rangle_1 \tag{1.32}$$

if now we use the relation obtained above we get:

$$a_1^\dagger |0\rangle_0 |0\rangle_1 = \frac{1}{\sqrt{2}}(i a_2^\dagger + a_3^\dagger) |0\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}}(i |1\rangle_2 |0\rangle_1 + |0\rangle_2 |1\rangle_3) \tag{1.33}$$

At the output, the single photon is in a superposition of states, between the two ports, with equal probability. This is an entangled state since cannot be described in terms of the modes 2 or 3 individually; in this case the single photon is entangled with the vacuum. The expectation value out of one port is:

$$\langle N_3 \rangle = \frac{1}{2}((-i \langle 1|_2 \langle 0|_1 + \langle 0|_2 \langle 1|_3) | a_3^\dagger a_3 | (i |1\rangle_2 |0\rangle_1 + |0\rangle_2 |1\rangle_3)) = \frac{1}{2} \tag{1.34}$$

but the second order correlator:

$$\langle N_3 N_4 \rangle = \frac{1}{2}((-i \langle 1|_2 \langle 0|_1 + \langle 0|_2 \langle 1|_3) | a_3^\dagger a_3 a_4^\dagger a_4 | (i |1\rangle_2 |0\rangle_1 + |0\rangle_2 |1\rangle_3)) = 0 \tag{1.35}$$

meaning that is not possible to measure the position of the photon in the two ports simultaneously.

1.4.2 PBS

The Polarization Beam Splitters (PBS) are special beamsplitters which can transmit horizontal polarized light and reflect the vertically polarized one. These devices can be described using the same framework above depicted with the following relations:

$$a_{0,H} = a_{2,H} \qquad a_{0,V} = i a_{3,V} \qquad a_{1,H} = i a_{3,H} \qquad a_{1,V} = a_{2,V} \tag{1.36}$$

1.4.3 Circulator

The circulator, presented in Fig 1.3, is a 3 port device that transmits light from port 1 to port 2 and from port 2 to port 3 blocking all the other possible configurations. Is really useful when working with fibers and is widely used for building interferometers. Again the circulator can be described by QM using the follow relations between the annihilation operators:

$$a_0^\dagger \to a_1^\dagger \qquad a_1^\dagger \to a_2^\dagger \tag{1.37}$$

Note that $a_0^\dagger = a_1^\dagger$ is not true.

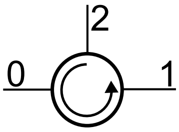


Figure 1.3: *Symbol of the circulator*

1.4.4 Quantum interferometry

In the thesis a lot of the work is based on the single photon interferometry and, in this section, we are going to apply the previous formalism in order to describe the internal functioning of a Mach-Zehnder (MZ) interferometer when only one photon is sent into it. The setup of a basic MZ interferometer, represented in Figure 1.4, consists in two beamsplitters, two mirrors and a phase modulator. With classical light, the incoming beam is split in two by the first beamsplitter, then one of the two beam is modulated with a phase modulator and, using the mirrors, the two

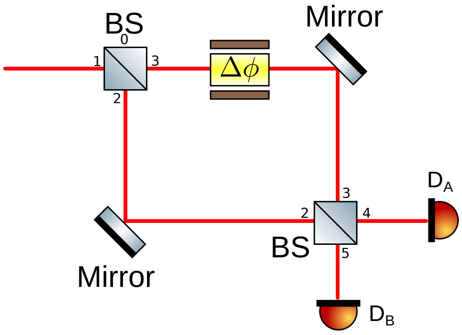


Figure 1.4: *Setup for a Mach-Zehnder interferometer*

beams enter the two input ports of the second beamsplitter. The intensity of the light detected by each detector depends on the value of the phase shift $\Delta\phi$ with the relations:

$$I_1(\Delta\phi) = \frac{1}{2} I_0 \left(1 + \cos\Delta\phi\right) \tag{1.38}$$
$$I_2(\Delta\phi) = \frac{1}{2} I_0 \left(1 - \cos\Delta\phi\right)$$

where I_0 is the total intensity of the incoming light. The effect is easy to explain in the context of classical electomagnetism using the superposition principle for the electric field, but how can be explained when only one photon is sent through the interferometer?
Using the conventions introduced in Sec 1.4.1 is possible to describe a single photon entering the fist beamsplitter through port 1 with the state:

$$|\varphi\rangle = |0\rangle_0 |1\rangle_1 \tag{1.39}$$

Using the relations between creation operators in a beam splitter we have seen that the output state is:

$$\frac{1}{\sqrt{2}}(|0\rangle_2 |1\rangle_3 + i |1\rangle_2 |0\rangle_3) \tag{1.40}$$

Both path employ a mirror, so a phase shift of $\pi/2$ is present in each and doesn't affect the relative phase. This relative phase instead is changed using a phase modulator in the upper arm (path 3). After the modulation the state can be written as:

$$\frac{1}{\sqrt{2}}(e^{i\Delta\phi} |0\rangle_2 |1\rangle_3 + i |1\rangle_2 |0\rangle_3) \tag{1.41}$$

At the second beamsplitter (we numbered the entering port in the same way as the corresponding output ports of the firs beamsplitter) we can reapply the relations for the creation operators, obtaining:

$$|1\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}}(|1\rangle_4 |0\rangle_5 + i |0\rangle_4 |1\rangle_5) \tag{1.42}$$

$$|0\rangle_2 |1\rangle_3 = \frac{1}{\sqrt{2}}(i |1\rangle_4 |0\rangle_5 + |0\rangle_4 |1\rangle_5) \tag{1.43}$$

so that the final state after the second beamsplitter is given by:

$$|\psi\rangle = \frac{1}{2}(e^{i\Delta\phi} - 1) |0\rangle_4 |1\rangle_5 + i(e^{i\Delta\phi} + 1) |1\rangle_4 |0\rangle_5 \tag{1.44}$$

The probability to see the photon in the detector A and B respectively is:

$$P_A(\Delta\phi) = |\langle 1|_4 \langle 0|_5 |\psi\rangle|^2 = \frac{1}{2}(1 + \cos(\Delta\phi) \tag{1.45}$$

$$P_B(\Delta\phi) = |\langle 0|_4 \langle 1|_5 |\psi\rangle|^2 = \frac{1}{2}(1 - \cos(\Delta\phi)) \tag{1.46}$$

The result is similar to the classic one but in this case is obtained for single photons. Moreover, the formalism introduced can be used to explain other interesting effects with no classical analogue like the Hong–Ou–Mandel effect [14]. Finally, in the single photon case, the visibility of the interferometer, that was defined as:

$$\mathcal{V} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{1.47}$$

must be defined from a statistical point of view:

$$\mathcal{V} = \frac{N_{max} - N_{min}}{N_{max} + N_{min}} \tag{1.48}$$

where N_{max}, N_{min} are the counts seen by the detectors in a fixed amount of time for the constructive and destructing interference.

CHAPTER 2

Cryptography in the quantum era

Cryptography is the art of hiding information in a string of bits meaningless to any unauthorized party. This is a really old discipline that plays a fundamental role in our modern society. The first forms of cryptography were found in the Egyptian civilization, where nonstandard glyphs were used to encode secret information. Since then all the civilization, from Chinese to Greeks or Romans are documented to have been using different forms of cryptography [15], especially during wars. In this case was essential to communicate with distant armies, in order to share information and strategies, but the communication had to be encrypted in a way that if the messenger had been intercepted by the enemy, no important information could be recovered. Since then cryptography evolved, with the creation of more and more complex algorithm and, little by little, entered in our everyday life. Today we rely on cryptography: e-commerce, home banking, financial transaction but also secure web browsing and secure handling of digital data are just few of the common operations performed everyday and made possible by cryptography. Unfortunately in a really near future all the cryptography as we know now could be made useless. Modern cryptography is based on hard NP problems that are solvable only in exponential time by any powerful computer. Anyhow the invention of a Quantum Computer, whose field of research is extremely active at the moment, has the possibility to solve this kind of problems in a faster way, thus breaking all the current cryptosystems. Moreover, in 2013 internal NSA memos leaked by Edward Snowden showed that the NSA was implicated in the insertion of a backdoor in the Dual_ECl_DRBG standard used in almost every cryptography library. The implications of such a backdoor were analysed in [16], where the author concluded that, depending on the protocol, the NSA could have broken the security in seconds on a normal desktop computer.

Luckily, quantum mechanics provides us the tools to defend ourselves against this apocalyptic future. The properties of single quantum system can, in fact, be used to build cryptographic systems invulnerable to any possible attack, thus unconditionally secure.

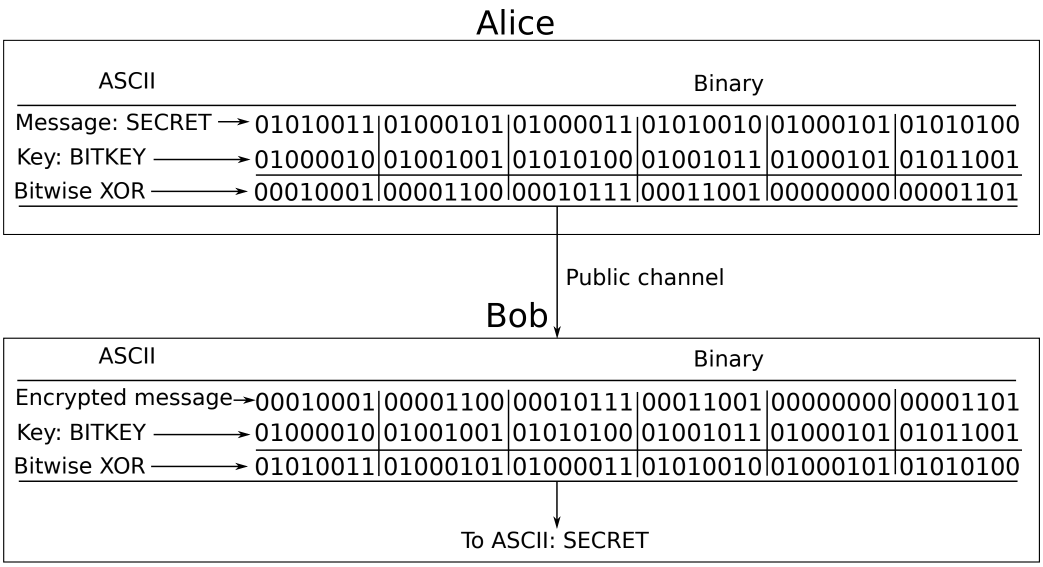
2.1 Classical cryptography

Classical cryptography can be divided in two big categories: private-key cryptography and public-key cryptography. The first one is the typical form of cryptography that anyone imagines: Alice and Bob have a secret key, Alice encodes, with some algorithm and a key, her message and sends it to Bob who can fully reconstruct the message using his key. This kind of cryptography is the oldest and the most commonly used before the 80's. In the 70's, another form of cryptography was invented: public-key cryptography. In this case the security still relies on a private key but the encryption can be done by anyone with a second, publicly shareable, key, avoiding the use of a secure channel for the key exchange. In the following section some example of these algorithms will be provided.

2.1.1 Protocols

A private key example: One time pad

In a private key cryptosystem, if Alice wants to send a message to Bob, she needs an encoding key, which allows her to encrypt her message and Bob must have a matching decoding key, which allows him to decrypt the encrypted message.
Over all the methods of encryption ever devised, there's a special one that has been mathematically proved to be completely secure. This is the Vernam cipher or one-time pad (OTP) and was invented in 1882 by Frank Miller. All the other ciphers, instead, are only computationally secure. This means that the probability of cracking the encryption key, using current computational technology and algorithms within a reasonable time, is supposed to be extremely small, yet not impossible. The OTP instead was proven to be unconditionally secure if the keys are composed of truly random data, are never used more than once and are kept secret. The mathematical proof was given in 1949 by the father of modern information theory, Claude Shannon [17]. For this reason, in theory, every cryptographic algorithm except for the OTP (if properly implemented) can be broken given enough ciphertext and time. Despite it's security the functioning of the OTP is quite simple. Alice and Bob need to have a secret key that is as long as the message they want to encrypt. Given the key and the message, Alice can perform a bitwise XOR operation with the two strings. The result is the encrypted message that is sent to Bob. Bob, using the same key used by Alice, can perform again the XOR operation with the incoming message and the key strings. The result of the operation is the original message. A practical example is presented in Fig. 2.1
However, the OTP suffers of some big limitations, related to the secure distribution of key bits. The OTP is secure only as long as the number of key bits is at least as large as the size of the message encoded, and key bits cannot be reused. This requires an high number of key-bits, that must be delivered in advance, kept secret and destroyed after the use since they are no longer secure. This form of key sharing is not very convenient because exposes the key to many threats and is not practical for very remote users that cannot have frequent physical contacts.
For this reasons, less secure but more practical scheme are commonly used today, like public key cryptography.



Alice

ASCII	Binary					
Message: SECRET →	01010011	01000101	01000011	01010010	01000101	01010100
Key: BITKEY →	01000010	01001001	01010100	01001011	01000101	01011001
Bitwise XOR →	00010001	00001100	00010111	00011001	00000000	00001101

Public channel

Bob

ASCII	Binary					
Encrypted message→	00010001	00001100	00010111	00011001	00000000	00001101
Key: BITKEY →	01000010	01001001	01010100	01001011	01000101	01011001
Bitwise XOR →	01010011	01000101	01000011	01010010	01000101	01010100

To ASCII: SECRET

Figure 2.1: *Practical example of OTP*

A public key example: RSA

Key distribution for private key cryptography has been the main problem for cryptographers throughout history, and even with the development of new telecommunication systems the process was too inefficient and subject to interception. For many years it seemed an unsolvable problem. But in 1973 a new system, based on asymmetric keys, was developed by Whitfield Diffie. The idea was further explored and the first implementation was published in 1976 with Martin Hellman and it's known as the Diffie-Hellman key exchange [18]. Unfortunately the Diffie-Hellman key exchange turned out to be vulnerable to man-in-the-middle attacks. For this reason in 1978, Ronald Rivest, Adi Shamir and Leonard Adleman published an improved version of the Diffie-Hellman protocol known as RSA, in honor to the authors [19]. The RSA today is one of the most used protocol for encryption and is widely used, especially for encryption over Internet.
The RSA, and public key encryption in general, relies on the use of a pair of asymmetrical keys. Unlike OTP, where both Alice and Bob shared the same secret key, Bob generates a pair of key, a public and a private one; the first is shared publicly and is used by Alice to encode the message that can be decrypted only with the use of the private key, hold by Bob and never disclosed. But how is possible to generate two keys with such properties? The best answer is to look how the RSA protocol actually works.
Bob key generation:

- He randomly chooses two big prime numbers, p and q of similar bitlength and computes the product $n = p \cdot q$. The length of n is the key length.
- He computes $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. $\varphi(x)$ is Euler's totient function.
- He chooses an integer e such that $1 < e < \varphi(n)$ and coprime with $\varphi(n)$
- He calculates d such $d \cdot e = 1(\mathrm{mod}(\varphi(n)))$

- The modulus n and e are publicly announced as public key.
- The private key consists of n and d. Also p, q, and $\varphi(n)$ must be kept secret because they can be used to calculate d.

Alice encryption:

- With an agreed padding protocol converts the message M to an integer m such that $0 \leq m < n$
- She converts m to a cyphertext c such that $c = m^e(\mathrm{mod}(n))$
- She sends c to Bob over a public channel

Bob decryption:

- He recovers m using his private key and $m = c^d(\mathrm{mod}(n))$
- He uses the same padding protocol as Alice to recover M from m

The protocol relies its security on the fact that given the public key (n, e), is extremely hard to compute p and q needed for computing d. This is a prime factorization problem, for witch no polynomial-time factoring algorithms are known now. This means that the time needed for modern computers to factorize n grows up exponentially in time with the length of n. On the contrary the encryption operation is very fast and takes from fraction of second to few seconds on modern PC, for the commonly used 2048 bit keys.
However, unlike the OTP, the RSA in not unconditionally secure, but only computational secure. This means that is theoretically possible to break it but with the current knowledge and technology this would take an enormous quantity of time.

2.1.2 Security and vulnerabilities

As stated above, the OTP was proven to be unconditionally secure, meaning that, if properly implemented, OTP is secure even against adversaries with infinite computational power. Claude Shannon's proved that the encrypted message gives absolutely no additional information about the original message and so even bruteforce attacks are useless. Trying all keys simply yields all plaintexts, all equally likely to be the actual message. The real problem for OTP is the key distribution. Given the high quantity of bits needed for the OTP and the fact that they cannot be used again, is hard to find a secure key distribution system. The users could met once and exchange a physical drive containing an huge quantity of pad-bits, but this solution is risky, because the pads needs to be kept secret before and after the use (destroyed). Finally, the OTP is impractical for web security, where the key point is the connection between users that cannot be physically in contact.
For what regards RSA and public-key, the biggest problem is that is only computational secure. Today no polynomial-time factoring algorithms are known, but there is no proof they don't exist and a more efficient algorithm could be found in future. Moreover, the security of public key cryptography depends on the length of the key, and this has been increased many time in these years, because advancing in math or technology proved that the used length was not secure anymore; for example for n smaller than 300 bits the factorization can be done in hours on a modern PC.

The record of factorization for the RSA is 768 bits and was performed in 2010 [20]. For this reason today the suggested keylength is 2048 bit.
Another threat for RSA was discovered in 1994 by P. Shor in [21]: quantum computers. Shor discovered a quantum algorithm that, executed on a quantum computer, performs the integer factorization in polynomial time. This means that a stable quantum computer with a sufficient number of qubits could use Shor's algorithm to break public-key cryptography schemes such as the RSA.
Finally, the RSA could be already be compromised. In 2013 leaks of NSA secret reports by Edward Snowden showed that the NSA was implicated in the insertion of a backdoor in the Dual_EC_DRBG random number generator used in RSA protocol. Many cryptography experts stated that this backdoor could have broken the RSA protocol completely, giving to the NSA full access to the plaintext [20]. This scandal focused once more the attention to the need of a new "self-checking" cryptography that can be trusted even if the maker of the protocol or of the devices are not trusted.
For all this reason in the last years a lot of effort has been put into Quantum Cryptography that can, in principle, solve all these problems, once for all.

2.2 "Standard" Quantum Key Distribution

In the previous section we saw that modern cryptography suffers of few critical security flags that can be used to compromise security in the near future. Quantum mechanics, the main enemy with quantum computers, of modern cryptography, however, provides also a way to solve the problem of secure key distribution. In fact, a theoretically secure protocol already exists within the reign of classical physics and is the OTP. The problem that cannot be solved using only classic physics is the distribution of the key, which is impossible to do safely and remotely. Quantum mechanics, instead, provides a way to randomly generate and distribute a key over a **public** channel: this is Quantum Key Distribution (QKD). The central point in QKD is that this key generation can be done securely, in the sense that, if the protocol is correctly implemented, the laws of QM guarantees that any eavesdropper that tries to intercept the message would inevitably introduce errors in the communication, revealing his presence to the users, that can abort the protocol and start another key generation.
The idea of Quantum Cryptography was first proposed in 1970 by Stephen Wiesner and then published in 1983 [22]. In this paper Wiesner proposed the use of conjugate observables for the communication. His work was further explored by Bennett and Brassard, who, in 1984, published an article [23] where they proposed and analysed a protocol for a secure quantum communication: the BB84. In the BB84, which is probably the most famous quantum protocol, the communication is performed using single qubit. The security of the resulting key is guaranteed by the properties of quantum mechanics, and thus is conditioned only on fundamental laws of physics on being correct. In another protocol, invented by A. Ekert in 1991 [24], the parties shared an entangled pair of particle and the security was assured by the violation of a Bell inequality.
Since the BB84 is the most employed and is already used on commercial QKD system will be taken as an example and discussed in the following section.

2.2.1 BB84 Protocol

The BB84 protocol in its original proposal consisted in two users, Alice and Bob, that wanted to communicate securely, and two communication channels: a quantum channel and a classical public channel. With this protocol they want to protect themselves from an eavesdropper, Eve, with an unlimited power that could do anything, within the laws of physics, to intercept their communication. For the encryption part Alice and Bob agree to use an OTP scheme, while they use the quantum protocol for the key generation and distribution. The QKD protocol schematized in Fig 2.2 represents the BB84 protocol implemented with photon's polarization.

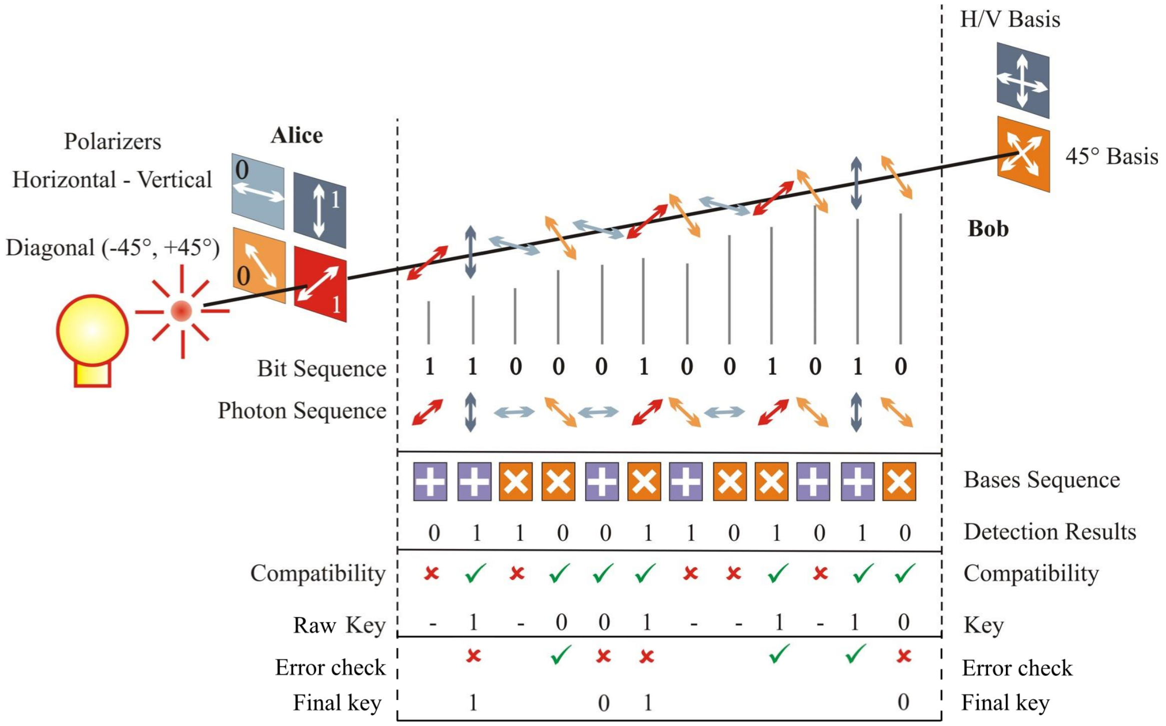


Figure 2.2: *Schematics of the BB84 protocol with photon's polarization encoding[25]*

Alice can prepare the photons she wants to send to Bob in one of the four polarization states coming from two mutually unbiased bases: for example horizontal, vertical, +45°,−45°. The states can be represented in a vector notation using Jones formalism (see Sec 3.1.2)

$$\text{Base } \bigoplus = \left\{ |H\rangle = \begin{pmatrix}1\\0\end{pmatrix},\ |V\rangle = \begin{pmatrix}0\\1\end{pmatrix} \right\} \tag{2.1}$$

$$\text{Base } \bigotimes = \left\{ |+\rangle = \frac{1}{2}(|H\rangle + |V\rangle) = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix},\ |-\rangle = \frac{1}{2}(|H\rangle - |V\rangle) = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \right\} \tag{2.2}$$

These states can be described using two bits: b_A for the base, such that $b_A = 0$ for $\bigoplus$ and $b_A = 1$ for $\bigotimes$ and s_A, with $s_A = 0$ for $|H\rangle, |+\rangle$ and $s_A = 1$ for $|V\rangle, |-\rangle$.
The procedure consists of six steps.

1. For each round of the quantum communication Alice randomly generates two bits, b_A, s_A and according to the value obtained she prepares the corresponding state and she sends it to Bob along the quantum channel. Bob, at each round, randomly generates a bit b_B and, according to the value, chooses one base, $\bigoplus$ or $\bigotimes$, and measures the photon in that base. The outcome of the measure is a bit: s_B. The process is repeated many times, until they collect a large number of bits. At this point the quantum part of the protocol is finished.

2. Alice and Bob publicly announce the value of their base's bits, b_A, b_B, through the classical public channel. They keep the rounds where they selected the same basis and they discard the others

3. At this point they share a certain amount of bits (s_A, s_B), randomly chosen, and they compare the outcomes. This part is the security check. Ideally, if there is no noise in the channel and no eavesdropper, the two bit-strings should match. If this is the case they go on with the protocol using the remaining bits. On the contrary, if errors are present this means that the channel is too noisy or that an eavesdropper is present. In this case, the protocol is aborted and starts again. Actually, the BB84 can tolerate a certain level of noise and a secret key can be established if the errors are less than a certain value. The actual parameter, used to check the security, is called Quantum Bit Error Rate (QBER) and is defined as:

   $$QBER = \frac{N_w}{N_w + N_r} \tag{2.3}$$

   where N_w is the number of events giving out a wrong output and N_r is the number of events leading to a successful results. The exchange is considered secure if the QBER is less then 11% for qubit [26].

4. After the security check, if successful, an error correction algorithm is performed. Alice and Bob exchange on the public channel a small portion of the remaining bits. With this operation they are able to correct the errors that could be still be present in their bitstrings.

5. Then privacy amplification is performed. This is a method for eliminating the information that Eve could gain during the quantum communication or during the error correction. After the privacy amplification Alice and Bob have two identical and secret bitstring.

6. The key is used by Alice to encrypt her message with an OTP cypher and is sent to Bob through the classical channel. Bob, that holds a key identical to the one used by Alice, can use it to recover the original message.

2.2.2 Security and vulnerabilities

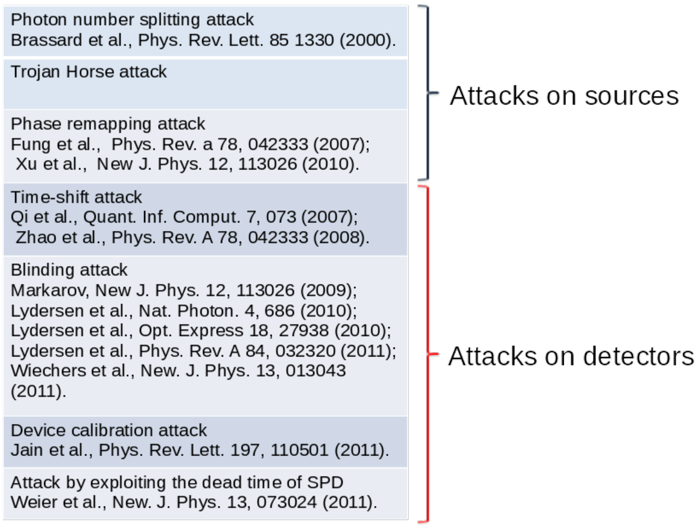
The security of BB84 can be intuitively described using three facts:

- Alice and Bob use a set of non orthogonal states

- The no-cloning theorem

- Information gains implies perturbation in QM

The idea is that if Alice and Bob are communicating non orthogonal states, for the No-Cloning theorem, Eve cannot perfectly copy the quantum state transmitted and, if she tries to do it, the state obtained by her necessary contains errors. On the other hand, if she tries to measure the state, she introduces errors in the communication which can be revealed by Alice and Bob.
This is a very naive and simplistic way to describe the security of the BB84, but during these years many physicists developed tools to formalize and rigorously demonstrate the security of these protocols. While the security proof with a perfect apparatus and a noise-free channel is quite straightforward, the fact that security can still be proven for an imperfect apparatus and noisy channels is far from obvious. In 2000 Shor and Preskill demonstrated that under some assumptions (that for the authors were quite practical) the BB84 protocol could offer unconditional security even with non-null noise (QBER < 11%) [26]. This unconditional security assures that QKD provides security against an Eve with an unlimited power, limited only by the law of physics. However in these years many practical attacks were proposed and realized against both prototype and commercial QKD systems. In Figure 2.3 some of them are listed.



Photon number splitting attack Brassard et al., Phys. Rev. Lett. 85 1330 (2000).	Attacks on sources
Trojan Horse attack	
Phase remapping attack Fung et al., Phys. Rev. a 78, 042333 (2007); Xu et al., New J. Phys. 12, 113026 (2010).	
Time-shift attack Qi et al., Quant. Inf. Comput. 7, 073 (2007); Zhao et al., Phys. Rev. A 78, 042333 (2008).	Attacks on detectors

Blinding attack
Markarov, New J. Phys. 12, 113026 (2009);
Lydersen et al., Nat. Photon. 4, 686 (2010);
Lydersen et al., Opt. Express 18, 27938 (2010);
Lydersen et al., Phys. Rev. A 84, 032320 (2011);
Wiechers et al., New. J. Phys. 13, 013043 (2011).	

Device calibration attack Jain et al., Phys. Rev. Lett. 197, 110501 (2011).	
Attack by exploiting the dead time of SPD Weier et al., New. J. Phys. 13, 073024 (2011).	

Figure 2.3: *List of attacks to QKD*

But how is possible to crack security of QKD if this has been mathematically proven to be unconditionally secure?
The key points are the assumptions made during the security proofs!
For the security proofs listed before some basic assumptions are always made:

- Eve must obey to the law of physics
- There is no information leakage from Alice and Bob laboratories (ie Eve doesn't know the settings used at each run)
- Alice and Bob have access to a trusted random number generator
- Alice and Bob have access to an authenticated public classic channel
- Alice and Bob have a **perfect** characterization of the physical functioning of their preparation and measurement apparatuses

If one of these assumptions is not respected, the security of the entire protocol cannot be guaranteed anymore. Among all the assumptions, the last one is clearly the most difficult to meet, since real devices always comes with some sort of imperfections. This discrepancy, between theoretical assumptions and experimental implementation of the protocols, opens the doors to a multitude of attacks that can completely compromise QKD. These attacks usually exploit the imperfections of Alice preparation stage, included the single photon source, or the inefficiencies of Bob's measurement apparatus.
The most common and documented attacks are:

- **Photon Number Splitting (PNS):** The current technology doesen't offer an on-demand single photon source. For this reason, usually weak coherent pulses (WCP) from a laser source are used. The photon number statistics of these sources, however, follows a Poisson distribution and the probability to have multi-photon emission is always non-zero. In this cases Eve can simply block all the single photon events, and for multiphoton events she forwards one of the photons to Bob and she can measure the others, without disturbing Bob's system, thus breaking the protocol [27]. The attack can be discovered using Decoy states: pulses with different mean photon number are used and by looking at the statistics of the received pulses Alice and Bob can understand if Eve is manipulating the photon number statistics.[28]

- **Intercept and resend:** Eve can intercept the qubit sent by Alice before it actually reaches Bob and she can measure it along some basis. According to the value she obtained then she can prepare and send a new qubit to Bob. However, doing so she introduces errors in the final measures on Bob's side. Using an optimal strategy Eve can lower the errors introduced down to 11% [26], and so this attack can be avoided if the QKD protocol is aborted if the security check finds out errors in the communication above this level.

- **Trojan horse:** In these attacks Eve can send bright pulses into Alice or Bob's apparatus. By looking at the reflections coming back from their devices she can learn the modulation they used, and so their settings [29]. This is equal to an information leakage from their lab. The vulnerability can be patched using insulators at the output of Alice and Bob's devices or attenuators but they are really insidious in 2-ways configurations.

- **Detector's blinding:** This class of attacks is probably the most successful one and has broken also commercial QKD systems [30]. In this attack Eve shines a continuous bright laser to Bob's detector, blinding it. In this regime, Bob's detectors are not single photon detector anymore: they click only if another bright pulse is shot at it, regardless of the quantum properties of that pulse. In this way Eve has the full control of Bob's detector and can make it click when she wants, compromising the protocol.

- **Misalignment:** In the ideal BB84 the states are supposed to be the ones of the $\oplus$ and $\otimes$ base. Any real implementation of the protocol, though, will inevitably introduce misalignment in the preparation of the states and in the alignment of the measurement bases with respect to this ideal situation. If these misalignment are not taken into account, Alice and Bob can incorrectly conclude that they have established a secure key[31].

These attacks show that, albeit QKD offers a theoretically unconditional security today real implementation are still far form the ideality, opening serious security flags. Few solution to this

problem can be addressed.
First, is possible to improve security proofs in order to include imperfection of the devices and start to relax the assumptions used. This path however, requires to consider all the imperfections, also the ones still unknown, making it quite impractical. Since the problem is technological, an option could be to empower research on these devices in order to obtain nearly-ideal devices. However, this is a big challenge and real devices will always have, even small, imperfections respect the ideal one.
Finally, a third possibility is to develop protocols that intrinsically do not depends on the internal functioning of Alice or Bob's devices. These protocols are called Device-Independent and will be discussed in the next paragraph.

2.3 Towards a more robust QKD implementation

The security flaws depicted in the previous section, profoundly worried researcher in the Quantum Cryptography field, since they could be used to completely break security of QKD. For this reason, in the last few years a lot of effort has been put to find a way out of this situation. In 1998 Mayers and Yao [32] conceived the idea of a "self testing" protocol, where security would be guaranteed based solely on simple test performed on the system, while treating the quantum devices as completely uncharacterized entities. After the initial proposal, many protocols followed and with them, also security proofs [33]. Interestingly, there is one thing that all the DI protocol have in common: they are all entanglement-based. This Full-Device-Independent protocol, however, requires many challenging technological problems to be solved before having a practical implementation. For this reason other protocols with a more feasible implementation, the Measurement-Device-Independent (MDI) and the Semi-Device-Independent(SDI), have been proposed.

