1222·2022 800 ANNI

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

MiME

Master's degree ICT Internet Multimedia Engineering

ICT for Internet and Multimedia - Photonics

Study for a Cross-Encoded Reference-Frame-Independent Quantum Key Distribution protocol

Supervisor:
Prof. Giuseppe Vallone

Co-supervisor:
PhD Costantino Agnesi

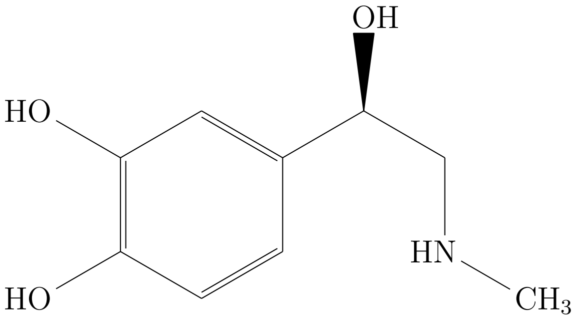
Author: Massimo Giacomin

Matricola N°: 1242797

Academic Year: 2021/2022

"Numquam ponenda est pluralitas sine necessitate" - William of Ockham

"Science cannot solve the ultimate mystery of nature.
And that is because, in the last analysis, we ourselves are part of nature
and therefore part of the mystery that we are trying to solve." - Max Planck



Abstract

Quantum Key Distribution is probably the most advanced application of Quantum Mechanics that finds concrete implementation in the real world. The enormous success reached in these few decades is to be attributed to its strong reliability, based on the theoretical assumption that it can, in principle, guarantee unconditional security.

Nowadays, several different strategies are studied and exploited in order to efficiently encode quantum information, obviously each one carrying its own advantages and drawbacks. However, the protocol investigated in this work can be defined as *cross-encoded*, since it hernesses two transitions, from *polarization* to *time-bin*, returning again to polarization. By means of this choice the advantages of both the encoding techniques can be achieved, extremely useful in hybrid networks, when both optical fibers and free-space links are implemented.

The most relevant aspect of the protocol here analyzed relies on its being *reference-frame-independent*, meaning that the requirement of a shared reference-frame that constantly adjust itself to properly measure the received states is no longer needed. This reduces the experimental difficulties introduced by performing active control for the alignment of the measurement basis.

This relaxation in terms of active control in the receiver apparatus is however compensated by the requirement of four single photo-detectors, one for each cardinal state in the equator of the Bloch sphere. Thus, the setup so implemented allows to retrieve an accurate description of the states collected by the receiver, as they appear in the equatorial plane identified by the measurement basis.

The final result is a robust three-state protocol, with no requirements in terms of calibration of the reference-frame, capable of achieving comparable results in terms of security with respect to more complex architectures.

Italian translation:

La distribuzione di chiave quantistica è probabilmente l'applicazione più avanzata della Meccanica Quantistica, che trova implementazioni concrete nel mondo reale. L'enorme successo acquisito in questi ultimi decenni è da attribuirsi alla solida affidabilità che essa è in grado di garantire, basandosi sui postulati teorici che ne garantiscono sicurezza incondizionata.

Al giorno d'oggi differenti strategie sono studiate e impiegate al fine di codificare in maniera efficace informazione quantistica; ovviamente ogni alternativa è foriera di propri vantaggi e svantaggi. Tuttavia il protocollo investigato in questo elaborato viene definito *a codifica mista*, dal motivo che esso sfrutta contemporaneamente due strategie differenti: la codifica in *polarizzazione* e quella detta in *time-bin*. Attraverso questa scelta sono sfruttati i vantaggi di entrambe le tecniche crittografiche, permettendo l'utilizzo combinato di reti ibride nelle quali sono impiegate sia fibre ottiche che collegamenti in spazio libero.

La caratteristica più importante del protocollo considerato è il suo essere *indipendente da qualsiasi sistema di riferimento*, il che significa che in applicazioni pratiche non è richiesto nessun sistema di controllo atto a correggere istantaneamente il sistema di riferimento sul quale vengono misurati gli stati di polarizzazione. In tal modo è possibile ridurre le limitazioni introdotte da un sistema in retroazione.

Questo rilassamento nel dispositivo ricevitore è tuttavia compensato dall'implementazione di quattro foto-rivelatori a singolo fotone, uno per ogni stato cardinale nell'equatore della Sfera di Bloch. Così facendo, il sistema progettato permette di derivare una descrizione accurata degli stati misurati al ricevitore, poichè essi appaiono nel piano equatoriale sul quale le basi di misura giacciono.

Il risultato finale porta ad un protocollo basato su tre stati quantistici, che non necessita di alcuna calibrazione del sistema di riferimento, capace di garantire risultati simili in termini di sicurezza a ciò che si più ottenere con architetture più complesse.

Contents

1 Introduction 1

2 Mathematical Methods 3

1 Useful Quantum Concepts 4

1 Mixed State Formalism 4

2 The Pauli Matrices 5

3 The Bloch Sphere 5

4 POVM 7

2 The BB84 protocol 7

3 The No-Cloning Theorem 9

4 Reference Frame Independence 10

3 Experimental Setup 17

1 Notions about the hardware 17

1 Passive devices 17

2 Active devices 23

2 Configuration of the experimental setup 28

4 Alice Station 31

1 The Pulsed Laser Source 31

2 iPognac 37

3 Polarization to Time-Bin Converter 43

5 Bob Station 47

1 Time-bin to Polarization Converter 47

2 The Receiver 51
1 Layout 52
2 Characterization 54
3 Computation of the Projectors 55

6 Experimental Tests 59
1 CW laser source 60
2 Pulsed laser source 65

7 Data Analysis 71

8 Conclusions 81

1 Introduction

We are living in a fascinating historical time. Over a period of about a hundred and fifty years the human kind has experienced uncountable technological breakthroughs that have made us get use to them. However this is far from what was usual up to a few generations ago. Until two hundred years ago the idea of future was a concept entirely different from what modern civilization considers today. Science was a speculative art restricted to few social classes. And then something changed.

The invention of the light bulb was just the beginning of an unstoppable process of progresses. After that, the vacuum tube was discovered, that led to the invention of the radiotelegraph and with it telecommunications were born. Scientists not only developed a method to amplify and manipulate signals, but invented a brand new branch of study, that took the name of *Information Technology*. Consequently, concepts as signal, security and intelligence changed their meaning forever.