2.3.1 Device-Independent QKD

Device independent protocols are all based on the violation of some Bell inequalities, and therefore they're all entanglement-based. The simplest protocol is just a slight variation of the E91 protocol proposed by A.Ekert in 1991 [24].
The protocol works in this way:

- A source generates a pair of entangled photons (the protocols works also for others kind of particles). One of these photons is sent to Alice and one to Bob. They both have a box that is able to measure the polarization of the photons along some axis, which depends on the settings of the machine. Alice can choose between three settings, and her choice can be represented with a trit $x = \{0, 1, 2\}$ while Bob's device has only two settings, $y = \{0, 1\}$.
  At each round of the experiment Alice and Bob randomly choose a value for a, b and they measure the incoming photon with that setting. The outcome of the measure is a bit a, b for Alice and Bob respectively. The settings are chosen such that for $x = \{0, 1\}$ and $y = \{0, 1\}$ they can obtain a maximum violation of the CHSH-inequality (Sec 1.3.1). The setting $x = 2$ instead should be aligned with the base of the setting $y = 1$. These settings are the one for which the experiment has the maximum performance but they are not required for the security of the protocol, where nothing is assumed about this devices.

- After performing the quantum communication n times, Alice and Bob reveal a subset of their settings and outcomes. They use the events with $x = \{0,1\}$ and $y = \{0,1\}$ to compute the CHSH inequality, S_{meas}. If the value is lower than the security bound S_b chosen (S_{max} is $2\sqrt{2}$) they abort the protocol. In this case they conclude that Eve, by interacting with their system, perturbed the states they've measured.
- If value measured is above or equal to the security parameter, they reveal their settings for each round and they select the events with the settings $x_i = 2$, $y_i = 1$.
- With the corresponding a_i and b_i they perform error correction and privacy amplification. They end up with two identical secure keys.

In this case the security relies only on violation of a Bell inequality and is guaranteed by a property of entanglement, called monogamy. The monogamy of entanglement states that two quantum systems that are maximally entangled cannot share any entanglement with a third system. In the case of the CHSH inequality, if Alice Bob and Eve (A,B,E) share a quantum state ρ and $\mathscr{B}_{AB}, \mathscr{B}_{AE}$ are CHSH operators for the pair Alice-Bob and Alice-Eve, the monogamy states that:

$$|Tr(\mathscr{B}_{AB}\rho)| + |Tr(\mathscr{B}_{AE}\rho)| \leq 4 \tag{2.4}$$

and so if Alice and Bob violate the CHSH inequality Alice and Eve (or Bob and Eve) cannot.[] Thanks to this property, given a violation of a Bell inequality, between Alice and Bob, is possible to upper-bound the information that Eve could have gained and so estimate the critical security parameter S_b. Besides, is important to stress that the security is guaranteed only by looking to the data obtained by the experiment, without assuming anything about the device used to perform the protocol. In this way the last assumption in the list 2.2.2 can be dropped, making DI protocol invulnerable to all the attacks described in the previous section.

The key point for the security of the DI protocol is the violation of a Bell inequality. Unfortunately this is also its main drawback. As already discussed in Sec 1.3, violations of a Bell inequalities are useful only if they are performed loophole-free. If this is not the case, the results are inconclusive. For the same reason, the security of a DI protocol is guaranteed only by a **loophole free** violation of the Bell inequality. This is a really tough challenge, especially for photonic implementation due to the low efficiency of detectors, making hard to close the detection loophole (a detailed explanation can be found in Sec 4.1.5). Moreover the rate achievable by DI is quite low (10^{-10} bits per pulse) compared to the rates possible with BB84 for example [33].

Since no one could perform a loophole free Bell test, except for [10][9] [8] that are still in hands of the peer-reviewer, other protocols, inspired by the DI have been proposed. These protocols offer a more practical implementation and an higher security compared to the "standard" QKD but, since they are forced to add some more assumption respect the DI, cannot reach the security of the DI.

2.3.2 Measurement-Device-Independent QKD

The Measurement-Device-Independent (MDI) is a relaxation of the DI paradigm and is focused on removing all the side-channels of the measurement device. This means that respect the DI it has one more assumption: that the preparation devices are working perfectly or that they are fully characterized. Despite the DI it can be implemented using standard optical components

with low detection efficiency and highly lossy channels. Moreover,it doubles the transmission distance that can be covered using conventional laser diodes.
MDI was first proposed in 2011 by Lo et al. [34] and since then many successful experimental realization have been performed [35][36][37], up to the stunning distance of 200 km [38]. The MDI is inspired by the DI protocol, where Alice and Bob receive an EPR pair, but completely reverse the setup: now Alice and Bob both prepare a photon each and they send the photons to a third untrusted relay (Charlie) that performs an entangling measure, known as Bell state measure. This measure, if successful, projects the two-photon state into a Bell state, which is revealed using two pairs of detectors. The scheme of the setup is sketched in Fig. 2.4 Alice and Bob can both prepare a photon in one of the BB84 states and they send it to an untrusted relay, Charlie, using Decoy states. Charlie performs a Bell State Measurement (BSM) on the two particles, projecting the two photons into an entangled state:

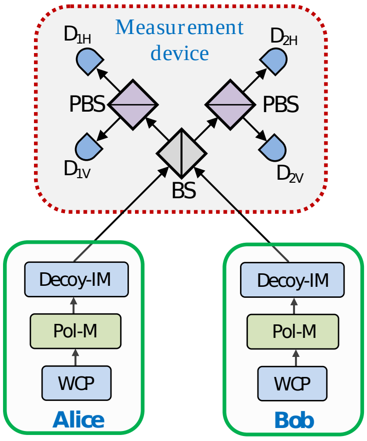


Figure 2.4: *Simple scheme of an MDI setup*

$$|\psi_{-}\rangle = \frac{1}{2}(|HV\rangle - |VH\rangle) \qquad |\psi_{+}\rangle = \frac{1}{2}(|HV\rangle + |VH\rangle) \tag{2.5}$$

Only 2 of the 4 possible Bell states are considered, because is impossible to build an optical implementation that can distinguish all the 4 Bell states without photon number resolving detectors. For the setup in Fig 2.4, if a coincidence detection occurs in $D1_H$ and $D2_V$ or $D2_H$ and $D1_V$, the BSM projected into the state $|\psi_{-}\rangle$, while if the coincidence is in $D1_H$ and $D1_V$ or $D2_H$ and $D2_V$, the projected state is $|\psi_{+}\rangle$. After the successful projection, Charlie broadcasts the successful events and the outcomes. Alice an Bob can use the decoy states method to evaluate de QBER. Alice and Bob then reveal their choices of bases over an authenticated channel and discard coincidence events where they use different bases to generate a sifted key. A secret key can be generated after error correction and privacy amplification.
This protocol, if one assume a perfect preparation from Alice and Bob, is equivalent to the time-reversed DI. Intuitively, the security of MDI-QKD relies on the fact that Charlie is post-selecting entanglement between Alice and Bob, who can verify such post-selected entanglement via authenticated public discussion of their polarization data. Since the detection system can be placed in an untrusted third party in MDI-QKD,the detection side channel are completely removed.
The main issues for the realization of MDI is linked to the BSM. To successfully obtain such measure, the two users must prepare and distribute the two photons in a way that when they arrive at

the BSM they are completely indistinguishable. In fact physics behind this protocol is based on the photon bunching effect of two indistinguishable photons at a 50:50 BS. This requirement is not an easy task to obtain for photons coming from completely different sources. Moreover also the distribution must be carefully controlled in order to have at BSM two photons with the same spectrum and arrival time.
Despite these big challenges, MDI has been already implemented in fiber using both polarization [37] and time-bin encoding [38], with key-generation rates of many order of magnitudes higher than the DI case ($\approx 10^{-5} \div 10^{-6}$).

2.3.3 Semi-Device Independent QKD

Besides DI and MDI, another protocol was proposed in order to strengthen the security of "standard" QKD and is called Semi-Device-Independent (SDI). The SDI, like the MDI, cannot offer a security as high as the DI, but was conceived to be more applicable. This protocol has been first proposed in 2011 by Pawlowski and Brunner [39] for QKD and then has been studied and applied also for the generation of true random numbers [40][41]. Also here one more assumption is introduced, respect the DI case, and regards the dimension of the quantum system exchanged: for the security proof is assumed that the dimension of the quantum system exchanged by the users is known. This is because the security is based on the violation of Dimension Witness (DW) inequality. This dimension witness can test the lower bounds on the dimension of classical or quantum systems. Like the DI case if a violation of this dimension witness is obtained, is possible to certify the security of the communication by only the results of the data extracted from the test, thus without assuming anything of the preparation and measurement devices (a more detailed overview is presented in Sec. 4.1). The SDI, unlike the DI, is designed to be a prepare'n'measure protocol and not an entanglement-based one, thus reducing a lot the experimental difficulties for its realization. Compared to the MDI, it seems to offer an higher level of security since apart from the dimension of the Hilbert space of the quantum system, doesn't assume anything else about the preparation device. However, like the DI, it needs high detection efficiencies to be secure and the security proofs are still in an early stage.
The SDI is probably the least explored protocol among all the above discussed and potentially offers a good trade off between the security of the DI and the experimental feasibility of the MDI. This is why in this Thesis we focused our attention on the experimental realization of this protocol.

2.3.4 Comparison

In order to better summarize the peculiarities and the drawbacks of each protocol, in Table 2.1, is presented a comparison of the pro and cons of each protocol.

Protocol	Pro	Cons
DI	• Minimal number of assumptions • Highest grade of security • Proven secure against the most general attack	• Requires entanglement, no p'n'm • Requires near unity transmission and detection efficiency • Hard to scale to networks • Low keyrate
MDI	• Removes detector's sidechannels • Already implemented • Double the distance • Good keyrate • Good for star-network	• Assumption about preparation • Very fine-tuned preparation
SDI	• Prepare'n'measure • More secure than MDI • Scalable to multi-party • Good for any-network	• Assumption on dimension • Requires high efficiency • Lacks of general security proofs

Table 2.1: *Summary of the pro and cons of each DI-like protocol*

CHAPTER 3

Polarization Stabilization

Working with optical fibers offers a lot of advantages respect the free-space alternative, but at the same time many new problems appear in this scenario. One crucial problem comes out when the control of polarization is needed and is caused by the intrinsic and induced birefringence of the fiber. The fiber's inner core is a circularly symmetric cylinder made of silica: because of the circular symmetry two orthogonal polarization mode should propagate with the same propagation factor inside the fiber. However because of internal defects, or because of external stress, the core exhibits effects of birefringence that can also change locally, thus resulting in a modification of the state of polarization. This means that, unless special polarization maintaining fibers are used, the state of polarization in input and at the output of the fiber will be, in general, different and can evolve with time. For many of our experiments we want to finely control the state of polarization of the light we are using (just think the importance of polarization transmission for a polarization-encoded BB84 protocol) and so we must find a way to control this dynamical polarization shift for all the duration of the experiment. One possible solution consists in the implementation of an active feedback system, that regularly measures the output state of polarization and automatically compensates for the change of polarization induced by the fiber. The components needed for the implementation of this real-time polarization stabilization are a polarimeter, needed for measuring the state of polarization of the light inside the fiber, and a polarization controller, placed before the polarimeter, which lets us change the in coming state of polarization of the photon to another arbitrary state of polarization .

Since for our application we need a fast polarimeter which can reconstruct all the four Stokes parameters S_i, and since the commercial ones couldn't fit all our needs, we decided to build our own polarimeter.

For the modulation we used a MPC1-01 Polarization Controller built by FiberControl.

In this chapter will be discussed the principle of operation of the polarimeter and the building process, from the optical part to the electronic and software point of view. Then the principle of working of the Polarization Controller will be presented and in the end we are going to discuss our feedback algorithm and the performance we can achieve with this setup.

3.1 Polarization

Polarization is a property of electromagnetic waves, that describes the direction of the oscillation of the electric field in a fixed position of space. So if $\boldsymbol{\varepsilon}(\mathbf{x},t)$ is the electric field of the wave , fixed $\mathbf{x}$, the direction of $\boldsymbol{\varepsilon}$ over time defines the polarization of the wave. Polarization is widely used in all field of classical telecommunication, since provides a physical way to encode information, and is widely used in quantum optics since the polarization of a single photon is a two level quantum system and so can be used as a qubit . In the next section will be briefly described the properties of polarization, a very helpful formalism for dealing with polarized states and the common elements used in optics for the control and modification of polarization.

3.1.1 Polarization Ellipse

The electric field $\boldsymbol{\varepsilon}(\vec{x},t)$ of an electromagnetic monochromatic plane wave travelling in vacuum along the z axis can be written as:

$$\boldsymbol{\varepsilon}(z,t) = \Re(\mathbf{A}e^{i2\pi\nu(t-\frac{z}{c})}) \tag{3.1}$$

where $\mathbf{A}$ is the complex amplitude of the wave that lies in a plane orthogonal to the z direction and can be decomposed as $\mathbf{A} = A_x\hat{\mathbf{x}} + A_y\hat{\mathbf{y}}$, ν is the frequency of the wave and c is the speed of light in vacuum. Since we want to take the real part of $\boldsymbol{\varepsilon}(z,t)$ we can decompose $A_j = a_j e^{(i\phi_j)}$, and we can write

$$\varepsilon(z,t)_x = a_x\cos(2\pi\nu(t-\frac{z}{c})+\phi_x) \tag{3.2}$$

$$\varepsilon(z,t)_y = a_y\cos(2\pi\nu(t-\frac{z}{c})+\phi_y) \tag{3.3}$$

These are the parametric equations of an ellipse of the form:

$$\frac{\varepsilon_x^2}{a_x^2}+\frac{\varepsilon_y^2}{a_y^2}-2\cos(\phi_y-\phi_x)\cos(\frac{\varepsilon_x\varepsilon_y}{a_x a_y}) = \sin(\phi_y-\phi_x)^2 \tag{3.4}$$

This ellipse, visible in Fig 3.1, is characterized by two angles: Ψ, that defines the rotation between the x axis and the mayor axis and χ which determines the ellipticity, the ratio between mayor and minor axis.
These two angles are related to the previously defined quantities by the relations:

$$r = \frac{a_y}{a_x} \tag{3.5}$$

$$\phi = \phi_y - \phi_x \tag{3.6}$$

$$\tan(2\Psi) = \frac{2r}{1-r^2}\cos\phi \qquad 0 \le \Psi \le \pi \tag{3.7}$$

$$\sin(2\chi) = \frac{2r}{1+r^2}\sin\phi \qquad \frac{-\pi}{4} \le \chi \le \frac{\pi}{4} \tag{3.8}$$

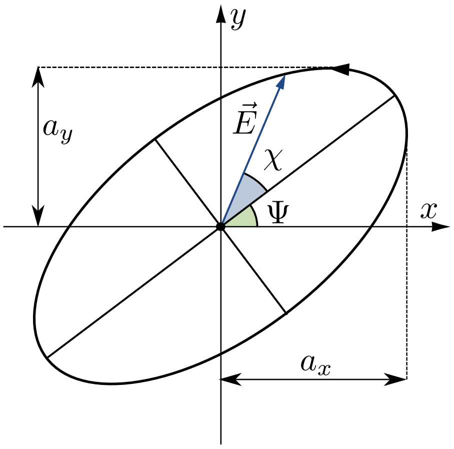


Figure 3.1: *Polarization ellipse*

The elliptical polarization is the most general case of polarization for a fully polarized wave, but, as we can see from equations 3.5-3.8, for particular values of the amplitude, this ellipse morphs into a circle or a line. The linear polarization can be obtained in two ways: by taking one of the two amplitude equal to zero ($a_i = 0$), making the ellipse to collapse into a line along the other axis. Another possibility is to set $\phi = \phi_y - \phi_x = 0 + n\pi$ for $n \in \mathbb{Z}$, having that $\chi = 0$; the direction of the line now is given by the ratio $r = a_y / a_x$ between the amplitudes.
The other special case is the one regarding circular polarization; this is achieved by setting $\phi = \pm\pi/2 + 2n\pi$ for $n \in \mathbb{Z}$ and $a_x = a_y = a$, so that equation 3.4 becomes

$$\varepsilon_x^2 + \varepsilon_y^2 = a^2 \tag{3.9}$$

These particular states are very important for Quantum Information Theory since they can be used for the encoding of photonics qubits.

3.1.2 Jones calculus

The Jones calculus is a formalism, introduced by R. Clark Jones [42], aimed to describe the state of polarization of an electromagnetic wave using a two component vector. This representation is very useful for understanding how polarised light evolves through mediums and is a simple and powerful way for the characterization of linear optics elements with 2x2 matrices.
Considering a monochromatic plane wave, Eq 3.1 describes the two orthogonal components of the electric field. These are determined by the complex amplitudes A_x, A_y and by the global phase $e^{i2\pi\nu(t-\frac{z}{c})}$, which describes the propagation of the wave in time. By dropping the last term, that doesn't affect the shape of the polarization ellipse, the two components can be written in a vector form:

$$\mathbf{J} = \begin{pmatrix} A_x \\ A_y \end{pmatrix} = \begin{pmatrix} a_x e^{i\phi_x} \\ a_y e^{i\phi_y} \end{pmatrix} \tag{3.10}$$

called Jones vector. Since usually one is interested only in the polarization state of the wave and not in it's intensity, the Jones vector is usually written in a normalized form obtained by dividing this vector by the total intensity $I = |A_x|^2 + |A_y|^2$ and by factoring the phase of the first component ϕ_x. In this way the vector depends only on the ratio r of the amplitudes and by the phase difference $\phi = \phi_y - \phi_x$ which, as seen in 3.8, are the parameters that characterize the polarization ellipse and the state of polarization. The special polarization states, described in the previous section, can be written using the Jones formalism are presented in Table 3.1.

Polarization State	Jones Vector	Polarization State	Jones Vector
Horizontal	$\|H\rangle = \begin{pmatrix}1\\0\end{pmatrix}$	Left Circular	$\|L\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$
Vertical	$\|V\rangle = \begin{pmatrix}0\\1\end{pmatrix}$	Right Circular	$\|R\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$
Linear at +45°	$\|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	Linear at angle θ	$\begin{pmatrix}\cos(\theta)\\\sin(\theta)\end{pmatrix}$
Linear at −45°	$\|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	General form	$\begin{pmatrix}\cos(\theta)\\e^{i\phi}\sin(\theta)\end{pmatrix}$

Table 3.1: *Jones representation of useful states of polarization*

By using this notation, the action of every linear optical component on the polarization of the light, can be expressed by a simple 2x2 matrix. This is a very powerful way to compute the action of even complicated setups: they can be modeled by writing the appropriate matrix for every basic component and then, by multiplying them, we obtain the matrix representing the action of the whole apparatus. Only few basic components are usually employed in common optical circuits, thus only these needs to be analyzed, all the others can be obtained as a combination. Some of these components will be presented now.

Linear Polarizer

One of the most common element is the linear polarizer. This element transmits the component of the electric field that lies along the direction of its transmission axis while blocking the orthogonal component. Considering its transmission axis parallel to the x-axis, the matrix for this element is given by:

$$M_p = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \tag{3.11}$$

Is easy to see that the output of a linear polarizer is always a linear polarized wave. Moreover the linear polarizer shows that these operators are not, in general, restricted to unitary operators.

Polarization rotator

Another component is the polarization rotator, which can be used to convert any incident linear polarization into linear polarization with a different angle respect the x-axis. The matrix is given by

$$M_{pr} = \begin{pmatrix}\cos(\theta) & -\sin(\theta)\\\sin(\theta) & \cos(\theta)\end{pmatrix} \tag{3.12}$$

For example, if the incoming light is a linearly polarized with an angle ϕ the output will be a linearly polarized with an angle $\theta + \phi$.

Wave retarders

Another important class of optical devices are the wave retarders or wave-plates. These components are made of birefringent crystals, with a fast and a slow axis that exhibits different refraction indexes along the two axes. When a plane wave passes through a wave retarder, the electrical field component along the fast axis propagates with a smaller refraction index compared to the component along the slow axis and at the output of the wave-plate, a relative phase difference is introduced between the two components. This phase difference depends on the thickness of the plate by:

$$\phi = \frac{2\pi\Delta n d}{\lambda} \tag{3.13}$$

with Δn the difference between the refraction indexes along the fast and slow axis, λ is the wavelength of the light and d the thickness of the plate.

The matrix for this type of components is given by:

$$M_{WR} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \tag{3.14}$$

and the component unchanged is the fast-axis while the retarded one is the slow-axis. Among all the wave retarders we can select two special types of retarders called: half-wave plate (HWP) and quarter-wave plate (QWP). The half-wave plate is a wave retarder with $\phi = \pi$ and converts +45° polarized light into -45° and vice versa. It also converts left circular to right circular and vice versa. The quarter-wave retarder instead has $\phi = \pi/2$ and converts ±45° linearly polarized light into circular and vice versa. These components are at the basis for any kind of polarization modulation in experiments.

Rotated components

Until now we have considered elements whose optical axis is aligned with the x-axis of the Jones vector but in general they can be misaligned and this clearly modifies the behaviour of the component. This can be modelled by a simple change of reference system, in fact the coordinate system transformation that relates the same element in two different reference systems rotated by an angle θ, is given by the rotation matrix:

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \tag{3.15}$$

so that the Jones vector and matrix of the two systems are connected by the relations:

$$\begin{aligned} \hat{\mathbf{J}}(\theta) &= R(\theta)\mathbf{J} \\ \hat{M}(\theta) &= R(\theta) M R(\theta)^{-1} \end{aligned} \tag{3.16}$$

For example the matrix for half-wave and quarter-wave retarders rotated at angle θ is given by:

$$M_{HWP}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \tag{3.17}$$

$$M_{QWP}(\theta) = \begin{pmatrix} \cos^2(\theta) + i\sin^2(\theta) & (1-i)\cos(\theta)\sin(\theta) \\ (1-i)\cos(\theta)\sin(\theta) & i\cos^2(\theta) + \sin^2(\theta) \end{pmatrix} \tag{3.18}$$

In appendix A are reported some useful example of how polarization states can be converted using half and quarter wave retarders.

3.1.3 Partially polarized light

Until now we considered only one monochromatic plane electromagnetic wave and we discussed about what is polarization for that single wave. But what happens, from the point of view of polarization, when we consider light produced by different sources, like the de-excitation of a group of atoms? The resulting electric field of the wave, thanks to the superposition principle, will be composed by the sum of all the electric fields of the waves produced by every source. If the all atoms emit light at the same time, with the same frequency and the same phase, the resulting light will be again a plane monochromatic wave with different amplitude and hence still fully polarized since the variation of the direction of the electric field is still a deterministic process. But if the emission of light is a random process and the atoms emit at different time and/or with different phases, the resulting electric field will fluctuate in random way, and so the light won't be fully polarized.

A quantitative way to define the degree of polarization of light is achieved by looking at the statistical properties of the random electrical field and, in particular, to the correlation function of the field $\boldsymbol{\varepsilon}$ [43] defined:

$$G_{i,j}(\tau) = <\varepsilon_i^*(t)\varepsilon_j(t+\tau)> \tag{3.19}$$

where $i, j = x, y$ is the considered component of the field and $< >$ represents the time average:

$$<A(t)> = \lim_{t\to\infty} \frac{1}{T}\int_0^T A(t)dt \tag{3.20}$$

For the degree of polarization, the relevant information is contained in the cross-correlation G_{xy} which can be expressed in a normalized form:

$$g_{x,y}(\tau) = \frac{G_{xy}(\tau)}{\sqrt{G_{xx}(0)G_{yy}(0)}} \tag{3.21}$$

This quantity express the mutual correlation between the x and the y component of the field, respect the time-lag τ and satisfies $0 \le |g_{xy}(\tau)| \le 1$ for any value of τ.

For quasi-monochromatic light the dependence from τ in Eq. 3.19 can be factorized as a global phase $e^{i\omega\tau}$ so that the relevant quantity becomes $|g_{xy}|$ which is independent from τ.

A value of $|g_{xy}| = 1$ means that the two component are perfectly correlated and so the light is fully polarized. On the other side if $|g_{xy|} = 0$ there is no correlation and the light is completely unpolarized. These are the two extreme cases, but intermediate states exist where correlation is not maximal and the corresponding light is called partially polarized; the continuous parameter that describes the degree of polarization is given by:

$$p = \sqrt{1 - 4\frac{I_x I_y}{(I_x + I_y)^2}(1 - |g_{xy}|^2)} \tag{3.22}$$

with $I_i = <\varepsilon_i^*(t)\varepsilon_i>$ the intensity of the i-th component.

3.1.4 Stokes parameters

Jones formalism is a really powerful tool for working with full polarized light or with a single electromagnetic waves, but it cannot describe partially polarized light.

In 1851 G. Stokes introduced [44] a new formalism which is better suited for dealing with partially polarized light and offers a different way for represent the state of polarization of a wave. Instead of building his description on the electric field of the wave, Stokes shifted his attention on the intensity of the wave, and defined four parameters:

$$
\begin{aligned}
S_0 &= I_H + I_V = <|\varepsilon_x|^2> + <|\varepsilon_y|^2> = G_{xx} + G_{yy} = I_t && (3.23)\\
S_1 &= I_H - I_V = <|\varepsilon_x|^2> - <|\varepsilon_y|^2> = G_{xx} - G_{yy} = Ip\cos(2\phi)\cos(2\chi) && (3.24)\\
S_2 &= I_+ - I_- = 2\Re(<\varepsilon_x^*\varepsilon_y>) \qquad = 2\Re(G_{xy}) = Ip\sin(2\phi)\cos(2\chi) && (3.25)\\
S_3 &= I_L - I_R = 2\Im(<\varepsilon_x^*\varepsilon_y>) \qquad = 2\Im(G_{xy}) = Ip\sin(2\chi) && (3.26)\\
& && (3.27)
\end{aligned}
$$

We can see from the relations above that Stokes parameters can be obtained in many different ways, and they're basically related to any aspect of polarized light described so far. The first column shows how Stokes parameters can be obtained using only the information about the intensity of the analyzed wave; in fact I_j is the intensity of the wave measured in the j-basis. As we can easily see the S_0 parameter is just the total intensity of the wave I_t. The second column points out how Stokes parameters are related to the coherence matrix, while the third express the relation between Stokes parameters and the two angles of the polarization ellipse. The degree of polarization presented in Eq 3.22 can be also expressed in terms of Stokes parameters:

$$p = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0} \tag{3.28}$$

The four parameters over described are usually grouped in a 4-vector:

$$\mathbf{S} = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} \tag{3.29}$$

called the Stokes vector.
If we are not interested in the intensity of the wave but only in the polarization properties, we can divide each of the Stokes parameters for S_0 so that $S_i \leq 1$ obtaining the normalized Stokes vector. A list of common normalized stokes vector is present in Table 3.2

$\lvert H\rangle = \begin{pmatrix}1\\1\\0\\0\end{pmatrix}$	$\lvert L\rangle = \begin{pmatrix}1\\0\\0\\1\end{pmatrix}$	$\lvert +\rangle = \begin{pmatrix}1\\0\\1\\0\end{pmatrix}$	Linear at angle $\theta = \begin{pmatrix}1\\\cos(\theta)\\\sin(\theta)\\0\end{pmatrix}$
$\lvert V\rangle = \begin{pmatrix}1\\-1\\0\\0\end{pmatrix}$	$\lvert R\rangle = \begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$	$\lvert -\rangle = \begin{pmatrix}1\\0\\-1\\0\end{pmatrix}$	Unpolarized $= \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$

Table 3.2: *Normalized stokes vectors*

3.1.5 Poincaré Sphere

From Table 3.2, one can immediately see that, by dropping the first component S_0, all the possible normalized Stokes vectors belong to an unity radius sphere, called the Poincaré Sphere. This representation was first proposed in 1892 by H. Poincaré.[45].

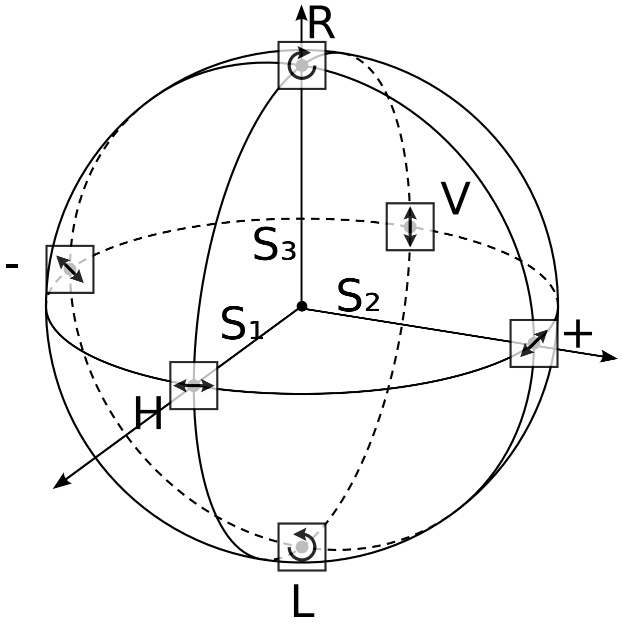


Figure 3.2: *Representation of the Poincaré Sphere*

This is an useful graphical representation for any possible state of polarization (SOP), where all the linear polarizations states lie on the sphere's equator, while the right and left circular polarizations are located on the north and south poles, respectively. All the remaining points on the surface are associated to the elliptical polarization states. Moreover, the radius of the Stokes vector on the sphere is equal to the degree of polarization, so every point on the surface of the sphere represents fully polarized light, while the origin of the sphere is an unpolarized state. All the other points inside are states of partially polarized light.

In this way is also easy to visualize the difference between Jones and Stokes vector, since the first can only describe points on the surface and not the entire sphere.

3.1.6 Mueller Calculus

The concepts of Jones matrix and Jones Calculus, presented in Sec. 3.1.2, can be extended to Stokes vectors by using a 4x4 matrix instead of a 2x2 like in Jones calculus. This generalization was first presented by H. Mueller in 1943 and is called Mueller calculus. Every Jones matrix J can be converted into a Mueller matrix M using:

$$M = A(J \otimes J^*)A^{-1}, \tag{3.30}$$

with A defined as:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & i & -i & 0 \end{pmatrix} \tag{3.31}$$

3.2 Polarimeter

The final goal is to obtain a fast polarization stabilization that must be way faster than the time scale on which polarization drift occurs. Clearly, the whole apparatus will be as fast as the slowest component, thus is mandatory to optimize every single element in order to get the best accuracy and speed. The first component analyzed is the polarimeter: a device that can measure the state of polarization of the incoming light. The requirements for this instrument are: complete reconstruction of the Stokes vector, be as fast as possible, have good accuracy and being able to be interfaced with a PC through a programming language. The few fast polarimeter commercially available didn't offered enough flexibility for our purpose, so we decided to build our own Stokes polarimeter.

3.2.1 Design of the Polarimeter

One of the first, and still very common, way to fully measure the all the Stokes parameter of a light beam, was proposed by G. Berry in 1977 [46] and is based on a rotating quarter-wave plate and a linear polarizer that can extract the information of the Stokes parameters through a Fourier analysis. This method can reach high precision but inevitably requires moving parts, limiting the maximum speed achievable. Moreover the alignment of the waveplate must be very precise and this can limit the accuracy obtainable by this kind of polarimeter. Since speed and accuracy are our main concerns, we decided to focus on other designs and implementations. A possible way to measure all four Stokes parameters simultaneously, employs division of wavefront (DOW) technique [47]. The beam is divided at least into four segments and a different stationary analyser is placed in each segment. Photodetectors positioned behind these fixed analysers record signals from each portion of the wavefront and determine the four Stokes parameters. The DOW technique, unfortunately, is limited by few factors: the beam must be uniformly polarized over its cross-section, the proportions of the total light flux in different wavefront segments has to be known, and the absolute response of all photodetectors must be the same or has to be calibrated. Furthermore this technique requires very precise tuning of all the optical components, such lenses, and is more difficult to employ with coherent illumination, due to coherent scattering and interference.

Another no moving parts design uses liquid crystals as variable and electrically-driven, wave retarders [48]. The main drawbacks of this implementation are: the requirement of expensive LCD, and the fact that LCD modulation has to be serial, limiting the speed of the entire apparatus.

One of the most interesting implementation that do not require moving parts and provides a simultaneous reconstruction is called Division of Amplitude (DoA) polarimeter and was first proposed in 1982 by R. M. Azzam [49] and then further developed in [50] and [51] for a four detector configuration. The idea behind this kind of polarimeter is simple and powerful at the same time. We have seen in section 3.1.4 that one possible way to calculate the Stokes parameters is registering the intensity in different basis:

$$\begin{aligned} S_0 &= I_H + I_V \\ S_1 &= I_H - I_V \\ S_2 &= I_+ - I_- \\ S_3 &= I_L - I_R \end{aligned} \tag{3.32}$$

The DoA polarimeter uses beamsplitters (BS) to divide the beam to be measured in two or more beams that are processed simultaneously. In particular, using wave plates and polarizing beam splitter (PBS), one can simultaneously measure the intensity of the light in two or more basis, and so using Eq 3.32, all the Stokes parameters can be retrieved. This method can employ as few as two detectors with analysis of two orthogonally polarized components of light, or it can measure the complete Stokes vector using four detectors, although an higher number of detectors can be used in order to improve the precision [52],[53],[54],[55],[56].

This method has many advantages: can be entirely built using common optical elements like BS, PBS and waweplates, is fast and the speed is virtually limited only by the speed of the detectors or the ADC and is stable respect temperature fluctuations. Anyway the main disadvantage of this setup is the calibration that can be tricky and will be deeply discussed after in this thesis.

For these reasons the DoA was selected as a starting point for our polarimeter and the final design adopted is presented in Figure: 3.3.

3.2.2 Theory of operation

While in the previous section we explained why we have chosen this particular design for the polarimeter among all the possible configurations, in this section will be presented the theory of operation of the polarimeter. By looking at Figure: 3.3, we see that the first element is the light source; we used mainly 2 different sources for testing the polarimeter: the first one is an Thorlabs FPL1009S: a continuous laser source working at 1550 nm and powered by a Fabry-Pérot laser diode with 100 mW typical max power and 10 nm FWHM spectral width. The output is a fully polarized light along the horizontal direction. The other is a Thorlabs SLD1005S, a non coherent, super-bright LED source, with 22 mW of continuous maximum power, 50 nm FWHM spectral width. The both are mounted inside a Thorlabs CLD1015, a LED/Laser driver with TEC that give us the possibility to easily change the optical power. We decided to use two different sources, a coherent and a non-coherent one, in order to test the response of the polarimeter to both fully

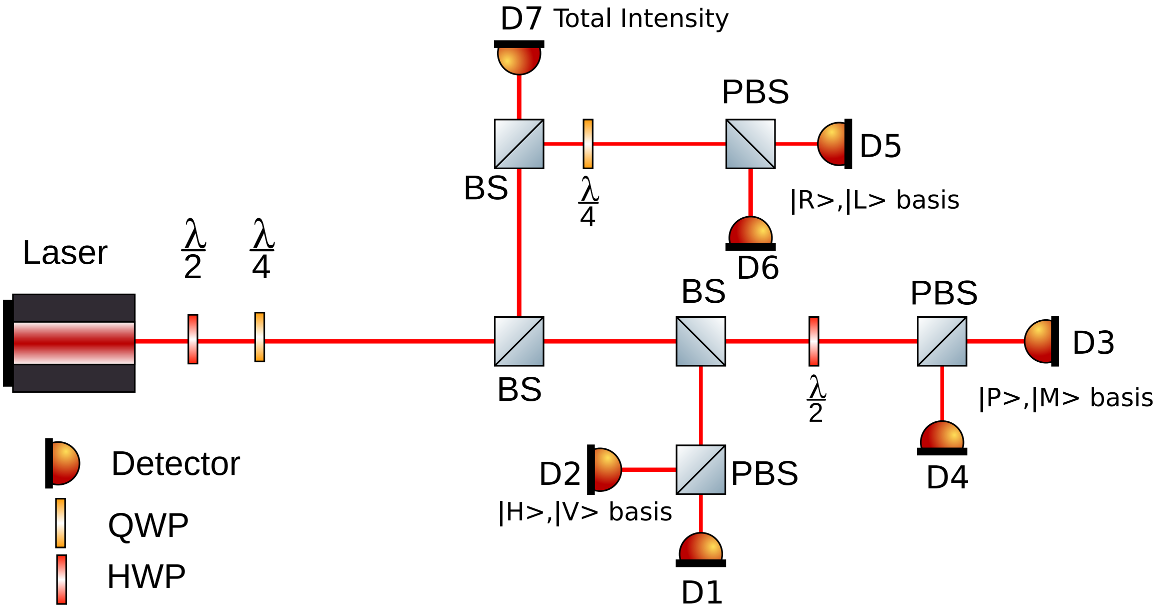


Figure 3.3: *Setup of the polarimeter*

and partially polarized light. From now on, for simplicity, only fully-polarized light is considered so when the source's properties are mentioned they are referred to the first one.
Since we want to be able to generate any possible state of polarization, in order to fully characterize the polarimeter, and since the laser can give us only horizontally polarized light, after the source a half-wave and a quarter-wave plate are placed. In this way the light coming from the laser is transformed to any possible state of polarization, by simply changing the angles of the two waveplates. By using the Jones formalism we can describe the action of the waveplates by an unique matrix:

$$HWP(\phi)\cdot QWP(\theta) = \begin{pmatrix} -\frac{\cos(2(\theta-\phi))-i\cos(2\phi)}{\sqrt{2}} & \frac{\sin(2(\theta-\phi))+i\sin(2\phi)}{\sqrt{2}} \\ \frac{i\sin(2\phi)-\sin(2(\theta-\phi))}{\sqrt{2}} & -\frac{\cos(2(\theta-\phi))+i\cos(2\phi)}{\sqrt{2}} \end{pmatrix} \tag{3.33}$$

The angles of the waveplates used are reported in table 3.3.

Final state	Half wave ϕ(rad)	Quarter wave θ (rad)
|H>	0	0
|V>	$\frac{\pi}{2}$	0
|+>	$\frac{\pi}{8}$	$\frac{\pi}{4}$
|->	$-\frac{\pi}{8}$	$\frac{\pi}{4}$
|L>	$\frac{\pi}{4}$	$\frac{\pi}{4}$
|R>	$-\frac{\pi}{4}$	$\frac{\pi}{4}$

Table 3.3: *Settings used for converting \|H> into any other state of polarization*

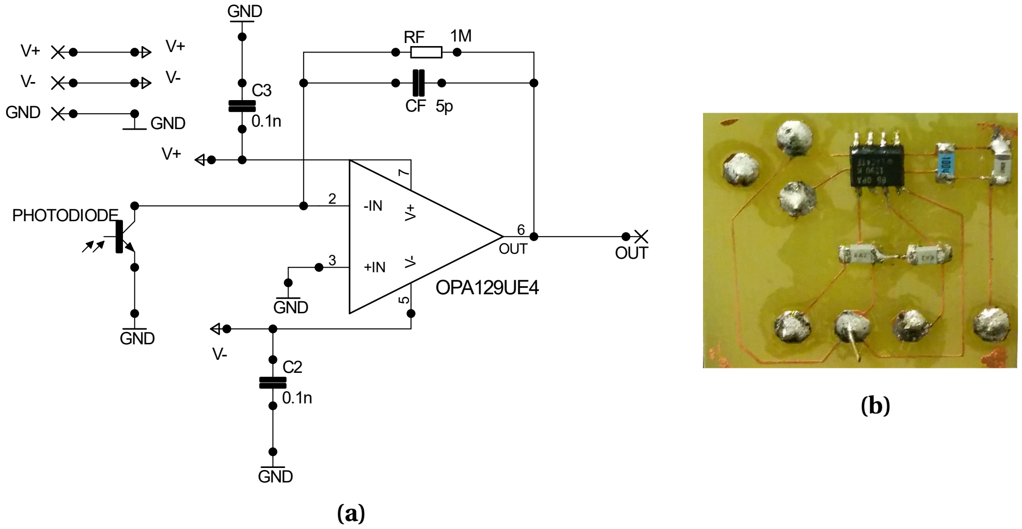
The system composed by the laser and the waveplates is our "simulated" source and will be used for characterization and calibration. The real part relative to the polarimeter will be now

described. The incoming beam goes through a beamsplitter that divides it into two different beams. Then these are divided again using two beamsplitters, one for each optical path.
So after three beamsplitters the initial beam is divided into four, each one with $1/4$ of the intensity of the initial one.
Then one of the four beams goes directly into one of the detectors; this is used as a power monitor and is also needed in the reference-free calibration method that will be discussed after. As explained in section 3.2.1 the DoA polarimeter requires to measure the polarization of the beam in two or more basis (three in our case), but how is possible to do that with standard free-space components? In fact, the polarization beamsplitters are built to transmit and reflect horizontally and vertically polarized light respectively, giving the possibility to measure only in the $|H>, |V>$ base. To measure in other basis, we placed an appropriate waveplate before the PBS. In this way the polarization of the incoming beam is "rotated" into the $|H>, |V>$ base and then measured by a common PBS. In order to clarify this statement lets give an example. Suppose the incoming light is fully polarized along, lets say $|+>$. If we measure this in the $|+>, |->$ base we should get the maximum intensity in one detector and nearly nothing (there will always be some noise or imperfection of the components) in the other one. If we use only a PBS we will get half of the maximum intensity in both detectors. But if we place an half wave plate rotated at $\pi/8$, $|+>$ will be converted into $|H>$ and $|->$ will be converted into $|V>$ and so the PBS will give full intensity in one detector and zero in the other, exactly what we wanted from a $|+>, |->$ base measurement. Everything said before can be exactly applied also for the $|L>, |R>$ case if we change the HWP at $\pi/8$ with a QWP at $\pi/4$.
Summing up: the initial beam is processed and divided into 7 beams whose intensity is registered by 7 detectors. The detectors convert the light intensity into an electric current which is amplified and then acquired with an Analog-to-Digital converter and recorded by a PC. Now there are several ways to reconstruct the Stokes parameters from these raw electrical signals: all depends on the specific calibration procedure one wants to apply. The calibration at first sight can appear as a trivial step but many factors contribute to make it quite tricky. For this reason a detailed description of the calibration is given in section 3.2.4.

3.2.3 Electonics

The electronic part of the apparatus consists only in the photodetector's circuit and in the ADC converter. The ADC is a NI-6001 from National Instruments, it consists of 8 Analog Inputs rated up to ± 10V and $20 kS/s$. The photodetector used is Hamamatsu G8370-01, a InGaAs PIN photodiode with low noise and low dark counts. This photodiode has a typical efficiency of $0.95\,\mathrm{A\,W^{-1}}$ at wavelength of 1550nm. The maximum dark current is 5 nA. However these photodiodes don't include a pre-amplifier in the package so, in order to collect a nice shaped signal, we had to design and build our own transimpedance amplifier circuit. The aim of this circuit is double: first, acts as a transimpedance circuit so it converts a current signal, the output of the photodiode, into a voltage signal and, at the same time, it provides an amplification of the original signal so that the output level can be optimized in order to use all the range offered by the ADC, improving the accuracy of the data gathering. Is also crucial to have this circuit as near as possible to the photodiode in order to minimize noise and interference.
At this point there are usually two ways to deal with a photodiode, called photoconductive and photovoltaic mode: with the first one one can reach grater speed while the second one offers a

better accuracy and lower noise. The practical difference is whatever a bias voltage is applied or not, between the P-I-N junction of the photodiode; if a reverse voltage is applied, the carriers are forced to move faster, thus increasing the speed of the photodiode, but also increasing the dark counts rate: this is the photoconductive mode. If no bias voltage is applied to the junction, the carriers are slower and the device itself has a lower bandwidth but the dark count rate and the noise is minimized.
By testing the photovoltaic mode, we saw that the speed we could reach was sufficient for our needs and we decided to use the photodetector in this mode. It provides a better accuracy and a lower noise, having no inverse current of saturation [57]. In figure 3.4 is showed the scheme of the circuit



(a)

(b)

Figure 3.4: *a) Schematic of the transimpedence amplifier used for the photodiode. b) PCB of the finished circuit*

The amplifier circuit is realized using an operational amplifier (OPA), an TI OPA129 [58] with a resistor (R_f) of 1 MΩ and a capacitor (C_f) of 5 pF in feedback. The photodiode is connected between ground and the inverting input of the opamp, while the non-inverting input of the OPA is connected to ground. This provides a low impedance load for the photodiode, which keeps the photodiode voltage low. The high gain of the OPA keeps the photodiode current equal to the feedback current through the feedback resistance. In this configuration the gain of the circuit is:

$$V_{out} = -R_f \cdot I_{phot} \tag{3.34}$$

Since we are interested in the DC level of the output, we need to care also of the possible offsets. The input offset voltage due to the photodiode is very low in this self-biased photovoltaic mode. This permits a large gain without any large output offset voltage. Other possible offset can be caused by bias current of the OPA. This current is caused by the gate/base currents of the transistor that can flow through the input stage because the input impedance of a real opa is finite and not infinite. These tiny currents can flow to external impedances, and in particular through the big feedback resistance giving to birth to a noticeable voltage offset. For this reason we choose the OPA129 among a wide selection of OPAs. The OPA129 in fact is designed for precision and low noise applications and is able to keep the bias current below 100fA [58]. One could ask why we have not chosen a smaller resistance and implement a two-stage amplifier in order to overcome this problem? The answer is that the resistor thermal noise is described by

$$VRM_{noise} = \sqrt{4K_b T N_{bw} R_f} \tag{3.35}$$

where K_b is the Boltzmann constant, T is the temperature, N_{bw} is the noise bandwidth and R_f is the feedback resistance. If we consider the SNR as:

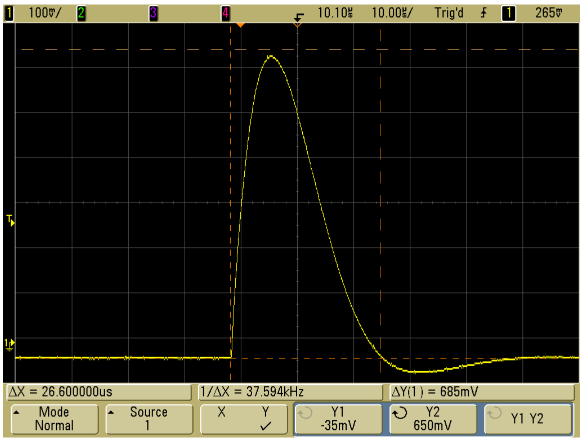
$$SNR = \frac{V_{signal}}{V_{noise}} \propto \sqrt{R_f} \tag{3.36}$$

so from the point of view of noise is way better to use a big resistor in the transimpedence stage since the SNR grows if R_f grows.

For what regards C_f, the purpose of this capacitor is to prevent the circuit to oscillate or gain-peaking effects. In fact the the non-null photodiode capacitance can raise instability problems because it creates a low-pass filter in the feedback path. Adding a capacitor in feedback creates a zero and modifies the pole of the low-pass filter. If the compensation is done right is possible to obtain stability for the circuit. The drawback of this approach is that, adding a feedback capacitor, causes the bandwidth of the amplifier to be reduced depending on the size of the capacitor. For our purpose we found that a C_F of 5 pF is the best compromise between stability and bandwidth.

Another thing to consider when one works with fast signals are decoupling capacitors. A decoupling capacitor's job is to supress high-frequency noise in power supply signals. They take tiny voltage ripples, which could otherwise be harmful to delicate ICs, out of the voltage supply. In a way, decoupling capacitors act as a very small, local power supply. If the power supply very temporarily drops its voltage, a decoupling capacitor can briefly supply power at the correct voltage.

The response of the amplifier to a 300 ps laser pulse is showed in Figure 3.5



ΔX = 26.600000us
1/ΔX = 37.594kHz
ΔY(1) = 685mV

Figure 3.5: *Voltage response of the preamp plus photodiode circuit to a* 300 ps *laser pulse.*

We can see that the signal response of the whole circuit to a typical 300 ps laser pulse is ≈ 26.6µs equivalent to a frequency of ≈ 37.594 kHz which is higher than the 28.57 kHz acquisition frequency of the ADC we are using, confirming that the photovoltaic mode is fast enough for our needs and so represents the best option for the preamplification circuit.

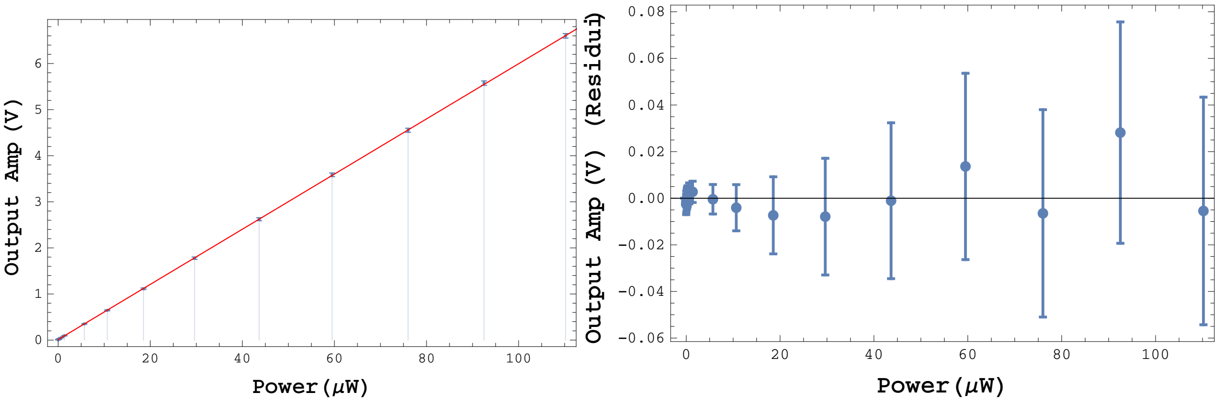


Figure 3.6: *Test of the linearity for one of the detector plus amplifier system*

Linearity

Before starting to use the photodiodes with the amplification stage is necessary to check that the response of the entire system is linear. The output voltage from the amplification stage should be ideally proportional to the light hitting the photodedectors. We already know that both the photodiode and the preamp are linear only in a certain region of operation, so we must ensure that the range we want to work with is inside the linear region. If this is not the case, a calibration of the Voltage(Light Intensity) relation is necessary in order to get non-biased results. In order to check the linearity we used an S122C optical power sensor based on a Ge Photodiode with a PM100D powermeter both from Thorlabs. The power sensor is specifically designed for the 700 - 1800 nm range and is certified from the company to have an uncertainty ≤ 5%. This powermeter was used to measure the power of the light coming from one end of a 50:50 beamsplitter connected to the CLD1015. The other end of the beamsplitter was directly connected to the input port of the polarimeter. The voltage output from the amplifier was digitalized and recorded with a National Instrument NI-6001 14bit ADC working in the 0-10 V range, thus having a resolution of 0.6 mV. Every value of the voltage recorded is obtained by averaging 1000 recordings and the errors associated are the standard deviations. With the CLD1015 we could easily change the power of the laser and then, by registering the output of the powermeter and the voltage output of each detector, we first plotted and then fitted the data with a linear function in the form $y = ax + b$. An example of the plot and the fit is presented in Fig 3.6 The result of the fit for each channel is presented in Table 3.4.

As we can see from the presented figures, both the fit and the residuals plot are showing a good agreement between the linear model and the data. Moreover, also the Pearson's R^2 is really close to unity, suggesting the validity of the linear relation. Anyway we need a quantitative and objective way for claiming that the data are linearly distributed. We choose to use the χ^2 test as a goodness-of-fit test for the data. For every value the critical χ^2_{cirt} is computed from the ν degrees of freedom and from the significance level $\alpha = 0.05$, a typical value for this kind of tests. Since for none of the channels the measured value of the χ^2 is larger than the corresponding χ^2_{cirt}, we cannot reject the null-hypothesis, that the data are consistent with the linear model.

Channel	a(V /µW)	b (V)	R^2	χ^2	$\nu(DoF)$	$\chi^2_{crit}(\alpha = 0.05)$
1	0.0772 ± 0.0002	0.021 ± 0.001	0.99989	8.8	14	23.7
2	0.0802 ± 0.0003	0.013 ± 0.002	0.99981	3.2	14	23.7
3	0.0735 ± 0.0001	0.0036 ± 0.0006	0.99996	2.2	14	23.7
4	0.0704 ± 0.0002	0.013 ± 0.001	0.99985	12.6	14	23.7
5	0.05985 ± 0.00009	0.0106 ± 0.0006	0.99997	2.1	14	23.7
6	0.06020 ± 0.00005	0.0101 ± 0.0004	0.99998	1.0	14	23.7
7	0.1664 ± 0.0003	0.014 ± 0.001	0.99997	6.6	11	19.7

Table 3.4: *Results of the fit for the linearity of the photodetection system*

3.2.4 Non idealities and calibration

Ideally the reconstruction of the Stokes parameters can be done using the optical power-voltage calibration discussed in the previous section and the definition of Stokes parameters given by Eq 3.32. Unfortunately this relation is good for our setup only if it is completely ideal. This, in practical terms, means that all the BS must be 50:50 and have no polarization-dependent losses, the PBS must have perfect transimissivity and refelctivity for horizontally and vertically polarized light, the waveplates must be perfectly aligned, the response of the photodiodes must be the same for all and there must be a perfect alignment of every component in the apparatus. These requirements are really strict and is almost impossible to satisfy all of them because of the limited precision reachable by the manufacturer of the components and because of the limited precision on the overall alignment. One possible solution is to perform a calibration, by launching known state of polarizations and retriving the intensities recorded by each detector, in order to create a model for the polarimeter that takes into account the non-idealities before described. One of the first calibration method was proposed in [51] and relies on the fact that, even with the defects taken into account, the intensities recorded by each detector are linear functions of the Stokes parameters. In vector form this means that the vector of intensities $\mathbf{I} = (I_1, I_2, I_3, I_4, I_5, I_6)^t$ is related to the Stokes vector $\mathbf{S} = (S_0, S_1, S_2, S_3)^t$ by the application of a matrix A

$$\mathbf{I} = A\mathbf{S} \tag{3.37}$$

and so $\mathbf{S}$ can be retrived by just inverting the equation:

$$\mathbf{S} = C\mathbf{I} \tag{3.38}$$

where $C = A^{-1}$ is a 4×6 matrix and is called instrumental or calibration matrix. This matrix contains all the information about the internal working of the polarimeter, defects included. The instrumental matrix can be evaluated launching 6 non degenerate known states of polarization $\mathbf{S_i}$ $i = \{0, ..., 6\}$ and recording the corresponding intensities from the detectors $\mathbf{S_i}$ and then calculating:

$$C = \begin{pmatrix} S_{0,1} & S_{0,2} & \dots & S_{0,6} \\ S_{1,1} & S_{1,2} & \dots & S_{1,6} \\ S_{2,1} & S_{2,2} & \dots & S_{2,6} \\ S_{3,1} & S_{3,2} & \dots & S_{3,6} \end{pmatrix} \cdot \begin{pmatrix} I_{1,1} & I_{1,2} & \dots & I_{1,6} \\ I_{2,1} & I_{2,2} & \dots & I_{2,6} \\ I_{3,1} & I_{3,2} & \dots & I_{3,6} \\ I_{4,1} & I_{4,2} & \dots & I_{4,6} \\ I_{5,1} & I_{5,2} & \dots & I_{5,6} \\ I_{6,1} & I_{6,2} & \dots & I_{6,6} \end{pmatrix}^{-1} \tag{3.39}$$

In the case where more than 4 detector are used, the current matrix I_{ij} has usually a null or nearly-null determinant [52], due to redundancies in the over-constrained system. This implies that the inversion of the matrix is impossible in the null case or is numerically unstable for the nearly-null case. In these cases Eq 3.39 can be rearranged in the form

$$C = \left(\begin{pmatrix} I_{1,1} & I_{1,2} & \dots & I_{1,6} \\ I_{2,1} & I_{2,2} & \dots & I_{2,6} \\ I_{3,1} & I_{3,2} & \dots & I_{3,6} \\ I_{4,1} & I_{4,2} & \dots & I_{4,6} \\ I_{5,1} & I_{5,2} & \dots & I_{5,6} \\ I_{6,1} & I_{6,2} & \dots & I_{6,6} \end{pmatrix} \cdot \begin{pmatrix} S_{0,1} & S_{0,2} & \dots & S_{0,6} \\ S_{1,1} & S_{1,2} & \dots & S_{1,6} \\ S_{2,1} & S_{2,2} & \dots & S_{2,6} \\ S_{3,1} & S_{3,2} & \dots & S_{3,6} \end{pmatrix}^{-1} \right)^{-1} \tag{3.40}$$

where the inverse is replaced by the Moore-Penrose pseudoinverse for non square matrices [59]. The use of the pseudoinverse gives better and consistent results since provides a least squares solution to a system of linear equations. After the calibration process is done, we know C for the wavelenght we used in the calibration, and we can compute the Stokes parameters by using Eq. 3.38. Although this method hugely improves the naive reconstruction given by Eq 3.32, still doesn't give good enough results. The main reason behind the limited accuracy obtainable using this method can be imputed to the way we generate the input states of polarization. In fact, as we can see in Figure 3.3, the different states of polarization are obtained rotating an half-waveplate and a quarter-waveplate and checking the intensity out of the corresponding detector. This is a very practical way for generate all the possible polarization from a linearly polarized source but the precision is limited to the precision on the angular setting of the waveplate and, without having a pre-calibrated source, cannot be improved.

"Reference-Free" Self-Calibration

A way to improve the previously presented calibration is described in [60] where the authors found a new method that doesn't require the states launched to be known. The advantage of this approach goes beyond the simple accuracy improvement and allows the experimenter to perform the calibration in a fully automated and remote way. Moreover, by only adding one more detector (for a total of 7 in our configuration) for monitoring the total intensity, also Polarization Dependent Losses (PDL) can be taken into account in the calibration matrix.

This calibration procedure relies on the imposition of a constraint on the input signals used to perform the calibration. The simplest and most robust constraint is to use signals with $DOP = 1$. This condition is relatively easy to verify in narrow linewidth lasers and can be transported over long lengths of fiber without significant degradation. The calibration matrix of the polarimeter is then adjusted so that measurements made at the polarimeter match the constraint on the input polarizations. The calibration procedure is performed in various steps:
First N different states of polarization are launched and for each one the intensities $\mathbf{I}_j$ $j = \{1, ..., N\}$ from the "basis" detector and the total intensity P_j from the new detector are recorded. Then we recall that $S_{0j} = P_j$ by definition and using Eq 3.38 to explicit S_{0j} we have:

$$P_j = \sum_{i=0}^{5} C_{0i} I_{ij} \tag{3.41}$$

Applying the least squares method the first row of the calibration matrix can be determined minimizing:

$$Q = \sum_j \left(\sum_{i=0}^{5} C_{0i} I_{ij} - P_j \right)^2 \tag{3.42}$$

which is satisfied for:

$$C_{0i} = Z^{-1} X|_i \tag{3.43}$$

$$Z_{ki} = \sum_{j=1}^{N} I_{kj} I_{ji} \tag{3.44}$$

$$X_k = \sum_{j=1}^{N} I_{kj} P_j \tag{3.45}$$

Now that we have determined the first row of the calibration matrix we can use Eq 3.38 to express for each run $\mathbf{S_j}$ in function of the 18 variables left in the calibration matrix:

$$S_{ij} = \sum_{k=0}^{k=5} C_{ik} I_{kj} \tag{3.46}$$

Now we can impose the initial constraint of $DOP = 1$ that can be expressed in terms of the Stokes parameters as:

$$S_0^2 = S_1^2 + S_2^2 + S_3^2 \tag{3.47}$$

In order to estimate the 18 variables we can minimize the function:

$$W = \sum_{n=1}^{N} \left(S_{1n}^2 + S_{2n}^2 + S_{3n}^2 - S_{0n}^2 \right)^2 \tag{3.48}$$

that express the relation $(DOP^2 - 1)^2$ and is an internal metric of the accuracy of the calibration. This expression has a minimum value of 0. Since this is a nonlinear least squares fit, it is useful to obtain an appropriate first guess that is as accurate as possible. To do this, we used the ideal calibration matrix for a polarimeter that measures projections onto a octahedron on the Poincaré sphere. This matrix assumes perfect polarizers and unity gains:

$$\begin{pmatrix} C_{00} & C_{01} & C_{02} & C_{03} & C_{04} & C_{05} \\ \eta & -\eta & 0 & 0 & 0 & 0 \\ 0 & 0 & \eta & -\eta & 0 & 0 \\ 0 & 0 & 0 & 0 & \eta & -\eta \end{pmatrix} \tag{3.49}$$

where η is a scaling factor given by the average of the first row. In our case the calibration was done with $N = 100$ and the state of polarization were launched by sending random value for the angle of the polarization controller placed before the polarimeter, but it can be done by simply shaking the fiber of the link. Then the nonlinear minimization was performed by the Minuit2 class of Cern's ROOT framework [61], using a combination of the MIGRAD and SIMPLEX algorithms. The whole process usually takes $\approx 11 - 12$s. Note that this optimization also has a sphere of minima in the space of the 18 variables, since a Stokes rotation R gives the same $DOP = 1$ condition, and so the matrices C and RC yield the same solution. The DOP metric is completely unchanged under such rotations, making W exactly the same. This means that the orientation of the reference system in the Poincaré sphere will be arbitrary and will depend on the specific minimum that the minimizer found. Anyway this is not a big problem since usually we are interested in differential measurements, for cancelling out the systematics, and so the effect of the random orientation is not important. However if we apply the same concept, after the reconstruction of C we can build a rotation R to rotate the C matrix, and so the reference system, without compromising the accuracy.

3.2.5 Optimization

Given the number of detectors, the best accuracy obtainable by the apparatus is the one that maximize the determinant of the calibration matrix[51]. This is obtained by choosing analyzers that maximize the spread of optimally detected states on the Poincaré sphere. For a four-detector system, this maximum spread requires that the optimally detected incident states represent vertices of a tetrahedron occupying the largest possible volume. Thus the arrangement with 4 detector projecting into two of the three $\{H, V\}$, $\{+, -\}$ and $\{R, L\}$ basis are not optimal. Moreover the realization of an optimal tetrahedron with only waveplates in the setups is quite tricky and much complex than considered six-detector geometry. In fact using six detectors the maximal spread is obtained if polyhedron is an octahedron and the combination of the three basis ($\{H, V\}$, $\{+, -\}$ $\{R, L\}$) are optimal. A graphical representation of this concept is showed in Figure 3.7

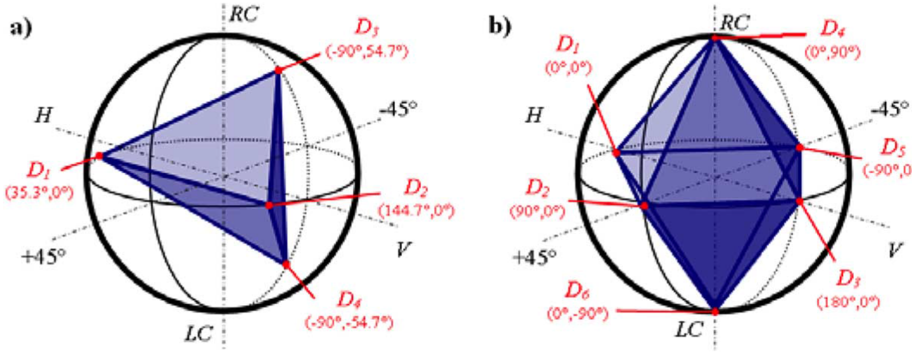


Figure 3.7: *Disposal of measuments on the Poincaré sphere for optimal reconstruction in the case of a) Four detectors b) Six detectors [60]*

Moreover, even if the DoA polarimeter requires only four measurands to uniquely determine four unknown Stokes parameters, an higher sampling in the space of parameters, and the inclusion of additional data, can be helpful to reduce disturbances that may perturb the system and can also help to average out noise with the consequent increase of the measurement accuracy. The first researches on this path were performed by R. M. A. Azzam in [62] [54] an then further explored in [56] and [52]. In these last two articles the authors studied how the increased number of measurands could help to lower the noise on the Stokes parameters introduced by the Shot and Gaussian noise, that inevitably affects the detectors. The results showed that the increased number of detectors improved by at least 20% the accuracy over the optimized 4-detector and, more important, the accuracy does not depend on the measured state. In Figure 3.8 is presented the noise on the reconstructed Stokes parameters depending on the input state of polarization for the non-optimized 4 detector configuration and for the 6 detector configuration.

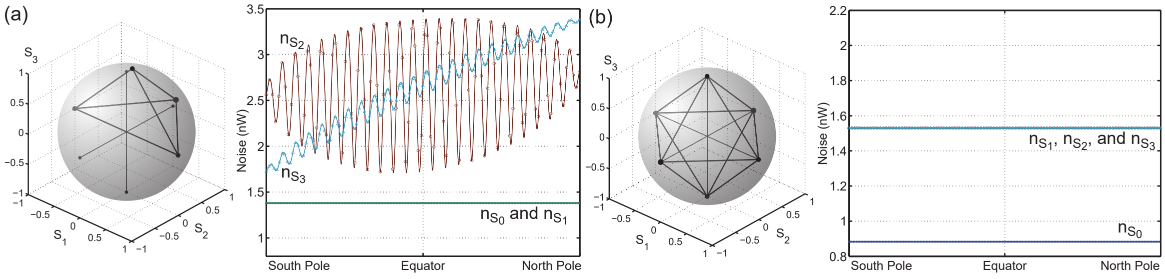


Figure 3.8: *Noise on the reconstruction of the Stokes parameters in the case a) non-optimized 4-detector b) optimized 6 detector configuration [56]*

3.2.6 Performance

The performance of the first calibration was tested using another reference polarimeter (rated to have ≈ 1% *SOP* accuracy) and calibrating our polarimeter respect the reference one so that they both have the same orientation on the Poincaré sphere. The results showed in Table B.1, presented for convenience in Sec A of the Appendices, shows that the discrepancy between the two polarimeters goes between the 0.1% and the 10% depending on the input state. For the second calibration method, the "Reference Free", since the orientation of reference system couldn't be aligned to the one of the reference and since we expect the accuracy to be comparable to the one of the reference polarimeter we decide to test it in a independent way. We used the HWP and the QWP before the polarimeter, and by rotating them by steps of 2 deg, we recorded the value of the corresponding Stokes parameters. Then the distribution of $S_i(\theta)$ is fitted with a curve in the form:

$$S_i = a\cos(w \cdot x + b) \tag{3.50}$$

The fitted value are then compared with the expected values: $A = 1$ and $w = 4$ while b depends only on the relative alignment between the "standard" reference of the Ponicaré sphere and the polarimeter's one. The results of the fit are presented in Figure 3.9 and in Table 3.5

Stokes parameter	a	$w(\,^\circ\mathrm{C}^{-1})$
S_1	0.996 ± 0.004	3.970 ± 0.007
S_2	0.991 ± 0.004	3.954 ± 0.008
S_3	0.993 ± 0.004	3.957 ± 0.009

Table 3.5: *Results of the fit*

As we can see the results are all compatible inside the 1% with the theoretical values. We also checked the Degree of Polarization of during this test and, as we can see from Figure 3.5 , it always lies inside the 2% deviation from the theoretical value expected that is 1. We can see that in some cases the physical bound Dop ≤ 1 is exceeded, but the deviation from the bound are still inside the errors, so compatible with the theoretical expectation and explainable in terms of statistical fluctuation or limits of our calibration procedure.