From this moment on, every effort to improve the performances in the communications has been made.

With the theorization of Quantum Mechanics, that revolutionized the rules of Physics giving a complete new understanding of Nature, new methods of communicating information have been formulated.

In general, every practical example in which Quantum Theory can be implemented is arousing the interests of investors worldwide.

According to *McKinsey* & *Company* [1], European Union has planned about $7.2 billions to invest in Quantum Technologies in the next five years, ten times the amount funded for the same market in 2020. And this is just a mere example of the increasing attractiveness this discipline is gaining in these years.

The field that among all the Quantum Information sciences has found the most promising results is the one of the Quantum Communications, that according to the theoretical framework of Quantum Mechanics is capable to guarantee *unconditional security*. This translates in the possibility of performing a confident exchange of information between two authenticated parties, and it is of paramount interest in all scenarios in which sensible data must be shared privately, as for example involving banking transactions or military communications.

Historically, the first ever protocol that implemented Quantum Key Distribution in a practical manner was presented in 1984 by Charles H. Bennett and Gilles Brassard [2] at the IEEE conference in India. From that time on, countless studies have been published, introducing improvements but also alternatives to this fundamental milestone [3].
This thesis describes one of these many variations, exploiting the advantages of an hybrid encoding to guarantee reliability and ease of implementation.

Chapter 2 aims to review some basic but useful contents of Quantum Information together with the mathematical tools required to treat the core topics. Chapter 3 is dedicated to introduce the framework of the protocol, with particular attention to the experimental setup, both software and hardware, with which the study is carried on. In chapters 4 and 5 the description will focuses on the transmitter and receiver stations, usually defined as *Alice* and *Bob*. Here the photonic source, along with the encoder and the decoder apparati, are explained. Chapter 6 will outline the experimental tests performed in the development of the final configuration, while chapter 7 is reserved to the analysis of the collected data for the estimation of the goodness of the protocol. Finally, in chapter 8 conclusions to the present work find room.

2 Mathematical Methods

As the bit is the fundamental element in classical information, in the Quantum framework this role is interpreted by the *qubit*. Despite these two concepts may appear similar with respect to their semantics, the difference in their physical interpretation is substantial: a bit can assume only a precise value between zero or one. General quantum states, of which a qu-*dit* is a representation, live instead in a linear vector space called *Hilbert space*. Thanks to this formalism, given a d-dimensional space, we can define a pure quantum state in terms of the basis vectors of the space itself, and according to the Dirac's notation it can be written as

$$|\psi\rangle = \sum_{n=0}^{d-1} \psi_n |n\rangle . \tag{2.1}$$

In Eq. (2.1) the coefficients $\psi_n = \langle n|\psi\rangle \in \mathbb{C}$ are defined as complex amplitudes, and according to the Born's rule, the probability to find the system described by $|\psi\rangle$ in the state $|n\rangle$ can be expressed as $p_n = |\langle n|\psi\rangle|^2$. It follows the *normalization* requirement on a generic quantum state, meaning that

$$\sum_{n=0}^{d-1} |\psi_n|^2 = 1 \tag{2.2}$$

Considering a space of dimension $d = 2$, the quantum system describes a qubit and assumes the parametric form

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle . \tag{2.3}$$

The shape shown in Eq. (2.3) introduces one of the most essential aspects of a quantum state, that is *quantum superposition.* A qubit, in principle, can encode simultaneously two states, that are the two basis vectors $|0\rangle$ and $|1\rangle$, and this is the main reason why Quantum

Information is considered to be more powerful with respect to its classical counterpart.

2.1 Useful Quantum Concepts

In this section we report the main concepts of Quantum Mechanics that can help the comprehension of the topics presented in the next chapters, according to what explained mainly in [4], [5] and [6].

2.1.1 Mixed State Formalism

In the treatment of real problems, it is more common to deal with non-isolated systems rather than perfectly isolated ones. In these situations, the state vector $|\psi\rangle$ must be replaced with a *density matrix* $\hat{\rho}$, that has the mathematical shape of an operator. In this case the state describing the system is unknown, and the only possible representation is by means of an ensemble of possibilities $\{|\psi_i\rangle\}_{i=1\ldots N}$ each with a defined probability p_i ($p_i > 0$, $\sum p_i = 1$). Furthermore, the states in the ensemble do not belong to the Hilbert space (in principle $N > d \equiv \dim(\mathcal{H})$) and they do not fulfil the orthogonality condition. The statistical density operator can thus be described as

$$\hat{\rho} = \sum_{n=1}^{N} p_n \left|\psi_n\right\rangle \left\langle\psi_n\right| , \tag{2.4}$$

and presents three fundamental properties that must be always respected. Firstly, each density matrix must be *hermitian*, meaning that $\hat{\rho}^\dagger = (\hat{\rho}^T)^* = \hat{\rho}$. Moreover, a given density matrix must show the following property: $\mathrm{Tr}(\hat{\rho}) = \mathbf{1}$. Lastly, it must be a non-negative operator, meaning that $\langle\psi|\hat{\rho}|\psi\rangle \geq 0 \; \forall \, |\psi\rangle$.

Recalling the algebraic definition of the *projector*, it is described as a linear operator that performs the projection of a generic state in a given basis $|\lambda_n\rangle$, usually expressed in the following form

$$\hat{\Pi}_n = \left|\lambda_n\right\rangle \left\langle\lambda_n\right| , \qquad \text{where} \qquad \hat{\Pi}_n^2 = \hat{\Pi}_n \tag{2.5}$$

Form this definition the concept of *purity* can be introduced. The purity of a state quantifies how far its density operator is from a projector, and is defined as

$$\mu(\hat{\rho}) = \mathrm{Tr}[\hat{\rho}^2]. \tag{2.6}$$

This value ranges in the interval $\frac{1}{d} \leq \mu \leq 1$, where d is the dimension of the Hilbert space. The state with the lowest possible purity $\frac{1}{d}$ is the *maximally mixed state* $\frac{\hat{\mathbb{1}}}{d}$.