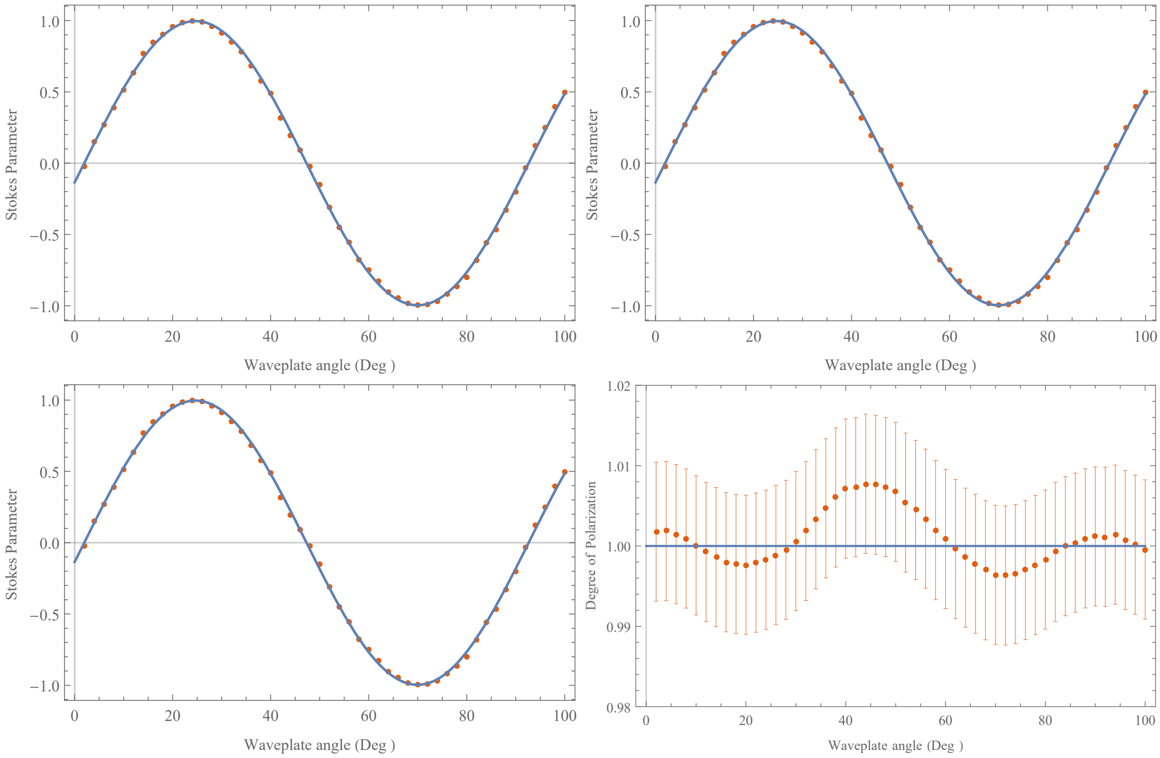


Figure 3.9: *In figure is showed the fit with the datapoint for S_1,S_2,S_3 and the DOP*

3.3 Polarization Controller

In order to control the polarization along the fiber we used a FiberControl MPC1-01, inline polarization controller. The device is an electronic polarization controller that can be operated and programmed remotely through GPIB IEEE 488.2 & RS-232 and BTM standard. The MPC1 is rated to have less than 1 dB of insertion loss, a minimum rotational resolution of 0.15 deg/step that can be varied to 1.5, 6, 15 deg/step.

3.3.1 Theory of operation

Internally the MPC1-01 is based on the electronic implementation of a Lefèvre loop, like the one showed in Fig. 3.10. This device, invented in 1980 by H.C Lefèvre [63], consist of three wave plates in a QWP-HWP-QWP configuration. Each wave plate is entirely fiber based and is made from a fiber coil where the radius and the number of turns determined the phase shift. The coil introduces stress in a fiber and therefore a change in the propagation index, and hence the phase, of two orthogonal polarizations. A rotation of the coil, will rotate the fast and slow axis of the coil, thus realizing a fixed-phase, rotating wave plate. For what concerns the QWP-HWP-QWP configuration, this is not casual. In fact this combination can transform any input state of polarization into any other state of polarization at the output. The idea in this case is quite intuitive. If we recall the Jones matrix of a QWP from Eq 3.18 and we do a bit of algebra we can find that for any input SOP it exist an angle θ that transforms that SOP into a linearly polarized

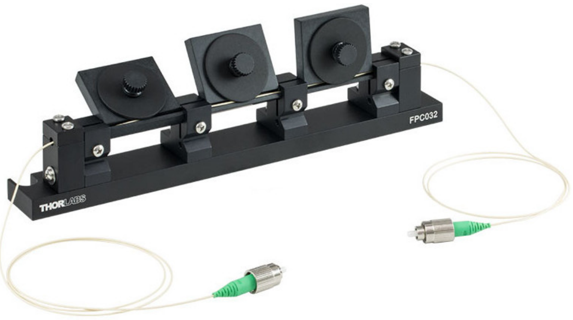


Figure 3.10: *An example of a Lefèvre controller*

one. The angle is given by:

$$\theta = \frac{1}{2}\arctan\frac{S_2}{S_1} \tag{3.51}$$

then is possible to use the HWP to rotate the input state along the plane of linear polarization and then by using again the other QWP is reconverted into the desired SOP. The MPC01-01 uses the internal electronic to control the motors mounted on the coil is such a way that when the user request a rotation of an angle θ the electronics knows how much rotation on the coil is needed to reach the equivalent of a rotation of θ on a standard waveplate. Each coil can be controlled independently with its own step size, having in total 6 degrees of freedom: three angles and three step-size.

3.4 Polarization Stabilization System

The polarization stabilization system in our case is composed by the polarization controller discussed in the previous section and by the polarimeter presented before. In our tests we inserted the polarization controller right after the laser, then we connected the fiber under test and the end of the fiber was finally coupled into the input of the polarimeter. The principle of working of the stabilization system is simple: first we set a reference SOP, this is the SOP we want to obtain out of the fiber and so the one read by the polarimeter. Then the the polarimeter reads the Stokes parameters of the incoming light and sends the data to a feedback system that calculates the variation that the polarization controller needs to perform in order to get closer to the reference SOP. The process is iterated until the distance between the reference and the measured SOP goes below a certain value (in our case $d_c = 0.001$). If the distance, in any moment, goes over d_c, the whole procedure starts again. The need of this iterative method is forced by the fact that we don't know the incoming state of polarization and also we don't know the reference system of both the polarization controller, and the polarimeter, so we cannot calculate the three angles of the waveplates *a priori*.

3.4.1 Feedback system

The feedback system, thus, is a crucial point in the entire polarization stabilization system. It can be implemented in a numerous of different an surprising ways; for example can be implemented directly on hardware with only analog electronics or it can exploit all the power of genetic

algorithms. We decided to implement it directly in C++, incorporating it inside the software for the control of the polarimeter. In this way the complexity of an inter-process communication is avoided.
The algorithm works in the following way: First, given the reference vector $\mathbf{S^{ref}}$, the algorithm reads the current value from the polarimeter $\mathbf{S^{meas}}$ and computes the distance

$$d = \sqrt{(S_1^{ref} - S_1^{meas})^2 + (S_2^{ref} - S_2^{meas})^2 + (S_3^{ref} - S_3^{meas})^2} \tag{3.52}$$

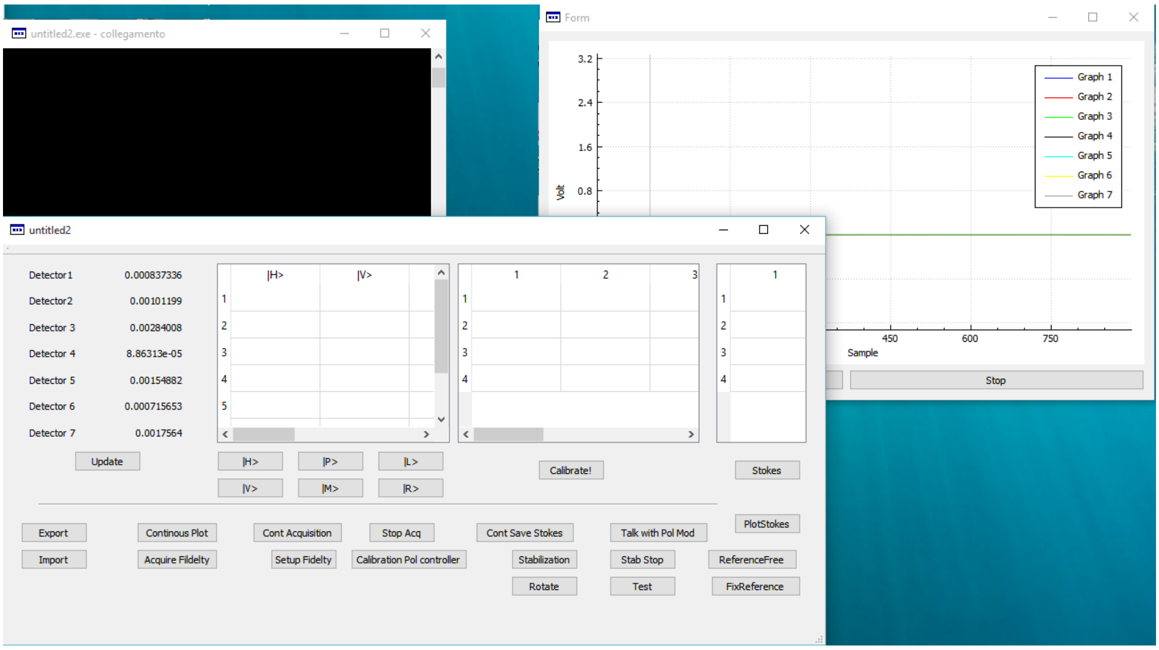
Depending on the value of d the algorithm selects the optimal step size for the increment; if d is large, we are far away from the reference point and so big steps will help us to converge faster, while if d is small, we already are near the reference point and so smaller steps will help us to have a better resolution. Then the first waveplate of the polarization controller is selected and a step is made randomly forward or backward. If the new distance is lower the process will continue until d decreases. If d is bigger the other direction is selected and the process goes on until d decreases. When d increases or sticks to the same value the process exits and selects the next waveplate repeating the above described procedure iteratively. When d goes below a specific tolerance value the algorithm keeps computing d without acting on the controller. Despite its simplicity the codes performs really well and is typically able to converge at the 95% of the reference value in $6-7$ iterations while at least $15-20$ iterations are needed to go below the $1-2$%. The response of the stabilization system sadly is limited not by the feedback or the readings from the polarimeter but by the GPIB protocol used for the communication between the MPC1 and the software. The protocol in fact requires at least 50 ms between two consecutive commands, limiting the overall performances of the system.

3.4.2 Software

The software for controlling the polarimeter and the entire polarization stabilization system has been written from scratch in C++ using only open source and multi-platform libraries including: Qt(5.x), ROOT, Eigen and Boost. In this way the software can be compiled and distributed on both Windows and Unix machines and all the sources are currently available under the Apache License 2.0 via `https://github.com/marcoavesani/untitled2`. The software is object-oriented and modularized with each class providing a wrapper to the basic functions; in this way if adding new hardware or function is needed the changes are localized inside the specific class and nothing has to be changed in the general function of the program itself. Currently the project is composed of 41000 lines of code and performs:

- Communication with the ADC and reading of voltages
- Conversion from raw voltage to optical power
- Plot of each voltage in realtime for monitoring
- Both method of calibration
- Import export of settings
- GPIB interface for the polarization controller

- Polarization stabilization algorithm
- Output of raw and extracted data in pipeline or text file
- Graphical User Interface(GUI) for a simplified interaction with the user



Detector1	0.000837336
Detector2	0.00101199
Detector 3	0.00284008
Detector 4	8.86313e-05
Detector 5	0.00154882
Detector 6	0.000715653
Detector 7	0.0017564

Figure 3.11: *GUI of the control program*

3.4.3 Results

The stabilization system has been tested on different fibers (Polarization mantaining and non) and on various length. In Figure 3.12 is presented a test where 50 km of spooled non polarization maintaining fiber are used.

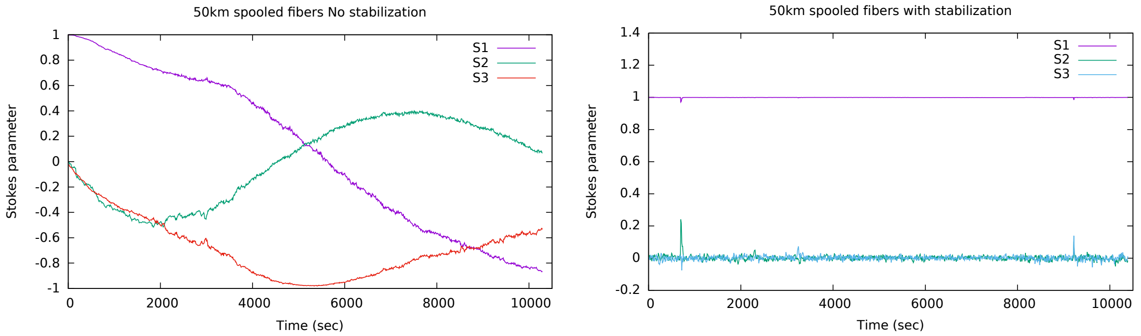


Figure 3.12: *Comparison of the polarization drift in 50km of spooled fiber with and without the stabilization system*

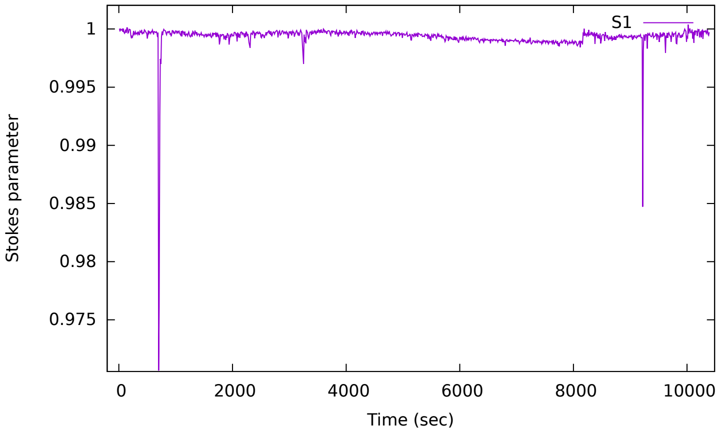


Figure 3.13: *Zoom of the S_1 parameter for the stabilized case*

From what we can see from the figures the stabilization system was working really well in the cases considered. One note on the spikes that can be seen in the stabilized case: the spikes are happening just after something perturbed for a short time the system. The two big ones, the first and the last, are caused by the close of one of the doors of the cabinet that was supporting the spooled fiber. The other small peak, visible in the zoomed picture, was caused by the closing of the door of the lab. This can show how polarization in fiber is sensible to external perturbation and so why an active stabilization is needed in fine-tuning applications.

CHAPTER 4

Semi-Device-Independent QKD: The experiment

In this thesis one of the main goals is to design and perform a Semi-Device-Independent (SDI) QKD experiment. The advantages of the SDI approach were discussed before but a global and deeper view will be developed through all this section. The initial part will describe the theory and the tools needed to understand the SDI framework, while the second part will be focused on the experimental realization of this QKD system.

4.1 Theoretical background and protocol description

In Section 2 we presented the actual limitations and threats that are mining the security offered by QKD. Although QKD is expected to provide theoretical unconditional security, the gap between theory and practical implementation can be exploited to completely crack the QKD system. We saw that is possible to build a protocol where the devices are completely uncharacterized to the users: they're black box and nothing is known or assumed on their internal functioning. This DI approach is based on non-locality and requires a loophole free violation of a Bell inequality, which is extremely hard to realize and, more important, to scale up to a network. For this reason the SDI was developed: it is based on the DI approach, but is realizable with the current technology paying the price of making one more assumption. Moreover SDI is based on a "prepare'n'measure" scheme and not on entanglement, making it less fragile and easier to generalize to 3 or more users.

The core of SDI QKD is presented in Fig. 4.1 and works in this way:

Alice holds an uncharacterized box,the state preparator, that can generate a system based on a set of possible settings $a = \{0, 1, 2, .., N-1\}$. Depending on the value of a, the box sends as an output a quantum system, ρ_a, of dimension d. Since Alice's preparator is a blackbox, the only thing we know is the dimension of ρ and we also assume that Alice preparations are unentangled from a possible eavesdropper, Eve. Bob holds another black box, the measurement box, with a set $b = \{0, 1, ..., M-1\}$ of settings that can be used to measure ρ_a. The output of Bob's measure can take k values and is denoted as $x = \{0, 1, 2, ..., k-1\}$. The boxes can also share classical variables $\boldsymbol{\lambda}$

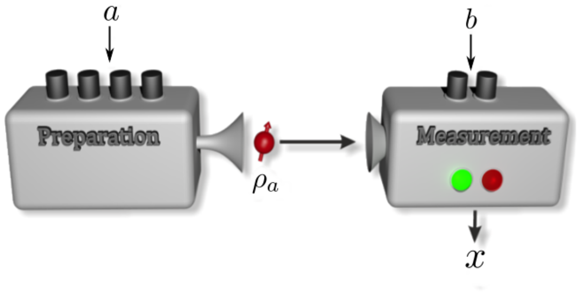


Figure 4.1: *Schematic representation of the SDI QKD protocol*

known to Eve but independent on the choice of the state.
The protocol, in order to be SDI, requires that the security of the system must be guaranteed with only the knowledge relative to the dimension of ρ and the data table $P(x|a,b)$, the probability of the outcome x, given the knowledge of a,b. The protocol above depicted is valid for any quantum system of dimension d, but in our case we will be focused in the qubit case.

4.1.1 Dimension assumption

The classical assumptions made by "standard" QKD (like BB84) are:

- The eavesdropper must obey to the law of physics
- There is no information leakage from Alice and Bob's lab
- Alice and Bob have access to trusted true random number generator
- Alice and Bob have an authenticated classical channel
- Alice and Bob have a perfect characterization of the physical functioning of their preparation and measurement apparatuses

The SDI QKD removes the last assumption, which is the most critical one, but adds one more assumption. This is often called the dimension assumption: it assumes that the dimension of the system used for the communication is known. Like all the other assumptions if it is not satisfied, security cannot be guaranteed anymore. The communication protocol realized in this thesis is based on qubits, so the case $d = 2$ will be discussed.
Imagine that Alice has a source capable of sending to Bob one of four different quantum states $\rho_{A,x} = \{\rho, \rho', \sigma, \sigma'\} \in \mathscr{H}_A$, that belong to a certain Hilbert space $\mathscr{H}_A$. During the transmission an adversary, Eve, can perform arbitrary unitary operations on the state sent, trying to obtain some information from it. After the operation, the transmitted state can be shared between Bob and Eve, and so acts on a Hilbert space given by $\mathscr{H}_B \otimes \mathscr{H}_E$. The assumption requires that the differences $\rho - \rho'$ and $\sigma - \sigma'$ between the source states (after the unitary attack) share their support on a common two dimensional subspace $\tilde{\mathscr{H}}_A$ of $\mathscr{H}_B \otimes \mathscr{H}_E$ [64].
This assumption is fundamental for the SDI protocol and clearly weakens the security respect the DI case. However, the assumption is quite reliable making the whole SDI protocol interesting.

In fact, with this formulation, we see that only the differences $\rho - \rho'$ and $\sigma - \sigma'$ are bounded, and not the absolute states $\rho_{A,x}$, which are free to live in higher dimensional Hilbert space. For instance, in an optical implementation, each qubit may be encoded in the polarization degree of freedom of a single photon, but may also possess a vacuum component and thus formally be a three-level system. Still, the differences only involve the genuine qubit parts and thus satisfy the qubit source assumption. Moreover, if there is no prior entanglement between Alice and Eve or Bob, the states sent by Alice are such that $\rho - \rho'$ and $\sigma - \sigma'$ have support in the same two-dimensional subspace. Under these conditions, after Eve's unitary attack the states will still share the same two-dimensional support and thus the qubit source assumption will be satisfied.

4.1.2 Dimension Witness: a lower bound on the system's dimension

Like the fully DI QKD, SDI QKD relies its security in the violation of an inequality. In the DI case, the inequality is a Bell inequality and its violation implies that non-local correlations are shared by the users. For SDI, the inequality that needs to be violated is a dimension witness inequality.

The concept of Dimension Witness (DW) was first introduced in 2008 [65] by Brunner and then realized in [66] [67] [68]. The authors showed that is possible to put a lower bound on the dimension of the Hilbert space of a quantum system transmitted between two parties. In a prepare and measure experiment, like the one depicted in 4.1, users can obtain the conditional probabilities $P(x|a,b)$ performing many times the exchange. Is then possible to build a linear function of the $P(x|a,b)$ called linear dimension witness, with the form:

$$W = \sum_{a,b,x} \alpha_{a,b,x} P(x|a,b) \leq C_d \tag{4.1}$$

for some well chosen coefficients $\alpha_{a,b,x}$ and where C_d is the maximal value obtainable for W using a classical system of dimension d. Like what happens for Bell's inequalities, a quantum system can violate the dimension witness's classical bound, meaning that for a given dimension is possible to obtain values of W higher than C_d but less or equal than Q_d, the quantum bound. Thus, given the experimental value of W is possible to certify that the exchanged system had a classical (quantum) dimension higher than d ($\tilde{d}$), where d ($\tilde{d}$) is the highest dimension for which C_d ($Q_{\tilde{d}}$) is violated. Moreover, since this dimension test is performed using only the information from $P(x|a,b)$, is also device independent [66]. The type of dimension witness depends directly on the choice of the coefficients $\alpha_{a,b,x}$ and they can also be constructed in non-linear forms. Recent researches proved that they're also deeply related to Bell inequalities and DI protocols [69][64]. Dimension witness allows to turn the dimension of Hilbert space, from a very abstract concept into an experimentally measurable property.

4.1.3 RAC and QRAC: the quantum advantage

Dimension witness and the SDI protocol described in Section 4.1, are connected with the so called Random Access Code (RAC) and its quantum version (QRAC).
The RAC is a communication task between two users: the first one, Alice, has n bits which is allowed to encode in m bits. These m bits are then sent to the second user, Bob, whom is asked to guess the value of any of the n initials bits. If $n \geq m$, Bob can always recover any bit with probability 1, since Alice is allowed to send all the information about the values she is holding. In the case $n \leq m$, Bob cannot know deterministically the values of the bits but, together with

Alice, can try to maximize his guessing probability p_{guess}. Both in fact are allowed to discuss a common strategy to apply before the beginning of the RAC. In the presented case the RAC is denoted with the symbol $n \to m$, meaning that Alice has n bit but she can send only m bit to Bob. We can perform this task also with quantum mechanical system, where Alice is allowed to encode the n bit in a m dimensional quantum system, obtaining a QRAC. The interesting thing is that sharing a single m-level quantum system, somehow gives an advantage respect the classical case, thus allowing Bob to retrieve the bits with an higher p_{guess}. We are now interested in the $2 \to 1$ case, where Alice holds 2 bits but can send only one to Bob, who must try to get the one of the two values. In the classical case their best strategy is simple: Alice always sends the first bit to Bob, then if Bob wants to retrieve the first one, he just need to read the value of the bit received, while in the case he wants the second he can randomly guess its value, having $\frac{1}{2}$ of probability to pick the right one. So on average the $p^C_{guess} = \frac{3}{4}$ for the classical case. In the quantum case, Alice can encode the two bits in a qubit, with the encoding presented in Table 4.1

a_1 a_0	0	1
0	$\|0\rangle$	$\|1\rangle$
1	$\|+\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|-\rangle = \frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

Table 4.1: *Encoding for the optimal* 2 → 1 *QRAC*

Then Bob can measure with the basis:

$$M_1 = \frac{\sigma_z + \sigma_x}{\sqrt{2}} \tag{4.2}$$

$$M_2 = \frac{\sigma_z - \sigma_x}{\sqrt{2}} \tag{4.3}$$

In this case, given the symmetry, the measures have the same distance in the Bloch sphere from all Alice's states, and so the probability of reconstruction for the QRAC does not depend on the input state. The situation is represented in Fig: 4.2.

In this case the guessing probability is $p^Q_g = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.854$, so higher than the classic case, giving a clear advantage to the QRAC over the RAC. The quantum advantage can be expressed with the ratio $r_g = \frac{p^Q_g}{p^C_g}$, taking in this case a value of $r_g \approx 1.138$. The above described strategy was proven in [70] to be the optimal strategy for the $2 \to 1$ QRAC, thus yielding the highest r_g. This advantage of the quantum system against the classic one is the key feature in the SDI, that enable us to guarantee security in the communication. The relation with the SDI protocol, described in section 4.1, is in fact clear: the bits hold by Alice are represented in the SDI protocol by the settings on her preparator, while the settings on Bob machine are representing the way for Bob to select which of the n bits he wants to recover. In this way we see that the SDI protocol can be also seen from the QRAC point of view.

Finally, since the maximum p_g is related to the classical or quantum dimensionality of the system, is directly connected to the dimension witness:

$$p_g = \frac{1}{8} \sum_{a,b,x} P(x|a,b) = \frac{W+4}{8} \tag{4.4}$$

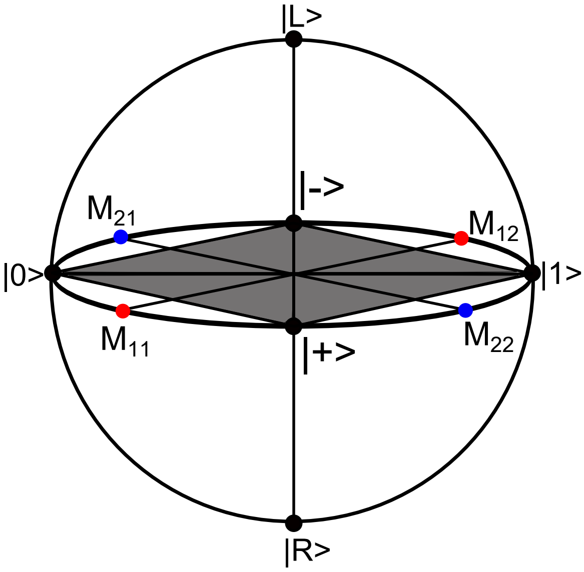


Figure 4.2: *Representation on the Bloch sphere of the optimal quantum strategy for the* $2 \rightarrow 1$ *QRAC*

in the case of the CHSH-inspired witness [39].
The language of QRAC so can be used to address SDI properties from another point of view: we will se that they turns out to be useful tool in the analysis of security for the SDI protocols.

4.1.4 Connection with Entanglement witnesses and DI protocols

In the description of DI and SDI protocols is possible to see common features shared by the two protocols. First, they both relies on the violation of some inequality. For the DI is a Bell inequality while for the SDI is a dimension witness. They both put constraints on the performance achievable by classic theory in some tasks, and the violation of both inequalities is an indicator that the system used for the communication doesn't admit a classical description. In the case of BI, limits are imposed on the correlation experienced by two space-like separated users, while in the case of DW, is the guessing probability p_g of a RAC that is limited. However, while for "standard" QKD, where devices can be trusted or characterized, exists a very well known equivalence between entanglement-based and prepare'n'measure implementation [71], for the DI protocol this equivalence is broken. The essence of the DI protocol is based on a Bell test, so on a test of non-locality, making it intrinsically entanglement based. On the other hand, prepare'n'measure scheme cannot be fully DI, since Alice could transmit her settings classically. Nevertheless a relation between BI and DW actually exists and is in general possible to build one starting from the other [69]. Let's take for example the simpler BI: the CHSH.
The scenario of the CHSH inequality has already been described in Sec 1.3.1 and if we call $x, y = 0, 1$ the settings for Alice and Bob and $a, b = 0, 1$ their outcomes, the CHSH can be written as:

$$I = \sum_{a,b,x,y} (-1)^{a+b+xy} P(a, b|x, y) \tag{4.5}$$

which is a particular form of

$$I = \sum_{a,b,x,y} \alpha_{a,b,x,y} P(a,b|x,y) \tag{4.6}$$

Now if we consider the prepare'n'measure, Alice doesn't register an outcome a but she can choose the state to send according to the setting given by two bits, that we can call $x, a = 0, 1$, in order to better show the similarities between the two protocols. Thus we can write:

$$P(a,b|x,y) = P(a|x,y)P(b|a,x,y) \tag{4.7}$$

and since the settings are chosen randomly from a flat distribution, we have $P(a|x,y) = 1/A$, where A is the size of the alphabet for a, in our case $A = 2$.
We have

$$W = \sum_{a,b,x,y} \frac{\alpha_{a,b,x,y}}{A} P(b|a,x,y) \tag{4.8}$$

that can be rewritten in the form:

$$W = \sum_{a,b,x,y} \beta_{a,b,x,y} P(a,b|x,y) \tag{4.9}$$

For the particular case of the CHSH this takes the form:

$$W = \frac{1}{2} \sum_{a,b,x',y} (-1)^{a+b+xy} P(b|a,x',y) \tag{4.10}$$

which is the form of the CHSH-inspired dimension witness. Sometimes in the thesis, or in other works, is possible to encounter another form of the CHSH-like dimension witness, written as:

$$D = (E_{x1,y1} + E_{x1,y2}) - (E_{x2,y1} + E_{x2,y2}) + (E_{x3,y1} - E_{x3,y2}) - (E_{x4,y1} + E_{x4,y2}) \tag{4.11}$$

with

$$E_{x_i,y_j} = P(1|x_i,y_j) - P(-1|x_i,y_j) \tag{4.12}$$

This form is identical to the one in Eq.4.10 except for being a factor 2 larger. Finally, is worth to mention that in [64] author showed that the DI and SDI share another common quantity: the min-entropy $H_{min}(A|E)$ of Alice's outcome conditioned to the side information of a potential eavesdropper. If the CHSH correlator $S = I$ for Eq 4.5 or $S = W$ 4.10 is used, $H_{min}(A|E)$ was proven to be:

$$H_{min}(A|E) \geq 1 - \log_2\left(1 + \sqrt{2 - \frac{S^2}{4}}\right) \tag{4.13}$$

This relation is very useful, both for the randomness certification in SDI QRNG protocols but also for security proofs for the SDI QKD.

4.1.5 The role of Detection Loophole in SDI QKD

It has already been stressed the Semi-Device-Independent QKD relaxes the assumption of perfect characterization of the preparation and measurement devices respect the standard QKD, thus making it more robust and secure. However any experimental implementation of SDI QKD still suffer noise and loss. Thus is important to understand if these losses or noises can influence and affect the security of the protocol. The non ideal efficiency is actually one of the biggest experimental problem, and is known as the *detection loophole*. The concept of detection loophole has been first developed in the context of experimental tests of Bell inequalities, and points out that a Bell test performed with non-ideal detectors, (efficiency $\eta < 1$) can be inconclusive even if it register a violation of the classical bound. In fact, if the detectors are not 100% efficient, they will inevitably lead to events where they not register a coincidence. In these cases the event is simply rejected. This procedure, however, implicitly assume that the photons actually seen by the detectors belong to the same distribution of the photons sent, in other words that there is a *fair sampling*. If this inefficiency is taken into account Eq. 1.24 must be modified and becomes

$$\left|E_{AB}(a,b|coinc)+E_{AB}(a,b'|coinc)+E_{AB}(a',b|coinc)-E_{AB}(a',b'|coinc)\right| \leq \frac{4}{\eta}-2 \tag{4.14}$$

where the expectation values E_{AB} are now conditioned to the event of having a coincidence [72] [73]. In this case the classical bound was found to be higher respect the ideal case, since a local hidden variable model can exploit the non-ideal efficiency to reproduce an higher correlation. From (4.14) is possible to see that there is a critical efficiency, η_{crit}, under which the violation doesn't exclude LHV theories. The η_{crit} is obtained when the right side of the equation is equal to the QM bound $2\sqrt{2}$ and this happens for $\eta_{crit} = \frac{2}{\sqrt{2}+1} \approx 0.8284$. This value can be lowered using non-maximally entangled states to $\eta_{crit} = 66.7$ [74].

A similar problem is present also in the SDI approach, where the violation of the dimension witness must be guaranteed without any knowledge of the devices, so without taking into account the expected efficiency of the detectors. This problem has been deeply explored in [75], looking also to the effects of noise in the communication channel. It has been found that for symmetric detection efficiency of the detectors (ie identical detectors at Bob), the critical $\eta_c = \frac{\sqrt{2}}{2}$. If one of the detectors has unity efficiency the η_c for the other can be arbitrary low. Recently some solutions have been found, but they requires some additional assumptions. The first solution, presented in [76][41], uses a nonlinear dimension witness in the form:

$$W = \det\begin{pmatrix} P(1|0,0)-P(1|1,0) & P(1|2,0)-P(1|3,0) \\ P(1|0,1)-P(1|1,1) & P(1|2,1)-P(1|3,1) \end{pmatrix} \tag{4.15}$$

With this witness is possible to violate the classical bound for every non-zero value of the efficiency η, if the preparation and measurement device are assumed independent. Anyhow there's another price to pay when using this witness. While for the linear dimension witness there is a linear dependence on η, when taking into account inefficiencies, for this witness the dependence is quadratic. This means that if one wants to reach a value near to the quantum bound, he needs a much more higher η in this case respect the linear one.

Another approach has been proposed in [77], where a **trusted** blocking device is used in order to limit the possible shared randomness between the preparation and measurement stage. The idea of using an extra assumption regarding the shared randomness between the devices was first proposed in [78], where is proved that with this assumption the detection loophole can be closed for any (non-null) value of the detection efficiency.