2.1.2 The Pauli Matrices

Fundamental objects in the Quantum Mechanics framework, the Pauli matrices are the set of $2x2$ complex Hermitian unitary matrices with the following form:

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.7}$$

$$\hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.8}$$

$$\hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.9}$$

They describe the spin measurement in the $\hat{x}$, $\hat{y}$ and $\hat{z}$ directions respectively.
The corresponding eigenvectors are

— $|0\rangle, |1\rangle$ (alternatively, $|H\rangle, |V\rangle$) for $\hat{\sigma_z}$,

— $|+\rangle, |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ (alternatively, $|D\rangle, |A\rangle$) for $\hat{\sigma_x}$,

— $|+i\rangle, |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm j\,|1\rangle)$ (alternatively, $|L\rangle, |R\rangle$) for $\hat{\sigma_y}$,

with eigenvalues ±1.

2.1.3 The Bloch Sphere

In the *Bloch Sphere* representation (see Fig. 2.1), a qubit density matrix can be parameterized as

$$\hat{\rho} = \frac{1}{2}(\hat{\mathbb{1}} + \vec{\sigma} \cdot \vec{r}) = \frac{1}{2}(\hat{\mathbb{1}} + r_x\hat{\sigma}_x + r_y\hat{\sigma}_y + r_z\hat{\sigma}_z) \tag{2.10}$$

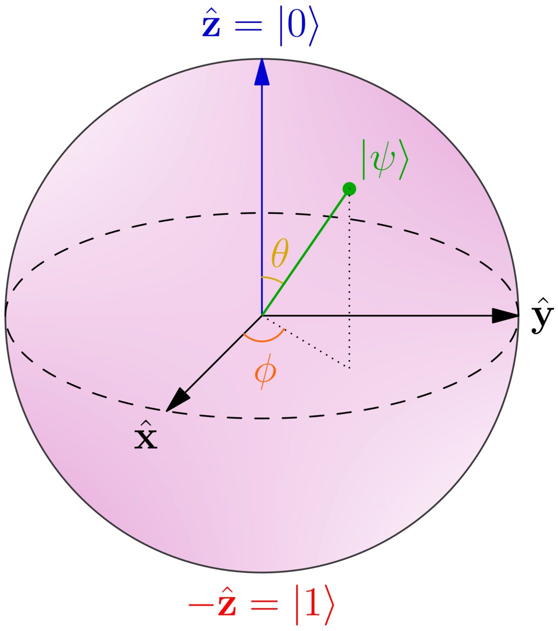


Figure 2.1: Bloch sphere representation of a qubit.

where $r_i \in \mathbb{R}\ \forall i$ are the coordinates of a point within the sphere, which have to satisfy $\|\vec{r}\| \leq 1$, and $\hat{\sigma}_i$ indicate the *Pauli matrices.*

For a pure state in the form expressed in Eq. (2.3), the corresponding $\vec{r}$ is a unit vector with components

$$\vec{r} = \begin{pmatrix} sin\theta cos\phi \\ sin\theta sin\phi \\ cos\theta \end{pmatrix} \tag{2.11}$$

while for a generic mixed state with $\|\vec{r}\| \leq 1$ the components of the vector become

$$\vec{r} = \begin{pmatrix} \mathrm{Tr}[\hat{\rho}\hat{\sigma}_x] \\ \mathrm{Tr}[\hat{\rho}\hat{\sigma}_y] \\ \mathrm{Tr}[\hat{\rho}\hat{\sigma}_z] \end{pmatrix} . \tag{2.12}$$

The maximally mixed state $\hat{\rho} = \frac{\hat{\mathbb{1}}}{2}$ is alternatively defined as *totally depolarized*, and presents $\vec{r} = 0$. Finally, with respect to Fig. 2.1, every equatorial state can be indicated by the equation

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right) \tag{2.13}$$

where the $|0\rangle$ corresponds to the north pole, while $|1\rangle$ represents the south pole.

2.1.4 POVM

In the framework of the *generalized measurement*, a class of measurement processes with an uncertain outcome, the standard formulation asserts that each physical system, which can be associated with an Hilbert space, can be measured by means of a *self-adjoint* operator $\hat{X}$ called *observable*. The eigenstates of this operator, $|x\rangle$, form an orthonormal basis for the Hilber space, where each vector comprising the basis corresponds to each possible outcome of that measurement. Moreover, the Born rule states that the probability that a particular measurement (performed with the observable $\hat{X}$) applied on a state $\hat{\rho}$ leads to specific outcome is computed as

$$p_x = \mathrm{Tr}\left[P_x \hat{\rho}\right]. \tag{2.14}$$

A generalization can be introduced exploiting the concept of *Positive Operetor-Valued Measurement* (POVM). As a matter of fact, POVMs are necessary to describe the effect on a subsystem of a projective measurement performed on a larger system.
POVMs are the most general kind of measurement in quantum mechanics since they are used in every application in which the final state a system ends up in is not relevant, but the only requirement is computing the probability outcome of a single observation.
POVMs are described by set of non-negative operators $\{\hat{F}_n\}_{n=1\ldots M}$, $\hat{F}_n \geq 0$, with the property

$$\sum_{n=1}^{M} \hat{F}_n = \hat{\mathbb{1}} \tag{2.15}$$

Each $\hat{F}_i$ represents a possible outcome of a measure with associated probability given by its expectation value $p_n = \mathrm{Tr}\left[\hat{F}_n \hat{\rho}\right]$[1].

2.2 The BB84 protocol

According to what reported by Simon Singh in [7], the story of the birth of quantum cryptography dates back to the idea of "Quantum Money" proposed by Stephen Weisner in the late 1960s. His idea of creating dollar bills with polarization of photons in order not

[1] In the case of a state vector $|\psi\rangle$ the probability of obtaining the output i is given by $p_i = \langle\psi| \hat{F}_i |\psi\rangle$.

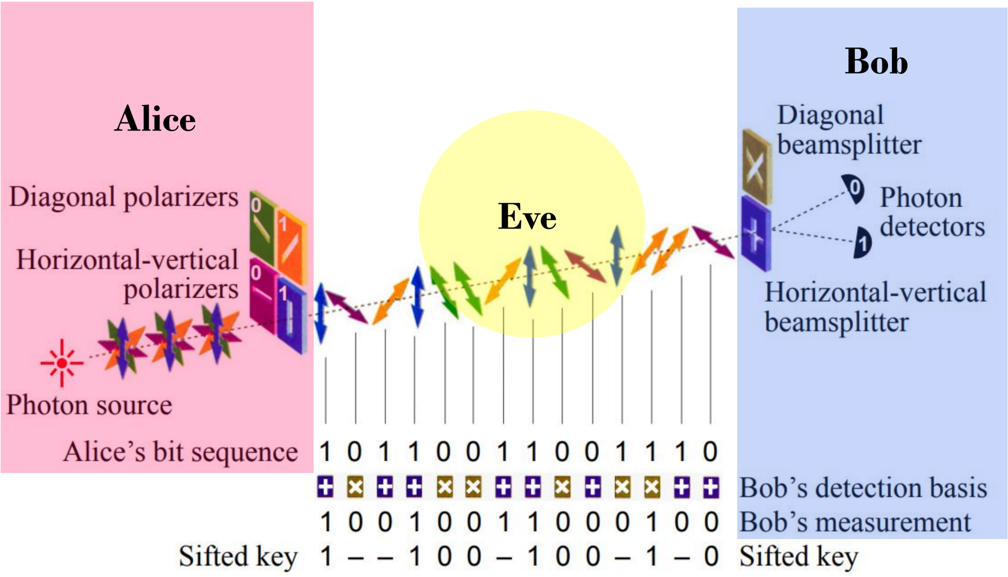

Alice
Diagonal polarizers
Horizontal-vertical polarizers
Photon source
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
⊞ ⊠ ⊞ ⊞ ⊠ ⊠ ⊞ ⊞ ⊠ ⊞ ⊠ ⊠ ⊞ ⊞ Bob's detection basis
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's measurement
Sifted key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted key
Eve
Bob
Diagonal beamsplitter
Photon detectors
Horizontal-vertical beamsplitter
0
1

Figure 2.2: Scheme of the BB84 protocol for QKD implemented with polarization encoding (https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography/).

to be corrupted was the first attempt to exploit two non commuting operators to obtain information that cannot be duplicated.

Despite the brilliant intuition, Weisner's idea was rejected by the scientific community.

It was only thanks to the Bennet and Bassard that this intuition come to life, in the framework of the BB84 protocol.

The idea is simple but deep and is schematized in Fig. 2.2. The sender, called Alice for simplicity, selects a string of random bits and encode each of them randomly in the eigenstates of the Pauli matrices $\hat{\sigma}_z$ and $\hat{\sigma}_x$, reported here for completeness:

$$\hat{Z}\text{ basis}:\begin{cases}|0\rangle\\ |1\rangle\end{cases}\qquad\qquad \hat{X}\text{ basis}:\begin{cases}|+\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\\ |-\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\end{cases}\tag{2.16}$$

Alice encodes zeroes half of the time into $|0\rangle$ and half into $|+\rangle$, and the same happens for ones, distributed between $|1\rangle$ and $|-\rangle$.

The receiver, Bob, collects the stream of qubits and since he does not know the basis used by Alice for the encoding of each state, he perform random measurements, choosing either $\hat{Z}$ or $\hat{X}$ basis with equal probability for each decoding.

The final result is a choice of the same basis between Alice and Bob in approximately one

half of the measurements, always retrieving the correct result by the two parties. On the contrary, when Bob measures in the wrong basis, he will obtain the right result one half of the time.
At the end Bob performed wrong measurements with probability of 25%.

After the exchange of the choice of the encoding bases (from Alice) and measurement bases (from Bob) through a classical authenticated channel (see below), the two discard the bits belonging to different choices, while keeping the bits with total correlation.

Considering a noiseless channel and the absence of external eavesdroppers, this protocol claims to guarantee unconditional security. This assumption is theoretically true, provided that the following conditions are satisfied:

— the acquisition of information from an external eavesdropper is only possible at the expense of disturbing the transmitted signal (*"No-Cloning Theorem"*),

— the existence of an authenticated public classical channel.

2.3 The No-Cloning Theorem

The No-Cloning Theorem states that it is impossible to create a perfect copy of an unknown quantum state, and can be proven easily.
Supposing to have a quantum cloning machine in order to clone the state $|\psi\rangle$, this machine would work as follows:

$$|\psi\rangle \otimes |a\rangle \implies \mathcal{U}_c\left(|\psi\rangle \otimes |a\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{2.17}$$

where $|a\rangle$ is an ancillary state and $\mathcal{U}_c$ is a proper unitary transformation.
Wanting now to clone a different state $|\phi\rangle$, the result exiting the machine would be

$$|\phi\rangle \otimes |a\rangle \implies \mathcal{U}_c\left(|\phi\rangle \otimes |a\rangle\right) = |\phi\rangle \otimes |\phi\rangle\,. \tag{2.18}$$

Applying now the inner product between Eq. (2.17) and Eq. (2.18), the result is

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2 \tag{2.19}$$

which admits two possible solutions: the two states are either equal or orthogonal to each other. According to this result, a cloning machine can only clone states that are mutually orthogonal, and therefore it is not able to generate to identical copies.
It can be shown that similar conclusions hold also for mixed states.

2.4 Reference Frame Independence

The final goal of this entire research is to develop an apparatus capable of performing Quantum Key Distribution, exploiting a hybrid encoding strategy in order to implement the formalism of Reference Frame Independence. With this terminology the Telecommunications scientists mean to describe a system that does not rely on the need to possess a shared reference frame between the authorized users. According to [8] this condition can be guaranteed by means of the alignment of the the polarization states in the case of polarization encoding, and the interferometric stability for phase encoding. Due to the practical infeasibility of exploiting an environment that is phase invariant, all practical QKD implementations require the active alignment of the frames of the transmitter and the receiver performed by classical communication.

Polarization encoding is usually preferable for free-space QKD applications, for both ground and satellite communications, as discussed in [9, 10, 11, 12]. This choice is influenced by three main factors. Firtsly, the distribution across atmosphere does not influence the polarization state of the photons used as carrier of information, removing the requirement of active compensation of the fluctuation of the quantum channel [13]. Secondly, the practicability of developing polarization encoders with long-term stability in time and low Quantum Bit Error Rate (QBER) has been demonstrated [14]. Lastly, the implementation of proper receivers based on polarization encryption can be achieve exploiting relatively cheap but efficient components as beam splitters, half-wave plates and quarter-wave plates.