4.1.6 Parallel QRAC

The detection loophole is a serious threat for SDI protocols and we have seen that it can be lifted using today's technology only adding more assumptions, like the independence of the devices or the lack of shared randomness. However, these are strong assumptions, hard to justify in practice. In a recent paper [79], the authors introduced and experimentally performed a non classicality test, based on dimension witness, without the fair sampling assumption or other auxiliary assumption, with an arbitrarily non-zero detection efficiency. The core of this new approach is the use of two preparation and two measurement devices, which are randomly paired in each round. The setup proposed for their protocol is presented in Figure. 4.3

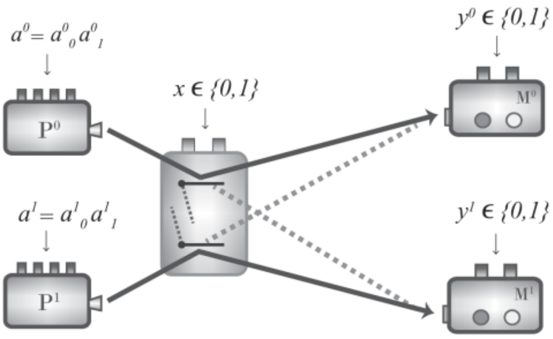


Figure 4.3: *Setup of the proposed protcol*

In practice what is performed is a parallel QRAC, with two sending devices and two measurement devices. Between these, an optical switch is interposed, that can connect the first two devices with the measurement one, in a straight o crossed configuration, depending on the setting he receives. The users, however, do not have access to information about the pairing before the conclusion of the quantum communication. In addition the strategy for handling the inconclusive events is changed: if the measurement devices do not register a click in a round, they pick a random value for the output. In this way the efficiency is faked to be 100%, but at the cost of a reduced maximum violation of the DW. In fact, if Q is the bound predicted by QM, the maximum value obtainable is:

$$Q_\eta = \eta Q + \frac{1}{2}(1-\eta) \tag{4.16}$$

In the article the authors show that is possible to find a test for which the classical value is $\frac{1}{2}$, and so any non-null value of η is sufficient to achieve a violation for QM. Moreover, the parallel setup is used to limit the amount of shared randomness that the users can experience. So the critical detection efficiency, depends only on one parameter δ, that express the shared correlation in the outcomes. In an experiment this parameter is determined by the correlations present because of the finite sample size. Thus, the picture can be seen from another point of view: given a certain value of the expected efficiency, is possible to roughly estimate how many runs of the experiment are needed to get a value of δ low enough to be a conclusive test. After the test, the correlation can be checked and, if is low enough, the test can be considered conclusive.
For our experiment we decided to modify the setup in order to be compatible with this kind of test. In this way, we can both test the feasibility of SDI QKD in fiber and we can collect data which can

be used to adapt this idea to our QKD protocol. However, even if the experiment was performed with a full parallel setup, this idea won't be discussed more in this thesis because is still under an heavy development.

4.1.7 Security proof

The central feature, in all the SDI protocols, is the violation of a dimension witness. This violation can be read in the language of QRAC, as a certification that the system exchanged by the users is quantum and not classical. In the previous sections the classical and quantum bound for the CHSH-like dimension witness was given, but the interesting question is: is sufficient to violate the classical bound (even with the fair sampling assumption) to claim security between the parties? This question was analyzed in the first paper about SDI QKD by Pawłowski and Brunner in 2011 [39]. Their answer to the question is: no.

The violation of the classical bound is enough for a non-classicality test but the requirements for a secure QKD protocol are way stricter. Their (asymptotic) analysis takes into account individual attacks, a subclass of the possible attacks performed by Eve, and is based on a really nice result by Csiszar and Körner [80], where they showed that Alice and Bob can obtain a secret key if $I(A:E) > I(A:E)$, where I (X:Y) is the mutual information between X and Y and is defined:

$$I(A:X) = \sum_j 1 - h(P_x(a_{y_j})) \tag{4.17}$$

where y_j is the basis chosen by X in the j^{th} run and $h(p)$ is Shannon's binary entropy

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x) \tag{4.18}$$

Another possible way is described in [40] and directly bounds the min-Entropy H_{min} thanks to the relation with the dimension witness. Anyway, independently from how the proof is obtained, the bound for security was found to be:

$$p^c_{guess} > \frac{5+\sqrt{3}}{8} \approx 0.8415 \tag{4.19}$$

for the guessing probability described in Sec 4.1.3. This critical value can be reformulated in terms of critical value for the witness using Eq. 4.4

$$W^c > 2.6403 \qquad D^c > 5.2806 \tag{4.20}$$

The critical value obtained are just below the quantum limit meaning that a practical realization of the protocol must be really fine-tuned, because the margin between security and maximal violation is very narrow.

One of the most successful class of attacks on QKD systems is composed by detector blinding attacks and in general in device manipulation attacks. In these attacks Eve can fully control the devices of Alice and Bob exploiting the imperfections of their apparatus. The most common is the detector blinding attack, where the characteristics of Single Photon Avalanche Diode (SPAD) are exploited. In particular, if the incoming intensity of the light is above a certain threshold the SPAD starts working in a linear regime and Eve, by sending special bright pulses to Bob can select which event are seen by him or not, breaking the security protocol [81]. This class of attacks

have been studied in the case of SDI QKD in [82]. Here the authors show that Eve cannot get any kind of informations taking control of Alice apparatus, instead controlling Bob's detectors can be harmful and this only depends on the detection efficiency on Bob's side. Interesting, critical detection efficiency, which depends on Bob's success probability, can be as low as 50%.
Is worth to mention that research in the field of security proofs for SDI protocols is still at the beginning and more optimal bounds are expected to be found in the near future.

4.1.8 The protocol

In Section 4.1 is reported the basic idea behind the SDI implementation: the security check. Alice chooses one over four states, depending on her input, and sends the state to Bob, who can measure the state in two basis, again depending on his settings. The optimal states and measure for the witnesses in Eq 4.10 and 4.11 are given by the states in Tab 4.1 and the measurments in 4.2. This minimal protocol is intended only for checking the security of the communication between Alice and Bob, but cannot be used for the generation of a secret key. Moreover the BB84 protocol cannot be re-implemented in this SDI and the reason is quite straightforward to show. Let Alice to send the 4 BB84 states, namely the eigenstates of $\sigma_z = \{|\psi_0\rangle = |H\rangle, |\psi_1\rangle = |V\rangle\}$ and $\sigma_x = \{|\psi_2\rangle = |+\rangle, |\psi_3\rangle = |-\rangle\}$ that have the property to form a mutually unbiased base in an Hilbert space of dimension 2. In the BB84 protocol Bob measures the incoming qubit along $M_0 = \sigma_z$ and $M_1 = \sigma_x$.
For this combination of states and measurement the CHSH-like dimension witness, considered in the form of Eq. 4.11 we have

$$E_{0,0} = P(1|0,0) - P(-1|0,0) = \langle H|\sigma_z|H\rangle - \langle H|\sigma_z|H\rangle = 1 \tag{4.21}$$

and the same calculus leads to $E_{0,0} = E_{2,1} = +1$ $E_{1,0} = E_{3,1} = -1$ $E_{0,1} = E_{1,1} = E_{2,0} = E_{3,0} = 0$ with a value of $D = 4$ equivalent to $W = 2$. So the BB84 cannot be, in any possible way, safe in a SDI approach since doesn't even violate the dimension witness and so can be reproduced by a classical system. Our solution to the problem is a "mix" of both strategies: the BB84 states are used for the key generation while the optimal states for the CHSH-like dimension witness are used for checking the security. Alice can now send not 4 but the 8 states presented in Table 4.2 and plotted in Fig 4.4 (the states are represented in function of θ while the notation for Tab 4.2 is the one of 1.2 that depends on $\frac{\theta}{2}$). Bob on the other hand can choose not 2 but 4 basis, Z,X,D,A,

Base	First state	Second state
Z	$\|H\rangle$	$\|V\rangle$
X	$\|+\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	$\|-\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$
D	$\|P\rangle = (\cos\frac{\pi}{8}\|H\rangle + \sin\frac{\pi}{8}\|V\rangle)$	$\|Q\rangle = (\cos\frac{5\pi}{8}\|H\rangle + \sin\frac{5\pi}{8}\|V\rangle)$
A	$\|T\rangle = (\cos\frac{3\pi}{8}\|H\rangle + \sin\frac{3\pi}{8}\|V\rangle)$	$\|U\rangle = (\cos\frac{7\pi}{8}\|H\rangle + \sin\frac{7\pi}{8}\|V\rangle)$

Table 4.2: *List of the states prepared and sent by Alice*

for the measurement. During the quantum communication phase, the states for Alice, and the

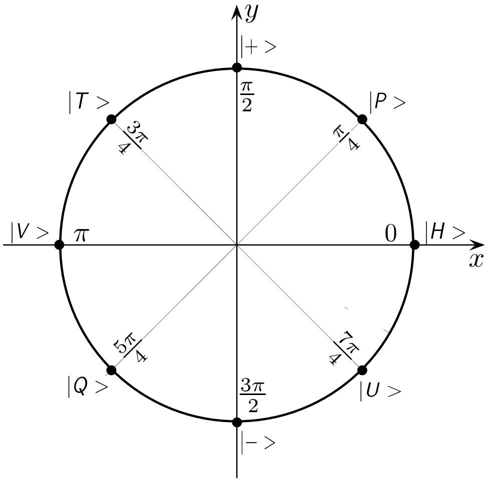


Figure 4.4: *Graphic representation of Alice states in function of the angle θ*

settings for Bob are chosen randomly at each run. When this part of the protocol is finished, they both announce their basis on an authenticated classical channel. Now, when the base selected by Alice matches the one picked by Bob, they both select that event as a key-generation event. If Alice picks X or Z and Bob D or A, or vice versa, the event is marked as a security check event. If the Alice and Bob bases are a pair of mutually unbiased basis, they discard the event. After they have marked all the events, they can compute the expectation values $E_{x,y}$ from the security check events, from which they obtain the value of the dimension witness. If the value is above the security level, they proceed to the secret key generation with the events marked as key-generation events. The protocol now is the same as the BB84 without the sifting part.

According to what said in Sec 4.1.6, the entire protocol can be adapted to the case of parallel QRAC. The only differences are that 2 state preparators and 2 measurement devices are present in this case, and that the settings of the switch are publicly announced only after the end of the quantum communication.

4.2 Classical postprocessing: the need of two identical keys

After the security check, Alice and Bob hold a pair of bitstring that form the raw-keys. These raw keys should be identical in an ideal experiment with no noise and no actions from Eve. Clearly this is quite unlikely in real experiments, where noise is always present. The two bitstrings, in general, are only correlated but they must be identical if they have to be used in a OTP protocol. For this reason error correction is performed. Error correction allow Alice and Bob, by exchanging information on the public channel, to correct their bitstrings until they exactly match. Using any possible attacks however Eve can gain some information about the key, introducing errors. After the error correction she can exploit these information to recover the key. For this reason Alice and Bob, after the error correction, perform a procedure of privacy amplification where they reduce the key and the information that Eve gathered. At the end of this procedure they have two secure identical keys, ready to be used.

4.2.1 Error Correction

Error correction is the first step of the classical post-processing and can be divided in three categories: direct, reverse and two-way. In the direct, Alice's key is supposed to be correct and Bob's one is corrected, in the reverse Alice and Bob's role are exchanged, while in the two-way none is considered correct, but the objective is to have at the end a pair of identical bitstrings. The best approach depends on the specific algorithm used for error correction and from the noise of the channel. The two-way iterative protocol used in this thesis is known as CASCADE and has been proposed in 1994 in [83]. The protocol works in this way: at each iteration i, Alice and Bob agree on a random permutation which they apply to their strings. After, they agree on the block size k_i and they divide their strings in blocks of k_i bits. At each pass the block size is doubled. Alice sends the parity p_j^A of each block to Bob, while Bob sends the parity of his block p_j^B to Alice. If $p_j^A = p_j^B$ they change block, but if $p_j^A \neq p_j^B$ an error is present and a binary search is performed. They split the block in half and they exchange the parity of the first half. If the parity agrees they go on with the other half, otherwise the sub-block is split again and the procedure continues until they find the error in a position x. During the preceding passes the position x belonged to different blocks, the collection of this blocks is called C. If we take the smallest block with a odd error in C, another error can be corrected with the binary search. The process continues until C is empty.
The minimum number of bits that must be exchanged c ,to correct a key of length N, is called Shannon limit and is given by:

$$c = Nh(e) \tag{4.22}$$

where e is the QBER and $h(x)$ is Shannon's binary function 4.18. However all the error correction protocols known so far cannot reach this bound, but they are characterized by an efficiency $f(e) > 1$ that must be multiplied to c in order to obtain the real number of bits disclosed. A study of the dependence of $f(e)$ on the QBER for the CASCADE can be found in [84].

4.2.2 Privacy amplification

The attacks performed by Eve can give her partial information about the key that Alice and Bob are holding. For this reason, after the error correction, they must ensure to reduce to minimum the amount of information that Eve has. This is possible to do using a process called privacy amplification. Alice and Bob, exploiting the knowledge they have about the QBER, can use an error-dependent hash-function to map the original key in a shorter output key. An upper bound on the information that Eve can get in function of the QBER, has been presented in [84] and the number of bit that must be removed is given by:

$$\tau_1(e) \leq \begin{cases} \log_2(1+4e-4e^2) & : e \leq \frac{1}{2} \\ 1 & : e > \frac{1}{2} \end{cases} \tag{4.23}$$

Considering both privacy amplification and error correction, the number of bits of the final key is given by:

$$n_f = N(1 - f(e)h(e) - \tau_1) \tag{4.24}$$

In this implementation the privacy amplification is performed using a Toeplitz matrix with dimension $n_f \times N$.

4.3 Designing the experiment

While the previous section was focused on the theoretical aspects behind the SDI QKD, the next section will be focused on the practical ones and the experimental realization of the protocol above depicted.
In Sec 4.1.8 the theoretical protocol used is presented, but the experimental implementation of this protocol can be done in an big number of creative and surprising ways, thus making fundamental to carefully plan and reflect on the optimal design. The first thing to consider, in the realization of a quantum communication experiment, is how to encode the qubit. In section 1.1 we saw that the qubit can be encoded using different particles: atoms, electrons, photons, and properties like spin, polarization and phase; but what is the optimal choice in this case? The common choice in the field of quantum communication are the photons. They travel at the highest possible speed and they can be transmitted for many kilometers with little attenuation with nearly no-interference along the communication. This is the reason why also classical telecommunication has switched from electrical to optical encoding in the last years. Today, optical fibers are the most promising medium for quantum key distribution and only a small part of the experiments are done in free-space, focused mainly on satellite quantum communication. All the commercial QKD systems are now fiber-based and quantum fiber communication achieved huge results for what concerns the distance of links, proving quantum secure communications at over 300km [85]. Moreover optical fiber are already used by classic telecommunication systems in the same wavelength band and a global fiber optical network is already deployed and used. Anyhow, sending quantum states over an optical fiber presents a lot of challenges. The main drawbacks of using optical fiber for QKD are:

- **Fiber's birefringence**. The core of optical fibers is made of silica and has a natural and induced birefringence, that changes the state of polarization of the light transmitted by the fiber randomly in time. In this case an active polarization stabilization system is required. (These aspects are deeper discussed in Sec 3)

- **Polarization dependence of optical components**. Many fiber optical components are polarization dependent and can introduce unwanted effect that must be compensated. The main example are LiNBo$_3$ modulators that usually are polarizing components.

- **Phase drifts**. In fiber based interferometric setups the stability of the interference depends on phase difference, that usually drifts randomly in time, because of the external stress applied to the fiber. This problem can be solved using an active phase tracking control or auto-stabilized setups (like the Plug'n'Play that will be discussed soon)

All these problems are present in a fiber-based QKD setup and the dominance of some over the others mostly depends on the encoding system used. If a polarization encoding is used for qubits, the first two effects are dominant while the last one is nearly negligible. On the contrary if phase encoding is used, only the last effect is really a problem.
In this experiment the encoding method is the phase, because if compared to polarization it can

better stabilized, with a Plug'n'Play setup, without an active monitoring. Another advantage of phase encoding is given by the modulation devices: while for phase encoding is possible to use standard phase modulator for classical telecommunication, that are commercially available and are rated up to 40GHz, fiber polarization controller are rare and expensive. Moreover they have only up to 1MHz of bandwidth.

But how does the phase encoding work? And how is possible to realize it in fiber?

4.3.1 Phase Encoding

The first proposal of a phase-encoding scheme was formulated in 1992 by Bennett et al. in [86] and was first realized by Townsend et al in 1993 [87]. The scheme relies on a interferometric setup, presented in Fig. 4.5, and the superposition properties of qubit.

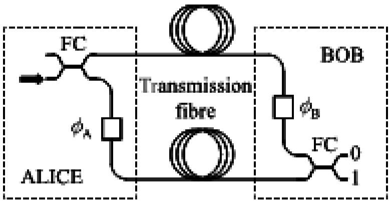


Figure 4.5: *Phase-encoded qkd system [88]*

Let's consider that only one photon at time is shot by the source. After the first beam-splitter or fiber coupler, the particle propagates, with some probability amplitudes, via two different paths: a the lower arm "0" and a upper "1". Then another beam-splitter or coupler directs the particle to one of the two possible output, connected to two detectors,D_0, D_1. Along each path between the two beam-splitters, there is a phase modulator(PM). After the first beam splitter, the wavefunction is a superpostion of two possible states, $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + |1\rangle$, then after the modulators, a relative phase difference $\phi_0 - \phi_1$ is added, and the state becomes, $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + e^{i(\phi_A - \phi_B)}|1\rangle$. Finally the second beam-splitter combines all the paths back together, leading to a single photon interference effect. The functioning of this single photon interferometer is presented in Sec 1.4.4, where the probability of seeing the photon in one of the two detectors is computed. This probability depends on $\Delta\phi = \phi_A - \phi_B$, and is

$$P_0(\Delta\phi) = \frac{1}{2}\left(1 + \cos\Delta\phi\right) \tag{4.25}$$

$$P_1(\Delta\phi) = \frac{1}{2}\left(1 - \cos\Delta\phi\right) \tag{4.26}$$

The described setup is suitable for QKD with phase encoding, in fact if one Phase Modulator is on Alice's side (PM_A) and one in on Bob's side (PM_B), they can implement any prepare'n'measure QKD protocol. For values of $\Delta\phi = 0$ we have $P_0 = 1, P_1 = 0$, for $\Delta\phi = \pi$ $P_0 = 0, P_1 = 1$ while, for $\Delta\phi = \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ we have $P_0 = 0.5, P_1 = 0.5$. This is exactly what happens for the polarization encoding with the states $|H\rangle, |V\rangle$ and $|+\rangle, |-\rangle$, in fact here $\{0, \pi\}$ and $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ are a pair of Mutually Unbiased Basis (MUB) and with the correspondence $|H\rangle \rightarrow 0$, $|V\rangle \rightarrow \pi$, $|+\rangle \rightarrow \frac{\pi}{2}$, $|-\rangle \rightarrow \frac{3\pi}{2}$, everything already said for the BB84 protocol is valid.

The same thing holds for our SDI QKD protocol described in Sec.4.1.8, where everything is equivalent if the set of corrspondence above listed is used. Moreover, the states presented if Fig 4.4 are already represented with the right phase correspondence.
Unfortunately the implementation presented in Fig. 4.5 is not practical and is not really used in any QKD experiment. It requires a careful balancing of the arms of an interferometer several kilometres long, which is not practical. The first scheme used was the one in [87], where two unbalanced Mach–Zehnder interferometers where used. By disregarding the photons travelling by the shortest and longest routes through the two unbalanced interferometers, it is possible to obtain the phase relationship described above. This approach still relies on the stringent condition of a constant phase relationship between the interferometer arms during the key exchange, but the conditions are significantly relaxed, compared to those for a single interferometer.
The double Mach–Zehnder scheme however, is not stable enough for a quantum communication without an active phase control, since it is susceptible to small path length changes in the arms of the interferometer (mainly due to thermal and mechanical perturbations).
For this reason, a total auto-compensating setup, named "Plug'n'Play", has been proposed in 1997 by Muller et al in [89], and rapidly gained a lot of popularity in the field, leading to commercial system based on this scheme.

4.3.2 Plug'n'Play setup

The Plug'n'Play setup, presented in Fig 4.6 is an auto-compensating interferometric setup composed by only one interferometer.

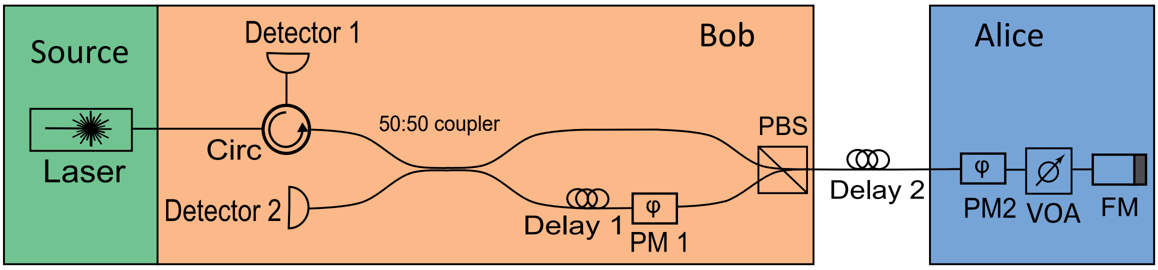


Figure 4.6: *Plug'n'play fiber interferometer*

It has been designed to automatically balance all the critical points needed for achieving a stable interferometry: timing, polarization, phase are all automatically compensated, making really long QKD experiments stable for hours and days without an active tracking [90]. Surprisingly the Plug'n'Play setup is quite simple but still extremely effective. The light source, commonly a short pulse from a laser, is placed not on Alice's side but on Bob's side and is emitting with a definite polarization, let's say horizontal. Then it enters in a fiber circulator that forwards the pulse incoming from port 1 to the second port, attached to a 50:50 2x2 fiber coupler. In this case, the coupler acts as a beamsplitter, where half of the signal goes in the short arm and half goes in the long one. Then, the polarization in the long arm is rotated by 90 degrees and both arms are connected to a PBS. After the PBS we have two pulses, orthogonally polarized, separated by a certain amount of time τ because of the path difference. At this time, the PM at Bob's side is not activated. Then, the pulses reach first Alice's PM, that is again left inactivated, and then the Faraday mirror (FM). Here they're reflected back and the polarization of the pulses is now changed to their respective orthogonal. Now, on the way back, the Variable Optical Attenuator (VOA) is activated and attenuates the signals to the single photon level; we need to work at the single photon level in order to assure the security of the QKD protocol. After that the pulses exited the VOA, Alice activates her PM only after that the first pulse has left the PM, modulating only the second and so changing the relative phase between the two pulses. In this way she can encode all the states needed for the protocol; in our case the one in Fig. 4.4. At the PBS the horizontally polarized pulse is transmitted in the short arm, while the vertically polarized is transmitted in the long one. Because of the polarization exchange, done by the FM, the two pulses make exactly the same path before interfering at Bob's coupler. Here the photon exiting from the coupler is revealed using single photon detectors. The arm of the coupler that was connected to the laser at the beginning uses a circulator to deviate the light coming from the coupler to the detector. Since the environmentally induced optical changes occur on a much longer time-scale than the transit time, any birefringence in the first transit is exactly compensated during the reflected path, making the setup auto-compensated.

The visibility and the stability of this kind of setup is generally extremely high.

Unfortunately, this setup for QKD suffers of some disadvantages typical of two-way systems. The most critical security flag is given by the possibility to perform a Trojan Horse attack. Eve can send a bright probe pulse and recover it through the strong reflection by the mirror at the end of Alice's system. In this way Eve can recover the phase of Alice's modulation [91]. This problem can be partially solved using very narrow modulation times, attenuators and detectors at Alice's side. Anyhow this is a serious flag and must be considered in the design process.

Moreover the in these two-way systems the repetition rate is limited by the round trip time of light inside the fiber that linearly scales with the length of the link.

4.3.3 Setup of the experiment

In this SDI QKD experiment we wanted to test, not only the feasibility of this protocol but also the possibility of removing the fair sampling assumption with currently available detectors whose efficiency is below the critical value η_{crit}. This will is motivated by the recent research involving the fair sampling assumption in the parallel execution of QRAC aimed to provide tests for non-classicality (see Sec 4.1.6). For this purpose we need to implement a SDI protocol involving four virtual users Alice, Alice', Bob and Bob' whose quantum communication channel are coupled by an optical switch. This switch, independently from the settings chosen by the 4 users, can choose between two possible routings: Alice⟷Bob and Alice'⟷Bob' or Alice⟷Bob' and Alice'⟷Bob.

This would be nearly impossible to do with a single-way phase encoding scheme, because it requires the construction and stabilization of four identical unbalanced Mach–Zehnder interferometers, which an extremely hard task. The plug'n'play instead can be done also if the two interferometers have a different unbalance length. Our final setup is presented in Fig. 4.7. This is clearly a parallel plug'n'play configuration where the two setup are coupled at Alice's side by an electronic 2x2 optical fiber switch that can connect two fiber input port to the two output port in the straight or crossed configuration dependending on the voltage applied.

The switch, when activated, starts the switching before the first photon enters the switch in the way forward, and ends when the photon exits the switch on the way back. Another alternative could have been that the switch is tuned on only after the photon exited the switch in the way

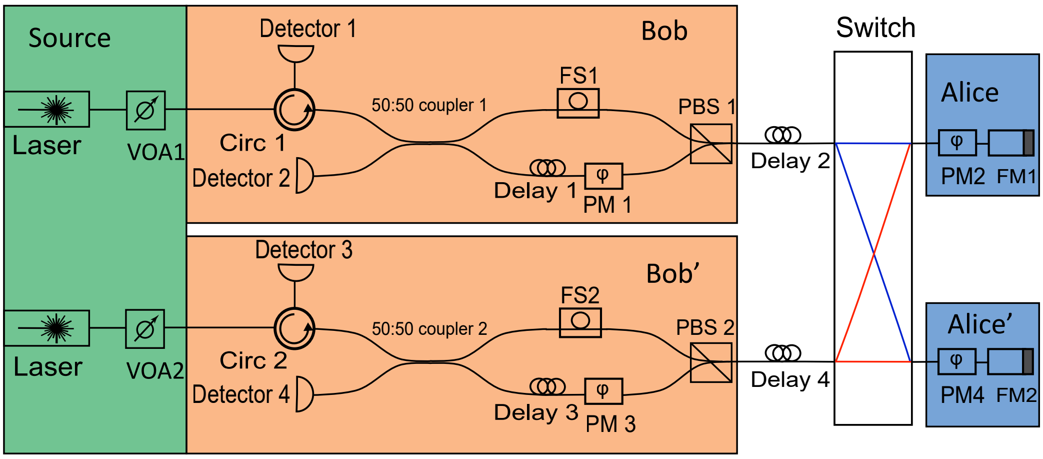


Figure 4.7: *Scheme of the apparatus*

forward, but this requires a phase stabilization between the two interferometers. Anyhow, the two interferometers used two fibers stretcher to match the path difference of the arms.
Respect the traditional configuration a variable optical attenuator is placed after the laser, in order to attenuate the pulse coming from the laser to the desired level. The attenuation is done here because of the finite attenuation between the port 1 and 3 of the circulator (40 dB) that would lead an extreme high number of leak detection in the Detector 1 and 3.
Let's look at the electronics now. The electric scheme is presented in Fig 4.8. Here an extremely

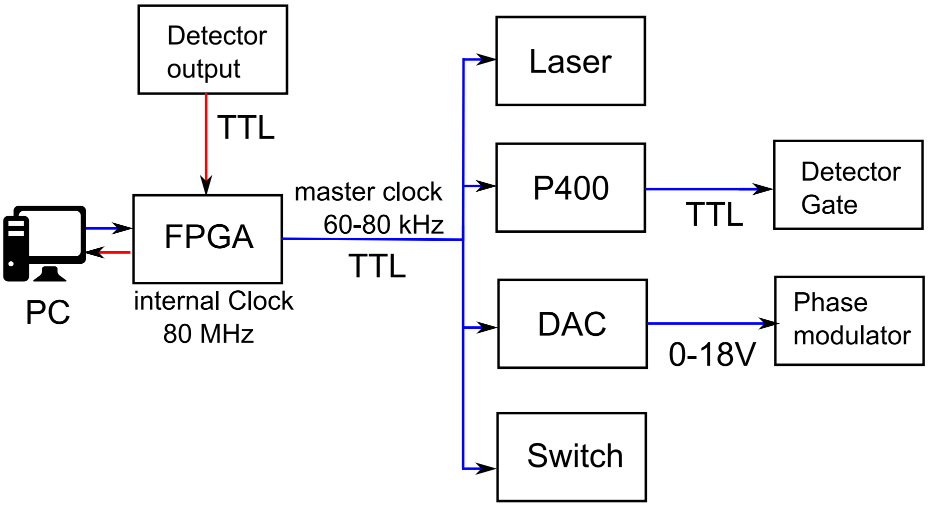


Figure 4.8: *Synchronization and electric connections*

careful synchronization must be obtained for all the active components: from the laser to the phase modulators and the detector: the precision needed for the synchronization is, in some parts, below the nanosecond level. The entire coordination is handled by a single PC with an programmable FPGA (NI-7831R). The main program is directly implemented in the FPGA and the PC is used as an host for the data retrieval.

The internal clock of the FPGA is 80 MHz. Since the FPGA is developed to process data in a massive parallel way the main drawback of working with this low clock is the temporal precision, that can be at most of 12.5ns. This is surely a good value, enough for triggering the laser and the switch, but some critical components require a better resolution. One of these components are the detectors. They are provided with a gating circuit used to lower the dark counts. In order to reveal the single photon, an TTL signal is needed to "open" the detection window that is 1 ns long. Since the FPGA doesn't have enough resolution, the FPGA is used to trigger a P400 digital delay generator with a resolution of 1 ps, that is used to trigger the four detectors.
The other critical components are the phase modulator. The phase modulators have a V_π, the voltage needed for having a π phase shift, of nearly 7V on a 50Ω impedance, a value too high to be handled by the FPGA. Moreover, Alice must modulate only one of the two "peaks" and must modulate it only after the reflection, as in the case represented in Fig 4.9 The time resolution and the rising time(≈ 100 ns) of the FPGA is not enough to drive the PM. For this reason, we have built a custom 8-bit Digital-to-Analog Converter (DAC), triggered by the FPGA or any other TTL/CMOS input, that can deliver 0 – 18V on a 50Ω impedance with rise/fall time in the order of 5 ns. The timing is adjusted using also the 50 Ω cables as delay line. Moreover, since the DACs have an higher precision on the voltage setting, the calibration of the PM is done first, using the one obtained in the previous section, and then finely tuned on the DAC using the attenuator and looking at the count rate on the detectors.

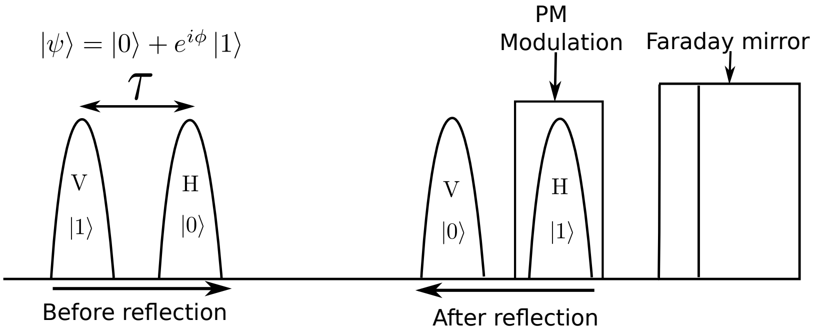


Figure 4.9: *Scheme of the timing required for Alice's phase modulator*

For what regards the master clock rate, this has been set to 60 – 80kHz because of afterpulsing effects in the detectors for repetition rates higher that 100 kHz. (This and other technical considerations will be deeply discussed in Sec4.4 where a closer look is given to the components used.)
In order to better clarify the ideas,lets see how an run of the experiment works:

- The program on the FPGA is started. The FPGA sends a TTL signal to trigger the laser source. The laser source (id300) emits a pulse of 1 mW at 1550 nm with 300 ps FWHM. The polarization of the pulse is horizontal.

- The pulse is attenuated by the variable optical attenuator so that the light is at the single photon level ($\mu = 0.1 \div 0.5$) after the Faraday mirror. The attenuation is fixed for all the duration of the experiment.

- The pulse enters the first port of an optical circulator and is are forwarded to the second port, connected to a 50:50 fiber coupler.

- Here the light can be transmitted to one or the other arms with 50% of probability. The upper arm is provided with a fiber stretcher that can modify the length of the fiber while the lower one has a delay line and a Phase Modulator. At this moment the phase modulator is turned off.

- The two arms are connected to the "exit" ports of a fiber polarization beamsplitter (PBS). The port connected to the longer arm rotates the polarization from horizontal to vertical, the other port doesn't change the incoming polarization. At the output of the PBS there are two pulses (like the ones in Fig 4.9), the first horizontally polarized and a second, after τ nanoseconds, vertically polarized. Here τ is the time equivalent to the length difference of the two arms. The same representation can be kept also with single photons, where now the amplitude of the two peaks represents the probability to find the photon. So, after the PBS we ac think to have two pulses, shifted by τ and with orthogonal polarizations, travelling in the fiber.

- The PBS is connected to a fiber delay line that, in real application, is the fiber link between Alice and Bob. Everything described so far is identically applied for the second apparatus that starts from Bob'.

- Now, in Alice's lab the two delay lines are connected to a 2x2 fiber switch. The switch connects the 2 input port and the 2 output ports in a straight or crossed configuration. The switch works in a non-latched mode and is activated with a TTL signal. In our case the timing and the TTL signal is directly provided by the FPGA. The FPGA's program contains a binary RNG (32-bit LSFR) directly implemented in the FPGA. The activation of the switch depends on the value of this random bit, extracted at each run. The value is then stored on the PC.