Discussing instead of the phase encoding approach, its main implementation can be found in the optical fibers-based networks. As a matter of fact polarization encoding is affected by random fluctuations once it is exploited in optical fibers due to the birefringence of the silica of which these devices are made, translating in an increase of the noise and a reduction of the secret key rate (SKR) [15]. On the contrary, the phase encoding solution circumvent this problem, exploiting in particular the *time-bin* strategy, whose design is based on the time-of-arrival of photons, and consequently the relative phase between the mentioned time-bins [16]. This alternative ensures the robustness of the communication against environmental modification of the state of polarization, at the cost of introducing strict requirements in terms of interferometric stabilization to guarantee reliable encoding and decoding of the superposition of the time-bins.

This work aims to study a cross-encoded variation of the BB84 QKD protocol, in which the encoding of states are achieved by means of polarization while the distribution of the key from the transmitter to the receiver is accomplished with time-bins. However, the true novelty of this alternative lies on the fact that it is capable of attaining a security level comparable to similar QKD protocols with active reference frame compensations, without requiring this constraint.

In accordance with the results proved by [17], based on the previous studies of [18, 19], the goal of this project has been to realize a RFI QKD procedure that secures the BB84 protocol with a hybrid cryptographic strategy. The core of this method is founded on the intent of exploiting polarization of quantum states to perform encoding and decoding of the information needed to be shared, while the transmission is achieved exploiting the versatility of the time-bin reference. In particular, to encode the key Alice employs the states ($|L\rangle$, $|R\rangle$, and $|D\rangle$). On the other hand, Bob makes use of the bases ($\hat{\mathbb{Z}}$ and $\hat{\mathbb{X}}$) to decode the key. In particular, the security is assessed estimating the statistics of the mismatches between these two bases.

Following the discussion proposed in [8], the three Pauli matrices in Eq. (2.7) are denoted for simplicity by $\{\hat{X}, \hat{Y}, \hat{Z}\}$ and one direction is assumed to be well defined[2]. Therefore the following is true: $\hat{Z}_A = \hat{Z}_B$[3]. The remaining two directions are considered to change slowly along the quantum channel, feature expressed by the equations

$$\hat{X}_B = cos(\beta\hat{X}_A) + sin(\beta\hat{Y}_A) \qquad \hat{Y}_B = cos(\beta\hat{Y}_A) - sin(\beta\hat{X}_A) \tag{2.20}$$

[2] In the usual QKD encoding case the well defined direction is the *circular basis* in polarization encoding and the *time basis* in time-bin encoding.

[3] The subscripts A/B indicates the Alice/Bob point of view.

where β is an unknown quantity that varies in time, assumed to interpret the phase drift between Alice and Bob, once the time-bin encoding is implemented.

The *prepare and measure* approach introduced by the BB84 protocol requires that at each run Alice selects randomly and independently one of the two available bases to generate the quantum state, that once collected by Bob, it will be measured with an independent choice over the same bases.
After the completion of the exchange of the entire rough key, the two parties announce their respective choices, keeping only the states in which the selection has been identical. From this consideration, the QBER is computed by

$$QBER = e_{\hat{Z}\hat{Z}} = \frac{1 - \langle \hat{Z}_A \hat{Z}_B \rangle}{2}. \tag{2.21}$$

In order to estimate the eventual Eavesdropper (Eve)'s information, Alice and Bob are required to use the knowledge collected on the other two bases, that are complementary to $\hat{Z}$, and that can be computed as

$$C = \langle \hat{X}_A \hat{X}_B \rangle^2 + \langle \hat{X}_A \hat{Y}_B \rangle^2 + \langle \hat{Y}_A \hat{X}_B \rangle^2 + \langle \hat{Y}_A \hat{Y}_B \rangle^2. \tag{2.22}$$

The number resulting from this formula will be of paramount importance to bound the information in possession of Eve.

Theoretically, the maximum value achievable in Eq. (2.22) is $C = 2$, under the condition of utilizing two maximally entangled states in the description of the two quantum states possessed by Alice and Bob after the distribution of a single bit of information. In this case the parameter $e_{\hat{Z}\hat{Z}}$ is equal to zero.
In the assumption of maintaining the QBER under the upperbound $e_{\hat{Z}\hat{Z}} \leq 15.9\%$ [17], the information in the hands of Eve can be calculated as

$$I_E = (1 - e_{\hat{Z}\hat{Z}}) \cdot h\left(\frac{1+\mu}{2}\right) + e_{\hat{Z}\hat{Z}} \cdot h\left(\frac{1+\nu(\mu)}{2}\right) \tag{2.23}$$

in which $h(x)$ denotes the *binary Shannon entropy*

$$h(x) = -\sum_{i=1}^{2} P(x_i) \cdot log_2 \left[P(x_i)\right], \tag{2.24}$$

and the parameters μ and ν are expressed by

$$\mu = min \left[\frac{\sqrt{C/2}}{1 - e_{\hat{Z}\hat{Z}}}, 1 \right] \tag{2.25}$$

$$\nu = \frac{\sqrt{C/2 - (1 - e_{\hat{Z}\hat{Z}})^2 \mu^2}}{e_{\hat{Z}\hat{Z}}}. \tag{2.26}$$

The mathematical derivation assumes to study an equivalent *entanglement-based version* of this protocol, in which Alice and Bob share the Bell state

$$\left|\Phi\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_A \left|0\right\rangle_B + \left|1\right\rangle_A \left|1\right\rangle_B \right) \tag{2.27}$$

and independently they perform a projective measurement on it to determine the received state.

Formally, each pair of photons shared between Alice and Bob is considered to be in the *two-qubit state* $\hat{\rho}_{AB}$, of which Eve hold a purification, described by

$$\hat{\rho}_E = \mathrm{Tr}_{AB}(\hat{\rho}_{ABE}). \tag{2.28}$$

In this notation $\hat{\rho}_{ABE}$ indicates the density matrix associated to the space shared by Alice, Bob and Eve after the distribution of the quantum key, that can be expressed as the outer product of the state in Schmidt decomposition

$$\left|\Psi\right\rangle_{ABE} = \sum_j \sqrt{\lambda_j} \left|\phi\right\rangle_{AB} \left|E_j\right\rangle, \tag{2.29}$$

in which $\langle E_i | E_j \rangle = \delta_{ij}$ represents the orthogonal basis of the system under the control of Eve.

We mention here, but it will be discussed later on during this study, that from the computation of the information possessed by an external eavesdropper I_E it is possible to derive an estimation of the secret key rate , which allows to study the amount of secure information that can be extracted from a specific QKD protocol, considering any possible strategy attack at disposal of Eve. It is defined as the number of secure bits of classical information that can be extracted from one stream of qubit per unit of time, formally

$$R = 1 - h\left(e_{\hat{Z}\hat{Z}}\right) - I_E. \tag{2.30}$$

The target of this RFI QKD protocol is to achieve the best possible lower bound on the C parameter. Following the argument proposed in [17], this issue can be faced assuming it to be a *minimization Semi-Definite Programming* (SDP) problem, which can be dealt according to the following interpretation:

$$\underset{\hat{\rho}_{AB}}{\texttt{minimize}}: \quad C_L \tag{2.31}$$

$$\texttt{subject to :} \begin{cases} Tr\left(\hat{E}_{ZZ}\hat{\rho}_{AB}\right) = e_{\hat{Z}\hat{Z}} \\ Tr\left(\hat{P}^{A}_{\alpha i} \otimes \hat{P}^{B}_{\chi j}\ \hat{\rho}_{AB}\right) = p_{\alpha i, \chi j} \\ Tr\left(\hat{\rho}_{AB}\right) = 1 \\ \hat{\rho}_{AB} \geq 0 \end{cases}$$

where $\{\alpha, \chi\} \in \{\mathbb{X}, \mathbb{Y}, \mathbb{Z}\}$ are the possible bases to be chosen and $\{i, j\} \in \{0, 1\}$ the classical symbols encoded in the photons.
In the scenario discussed in this three-state protocol the constraints over the choice performed by Alice in the encoding procedure become

$$\alpha \neq \mathbb{Y} \qquad \text{and} \qquad i = 0 \quad \text{if} \quad \alpha = \mathbb{X}\ . \tag{2.32}$$

Furthermore, the notations $\hat{E}_{ZZ}$ and $\hat{P}_i = |i\rangle\langle i|$ indicate respectively the *error operator* in the $\mathbb{Z}$ basis and a *projective measurement* performed on the entangled state $\hat{\rho}_{AB}$. Finally, the term $p_{\alpha i, \chi j}$ represents the probability that Bob receives a state $|\chi_j\rangle$ given that Alice has obtained the state $|\alpha_i\rangle$ once she has measured her photon (in the entanglement based version of the BB84 protocol).

The presented optimization problem can be solved exploiting the `MATLAB` package

CVX, designed to perform convex optimization operations [20, 21].

Further discussions about this tool and its applications will be made in the following chapters.

3 Experimental Setup

3.1 Notions about the hardware

In the following section are presented the main optical components implemented in the discussed experiment. For each device a brief description of the working principle is reported, together with the mathematical model and the datasheet specifications provided by the constructor.

3.1.1 Passive devices

Beam Splitter

The main optical device that is exploited in the experimental setup is the beam splitter (BS), whose principal function is to split an optical beam into two separated beams with different orientation.

In particular, in our apparatus we use three different types of beam splitter, that are the non-polarizing cube BS, the polarizing cube BS and the fiber-based Fast-Axis-Blocking BS (FAB-BS).

The behaviour of a generic BS can be studied according to the BS operator, which has the following form

$$\widehat{BS} = \begin{pmatrix} t & r \\ r & t \end{pmatrix} \tag{3.1}$$

where t and r are set to be respectively the transmission and reflection coefficients, whose constraint is

$$|t + r|^2 = 1. \tag{3.2}$$

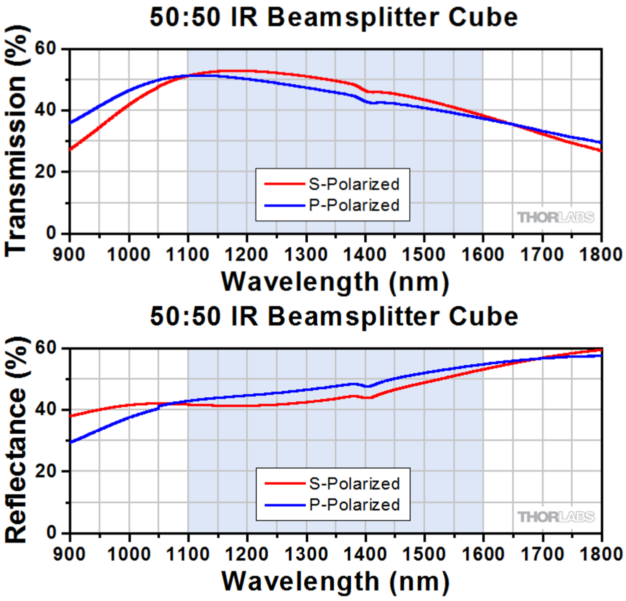


Figure 3.1: Transmission and reflectance spectra of the `BS015 - 50:50 Non-Polarizing Beamsplitter Cube` by Thorlabs considering two input polarization states. The blue shaded regions denote the transmission and reflection bands for which the performance is guaranteed to meet the stated specifications (https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=6208#).

An ideal non-polarizing BS here exploited is described by the operator

$$\widehat{BS} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} ; \tag{3.3}$$

it is commonly named as 50:50 BS since, in principle, it whether transmits or reflects the incoming photon with equal probability. It has a working range of wavelengths in which it guarantees high efficiency both in transmission and reflection.
The datasheet related to the device chosen for the experiment is reported in Fig. 3.1, where we show the transmission and reflectance spectra of the `BS015 - 50:50 Non-Polarizing Beamsplitter Cube` by Thorlabs.