- The two signals enter in their respective path and they pass through Alice and Alice' PM, that are kept off. Alice and Alice' PM must be polarization independent.

- After the PM they are reflected by the Faraday Mirror, that changes the polarizations to their corresponding orthogonal. From now the modulation starts.

- On the way back, the FPGA, generates two random numbers from (0 to 7). These numbers correspond to the settings needed for the state preparation at Alice and Alice' sites. The number generated is sent to a custom built DAC that generates a sharp square wave with an amplitude that ranges from 0 to 18V, depending on the transmitted number. This wave is sent with a 50 Ω cable to the PM that modulate the second, "peak", preparing the qubit. In this way Alice and Alice' states are encoded and the settings are stored in the PC.

- The two qubits enter again in the switch that is still active, in this way they come back on the same path they used in the way forward. The activation signal is long just enough to let the last peak to leave the switch. After the switch returns to its original configuration (straight). Then they go trough the delay line up to the PBS.

- Here, since the two "peaks" have opposite polarization respect the way forward, the first peak, having a vertical polarization enters goes is transmitted to the long path, while the second, having an horizontal polarization, goes trough the short. Like in Alice and Alice' case, other two random number are generated (from 0 to 4), sent to the DAC that controls the PM which is responsible to modulate the qubit. Also in this case the values of the settings are sent to the PC.

- After the modulation, since one peak did the Long-Short path and the other the Short-Long, the peaks interfere at the coupler and the single photon is emitted in one of the two arms.
- At this point the synchronization program on the FPGA generates a TTL pulse that is sent to the P400 pulse generator. This pulse is used as a trigger for the four independent channel of the P400. Each channel is connected to the gating electronics of one Single Photon detectors. After receiving the trigger the P400 waits a different and programmed amount of time before sending a TTL pulse to the gating circuitry. In this way is possible to achieve a time resolution better than the one imposed by the FPGA's clock.
- The output of the detection from the detectors is encoded by the detector's circuitry into a TTL pulse that is sent directly to the FPGA. The FPGA reads the value and sends it to the PC.
- This ends one round. All the process is repeated for all the duration of the quantum exchange.

A photo of the final setup is presented in Fig. 4.10

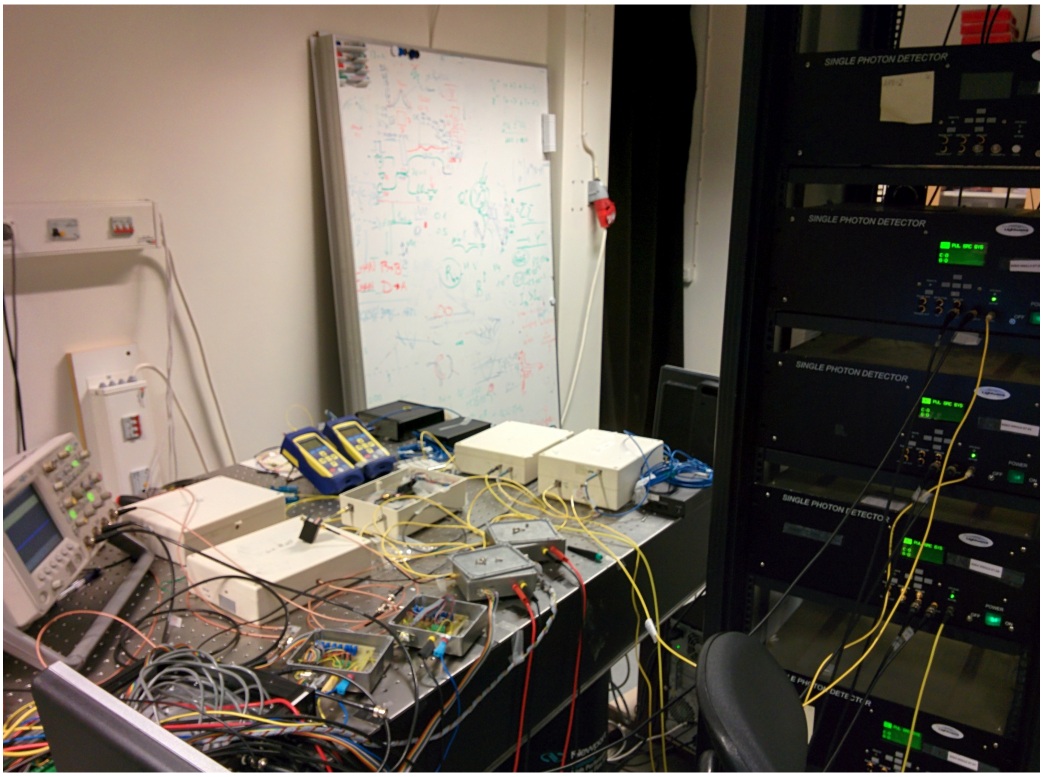


Figure 4.10: *A photo of the complete setup*

4.4 Electronic and Instrumentation

In this section will be briefly discussed the components used for the protocol.

Fiber Stretchers

The fiber stretchers used are the FST-001 by General Photonics. The stretching effect is obtained using four piezoelectric actuators near the fiber. Each of the four piezos can be controlled independently, allowing high resolution. Piezos can be controlled with an analog signal or a 12-bit TTL signal. In our case the control has been done with a digital signal, using directly the FPGA. Thanks to these fiber stretchers is possible to finely tune the path difference in the unbalanced Mach-Zehnder interferometers. In particular the two interferometers were connected together, by connecting the output of one to the input of the other, then the fiber stretchers were activated until an interference pattern was observed and then optimized by searching for the best visibility.

Circulator

The fiber circulator is a 3 port optical device with really nice transmissions features. The device transmits light from port 1 to port 2 and from port 2 to port 3 while blocking all the other possible configurations. This device is fundamental for the plug'n'play configuration where the first arm of the first coupler is used to "inject" the light pulse coming from the laser but is also used for retrieving the output from the interference. The circulators used in the setup are THORLABS CIR1550PM with insertion loss equal to 0.9 dB of insertion loss and 40 dB of isolation.

Faraday Mirror

A Faraday mirror is an optical device that can reflect light, changing the incoming state of polarization to its orthogonal. The Faraday mirror is obtained combining a simple mirror with a 45° Faraday rotator. The Faraday rotator (FR) is a magneto-optic device that can change the polarization of the incoming light thanks to the magnetic field. In this device the lines of the magnetic field are aligned with the propagation direction of the light. The material through which the lights propagates can change the angle of polarization of an incoming linearly polarized light proportionally to the magnitude of the magnetic field and to the length of the material. Since the angle of rotation does not depends on the direction of the light, unlike waveplates, if a mirror is placed after the FR the effect is doubled. In this way if we combine a Faraday rotator with a 45° of rotation angle and a mirror we obtain a Faraday Mirror. The model we used are MFI-1550-FC from Thorlabs.

Couplers

The fiber coupler is the fiber equivalent of beamsplitters. In our setup we used 2 2x2 50:50 SM fiber coupler from Thorlabs (model TW1550R5F2).

PBS

The polarization beamsplitters are three port devices and the one we used are made with polarization maintaining fibers. The model we used are 50:50, the PBC1550PM-FC from Thorlabs.

FPGA

The central component that controls all the setup is a Field Programmable Gate Array (FPGA). In our case the board is a NI-7831R by National Instruments, powered by a Xinlix Virtex II FPGA with 1 million of logic gates . The board is equipped with 8 analog inputs and 8 analog outputs rated to work in the ±10V range. The raise/fall time is 1µs. The board has also 96 digital input/output that can handle voltages up to 3.3V and with 100ns rise/fall time. The internal clock of the board is 40MHz but it can be raised to multiples of this clock. The board is connected to an host PC trough the PCI interface and the data on the board are kept in a small buffer an then transferred to the PC using a FIFO (First-In-First-Out) communication protocol.

Digital Delay Generator P400

The P400 from Highland Technology is an amazing square wave generator. It has 4 independent channels at 50 Ω impedance that can go from -5 to $+11.8$V. The maximum repetition rate is 10 MHz and the time resolution for the delay is 1 ps with a programmable delay up to 1000s. The slew rate is rated to be $4\text{V}\,\text{ns}^{-1}$ but on our sample we measured a risetime of 1ns with 11.8V of amplitude. Our model was provided also with 4 high voltage channels 0 to 50V at low impedance. The model has also an Ethernet port for remote controlling through telnet, but are needed approximately half a second between one command and the other. The high temporal resolution of the P400 made it perfect for the synchronization of the gating electronics.

Single Photon Detectors

One of the hardest technological challenge nowadays is the efficient detection of single photons. In our experiment we used photons at 1550nm; the energy of these photon is lower than the Si bandgap so solid state detectors are made with InGaAs Single Photon Avalanche Diode. These devices works as an avalanche diode, with a biasing stage that puts the diode above the breakdown voltage for a window long 1 ns. If during this window a photon interacts with the detector the breakdown occurs, triggering an avalanche effect that forms a signal. This signal is then compared to a threshold value with a discriminator in order to output a nice TTL pulse. In particular our model is a PGA-600 by Princeton Lightwave. The quantum efficiency is rated to be above 20%, which is an excellent value for these kind of detector at in this wavelength band. The two main problems of these detectors are: dark counts and afterpulsing. Dark counts are registered counts without any incident light, mostly of thermal origin and can therefore be strongly suppressed by using a cooled type of detector. This is the case of the PGA-600 which operates at temperatures in the $217-230$[K] range. In this way the dark count rate is limited to 10^{-5} per trigger. This is a small value but, due to the high attenuation of the setup, is the limiting factor to the visibility of the interferometer.
The afterpulsing is an effect caused by carriers that become trapped during an avalanche and are subsequently released in the next gate-on period. This can be included in the dark count rate but, unlike the thermal events, depends on the repetition rate used. The PGA-600 after 100 kHz has serious afterpulsing effects and this is the main bottleneck for the repetition rate of the entire protocol.

Photon source

Ideally for QKD experiments, single photon sources should be used. Unfortunately, we still lack of real on-demand single photon sources that can reliably produce photon at good repetition rates. For this reason WCP are commonly used and are made attenuating a pulsed laser source to the single photon level, or below, with an optical attenuator. Since the photon statistics of a laser follows a Poisson distribution, multiphoton events cannot be deleted, they can only be reduced. In fact the probability of obtaining a n photon pulse giving a mean photon number μ is given by:

$$P(n) = e^{-}\mu\left(\frac{\mu^n}{n!}\right) \tag{4.27}$$

For $\mu = 1$ the proability of having multiphoton events $P(n > 1) = 0.264$ is extremely high: more than one events over four is a multiphoton event. Multiphoton events are extremely insidious for two reasons: fist they expose the QKD system to the Photon number splitting attack (Sec. 2.2.2), second they clearly violate the qubit assumption for SDI QKD, since the n photon state lives in $\mathscr{H}_{tot} = \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \cdots \otimes \mathscr{H}_n$. For these reasons a common choice for QKD experiment is to use $\mu = 0.1$ where the $P(1) = 0.09$ and $P(n > 1) = 0.005$. This improves a lot the situation but it doesn't solve it completely: the realization of single photon source is still required.

Laser

The laser source used is an IdQuantique id300: a 1 mW of peak power at 1550nm Fabry-Pérot laser, with 300 ps FWHM. The laser is externally triggered and can reach up to 500MHz of repetition rate. The light at the output is horizontally polarized. The high stability and the short FWHM makes it perfect for our purpose.

Attenuator

In our setup we used a variable optical attenuator with fiber connections: the DA-100-SC-1550-9/125-P-50 from OZ Optics. The variable attenuator has −1.6dB of insertion loss and can attenuate from 0 to 60dB with steps of 0.01dB.

Phase Modulator

The Phase Modulators used exploits the electo-optical properties of LiNBo$_3$. In particular, in these devices the refraction index is a a function of the strength of the local electric field. By changing the field is thus possible to change the speed of light in the material and so, the phase. To obtain a linear modulation the geometry of the electrodes inside the modulator is like the one of a planar capacitor. Two parallel plates are inserted on the surfaces of the material and the electric field generated depends linearly on the potential, generating a linear modulation. However this linearity is valid only for small values of the potential, usually below the 20V, while for higher potentials the linearity is not preserved. Unfortunately the modulation also depends on the temperature, causing a random phase shift. This effect however is not influent in our case because of the plug'n'play configuration. Moreover, usually they are also polarization dependent. In our case the PM used are made the APE PM-150-005 by JDSU. They are rated to have a 500 MHz bandwidth and have 3.5dB of insertion loss. The V_π is 6.73 V. Because of the polarization dependence they all include a horizontal polarizer. In this way they cannot be used ad Alice and Alice' stations because of the polarizer. Here the polarizers would block one pulse on the way forward an the other (because of the FM) on the way back. For this reason a special polarization independent configuration, requiring two PM, has been used.

Polarization Indepenendent PM

The polarization independent PM is based on the configuration proposed in [92] and can be seen in Fig. 4.11 The first PBS splits the two pulses, depending on their polarization, then each one is modulated by an independent phase modulator, both synchronized with the same reference signal, and then the signal are recombined as they were before using another PBS. Given the symmetry, on the way back the description is the same. Thanks to this little trick we can use the phase modulators with the polarizers also for Alice and Alice' stations.

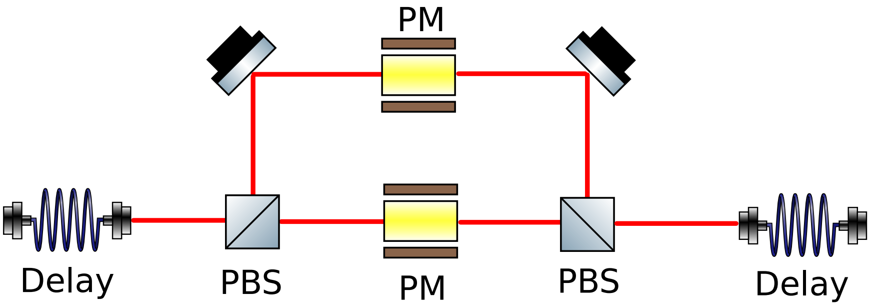


Figure 4.11: *Polarization Independent Phase Modulator*

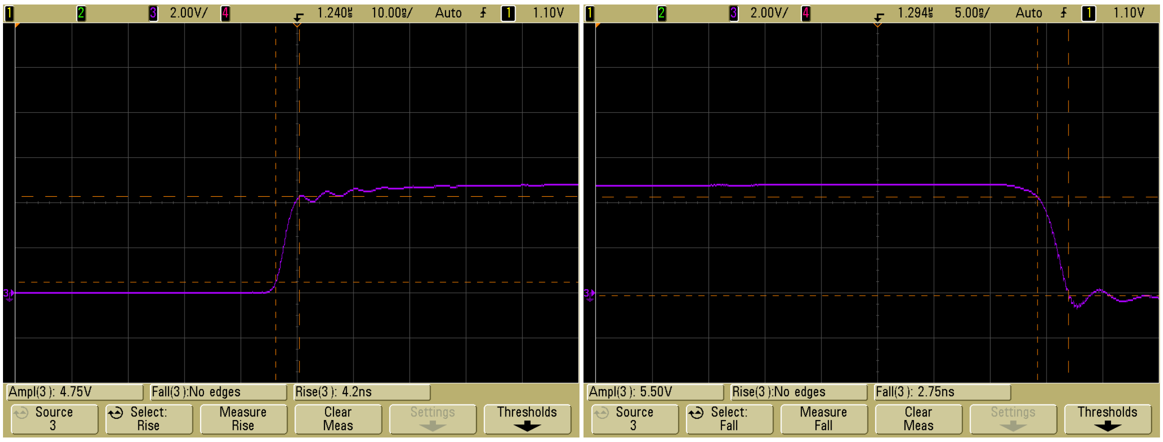
Optical switch

The optical switch is a 2x2 switch manufactured by Agiltron of the NanoSpeed class (model NSSW-22-5-1-1-1-3-1-2). This is as solid state switch with no moving part that can switch optical signals with a maximum response time of 300ns (typical 100ns) with 100kHz of repetition rate (external board needed). The insertion loss at 1550nm is 0.8dB and the maximum crosstalk is 30dB. The switch is controlled with a 3.3 or 5 V signal.

Custom built DAC

One of the main problem in the realization of a phase-encoded QKD system is the precision needed for the modulation. As described in 4.4 the PM we had access to are characterized by a V_π of the order of $7V$, and the maximum modulation needed is $\frac{7\pi}{4}$ close to the $12-13$V range. Moreover , in order to successfully modulate only one peak, the modulation signal should have really fast rise and fall times, in the order of few nanoseconds. These two requirements, high output voltage and fast rise time are critical for a successful implementation but at the same time is challenging to have both. A device that have the right performance is the P400, with rise/fall times of less than a nanosecond and amplitude up to 50V. However the P400 doesn't have any way to change the settings from run to run (the built in Ethernet communication is too slow for our purpose) making it useless for a real QKD test. On the other hand the FPGA gives us the

ability to change the output at each run but the analog outputs, limited to 10V, have rise times on the order of 1µs. The digital I/O on the other hand have rise-times of 100ns but are limited to 3.3V.
One option could be to use op-amps and comparators to amplify and sharpen the signal coming from the FPGA. Unfortunately, there are no commercial devices that match our requirements. For this reason we decided to build a custom DAC that could fit our needs. In this case the DAC has 8 digital inputs (like the maximum number of settings of Alice's device) and 1 50 Ω RF output that will be used for the connection with the PM. The core of the circuit works in this way: Each of the 8 3.3V TTL input triggers an UCC27517DBVT MOSFET Gate Driver. This device is controlled with a TTL/CMOS input and can deliver up to 18 V with max rise/fall times of 12 ns. The output of the IC is then attenuated using a resistive attenuator, where one of the resistence is a 25-turn 500 Ω trimmer. Adjusting this value is possible set the amplitude of the resulting wave. Finally the signal goes trough a sckotty diode and then is connected to the 50 Ω SMA connector for the RF output. In this way is possible to obtain 8 different modulations, one for each state that Alice needs to prepare. The performance of the entire circuits are way better respect the maximum (and also typical) values in the datasheet and are shown in Fig. 4.12



Ampl(3): 4.75V Fall(3):No edges Rise(3): 4.2ns

Ampl(3): 5.50V Rise(3):No edges Fall(3): 2.75ns

Figure 4.12: *Performance of the DAC*

As we can see the rise time is 4.2ns and the fall time is 2.75ns, good enough for our purpose.

4.5 Software for instrument control and data analysis

The software used for this experiment has been divided in two parts: one, written in Labview, controls the experiment and saves the raw data while the other, written in C++, is used for the data analysis only. In this way is possible to exploit the points of strength of both languages: the easiness of controlling hardware given by Labview and the uncomparable speed offered by C++. Moreover, once the raw data are saved, multiple different analysis can be performed to the same data off-line.

4.5.1 FPGA program

The FPGA program is divided in two sections: the host, executed on the PC and the fpga, executed on the FPGA. The host is used only for the initialization of the setup and the data recovery: it keeps "listening" the communication channel open with the FPGA program for new data and as soon as he can it grabs the new data freeing the FPGA buffer. The data are kept in memory and then saved into the hard drive. Since the memory⟷disk management with Labview is far from optimal, the program divides the entire execution in subsections or "loops", saving data from memory to disk after each loop. In this way there is no risk to fill up all the memory of the host and the number of loops is chosen to minimize the time lost for this operation. The data exchange is done with a DMA FIFO (First-In-First-Out) trough the PCI connection; this is the fastest method offered by Labview and has turned out to be sufficient for all our needs.
Another important point is the random number generation. Ideally for a QKD protocol Alice and Bob should have access to true random number generators, however the work of this thesis is focused on exploring the possibilities of SDI and not to provide a commercial QKD system. For this reason the RNG requirement is relaxed (this is quite common for QKD lab experiments) and a pseudo-random-number-generator (PRNG) is used. The PRNG is implemented directly in the on the FPGA using the Linear Feedback Shift-Register (LFSR) written in Labview. The LFSR can be efficiently implemented in FPGAs that can produce 32-bit random numbers at rates of up to 500MHz (in our case we are limited by the 80 MHz internal clock of our Virtex II). The method used is like the one proposed in the Application note 052 by Xilinx [93] , where all the optimal taps for LFSR from 2 to 168 bits are reported. A future upgrade is in plan to use real random number generators, for example based on Generalized Ring Oscillators on FPGA [94] or optical QM setups.

4.5.2 Analysis program

The analysis program, instead, works offline and takes the raw data in output from the FPGA program. The file contains the settings used by Alice,Alice', Bob and Bob', the bit regarding the switch and the outcomes of the measures. The program using the information is able to calculated the data table $P(b|a,x,y)$ and the value of the dimension witness. Then two binaries files containing Alice and Bob raw keys are generated and processed with the AIT QKD framework (more details in) for the error estimation and the privacy amplification. At the end two identical key are generated. Other to the violation of the dimension witness the QBER, the raw data bitrate and the efficiency of the post-processing is computed.
Again for a fully working QKD setup the fist part, the evaluation of the dimension witness, should be done on two different computers (or threads) in order to have a realistic user simulation. However at this stage our attention is focused on the development and analysis of the protocol and this details can be taken into account in a later stage.

4.5.3 The AIT QKD framework

The AIT QKD framework is an open source project that aims to provide a fully functional suite for the data processing of a QKD protocol. The project is developed in C++ (11) and is extremely modular. There is a core interface over the DBUS where all the modules are attached. Every module uses the DBUS for the interpocess communication and they're all linked and executed in chain. The package already provides all the needs for a successful BB84 implementation. From the interface to the hardware, to sifting, error estimation, error correction privacy amplification and integrity check. All developed over a TCP/IP network stack fully compatible for the execution of the protocol over the Internet. In our experiment we explored the functionalities offered by this amazing software and we used the framework for the classical post-processing part: error correction, privacy amplification and integrity check. The raw keys for Alice and Bob were prepared with the C++ analysis program into suitable binary files. Then two process on the same local machine were set up for the execution of the classical processing. In this way the network communication in simulated on one local machine. However the generalization to two different users over the internet is trivial. The error correction is based on the CASCADE algorithm [95] while the privacy amplification is based on Toeplitz matrices [96] The software runs all the classical part and at the end an identical binary file is produced for each user: the key file. In the metadata of the file are written the statistics of the post-processing.

4.6 Results

4.6.1 Calibration of the phase-modulators

The first test needed for the execution of the experiment is a calibration: the calibration of the phase modulators. The phase modulators can change their refraction index, and so the phase of the light travelling into it, by applying a voltage difference across their electric contacts. However they are not calibrated and we don't know the relation between the phase shift and the voltage applied so we have measured this relation. The setup for the test is presented in Fig. 4.13 and is a simplified version of the plug'n'play QKD setup described in Section 4.3.2 Since no attenuator is used, is possible to detect light pulses with normal photodiodes. In this case two Thorlabs SIR5−FC, 5GHz InGaAs FC/PC-Coupled Photodetectors are used. The signal coming from the detectors is acquired with a digital oscilloscope: a MSO6054A from Agilent with 500 MHz of bandwidth. The modulation of the PM is performed with the P400. The entire acquisition is fully automatized using a Labview script: the script controls the P400, which modulates the PM from −5 to 10.1V with steps of 0.01V. For each step the Labview program acquires the pulse generated by the detectors from the oscilloscope, calculates the amplitude and the errors on the amplitude and then saves the data in a file. The errors are calculated using the specifications in the manual of the oscilloscope. The formula describing the interference in a Mach-Zehnder interferometer

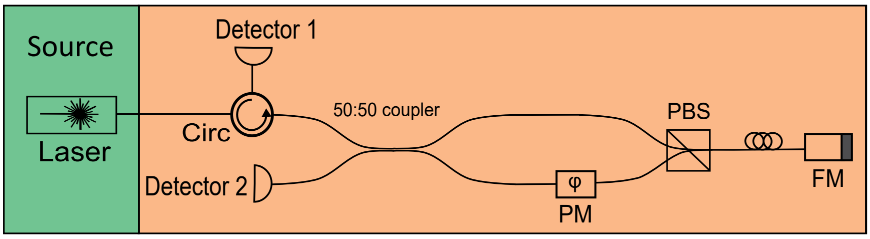


Figure 4.13: *Setup for the calibration of the PM*

can be expressed as:

$$D_1 = \frac{I_0}{2}(1+\cos(\omega\Delta\phi+\phi_0)) \qquad D_2 = \frac{I_0}{2}(1+I_0\sin(\omega\Delta\phi+\phi_0)) \tag{4.28}$$

where D_1, D_2 are the intensities at the two detectors, I_0 the intensity of the incoming light, $\Delta\phi$ is the phase differece created by the PM and ϕ_0 another constant phase shift given by other elements in the interferometer. During the measurements an interference was present and the signals resulted shifted down by a constant value, for this reason the calibration was don with a function in the form:

$$I(x) = \frac{I_0}{2}(1+\cos(\omega x+\phi_0))+c \tag{4.29}$$

The results for a representative is shown in Fig 4.14 while all the results are presented in Table 4.3 As we can see there are only slight differences in the parameter ω meaning that the phase modulators have more or less the same modulation. The variance in the parameter I_0 instead is caused by the different insertion losses, not only due to the PM. The calibration confirms that a relative high voltage is needed for a π phase shift: $V_\pi \approx 6.67$V. These calibrations will be used for all the experiments involving the Phase Modulators.

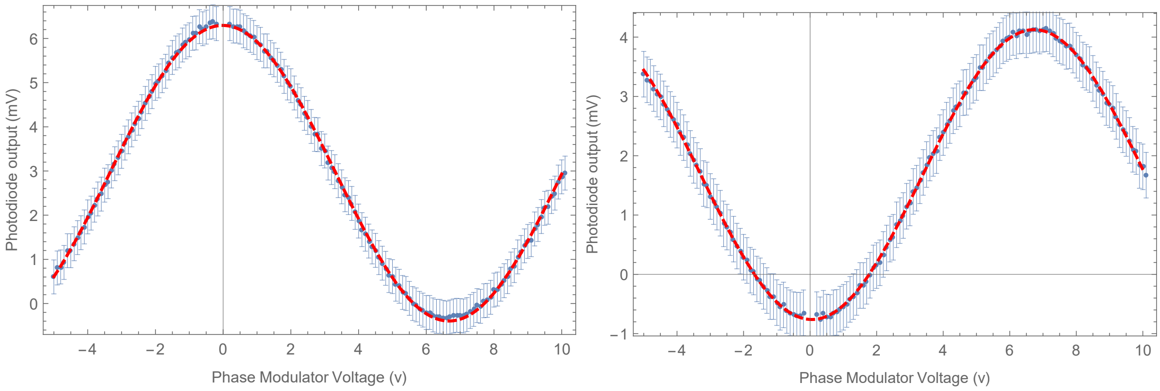


Figure 4.14: *Results of the modulation for the two detectors.*

	I_0(mV)	ω (rad V^{-1})	ϕ (rad)	c(mV)
PM 1	5.47 ± 0.01	0.4504 ± 0.0005	0.042 ± 0.002	-0.364 ± 0.007
PM 2	6.69 ± 0.01	0.4702 ± 0.0004	0.005 ± 0.002	-0.395 ± 0.008
PM 3	8.65 ± 0.02	$0.465, 0.001$	0.011 ± 0.009	-1.047 ± 0.009
PM 4	2.688 ± 0.006	0.4451 ± 0.0005	-0.065 ± 0.002	-0.371 ± 0.007
PM 5	1.313 ± 0.006	0.4592 ± 0.0009	-0.013 ± 0.005	-0.334 ± 0.007
PM 6	1.135 ± 0.005	0.461 ± 0.0009	-0.0244 ± 0.004	-0.328 ± 0.006

Table 4.3: *Results of the calibration*

4.6.2 A first test of the apparatus: testing the dimension of a quantum system

In order to see what our setup was capable of, after the construction, we decided to test it in order to see what could be the maximum violation of the dimension witness we could get. The tests

that can be found in literature are mainly free-space based [68][78], while the fiber based used heralded single photon source and polarization encoding[41]. Is thus fundamental to have an idea of how this setup can be compared to the ones already proposed, before actually going on with the experiment; if the performance are not sufficient the entire design must be changed.
The setup under test was the plug'n'play in Fig 4.6. The setup is "half" part of the final setup and can give us good indications on the final performances simplifying a lot the control mechanism respect the complete version.
Unlike the final version the settings of the two PM modulators are not set randomly. Alice always sends the BB84 states while Bob "scans" the space of parameters by applying different voltages on his modulator, scanning the range from −5 to 10.2V with steps of 0.1V. The control and acquisition is automatized by a Labview program on the FPGA that controls the P400, used for driving the modulators, and counts the detections from the detectors. For each step the number of count for each detector is obtained, then these values are divided for the total counts giving the data table $P(b|a,x,y)$. Another program written in C++ computes the value of the dimension witness and its (statistical), error in function of the two possible measures performed by Bob $D(M_1,M_2)$. The form of the witness is the one given by Eq: 4.11 The results are presented in Figure. 4.15
The maximum value for the violation obtained is 5.616 ± 0.015. This high value, the highest known to the author at the moment of writing, for the dimension witness has been made possible thanks to the incredible stability and visibility offered by the plug'n'play configuration. In this case the visibility, was really high: $\mathcal{V} = 99.67\%$. This great result confirms that the setup works really well and is good for our QKD purpose.

4.6.3 Complete protocol

In this section the results of the complete protocol, described in Section 4.1.8, and performed with the setup described in Sec. 4.3.3 are presented. The entire protocol was performed at different values of the mean photon number $\mu = 0.1, 0.2, 0.5$ in order to understand the effects of the dark counts on the visibility and on the violation of the dimension witness. Moreover these different values can be used for the study of the performance of the with Decoy states. For each value of μ is computed the dimension witness, the visibility, the raw key rate and the QBER. The QBER in this protocol has not the same role as in the BB84, since here the security is checked trough the value of the dimension witness, however is a good indicator of the quality of the communication task. The errors on the DM and on the visibility are calculated trough propagation, considering a Poisson distribution for the counts revealed by the detectors. The values of the dimension witness obtained were always well above the threshold for security ($D_s = 5.28$), but slightly below the value obtained in the dimension witness test of Sec 4.6.2. This is probably caused by the

μ	Dimension witness	Visibility	QBER	Raw key rate (bps)
0.1	5.472 ± 0.013	0.972 ± 0.002	1.72%	60.5
0.2	5.526 ± 0.009	0.981 ± 0.001	1.09%	112.91
0.5	5.577 ± 0.006	0.9863 ± 0.0008	0.74%	240.61

Table 4.4: *Results of the complete SDI QKD protocol*

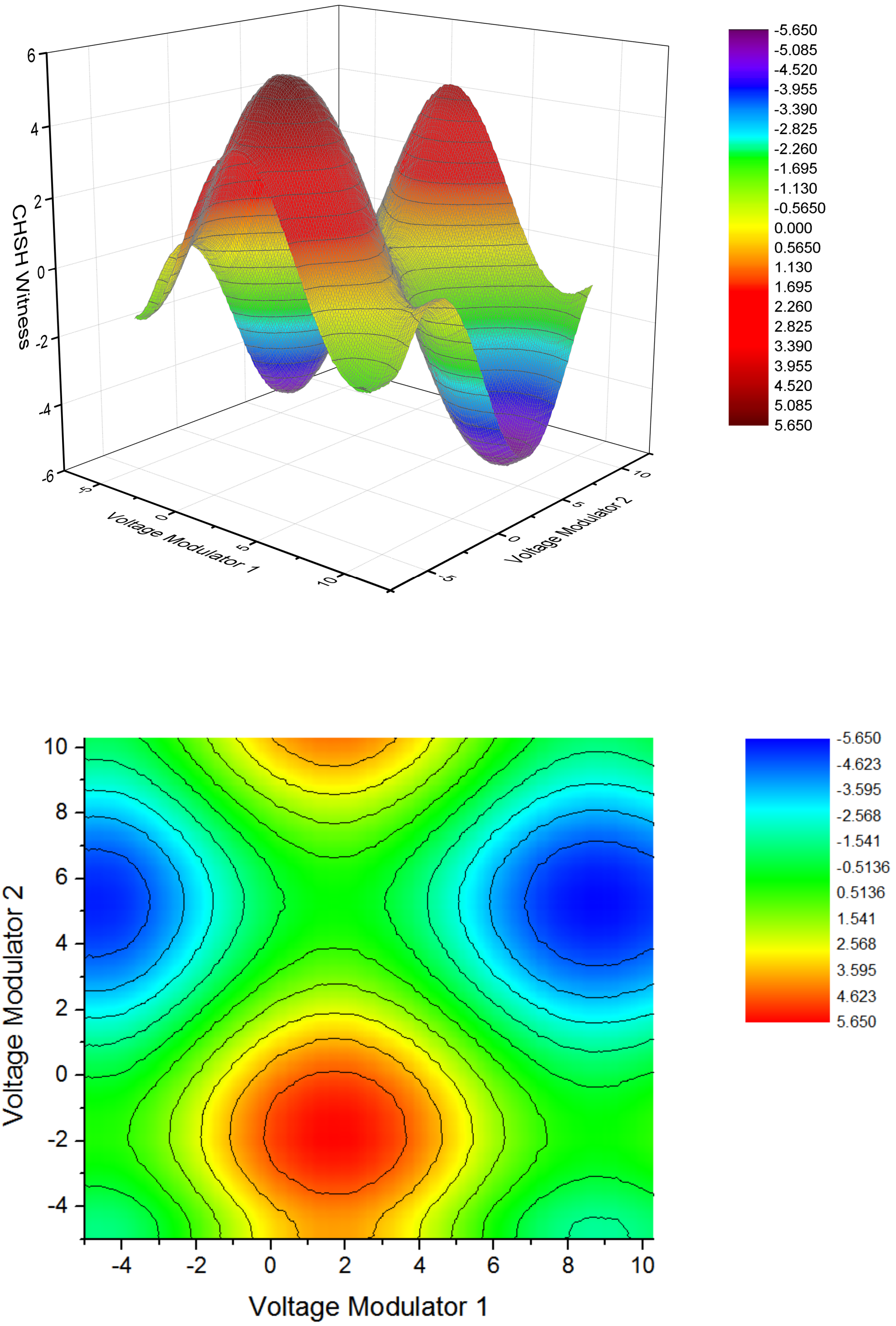


Figure 4.15: *Results of the modulation for the two detectors.*

increased complexity of the setup and the limited precision in the alignment of the states and basis. Moreover at low μ the effect of dark counts is relevant, lowering the visibility, and thus limiting the value of the witness.

4.6.4 Classical post-processing

After the classical post-processing the key obtained for the two users are identical in all the three cases. This can be checked by the users using a one way hash function and checking the hash over the public channel. In Table 4.5 are reported the final statistics:

μ	Percentage of used bits	QBER	Final key rate (bps)
0.1	34.44%	1.72%	39.66
0.2	29.59%	1.09%	79.50
0.5	15.12%	0.74%	204.24

Table 4.5: *Results of the complete SDI QKD protocol*

4.6.5 Discussion

The results obtained are really exciting in the optic of a SDI QKD, especially the violations of the dimension witness. For what regards the key generation rate, this is quite low if compared to modern QKD systems, expecially others MDI. In [38] for exaple a key rate of 10^2 bps is obtained for a 50 km link. Clearly our setup is limited by the afterpulsing effect of the detectors and with an upgrade of these the repetition rate could be increased by one or two order of magnitude However, is important to remind that the experiment performed is a preliminary study,a proof of principle, and that there are still some critical points that need to be addressed. Fist of all, this implementation is vulnerable to the PNS attack and so decoy states must be employed. Employing decoy states can increase not only security but also the key rate, giving the possibility of generating the key at an higher μ (for our QBER the optimal μ would be 0.5 [97].) That's why data has been taken for different value of μ, in order to estimate the performance of a possible decoy. Then another problem in the Trojan horse attack, this has been limited carefully checking the modulation times at Alice station but is not completely closed. Then here Pseudo-random number generator have been used while a proper implementation would require fully true random number generators. Finally, the fair sampling assumption is still required and the analysis of the extension of the procedure described in Sec 4.1.6 is still under development. However, recent advances in the detector's field has led to the commercialization Superconducting Nanowires Single Photon Detectors (SNSPD) with detection efficiencies of over 40% and they're expected to increase it up to 95%, without afterpulsing [98]. This could open new ways for the implementation of SDI and other QKD protocols.

CHAPTER 5

Random number generation and certification

Random numbers play a central role in many areas of modern society: computer simulations, gambling, standard cryptography and quantum cryptography.

In the previous chapters we saw how the role of random numbers is fundamental in cryptography: in both, classical and quantum, it's essential for the security of the entire protocol. Is not a coincidence that the NSA has chosen to put a backdoor in the random number generator to break RSA.

Today, most of the random number generators (RNG) are based on the laws of classical physics. Classical physics, however, is fundamentally deterministic and these RNG cannot be really random. For this reason, this kind or RNG are called Pseudo Random Number Generators, because their output is generated using deterministic algorithms, that sooner or later are going to manifest some sort of patters. Quantum mechanics, instead, relies on the concept of randomness, making it a good place to start looking when the objective is to build True Random Number Generators (TRNG).

In the last years, an intense research has been performed on the development of Quantum Random Number Generators (QRNG), that are able to exploit quantum systems in order to extract true randomness. These devices are now also commercially available.

However, even for QRNG two issues have been highlighted recently. The first is: how is possible to certify the amount of randomness present in the output of our QRNG? The second is: can we find some protocols that can generate randomness without having to worry, and so trust, about the internal working of the devices? In this chapter we are going to see how a SDI approach to quantum random generation and certification, can answer to these questions. At the end we present the results we could obtain with the apparatus described in the previous chapters.

5.1 Quantum solutions to a classical problem

The problem of generating true random numbers is really old but, in the last years, has gained more and more importance. The need of true random numbers is not limited to cryptography,

but is also required for scientific simulations and fair gambling. Albeit an intuitive definition of randomness is commonly shared by anyone, is really hard to precisely define and test what is random and what is not.
We can say that a random number is a number generated by a process that cannot be predicted and reproduced. But with this definition a big problem arises. If we are given a number, how can we say if this is random or not?
For an infinite number this could be done by looking if the Shannon's entropy is also infinite. But how is it possible for finite numbers? For a finite string of random bits is not possible to verify if it is random or not. We can only check that it shares some statistical properties of randomness:

1. **Unpredictability**: is not possible to predict the following bit of a random string having the knowledge of all the preceding.
2. **Uniformness**: there should be an equal number of 0's and 1's in the string in order to be unbiased
3. **Lacks of patterns:** Patterns are the manifestation of a structure in the generation of the numbers, meaning that the observed is only *apparent randomness*

with these requirements is clear that no randomness can be obtained in the world of classical physics. Classical physics is completely deterministic and any classical process admits a perfect description. Randomness observed in this context is only apparent and is mainly due to the chaotic behaviour of some complex systems. These events are extremely susceptible to initial conditions and perturbation, making hard to predict the outcome in a long run. However, despite their complexity, the evolution is still completely deterministic.
On the contrary, quantum mechanics is based on randomness and many simple experiments performed with QM systems can be intrinsically random in their output.
One of the simplest case, is a single photon sent to a beamsplitter. In this case, if the the BS is 50:50, the output will be a completely random string of unbiased bits[99]. Along this simple experiment, many others setups have been proposed and now, quantum random number generators are commercially available.
Also in this case, some of the problems previously discussed for QKD arise. In the case above depicted, the user cannot certify the randomness of the measurements unless he can obtain a perfect description about the functioning of his device. But, since the device is manufactured by a third person (who could conspire against him) he cannot establish the presence of private randomness, without trusting the device. This opens a serious security flag, since one can never exclude that the numbers were generated in advance by the adversary and copied into a memory located inside the device or that the device contains, in general, a backdoor. Moreover, in any real experiment the randomness of measurement is unavoidably mixed up with an apparent randomness which results from noise or lack of control of the quantum devices. This opens the problem on how to extract the real from the apparent randomness.
For the above mentioned reasons, the world of QRNG started to look at new and better ways for randomness generation. Taking inspiration from DI protocols for QKD, first Coleback, using the GHZ test [100], and then Pironio [101], using the CHSH inequality , in 2010 conceived and explored the idea of a DI protocol for QRNG. The main idea is to use, like the DI QKD, uncharacterized boxes in order to check the violation of a Bell inequality. If the violation is obtained, the system used is certified to be quantum and the outcomes are truly random. Since these DI-QRNG

requires some random numbers as input (for the choice of the settings used in the Bell test), it is more properly a device-independent random number expansion protocol (we are not going to distinct RNG and RNE in the following discussion). Moreover, the amount of randomness in the output string can be linked to the numerical violation of the Bell inequality.
If we consider $P(a,b|x,y)$ the probability of having a,b as outcome of the measurement given the settings x,y, we can quantify the randomness of the output pairs, conditioned on the input pairs by the average min-entropy $H_{min}(A,B|X,Y)$ [101], defined as:

$$H_{min}(A,B|X,Y) = -\log_2(\max_{\{a,b\}}\{P(a,b|x,y)\}) \tag{5.1}$$

In the same paper the authors show how is possible to give a lower bound to the H_{min} in function of the observed value of the CHSH inequality S:

$$H_{min}(A,B|X,Y) \geq 1 - \log_2\left(1+\sqrt{2-\frac{S^2}{2}}\right) \tag{5.2}$$

This is possible because the violation of the CHSH Bell inequality is compatible only with a restricted number of different $\{P(a,b|x,y)\}$, and the maximum value of such group can be analytically bounded for each value of S.
In this way a bound is given also on the randomness produced by the quantum devices, independent of any apparent randomness that could arise from noise or limited control over the experiment.
Unfortunately, this approach requires entanglement and a loophole free violation of a Bell inequality, making the DI setup complex and with the same problems already encountered and discussed for DI-QKD.

5.2 A Semi-Device-Independent approach

The need of entanglement is a big drawback for the implementation of DI-RNG since adds a lot of complexity to the setups and prevents to obtain high rates. Moreover, the need of a loophole free violation of a Bell inequality requires very high detection efficiencies, that cannot be achieved yet. We have seen in Sec 2 that the same thing happened for DI-QKD and in order to overcome this limitations, new slightly weaker but more practical protocols were proposed. This is the case also for SDI-QRNG, that was first proposed by Li et al in 2011 [102], just after the SDI-QKD proposal. The protocol is nearly the same as the QKD case and is based on a 2 → 1 QRAC for qubit. In this way, adding the assumption that the dimension of the system exchanged is known, is possible to expand randomness in a prepare'n'measure way, without the need of a Bell test, and so, without entanglement. It's possible to treat the dimension witness in a similar way as Bell inequalities are treated in the DI case. Moreover, is possible to find a relation between the min-entropy H_{min} and the dimension witness, that can be used as a parameter for the certification of the randomness extracted by the protocol. Finally, since the value of the dimension witness can be computed only from the data and it can be done in real-time, the SDI-RNG can be considered also a real-time self testing RNG, as pointed out in [41].
In this thesis we have adapted our system, already built for the QKD, in order to test the performance that it can achieve in the context of SDI-RNG. Moreover, since our configuration is built

upon a parallel QRAC structure, the data obtained can be further studied in the optic of SDI-RNG without the fair sampling assumption.

But let's start looking more deeply the functioning of this protocol.

From the point of view of the quantum communication, the task performed is a QRAC: there are two black boxes, a preparation and a measurement device, that can exchange a system ρ_a^d of dimension d. The system can be prepared using different settings on the preparation device $a = \{a_0, a_1.., a_{2n-1}\}$. The measurement box has m settings, $b = \{b_0, b_1, ..b_{n-1}\}$, used to measure the incoming system ρ_a^d with the operators M_b obtaining an outcome $x = \{0, 1, ..d-1\}$. The process is repeated many times and the $P(x|a,b)$ are computed from the data and used to compute the value of a dimension witness.

In our case the task is a $2 \rightarrow 1$ QRAC for qubit performed in parallel, (see Sec 4.3.3). As we said before in these contexts the min-entropy H_{min} is used to measure the minimum randomness of the output x, and for this protocol it can be written as:

$$H_{min}(A,B|X,Y) = -\log_2(\max_{\{a,b,x\}}\{P(x|a,b)\}) \tag{5.3}$$

where the maximization is taken on all the setting and outcomes possible. We have to remember that the certification of the randomness must be done without any knowledge on ρ_a or M_b, for being SDI. This means that the evaluation of $\max_{\{a,b,x\}}\{P(x|a,b)\}$ can be done only by optimizing over all parameter settings that could reproduce the observed data, and then choose the least random result. With the assumption on the dimension d of the system exchanged, this is possible thanks to the dimension witness, which is a function of only the $\{P(x|a,b)\}$. Given the dimension, it exists a threshold value for the witness obtainable using classical system of that dimension, so if a violation is measured, that cannot be produced by a classical mix of deterministic strategies, and so randomness can be certified.

The problem can be expressed more formally in terms of an optimization problem:

$$\begin{aligned} \text{maximize} \quad & max_{a,b,x}\{P(x|a,b)\} \\ \text{subject to} \quad & P(x|a,b) = \mathrm{Tr}(\rho_A M_b^x) \\ & W(\rho_a, M_b^x) = \bar{W} \end{aligned} \tag{5.4}$$

where the optimization in performed over arbitrary ρ_a and M_b^x. The solution of this optimization provides the min-entropy bound of the measurement outcome, for the given two-dimensional quantum witness $\bar{W}$.

The maximum value of the min-entropy is obtained for the maximum violation obtainable by QM and is $H_{min} \approx 0.2284$.[102].

Is important to note that this value, expressed by H_{min}, quantifies the intrinsic minimum quantum randomness that can be generated by the experiment, and it's not influenced by the noise of lack of control of the devices.

However, like in the SDI-QKD, the violation of the classical bound is not enough for being able to extract randomness in the SDI-RNG protocol. The critical value of the witness W_{crit} depends on the particular form of the witness used.

In Figure 5.1 are presented the H_{min} in function of the witness value, for two different witnessed: the first one is the CHSH-inspired (the one given by eq 4.10 and with the QM bound at $2\sqrt{2}$)[103], the second one is the determinant witness (given by Eq: 4.15).[104].

For the CHSH-like witness the bound is the same that assures security in the QKD case and is

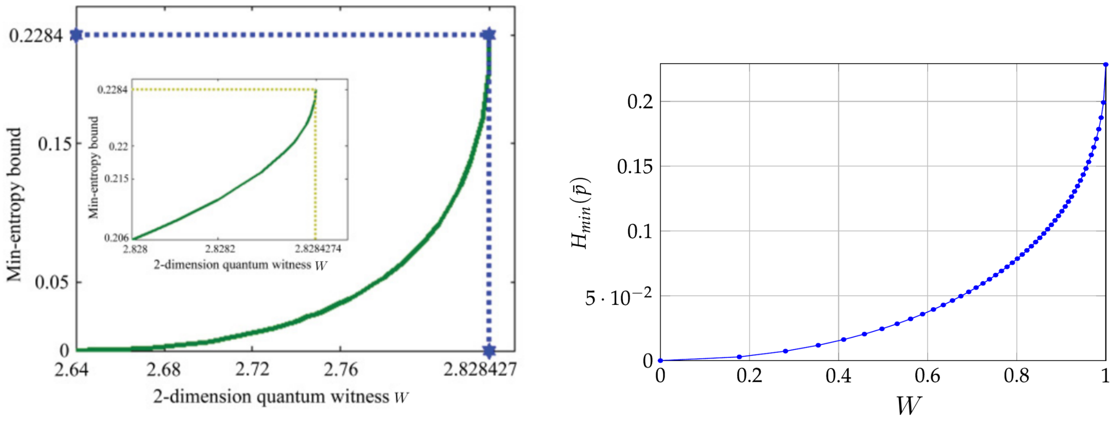


Figure 5.1: *Results of the optimization fo the 1) CHSH-like DW 2) Determinant DW*

≈ 2.64. This value is really close to the QM bound and so requires a careful experimental implementation.

In the case of the determinant witness, the critical value actually coincides with the classical bound, $W_{crit} = W_{classic}$. This makes this witness more robust and more practical for real world application. This is the reason why the only experimental SDI-RNG realized so far used this witness.[41]. However there's a price to pay for this robustness. In fact, this witness is derived under the assumption that the devices are independent, which is a fairly strong assumption.

Since we don't want to rely on such a strong assumption, we are going to use only the CHSH-like.

5.3 Analytical evaluation of the min-entropy

We have seen that, in order to be able to certify the amount of randomness present in our final outcome, we need to find a relation between the $max_{a,b,x}\{P(x|a,b)\}$ and the violation of the dimension witness.

In the previous chapter we stated that this is possible solving an optimization problem, reported in 5.4. Such problem has been solved, for the CHSH case, with the Levenberg-Marquadrt alghoritm first [102] and then with semidefinite-programming (which is guaranteed to find the global minimum) in [69] [105].

For the determinant witness, instead, it was possible to obtain an analytical relation using the assumption of independence and already in [76] that relation is presented. Having an analytical relation extremely simplifies the entropy estimation since is not necessary to perform every time the optimization in order to get the exact value of the entropy that corresponds to the measured witness. Luckily, in an extremely recent article, Li et al [40], discovered such relation also for the CHSH case.

They found that for the 2 → 1 QRAC the maximal $p = max_{a,b,x}\{P(x|a,b)\}$ and the corresponding maximal violation of the witness W_p^{max} are related by:

$$W_p^{max} = \max_r \left\{(2p-1)r^2 + 2\sqrt{(1-p)p}\sqrt{1-r^2}\,r + 2\sqrt{1-r^2} + r\right\} \tag{5.5}$$

where the maximization is done over r which are the real roots of the equation:

$$4\left(2p+4\sqrt{(1-p)p}-1\right)x^3-4\left(2p+2\sqrt{(1-p)p}-1\right)x-(2p-1)^2+4x^4+x^2=0 \tag{5.6}$$

Using the definition of min-entropy we have:

$$p=-2\log_2\left(g(W^{max})\right) \tag{5.7}$$

with $g(W^{max})$ given by the inverse of function 5.5.
This relation has been used for the min-entropy estimation in this thesis.

5.4 Randomness Extraction

In the previous section we have seen how is possible to certify, in a SDI scenario, the minimum randomness produced using only the information retrieved from the data obtained.
However the "true" randomness is mixed with classical noise and inevitable imperfections afflicting the setup, requiring an extra processing of the data before being able to obtain the final true random number.
This operation is called randomness extraction and has been widely used also for non-DI QRNG. In fact, these generators, because of imperfection or because of the way they are implemented, cannot provide an uniform distribution of the output bit, that are characterized by a bias. The random extraction permits to obtain almost-uniformly distributed bits from the input biased random numbers, paying the price of reduction of the total bits. Randomness extractor are used also in the privacy amplification step of QKD, since they can also remove partially correlated side informations from a random source·
So randomness extractor are the right tools to extract the randomness certified by the min-entropy just evaluated, but how do they work?
The most used method for randomness extraction is based on seeded extractor, and in particular on the 2-universal hashing extractors.
A seeded extractors is function that takes a weak binary random source of n bit, X, with min-entropy,$H_{min}(X) = k$ and a short uniform seed S, composed of d bits and produces an output string of l bits which is nearly uniform. The extractor is said to be strong, if the output is approximately independent of the seed[106]. More formally the strong extractor can be defined as a function:

$$\text{Ext}:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^l \tag{5.8}$$

such that $Y=\text{Ext}(X,S)$ is ϵ-close to an uniform distribution:

$$\delta(P_{\text{Ext}(X,S),S},U_l\times U_d)=|P_{\text{Ext}(X,S),S}-U_l\times U_d|\leq\epsilon \tag{5.9}$$

where U_i is the uniform distribution.

The practical realization of seeded extractors can be done in many ways but the most used is surely the one that involves the universal$_2$ hashing functions. An hashing function is a function that maps a n-bit block N into an m-bit block M. The family H of hashing function from N to M is called universal if two input elements are mapped into the same output for no more than $\frac{1}{|M|}$

times. The hashing function have been widely used in many other context before randomness extraction: databases, authentication and crypthography are just few of these fields. The usefulness of the universal hashing function in the context of randomness extraction has been first pointed out by Impagliazzo et al. in 1989 [107] who proved a fundamental result called: Leftover hash lemma. The theorem says that given a n-binary source X and a randomly chosen hash function f coming from a family H of universal hash function, the resulting l-bit string given by $f(X)$ is at most ϵ far from the uniform distribution with ϵ:

$$\epsilon = \frac{1}{2}\sqrt{2^{l-nH_{min}(X)}} \tag{5.10}$$

This means that for every $\epsilon \geq 0$ a function f exists, such that:

$$l = \left(nH_{min}(X) - 2\log\left(\frac{1}{\epsilon}\right)\right) \tag{5.11}$$

and so the f function acts exactly like a random extractor [108].
Since any linear function from $\{0,1\}^n$ to $\{0,1\}^l$ belongs to an universal hashing family [109], these function can be represented with $n \times l$ matrices with binaries entries. Moreover, also binary $n \times l$ Toeplitz matrices form a class of universal hash functions. For these special matrices the number of independent entries is $l + n - 1$, reducing the size of the seed needed. For this reason, Toeplitz matrices are the most used randomness extractor used nowadays. Summing up, the random extraction with these matrices works like this:

- The initial n bit string X is obtained and the min-entropy is calculated $H_{min}(X) = l$
- An $n \times l$ Toeplitz matrix M_S is created using a random seed S of $n + l - 1$ bits
- The extraction is performed performing the vector-matrix multiplication $y = M_S X$
- The output is the l bit extracted random bit string.

Is worth to note that more efficient extractors have been proposed, like the Trevisan extractor [110], but the simplicity and the speed of the Toeplitz matrices makes them still the most common approach.

5.5 Checking randomness

The generated random numbers are also tested, in order to check the quality of the extracted randomness. The check is done by performing a series of test on the random numbers, looking for biasing, correlation and patterns. We decide to use the suite provided by NIST, which is a fairly common solution for the cryptography field. Another, more complete, possibility is given by the DIEHARDER suite, but since it requires at least 10 MB of data, couldn't be used in our case. We must note that this test provides only an indication of the goodness of the random generation but it cannot be considered as a real randomness check. In other words, since the possible patterns and form of correlation in the random sequence are infinite, and since the test executed are finite, if the test are not passed this is clearly an indication that the random source is not good but if the tests are all passed this doesn't mean that the bit sequence is truly random. The NIST

suite performs a series of tests and for every test an hypothesis testing is performed too. Here two hypothesis are considered: H_0, the null hypothesis which is the one under test, and H_1, the alternate hypothesis, mutually exclusive respect H_0. As we saw in Sec 3.2.3, once H_0 and H_1 are selected, a scalar function of the observations, called test statistic t, is chosen and is performed on the data, yielding a value t_m. Then, assuming that H_0 is true, the probability density function (PDF) of t is calculated. The integral on the right (left) side from the mesured point t_m over the PDF for a right (left) one-tailed test is called p-value. The p-value p can be seen as the probability, under the assumption that H_0 is true, to obtain data as extreme as the one observed. The p-value is then compared to the pre-established significance α of the test, the probability of type I errors, so the probability of rejecting H_0 when this is true, and if the p-value is such tat $p < \alpha$, the H_0 is rejected, since there are strong evidences against H_0. The significance α must be chosen in advance, and common values are $0.1, 0.05, 0.001$. In our case the NIST suite uses $\alpha = 0.01$.
However, we must remember that the p-value is a frequentist tool and so it doesn't express a probability statement on the hypothesis, but it's only a tool used in the rejection or the hypothesis.
In the case of the NIST suite, the null hypotesis H_0 states that the observed numbers are random, while the alternative H_1 states that they are not random. The suite performs a total of 15 different categories of tests. For each of these tests, this is performed on m subsamples of the initial random sequence, leading to a p-value. For each one if $p < \alpha$ the test is considered failed, while for $p > \alpha$ is passed. If the proportion of the passed test lies in the region $(1-\alpha) \pm 3\sqrt{\frac{\alpha(1-\alpha)}{m}}$ the test is considered passed.
The second test,instead, relies on the p-values of the p-values (PoP). In fact the p-values are expected to be uniform and so they can be used as a test.
The m p-values are divided in classes of 10, from 0 to 1, and an histogram is built. The PoP is obtained performing a Goodness of Fit (GoF) test using the χ^2:

$$\chi^2 = \sum_{i=1}^{10} \frac{(S_i - \frac{m}{10})^2}{\frac{m}{10}} \tag{5.12}$$

where S_i is the number of p-values in the ith bin.
Given the χ^2 the PoP is computed using:

$$Pop = \tilde{\Gamma}(K, c) \tag{5.13}$$

where $\tilde{\Gamma}(a, b)$ is the incomplete complementary gamma function, $K = \frac{9}{2}$ is half the degrees of freedom, and $c = \frac{\chi^2}{2}$ (the relation is equivalent to the right side integration above defined but is more compact).
The PoP test is conidered passed if it is $PoP > 0.0001$.

5.6 Results

For the random generation the setup is identical to the one described in Section 4.3.3 in the context of SDI-QKD, while the protocol is also similar but with only four preparation states $\{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\}$ and two measurements $\{\frac{\pi}{4}, -\frac{\pi}{4}\}$. As previously described, a $2 \rightarrow 1$ QRAC with qubits is performed and the preparation and measurements states are selected in order to get the maximum violation of the CHSH-like dimension witness, considered in this chapter in the form 4.10.

The results are here presented for the data of the SDI-QKD in Table 5.1. Only the data obtained at $\mu = 0.5$ are used for the NIST's test, since after the extraction, they were the only set with enough bytes.

μ	Dimension witness	H_{min} (per bit)	Raw rate (bps)	Extracted rate (bps)
0.1	5.472 ± 0.013	0.0388379	121	4.326
0.2	5.526 ± 0.009	0.07327371	225.82	16.11
0.5	5.577 ± 0.006	0.127316	481.22	57.74

Table 5.1: *Results of the SDI randomness expansion*

The raw rate and the extracted rate are in this case double respect the SDI-QKD since the state used are the combination of the preparations $\{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\}$ with the two measurements $\{\frac{\pi}{4}, -\frac{\pi}{4}\}$ and $\{\frac{5\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$ with the measurements $\{0, \frac{\pi}{2}\}$. In the SDI-QKD the key-generation was done instead using, the combinations with the same basis for the preparation and the measurement, which are half of the above. Moreover, the rate can be doubled again of a factor two if the quantum communication part is performed with only the states $\{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\}$ and two measurements $\{\frac{\pi}{4}, -\frac{\pi}{4}\}$, instead of the 8 preparations and 4 measurments used for the QKD.

The NIST battery of test is performed first on the raw data and then on the extracted data. The results are presented in Table. 5.2.

	Raw Data		Extracted Data	
Test	PoP	conclusion	PoP	conclusion
Monobit	1.863E-61	Failed	0.428	Passed
Blockfrequency	2.288E-03	Passed	0.466	Passed
Runstest	6.766E-01	Passed	0.606	Passed
Longest run ones	8.062E-03	Passed	0.825	Passed
Binary matrix rank	8.300E-02	Passed	0.740	Passed
Spectraltest	4.360E-01	Passed	0.681	Passed
Non overlapping template matching	1.011E-04	Passed	0.233	Passed
Overlapping template matching	1.849E-02	Passed	0.689	Passed
Maurers universal	4.817E-01	Passed	0.326	Passed
Linear complexity	7.317E-01	Passed	0.378	Passed
Aproximate entropy	7.662E-12	Failed	0.764	Passed
Cumultative sums	4.557E-62	Failed	0.454	Passed
Random excursions	7.984E-01	Passed	0.413	Passed
Random excursions variant	7.933E-01	Passed	0.651	Passed
Cumultative sum reverse	3.846E-62	Failed	0.535	Passed

Table 5.2: *Results of the NIST's battery of tests*

As we could expect, the raw data do not pass all the test provided by the suite, indication that bias and/or correlation are present in the output of the generator. The extracted data instead are able to pass all the test proposed. Again, this result must not be interpreted as a clear statement about the randomness of the source, it only gives us an indication that patterns and correlations tested are not present in the output data.

5.7 Discussion

The results presented, show the feasibility of the random extraction task in a SDI scenario. Extending the results of [41], this implementation shows how, thanks to the great visibilities offered by the plug'n'play setup, is possible to use the CHSH-like dimension witness to certify randomness. Unlike their result, with this witness the assumption of independence of the devices can be abandoned.

However, this implementation still relies on the fair sampling assumption, due to the finite detection efficiency η.

The big problem of this SDI approach is, however, the generation rate. We have seen that the maximum number of bits, is certified by H_{min} that exponentially decreases with the distance from the maximum violation of the DM. This number in our test was in the $[0.03 : 0.127]$. With these low efficiencies the repetition rate must be increased a lot in order to get a reasonable generation rate. In our case the round trip time is 644ns and so the maximum repetition rate is in the order of 1.5MHz. Thus, even upgrading with better detectors against afterpulsing, the rate would increase of one order of magnitude. One solution could be the integration of the system on waveguides, enabling the miniaturization of the system, with benefits on both the rate attainable and on the total stability of the entire system.

Moreover a deeper study on finite size effects and the role of the multiphoton components are needed. Anyhow, this test was intended as a study of feasability, a proof of principle, and the results obtained clearly confirm that SDI-RNG can be a valid alternative for secure random expansion.

CHAPTER 6

Conclusions

6.1 Achievements

In this work we have explored the framework of Semi-Device-Independent quantum protocols for both Quantum Key Distribution and Random Number Expansion. We have carried out a proof-of-principle experiment aimed to test the possibility of the realization of a SDI-QKD system in fiber. To the author's knowledge this is the first real implementation proposed and realized. The experiment has been implemented using a plug'n'play phase encoding configuration in fiber at 1550nm, in order to be compatible with the modern telecommunication standard and technologies. As a part of the preliminary tests, the CHSH-like dimension witness has been tested: the reported violation value is the highest known to the author and the first obtained in fiber for this particular witness. The results showed that, thanks to extreme stability of the plug'n'play configuration, the QKD protocol can effectively realized and the obtained rate are already suitable for a secure communication, even if it's still far from the rates achieved with faster, but less secure, "standard" QKD [111]. The setup was also designed in order to take the data required for the evaluation of a new scheme for SDI-QKD, based on parallel QRACs. This scheme has been proposed in the context of non-classicality test and can be used to abandon the fair sampling assumption from the list of assumption needed from the protocol. Thanks to these data the extension of this idea to the SDI-QKD is under development. The realization of the experiment required working in multiple different context: from quantum optic to fiber optics, from software and FPGA coding to electronics. Especially in the last field, it motivated us to build new ancillary components, like the DAC, that have proven to deliver great performances and will be used in future for other experiments as well.Moreover, we have shown how the same apparatus can be used also for another SDI protocol: randomness expansion. Using the data gathered from the QKD experiment we were able to certify the randomness of the obtained data using only the information extracted from the data. The randomness extraction provided encouraging results, similar to the ones presented in [41], but without the assumption on the Independence of the devices. However, a deeper study on the finite size and multi-photon effects are required. Also in this case this is the first SDI-RNE protocol realized with the CHSH-like dimension witness.

Finally, as a side project, a complete polarization stabilization system has been designed and tested. The stabilization system required the building of an accurate and fast complete Stokes polarimeter, designed with only standard free-space and fiber optic components. Because of the difficulties required for the calibration, a self-testing "reference-free" calibration procedure has been implemented, both on software and in the hardware of the polarimeter, making it able to match the required accuracy. The polarimeter has been interfaced with a commercial polarization controller through an homemade C++ program that controls the stabilization. The results showed an impressive stabilization over a long period of control. Both the software for the control of the polarimeter and for the polarization stabilization have been released as open source.

6.2 Future Upgrades and new perspectives

The setup realized in this thesis is just a proof-of-principle and needs few things to be addressed out for the realization of a complete system. First, the protocol still relies on the fair sampling assumption since the efficiency η of our detectors is below the critical value. This problem can be addressed in two ways: the first requires new detectors with higher perform aces in the 1550 nm band. Recently such detectors have been proposed by various groups and they're believed to achieve η up to 95% with a bandwidth in the GHz range [98]. The other possibility is to develop new methods, like the parallel QRAC for non classicality tests (Sec 4.1.6), that permits to obtain security without the fair sampling assumption. The second stringent requirement is randomness. In our protocol we used pseudo random number generators to select the preparation and the measurement settings. However, true randomness should be used and for this reason an upgraded version should use some TRNG, that are now commercially available. Moreover the setup under test is only few meters long. In order to evaluate the real-world performances, and the degradation due to losses, a link of several kilometres between the users should be used. Then, the synchronization and the configuration of the entire system is done using only one FPGA to control everything, in a real implementation, two separate electronics, one for Alice and one for Bob, should be used along with an efficient synchronization system. Finally, two serious attacks must be taken into account: the first the PNS attack, can be neutralized using Decoy states, that are already in plan for the next upgrade, and then the Trojan Horse, that can be solved using specific attenuators and detectors on Alice's side or switching to a one-way configuration. This one-way configuration could also improve the maximum repetition rate currently limited by the round trip time of the system.

For what concerns the SDI-RNE, what already said for the fair sampling assumption remains valid also in this case. A more profound study on the finite size effects and on the effects of a multi-photon components should be carried out. Moreover the total performances can be drastically increased switching to a system-on-a-chip configuration on waveguides, maybe at different wavelengths.

We want to stress that this is a preliminary study on the possibilities offered by SDI protocols. The major part of the few papers written on SDI have been published in this year, meaning that this approach is quite new but at the same time the interest on this argument is growing rapidly. Moreover dimension witness and QRACs are turning out to be excellent tool to exploit the properties of single qudits, that can be used to enhance performances in communicational or computational tasks.