Differently, the PBS has the function to separate incoming photons with orthogonal polarization. In particular, a photon with horizontal polarization $|H\rangle$ is transmitted toward the initial direction of propagation, while a vertically polarized $|V\rangle$ photon is reflected toward a different output port, usually placed in a direction orthogonal to the propagation one. This enables the possibility to discriminate photons with opposite sym-

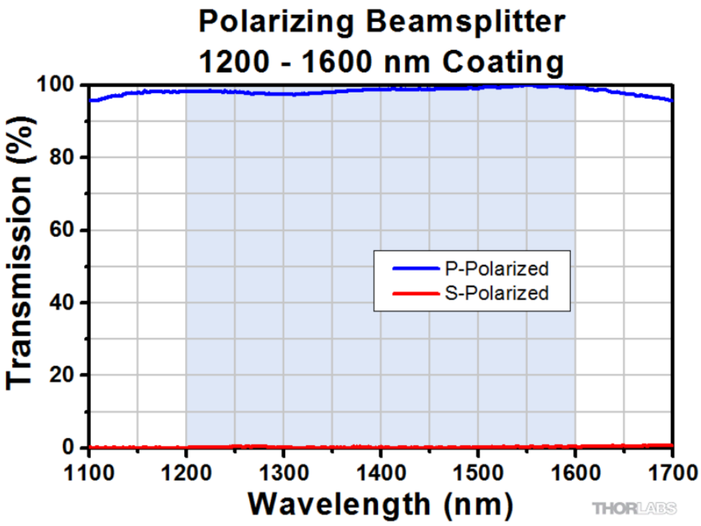


Figure 3.2: Transmission spectrum of the PBS254(/M) Polarizing Beamsplitter Cube bu Thorlabs. The blue shaded region denotes the transmission band for which the performance is guaranteed to meet the stated specifications (https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=4137).

bols in polarization encoding, as will be explained in detail in the next chapters.
The device chosen in our setup is the PBS254(/M) Polarizing Beamsplitter Cube by Thorlabs, whose spectrum is reported in Fig. 3.2. According to the provided datasheet, the considered PBS has a transmission efficiency of at least 90% and a reflection efficiency of at least 99.5% inside the range between 1200 [nm] and 1600 [nm].

The last beam-splitting component relevant for this study is the FAB-BS. This element behaves like a polarizing filter in the sense that it allows the passage of the solely horizontal light, that usually is the polarization that enters the slow axis of a generic optical fiber, while it blocks the vertically polarized light. Its usage in the final apparatus will be explained later during this discussion.

Wave Plate

Another optical tool that is of paramount importance to manipulate beams of light inside an optical circuit is the wave plate (WP), named also *retarder*. This is an optical device built to alter the polarization state of the light wave passing across it. The birefringency of the crystal constituting the wave plate is able to modify the velocity of an incoming photon based on its polarization orientation, therefore performing a rotation of the overall polarization state according to the formula

$$\Gamma = \frac{2\pi \Delta n L}{\lambda_0} \qquad \widehat{WP} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-j\Gamma} \end{pmatrix} \tag{3.4}$$

where Γ indicates the relative phase between the input and the output polarizations, Δn is the birefringence factor, L is the thikness of the WP and λ_0 is the vacuum wavelength of the entering light. In Eq. (3.4) is also shown the operator of the general *wave retarder*[1].

Wave plates of particular interest are the *half-wave plate* (HWP), which introduces a phase delay of $\Gamma = \pi$, and the *quarter-wave plate* (QWP, $\Gamma = \pi/2$), whose action can be described by the following transformation matrices

$$H\widehat{W}P = \hat{R}(\theta) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Q\widehat{W}P = \hat{R}(\theta) \begin{pmatrix} 1 & 0 \\ 0 & -j \end{pmatrix} \tag{3.5}$$

where $\hat{R}(\theta)$ represents the rotation matrix, that collects the information about the relative rotation between the incoming polarization and the direction of orientation of the axis of the wave plate, and whose expression is described by

$$\hat{R}(\theta) = \begin{pmatrix} cos(\theta) & sin(\theta) \\ -sin(\theta) & cos(\theta) \end{pmatrix}. \tag{3.6}$$

In particular, referring to well defined input polarization states, we focus on the main useful transformations performed by these two devices:

— HWP:

  - converts *linearly polarized wave* into *linearly polarized wave* (rotation of the polarization axis)
  - converts *circularly polarized wave* into *circularly polarized wave with switched handedness*

[1] In this representation we are considering that the fast axis of the crystal is aligned along the x direction of a reference frame placed on the input face of the device.

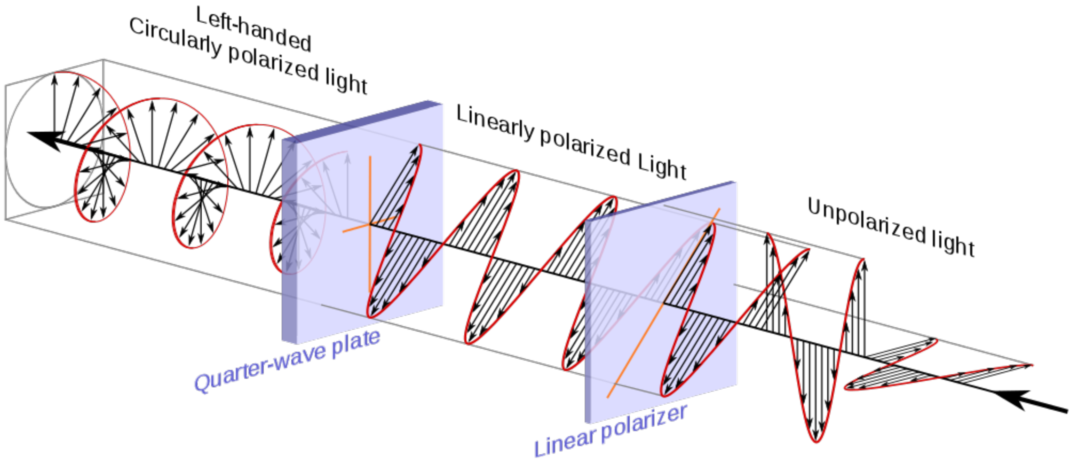


Figure 3.3: Cascade of HWP and QWP to create circularly polarized light (https://en.wikipedia.org/wiki/Waveplate).

— QWP:

- converts *linearly polarized wave* into *circularly polarized wave* (unless the polarization is aligned with one of the two axes of the retarder that in this case it appears transparent)
- converts *circularly polarized wave* into *linearly polarized wave*

Furthermore, is worth mentioning one simple setup widely implemented in optical apparatus, which sees the combination of an HWP followed by a QWP as depicted in Fig. 3.3. This last combination of retarders will be shown in the following section in the description of both the transmitter and the receiver, in which it will be discussed the significance of this simple device to the feasibility of this RFI protocol.

Polarizing Filter

Due to the non-idealities introduced by the PBSs, that inevitably let some photons with wrong polarization passing through their ports, we have introduced one polarizing filter at the reflection output of each PBS in the receiver configuration (see Section 2).
What this device does is simply to allow the passage of photons with a specific polarization, blocking all photons differently polarized. This implementation helps to increase the extinction ratio of the signal exiting the BS. As a matter of fact, inefficiency in the routing of photons distorts the measurements at the final photodetectors.