Appendices

APPENDIX A

Jones Matrix Tables

Below are listed the trasformation between the principal states of polarization attainable with Half wave plates and Quarter wave plates

Input State	Output	States			
HWP angle →	0	$\frac{\pi}{8}$	$\frac{\pi}{4}$	$\frac{3\pi}{8}$	$\frac{\pi}{2}$
$\vert H\rangle$	$\vert H\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert -\rangle$	$\vert H\rangle$
$\vert V\rangle$	$\vert V\rangle$	$\vert -\rangle$	$\vert H\rangle$	$\vert +\rangle$	$\vert V\rangle$
$\vert +\rangle$	$\vert -\rangle$	$\vert H\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert -\rangle$
$\vert -\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert -\rangle$	$\vert H\rangle$	$\vert +\rangle$
$\vert L\rangle$	$\vert R\rangle$	$\vert R\rangle$	$\vert R\rangle$	$\vert R\rangle$	$\vert R\rangle$
$\vert R\rangle$	$\vert L\rangle$	$\vert L\rangle$	$\vert L\rangle$	$\vert L\rangle$	$\vert L\rangle$

Input State	Output	States			
QWP angle →	0	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{3\pi}{4}$	π
$\vert H\rangle$	$\vert H\rangle$	$\vert L\rangle$	$\vert H\rangle$	$\vert R\rangle$	$\vert H\rangle$
$\vert V\rangle$	$\vert V\rangle$	$\vert R\rangle$	$\vert V\rangle$	$\vert L\rangle$	$\vert V\rangle$
$\vert +\rangle$	$\vert R\rangle$	$\vert +\rangle$	$\vert L\rangle$	$\vert +\rangle$	$\vert R\rangle$
$\vert -\rangle$	$\vert L\rangle$	$\vert -\rangle$	$\vert R\rangle$	$\vert -\rangle$	$\vert L\rangle$
$\vert L\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert -\rangle$	$\vert H\rangle$	$\vert +\rangle$
$\vert R\rangle$	$\vert -\rangle$	$\vert H\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert -\rangle$

APPENDIX B

Polarimeter calibration

SOP Reference	SOP Polarimeter	Distance	SOP Reference	SOP Polarimeter	Distance
$\begin{pmatrix} 0.002 \\ 0.001 \\ 0.992 \end{pmatrix}$	$\begin{pmatrix} -0.003 \\ -0.003 \\ 1.001 \end{pmatrix}$	0.010	$\begin{pmatrix} 0.598 \\ -0.496 \\ -0.624 \end{pmatrix}$	$\begin{pmatrix} 0.655 \\ -0.494 \\ -0.647 \end{pmatrix}$	0.061
$\begin{pmatrix} 0.861 \\ 0.145 \\ 0.490 \end{pmatrix}$	$\begin{pmatrix} 0.870 \\ 0.131 \\ 0.481 \end{pmatrix}$	0.019	$\begin{pmatrix} 0.695 \\ -0.718 \\ -0.001 \end{pmatrix}$	$\begin{pmatrix} 0.769 \\ -0.671 \\ -0.031 \end{pmatrix}$	0.092
$\begin{pmatrix} 0.959 \\ 0.269 \\ 0.012 \end{pmatrix}$	$\begin{pmatrix} 0.954 \\ 0.213 \\ -0.002 \end{pmatrix}$	0.058	$\begin{pmatrix} -1.000 \\ 0.000 \\ 0.001 \end{pmatrix}$	$\begin{pmatrix} -1.001 \\ -0.001 \\ 0.000 \end{pmatrix}$	0.002
$\begin{pmatrix} 1.000 \\ 0.000 \\ 0.000 \end{pmatrix}$	$\begin{pmatrix} 0.998 \\ -0.007 \\ -0.001 \end{pmatrix}$	0.008	$\begin{pmatrix} 0.000 \\ 1.000 \\ 0.000 \end{pmatrix}$	$\begin{pmatrix} 0.000 \\ 1.000 \\ 0.000 \end{pmatrix}$	0.001
$\begin{pmatrix} 0.000 \\ -1.000 \\ 0.000 \end{pmatrix}$	$\begin{pmatrix} 0.005 \\ -0.993 \\ 0.000 \end{pmatrix}$	0.008	$\begin{pmatrix} 0.810 \\ 0.550 \\ 0.198 \end{pmatrix}$	$\begin{pmatrix} 0.797 \\ 0.502 \\ 0.200 \end{pmatrix}$	0.049
$\begin{pmatrix} -0.658 \\ 0.547 \\ 0.501 \end{pmatrix}$	$\begin{pmatrix} -0.697 \\ 0.502 \\ 0.524 \end{pmatrix}$	0.064	$\begin{pmatrix} 0.008 \\ 0.350 \\ 0.933 \end{pmatrix}$	$\begin{pmatrix} 0.018 \\ 0.342 \\ 0.947 \end{pmatrix}$	0.020
$\begin{pmatrix} 0.826 \\ 0.384 \\ -0.395 \end{pmatrix}$	$\begin{pmatrix} 0.830 \\ 0.347 \\ -0.404 \end{pmatrix}$	0.038	$\begin{pmatrix} -0.619 \\ -0.786 \\ -0.042 \end{pmatrix}$	$\begin{pmatrix} -0.583 \\ -0.782 \\ -0.043 \end{pmatrix}$	0.036
$\begin{pmatrix} 0.322 \\ 0.896 \\ -0.293 \end{pmatrix}$	$\begin{pmatrix} 0.304 \\ 0.846 \\ -0.302 \end{pmatrix}$	0.054	$\begin{pmatrix} 0.963 \\ -0.210 \\ -0.138 \end{pmatrix}$	$\begin{pmatrix} 0.967 \\ -0.218 \\ -0.142 \end{pmatrix}$	0.010

$\begin{pmatrix} 0.997 \\ 0.026 \\ -0.008 \end{pmatrix}$	$\begin{pmatrix} 0.998 \\ 0.009 \\ -0.011 \end{pmatrix}$	0.017	$\begin{pmatrix} 0.138 \\ 0.841 \\ -0.520 \end{pmatrix}$	$\begin{pmatrix} 0.146 \\ 0.834 \\ -0.549 \end{pmatrix}$	0.030
$\begin{pmatrix} 0.364 \\ -0.777 \\ -0.507 \end{pmatrix}$	$\begin{pmatrix} 0.385 \\ -0.776 \\ -0.505 \end{pmatrix}$	0.021	$\begin{pmatrix} -0.463 \\ 0.236 \\ -0.865 \end{pmatrix}$	$\begin{pmatrix} -0.479 \\ 0.231 \\ -0.878 \end{pmatrix}$	0.021
$\begin{pmatrix} -0.875 \\ 0.384 \\ -0.311 \end{pmatrix}$	$\begin{pmatrix} -0.899 \\ 0.373 \\ -0.318 \end{pmatrix}$	0.027	$\begin{pmatrix} 0.522 \\ 0.042 \\ -0.842 \end{pmatrix}$	$\begin{pmatrix} 0.527 \\ 0.047 \\ -0.825 \end{pmatrix}$	0.018
$\begin{pmatrix} 0.456 \\ 0.856 \\ -0.233 \end{pmatrix}$	$\begin{pmatrix} 0.449 \\ 0.868 \\ -0.214 \end{pmatrix}$	0.024	$\begin{pmatrix} -0.898 \\ 0.149 \\ 0.397 \end{pmatrix}$	$\begin{pmatrix} -0.879 \\ 0.097 \\ 0.371 \end{pmatrix}$	0.061
$\begin{pmatrix} 0.071 \\ -0.116 \\ 0.991 \end{pmatrix}$	$\begin{pmatrix} 0.124 \\ -0.172 \\ 0.929 \end{pmatrix}$	0.099	$\begin{pmatrix} -0.519 \\ -0.421 \\ 0.733 \end{pmatrix}$	$\begin{pmatrix} -0.530 \\ -0.386 \\ 0.764 \end{pmatrix}$	0.048
$\begin{pmatrix} -0.944 \\ -0.210 \\ 0.238 \end{pmatrix}$	$\begin{pmatrix} -0.967 \\ -0.188 \\ 0.276 \end{pmatrix}$	0.050	$\begin{pmatrix} -0.301 \\ 0.080 \\ 0.944 \end{pmatrix}$	$\begin{pmatrix} -0.287 \\ 0.069 \\ 0.956 \end{pmatrix}$	0.021

Table B.1: *"Measurment of the fidelity of the calibration for the polarimeter*

Bibliography

[1] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: 299 (Oct. 1982), p. 802. DOI: 10.1038/299802a0 (cit. on p. 5).

[2] V. Bu žek and M. Hillery. “Quantum copying: Beyond the no-cloning theorem”. In: *Phys. Rev. A* 54 (3 Sept. 1996), pp. 1844–1852. DOI: 10.1103/PhysRevA.54.1844 (cit. on p. 5).

[3] A. Einstein, B. Podolsky, and N. Rosen. “Can Quantum-Mechanical Description of Reality Be Considered Complete?” In: *Physical Review* 47 (1935), pp. 2–5. ISSN: 0031-899X. DOI: 10.1103/PhysRev.48.696 (cit. on p. 6).

[4] John S. Bell. “On the Einstein Podolsky Rosen Paradox”. In: *Physics* 1.3 (1964), pp. 195–200. ISSN: 01923188. DOI: 10.1002/prop.19800281202. arXiv: 1409.4807 (cit. on p. 6).

[5] S. J. Freedman and J. F. Clauser. “Experimental Test of Local Hidden-Variable Theories”. In: *Physical Review Letters* 28 (Apr. 1972), pp. 938–941. DOI: 10.1103/PhysRevLett.28.938 (cit. on p. 6).

[6] A. Aspect, P. Grangier, and G. Roger. “Experimental Tests of Realistic Local Theories via Bell’s Theorem”. In: *Physical Review Letters* 47 (Aug. 1981), pp. 460–463. DOI: 10.1103/PhysRevLett.47.460 (cit. on p. 6).

[7] A. Aspect, J. Dalibard, and G. Roger. “Experimental Test of Bell’s Inequalities Using Time-Varying Analyzers”. In: *Physical Review Letters* 49 (Dec. 1982), pp. 1804–1807. DOI: 10.1103/PhysRevLett.49.1804 (cit. on p. 6).

[8] B. Hensen et al. “Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km”. In: *ArXiv e-prints* (Aug. 2015). arXiv: 1508.05949 [quant-ph] (cit. on pp. 6, 24).

[9] M. Giustina et al. “A significant-loophole-free test of Bell’s theorem with entangled photons”. In: *ArXiv e-prints* (Nov. 2015). arXiv: 1511.03190 [quant-ph] (cit. on pp. 6, 24).

[10] L. K. Shalm et al. “A strong loophole-free test of local realism”. In: *ArXiv e-prints* (Nov. 2015). arXiv: 1511.03189 [quant-ph] (cit. on pp. 6, 24).

[11] John F. Clauser and Michael a Horne. "Experimental consequences of objective local theories". In: *Physical Review D* 10.2 (1974), pp. 526–535. ISSN: 05562821. DOI: 10.1103/PhysRevD.10.526 (cit. on p. 6).

[12] B.S. Cirel'son. "Quantum generalizations of Bell's inequality". English. In: *Letters in Mathematical Physics* 4.2 (1980), pp. 93–100. ISSN: 0377-9017. DOI: 10.1007/BF00417500 (cit. on p. 9).

[13] Christopher Gerry and Peter Knight. *Introductory quantum optics*. Cambridge university press, 2005 (cit. on p. 10).

[14] C. K. Hong, Z. Y. Ou, and L. Mandel. "Measurement of subpicosecond time intervals between two photons by interference". In: *Physical Review Letters* 59 (Nov. 1987), pp. 2044–2046. DOI: 10.1103/PhysRevLett.59.2044 (cit. on p. 13).

[15] SV Kartalopoulos. "A primer on cryptography in communications". In: *IEEE Communications Magazine* 44.4 (2006), pp. 146–151. ISSN: 0163-6804. DOI: 10.1109/MCOM.2006.1632662 (cit. on p. 14).

[16] Stephen Checkoway et al. "On the practical exploitability of Dual EC in TLS implementations". In: *USENIX Security*. Vol. 1. 2014 (cit. on p. 14).

[17] Claude E Shannon. "Communication Theory of Secrecy Systems". In: *Bell System Technical Journal* 28.4 (1949), pp. 656–715. ISSN: 07246811. DOI: 10.1002/j.1538-7305.1949.tb00928.x (cit. on p. 15).

[18] Whitfield Diffie and Martin E. Hellman. "Multiuser Cryptographic Techniques". In: *Proceedings of the June 7-10, 1976, National Computer Conference and Exposition*. AFIPS '76. New York, New York: ACM, 1976, pp. 109–112. DOI: 10.1145/1499799.1499815 (cit. on p. 16).

[19] R. L. Rivest, a. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126. ISSN: 00010782. DOI: 10.1145/359340.359342 (cit. on p. 16).

[20] Thorsten Kleinjung et al. *Factorization of a 768-bit RSA modulus*. Cryptology ePrint Archive, Report 2010/006. http://eprint.iacr.org/. 2010 (cit. on p. 18).

[21] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Scientific and Statistical Computing* 26 (1995), p. 1484. ISSN: 0097-5397. DOI: 10.1137/S0097539795293172. arXiv: 9508027 [quant-ph] (cit. on p. 18).

[22] Stephen Wiesner. *Conjugate coding*. 1983. DOI: 10.1145/1008908.1008920. arXiv: arXiv:1011.1669v3 (cit. on p. 18).

[23] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560, Part 1 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}, pp. 7–11. ISSN: 0304-3975. DOI: http://dx.doi.org/10.1016/j.tcs.2014.05.025 (cit. on p. 18).

[24] A. K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical Review Letters* 67 (Aug. 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661 (cit. on pp. 18, 23).

[25] N Gisin et al. “Quantum cryptography”. In: *Reviews Of Modern Physics* 74.1 (2002), pp. 145–195. ISSN: 0034-6861. DOI: 10.1103/RevModPhys.74.145 (cit. on p. 19).

[26] Peter W. Shor and John Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. In: *Physical Review Letters* 85.2 (2000), pp. 441–444. ISSN: 00319007. DOI: 10.1103/PhysRevLett.85.441. arXiv: 0003004 [quant-ph] (cit. on pp. 20–22).

[27] Antonio Acin, Nicolas Gisin, and Lluis Masanes. “From Bell’s theorem to secure quantum key distribution”. In: *Physical Review Letters* 97.12 (2006), pp. 1–4. ISSN: 00319007. DOI: 10.1103/PhysRevLett.97.120405. arXiv: 0510094 [quant-ph] (cit. on p. 22).

[28] H -K. Lo, X Ma, and K Chen. “Decoy state quantum key distribution”. In: *Physical Review Letters* 94.23 (2005), p. 230504. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.94.230504. arXiv: 0411004 [quant-ph] (cit. on p. 22).

[29] N. Gisin et al. “Trojan-horse attacks on quantum-key-distribution systems”. In: *Physical Review A* 73.2 (2006), p. 022320. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.73.022320. arXiv: 0507063 [quant-ph] (cit. on p. 22).

[30] Lars Lydersen et al. “Hacking commercial quantum cryptography systems by tailored bright illumination”. In: *Nature Photon* 4.686 (2010), p. 5. ISSN: 1749-4885. DOI: 10.1038/NPHOTON.2010.214. arXiv: 1008.4593 (cit. on p. 22).

[31] Erik Woodhead and Stefano Pironio. “Effects of preparation and measurement misalignments on the security of the Bennett-Brassard 1984 quantum-key-distribution protocol”. In: *Physical Review A - Atomic, Molecular, and Optical Physics* 87.3 (2013), pp. 1–7. ISSN: 10502947. DOI: 10.1103/PhysRevA.87.032315. arXiv: 1209.6479 (cit. on p. 22).

[32] Dominic Mayers and Andrew Chi-chih Yao. “Quantum cryptography with imperfect apparatus”. In: *Proc. IEEE Symp. on Found. of Comp. Sc.* 1998, pp. 503–509. ISBN: 0-8186-9172-7. DOI: 10.1109/SFCS.1998.743501. arXiv: 9809039 [quant-ph] (cit. on p. 23).

[33] Umesh Vazirani and Thomas Vidick. “Fully Device-Independent Quantum Key Distribution”. In: *PRL* 140501.October (2014), pp. 1–6. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.113.140501. arXiv: 1210.1810 (cit. on pp. 23, 24).

[34] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement device independent quantum key distribution”. In: *Physical Review Letters* 108.13 (2012), pp. 1–5. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.108.130503. arXiv: arXiv:1109.1473v2 (cit. on p. 25).

[35] Yang Liu et al. “Experimental measurement-device-independent quantum key distribution”. In: *Physical review letters* 111.13 (2013), p. 130502 (cit. on p. 25).

[36] T Ferreira da Silva et al. “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits”. In: *Physical Review A* 88.5 (2013), p. 052303 (cit. on p. 25).

[37] Zhiyuan Tang et al. “Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution”. In: *Physical review letters* 112.19 (2014), p. 190503 (cit. on pp. 25, 26).

[38] Yan-Lin Tang et al. “Measurement-device-independent quantum key distribution over 200 km”. In: *Physical review letters* 113.19 (2014), p. 190501 (cit. on pp. 25, 26, 83).

[39] Marcin Pawłowski and Nicolas Brunner. “Semi-device-independent security of one-way quantum key distribution”. In: *Physical Review A* 84.1 (July 2011), p. 010302. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.84.010302. arXiv: 1103.4105 (cit. on pp. 26, 57, 61).

[40] Dan-Dan Li et al. “Security of Semi-Device-Independent Random Number Expansion Protocols”. In: *Scientific Reports* 5 (2015), p. 15543. ISSN: 2045-2322. DOI: 10.1038/srep15543 (cit. on pp. 26, 61, 88).

[41] T. Lunghi et al. “Self-Testing Quantum Random Number Generator”. In: *Physical Review Letters* 114.15 (2015), p. 150501. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.114.150501. arXiv: 1410.2790 (cit. on pp. 26, 59, 81, 86, 88, 93, 94).

[42] R. C. Jones. “A New Calculus for the Treatment of Optical Systems”. In: *J. Opt. Soc. Am.* 31.7 (July 1941), pp. 488–493. DOI: 10.1364/JOSA.31.000488 (cit. on p. 30).

[43] Joseph W Goodman. “Statistical optics”. In: *New York, Wiley-Interscience, 1985, 567 p.* 1 (1985) (cit. on p. 33).

[44] G.G. Stokes. *On the Composition and Resolution of Streams of Polarized Light from Different Sources.* Proceedings of the Cambridge Philosophical Society : Mathematical and physical sciences. Cambridge Philosophical Society, 1852 (cit. on p. 34).

[45] H. G. Jerrard. “Transmission of Light through Birefringent and Optically Active Media: the Poincaré Sphere”. In: *J. Opt. Soc. Am.* 44.8 (Aug. 1954), pp. 634–640. DOI: 10.1364/JOSA.44.000634 (cit. on p. 35).

[46] H. G. Berry, G. Gabrielse, and A. E. Livingston. “Measurement of the Stokes parameters of light”. In: *Appl. Opt.* 16.12 (Dec. 1977), pp. 3200–3205. DOI: 10.1364/AO.16.003200 (cit. on p. 36).

[47] E. Collett. “Determination of the ellipsometric characteristics of optical surfaces using nanosecond laser pulses”. In: *Surface Science* 96 (June 1980), pp. 156–167. DOI: 10.1016/0039-6028(80)90300-3 (cit. on p. 36).

[48] J. Larry Pezzaniti and Russell A. Chipman. “Mueller matrix imaging polarimetry”. In: *Optical Engineering* 34.6 (1995), pp. 1558–1568. DOI: 10.1117/12.206161 (cit. on p. 37).

[49] R.M.A. Azzam. “Division-of-amplitude Photopolarimeter (DOAP) for the Simultaneous Measurement of All Four Stokes Parameters of Light”. In: *Optica Acta: International Journal of Optics* 29.5 (1982), pp. 685–689. DOI: 10.1080/713820903. eprint: http://dx.doi.org/10.1080/713820903 (cit. on p. 37).

[50] R. M. A. Azzam. “Arrangement of four photodetectors for measuring the state of polarization of light”. In: *Opt. Lett.* 10.7 (July 1985), pp. 309–311. DOI: 10.1364/OL.10.000309 (cit. on p. 37).

[51] R. M. A. Azzam, I. M. Elminyawi, and A. M. El-Saba. “General analysis and optimization of the four-detector photopolarimeter”. In: *J. Opt. Soc. Am. A* 5.5 (May 1988), pp. 681–689. DOI: 10.1364/JOSAA.5.000681 (cit. on pp. 37, 43, 46).

[52] R.B. Walker et al. “Improved FBG Polarimeter Design Evaluated Using VCM Extension to Elliptical Polarization”. In: *Lightwave Technology, Journal of* 28.7 (Apr. 2010), pp. 1032–1041. ISSN: 0733-8724. DOI: 10.1109/JLT.2010.2040138 (cit. on pp. 37, 44, 46).

[53] J. Scott Tyo. “Design of optimal polarimeters: maximization of signal-to-noise ratio and minimization of systematic error”. In: *Appl. Opt.* 41.4 (Feb. 2002), pp. 619–630. DOI: 10.1364/AO.41.000619 (cit. on p. 37).

[54] Y. Cui and R. M. A. Azzam. “Sixteen-beam grating-based division-of-amplitude photopolarimeter”. In: *Opt. Lett.* 21.1 (Jan. 1996), pp. 89–91. DOI: 10.1364/OL.21.000089 (cit. on pp. 37, 46).

[55] Alba Peinado et al. “Optimization and performance criteria of a Stokes polarimeter based on two variable retarders”. In: *Opt. Express* 18.10 (May 2010), pp. 9815–9830. DOI: 10.1364/OE.18.009815 (cit. on p. 37).

[56] David Lara and Carl Paterson. “Stokes polarimeter optimization in the presence of shot and gaussian noise”. In: *Opt. Express* 17.23 (Nov. 2009), pp. 21240–21249. DOI: 10.1364/OE.17.021240 (cit. on pp. 37, 46, 47).

[57] Texas Instruments. *Designing photodiode amplifier circuits with opa128.* Tech. rep. Jan. 1994 (cit. on p. 40).

[58] Texas Instruments. *OPA 129 datasheet.* Tech. rep. 2007 (cit. on pp. 40, 41).

[59] E. H. Moore. “On the reciprocal of the general algebraic matrix”. In: *Bulletin of the American Mathematical Society* 26 (), pp. 394–395 (cit. on p. 44).

[60] V. Mikhailov, S. Dunn, and P.S. Westbrook. “In-line, high speed fibre polarimeter with large calibration bandwidth and accurate reference-free calibration procedure”. In: *Optical Communication (ECOC), 2010 36th European Conference and Exhibition on.* Sept. 2010, pp. 1–3. DOI: 10.1109/ECOC.2010.5621342 (cit. on pp. 44, 46).

[61] “ROOT Mathematical Libraries: Minuit2 Minuit2 Minimization Package”. In: () (cit. on p. 45).

[62] R. M. A. Azzam. “Division-of-amplitude photopolarimeter based on conical diffraction from a metallic grating”. In: *Appl. Opt.* 31.19 (July 1992), pp. 3574–3576. DOI: 10.1364/AO.31.003574 (cit. on p. 46).

[63] HC Lefevre. “Single-mode fibre fractional wave devices and polarisation controllers”. In: *Electronics Letters* 16.20 (1980), pp. 778–780 (cit. on p. 48).

[64] Erik Woodhead and Stefano Pironio. “Secrecy in Prepare-and-Measure Clauser-Horne-Shimony-Holt Tests with a Qubit Bound”. In: *Phys. Rev. Lett.* 115 (15 Oct. 2015), p. 150501. DOI: 10.1103/PhysRevLett.115.150501 (cit. on pp. 54, 55, 58).

[65] Nicolas Brunner et al. “Testing the dimension of Hilbert spaces”. In: *Physical review letters* 100.21 (2008), p. 210503 (cit. on p. 55).

[66] Rodrigo Gallego et al. “Device-Independent Tests of Classical and Quantum Dimensions”. In: *Phys. Rev. Lett.* 105 (23 Nov. 2010), p. 230501. DOI: 10.1103/PhysRevLett.105.230501 (cit. on p. 55).

[67] Johan Ahrens et al. “Experimental Tests of Classical and Quantum Dimensionality”. In: *Phys. Rev. Lett.* 112 (14 Apr. 2014), p. 140401. DOI: 10.1103/PhysRevLett.112.140401 (cit. on p. 55).

[68] Johan Ahrens et al. "Experimental device-independent tests of classical and quantum dimensions". In: *Nature Physics* 8.8 (2012), pp. 592–595. ISSN: 1745-2473. DOI: 10.1038/nphys2333. arXiv: 1010.5064 (cit. on pp. 55, 81).

[69] Hong-Wei Li et al. "Relationship between semi- and fully-device-independent protocols". In: *Physical Review A* 87.2 (Feb. 2013), p. 020302. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.87.020302. arXiv: 1210.0486 (cit. on pp. 55, 57, 88).

[70] A. Ambainis et al. "Dense Quantum Coding and a Lower Bound for 1-way Quantum Automata". In: *eprint arXiv:quant-ph/9804043* (Apr. 1998). eprint: quant-ph/9804043 (cit. on p. 56).

[71] Charles H. Bennett, Gilles Brassard, and N. David Mermin. "Quantum cryptography without Bell's theorem". In: *Physical Review Letters* 68.5 (1992), pp. 557–559. ISSN: 00319007. DOI: 10.1103/PhysRevLett.68.557 (cit. on p. 57).

[72] Anupam Garg and N. D. Mermin. "Detector inefficiencies in the Einstein-Podolsky-Rosen experiment". In: *Phys. Rev. D* 35 (12 June 1987), pp. 3831–3835. DOI: 10.1103/PhysRevD.35.3831 (cit. on p. 59).

[73] Jan-Åke Larsson. "Bell's inequality and detector inefficiency". In: *Phys. Rev. A* 57 (5 May 1998), pp. 3304–3308. DOI: 10.1103/PhysRevA.57.3304 (cit. on p. 59).

[74] Philippe H. Eberhard. "Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment". In: *Phys. Rev. A* 47 (2 Feb. 1993), R747–R750. DOI: 10.1103/PhysRevA.47.R747 (cit. on p. 59).

[75] Hong-Wei Li et al. "Detection efficiency and noise in a semi-device-independent randomness-extraction protocol". In: *Phys. Rev. A* 91 (3 Mar. 2015), p. 032305. DOI: 10.1103/PhysRevA.91.032305 (cit. on p. 59).

[76] Joseph Bowles, Marco Túlio Quintino, and Nicolas Brunner. "Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices". In: *Phys. Rev. Lett.* 112 (14 Apr. 2014), p. 140407. DOI: 10.1103/PhysRevLett.112.140407 (cit. on pp. 59, 88).

[77] G. Cañas et al. "Experimental quantum randomness generation invulnerable to the detection loophole". In: *ArXiv e-prints* (Oct. 2014). arXiv: 1410.3443 [quant-ph] (cit. on p. 59).

[78] Rodrigo Gallego Lopez and Antonio Acin dal Maschio. "Device-independent information protocols: measuring dimensionality, randomness and nonlocality". In: (2013) (cit. on pp. 59, 81).

[79] A. Hameedi et al. "An unconditional experimental test of Nonclassicality". In: *ArXiv e-prints* (Nov. 2015). arXiv: 1511.06179 [quant-ph] (cit. on p. 60).

[80] I. Csiszar and J. Korner. "Broadcast channels with confidential messages". In: *Information Theory, IEEE Transactions on* 24.3 (May 1978), pp. 339–348. ISSN: 0018-9448. DOI: 10.1109/TIT.1978.1055892 (cit. on p. 61).

[81] Ilja Gerhardt et al. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system." In: *Nature communications* 2.2027 (2011), p. 349. ISSN: 2041-1723. DOI: 10.1038/ncomms1348. arXiv: 1011.0105 (cit. on p. 61).

[82] Anubhav Chaturvedi et al. “Security of QKD protocols against detector blinding attacks”. In: (2015), pp. 1–7. arXiv: 1504.00939 (cit. on p. 62).

[83] Gilles Brassard and Louis Salvail. “Secret-Key Reconciliation by Public Discussion”. English. In: *Advances in Cryptology — EUROCRYPT ’93*. Ed. by Tor Helleseth. Vol. 765. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1994, pp. 410–423. ISBN: 978-3-540-57600-6. DOI: 10.1007/3-540-48285-7_35 (cit. on p. 64).

[84] Norbert Lutkenhaus. “Security against individual attacks for realistic quantum key distribution”. In: *Phys. Rev. A* 61 (5 Apr. 2000), p. 052304. DOI: 10.1103/PhysRevA.61.052304 (cit. on p. 64).

[85] Boris Korzh et al. “Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre”. In: *Nature Photonics* 9.3 (2014), p. 7. ISSN: 1749-4885. DOI: 10.1038/nphoton.2014.327. arXiv: 1407.7427 (cit. on p. 65).

[86] CharlesH. Bennett et al. “Experimental quantum cryptography”. In: *Journal of Cryptology* 5.1 (1992), pp. 3–28. ISSN: 0933-2790. DOI: 10.1007/BF00191318 (cit. on p. 66).

[87] P.D. D Townsend. “Single photon interference in 10 km long optical fibre interferometer - Electronics Letters”. In: *Electronics Letters* 29.7 (1993), p. 634. ISSN: 00135194. DOI: 10.1049/el:19930424 (cit. on pp. 66, 67).

[88] M. Fox. *Quantum Optics : An Introduction: An Introduction*. Oxford Master Series in Physics. OUP Oxford, 2006. ISBN: 9780191524257 (cit. on p. 66).

[89] A. Muller et al. “”Plug and play” systems for quantum cryptography”. In: *Applied Physics Letters* 70.7 (1997), pp. 793–795 (cit. on p. 67).

[90] D Stucki et al. “Quantum key distribution over 67 km with a plug’n’play system”. In: *New Journal of Physics* 4.1 (2002), p. 41 (cit. on p. 67).

[91] Nicolas Gisin et al. “Quantum cryptography”. In: *Rev. Mod. Phys.* 74 (1 Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145 (cit. on p. 68).

[92] Jan Bogdanski, Nima Rafiei, and Mohamed Bourennane. “Experimental quantum secret sharing using telecommunication fiber”. In: *Phys. Rev. A* 78 (6 Dec. 2008), p. 062307. DOI: 10.1103/PhysRevA.78.062307 (cit. on p. 76).

[93] Peter Alfke. *Efficient Shift Registers, LFSR Counters, and Long PseudoRandom Sequence Generators*. Tech. rep. Xilinx, 1996 (cit. on p. 78).

[94] D. Schellekens, B. Preneel, and I. Verbauwhede. “FPGA Vendor Agnostic True Random Number Generator”. In: *Field Programmable Logic and Applications, 2006. FPL ’06. International Conference on*. Aug. 2006, pp. 1–6. DOI: 10.1109/FPL.2006.311206 (cit. on p. 78).

[95] Gilles Brassard and Louis Salvail. “Secret-key reconciliation by public discussion”. In: *advances in Cryptology—EUROCRYPT’93*. Springer. 1994, pp. 410–423 (cit. on p. 79).

[96] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau. “Practical issues in quantum-key-distribution postprocessing”. In: *Phys. Rev. A* 81 (1 Jan. 2010), p. 012318. DOI: 10.1103/PhysRevA.81.012318 (cit. on p. 79).

[97] V. Scarani et al. "The security of practical quantum key distribution". In: *Reviews of Modern Physics* 81 (July 2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. arXiv: 0802.4155 [quant-ph] (cit. on p. 83).

[98] Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. "Counting near-infrared single-photons with 95% efficiency". In: *Opt. Express* 16.5 (Mar. 2008), pp. 3032–3040. DOI: 10.1364/OE.16.003032 (cit. on pp. 83, 95).

[99] Christian Gabriel et al. "A generator for unique quantum random numbers based on vacuum states". In: *Nature Photonics* 4.10 (2010), pp. 711–715. ISSN: 1749-4885. DOI: 10.1038/nphoton.2010.197 (cit. on p. 85).

[100] Roger Colbeck and Adrian Kent. "Private randomness expansion with untrusted devices". In: *Journal of Physics A: Mathematical and Theoretical* 44.9 (2011), p. 095305 (cit. on p. 85).

[101] S Pironio et al. "Random numbers certified by Bell's theorem." In: *Nature* 464.7291 (2010), pp. 1021–1024. ISSN: 0028-0836. DOI: 10.1038/nature09008. arXiv: 0911.3427 (cit. on pp. 85, 86).

[102] Hong-Wei Li et al. "Semi-device-independent random-number expansion without entanglement". In: *Physical Review A* 84.3 (2011), p. 034301. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.84.034301. arXiv: 1108.1480 (cit. on pp. 86–88).

[103] Hong-Wei Li et al. "Semi-device independent random number expansion protocol with n to 1 quantum random access codes". In: *Physical Review A* 85 (2012), p. 052308. arXiv: 1109.5259 (cit. on p. 87).

[104] Joseph Bowles, Marco Túlio Quintino, and Nicolas Brunner. "Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices". In: *Phys. Rev. Lett.* 112 (14 Apr. 2014), p. 140407. DOI: 10.1103/PhysRevLett.112.140407 (cit. on p. 87).

[105] Piotr Mironowicz, Hong-Wei Li, and Marcin Pawłowski. "Properties of dimension witnesses and their semidefinite programming relaxations". In: *Physical Review A* 90.2 (2014), p. 022322. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.90.022322. arXiv: 1405.3971 (cit. on p. 88).

[106] Anindya De et al. "Trevisan's extractor in the presence of quantum side information". In: *Siam Journal of Computing* 41.4 (2012), pp. 915–940. ISSN: 0097-5397. DOI: 10.1137/100813683. arXiv: 0912.5514 (cit. on p. 89).

[107] Russell Impagliazzo, Leonid a Levint, and Michael Luby. "Pseudo-random generation from one-way functions (Extended Abstract)". In: *STOC '89 Proceedings of the twenty-first annual ACM symposium on Theory of computing* (1989), pp. 12–24. DOI: 10.1145/73007.73009 (cit. on p. 90).

[108] Marco Tomamichel et al. "Leftover hashing against quantum side information". In: *IEEE Transactions on Information Theory* 57.8 (2011), pp. 5524–5535. ISSN: 0018-9448. DOI: 10.1109/TIT.2011.2158473. arXiv: 1002.2436 (cit. on p. 90).

[109] Lawrence J Carter and Mark N Wegman. "Universal classes of hash functions". In: *Annual ACM Symposium on Theory of Computing.* 1977, pp. 106–112. ISBN: 0022-0000. DOI: 10.1145/800105.803400 (cit. on p. 90).

[110] Luca Trevisan. “Extractors and pseudorandom generators”. In: *Journal of the ACM* 48.4 (2001), pp. 860–879. ISSN: 00045411. DOI: 10.1145/502090.502099 (cit. on p. 90).

[111] D. Lancho et al. “QKD in Standard Optical Telecommunications Networks”. In: 19.11 (2010). DOI: 10.1007/978-3-642-11731-2{_}18. arXiv: 1006.1858 (cit. on p. 94).