Collimator

This item, together with the fiberport, has the task to switch between the propagation in free-space and in optical fibers. If not well tuned, these devices are one of the main causes of losses inside the optical path.

The collimator can be found in the market in several different realization, mainly according to its degrees of freedom, that make it being more versatile or more fine in the tuning. The totality of the collimators are composed by an internal lens (usually aspheric), whose distance from the head of the optical fiber determines the position of the *waist* of the laser beam, that we remind to be the position along a collimated beam at which the beam itself presents the minimum radius, and therefore the maximum intensity per unit of area. Working with collimated beams allows to increase the amount of exploitable photons across the entire apparatus, reducing the losses and increasing the SNR[2].

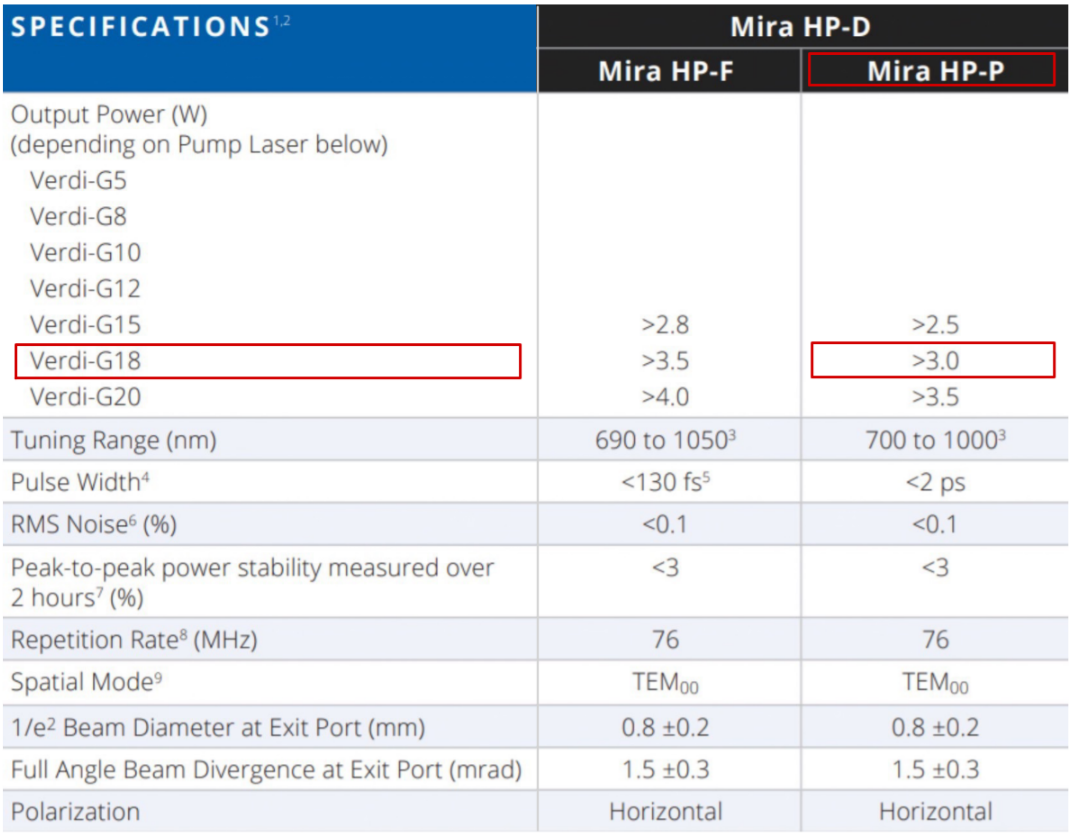
For the realization of this apparatus two different types of collimators have been used that are the *fixed focus* and the *variable focus*. The latter have been extremely useful to converge the beams collected in the four output branches of the receiver, allowing to acquire up to 90% of coupling.

To be exhaustive, the device chosen to be inserted in the experiment is the `CFC11P-C - Adjustable Fiber Collimator` by Thorlabs (`https://www.thorlabs.com/thorproduct.cfm?partnumber=CFC11P-C`), with effective focal length $f = 11.0\ [mm]$ and $1050-1620\ [nm]$ Anti Reflection Coating.

Fiberport

The fiberport is a coupling device with functionalities similar to those of the collimator, that however offers better features in terms of adjustment of the beam collimation and beam orientation in both horizontal and vertical direction. These advantages in terms of accuracy are at the expense of obtaining a more complex calibration procedure.

[2] SNR="Signal to Noise Ratio"=Signal Power/Noise Power.



SPECIFICATIONS[1,2]	Mira HP-D	
	Mira HP-F	Mira HP-P
Output Power (W) (depending on Pump Laser below)		
Verdi-G5		
Verdi-G8		
Verdi-G10		
Verdi-G12		
Verdi-G15	>2.8	>2.5
Verdi-G18	>3.5	>3.0
Verdi-G20	>4.0	>3.5
Tuning Range (nm)	690 to 1050[3]	700 to 1000[3]
Pulse Width[4]	<130 fs[5]	<2 ps
RMS Noise[6] (%)	<0.1	<0.1
Peak-to-peak power stability measured over 2 hours[7] (%)	<3	<3
Repetition Rate[8] (MHz)	76	76
Spatial Mode[9]	TEM_{00}	TEM_{00}
$1/e^2$ Beam Diameter at Exit Port (mm)	0.8 ±0.2	0.8 ±0.2
Full Angle Beam Divergence at Exit Port (mrad)	1.5 ±0.3	1.5 ±0.3
Polarization	Horizontal	Horizontal

Figure 3.4: Datasheet of the Mira™ HP-P Ti:Sapphire Laser powered via the laser pump Verdi V-18. https://www.coherent.com/content/dam/coherent/site/en/resources/datasheet/lasers/mira-ds

3.1.2 Active devices

Pulsed Laser Source

Among the active devices implemented in the setup presented here, for sure the laser source is one of the most important and critical for the realizability of the protocol. An inefficient generation of the laser pulses can be detrimental in the performances of the entire communication apparatus.

After some tests performed with different integrated diode lasers that did not show proper characteristics in the generation of Gaussian pulses, the choice has fallen on the most efficient light source at disposal of the Quantum Future group, that is the Mira™ HP-P Ti:Sapphire Laser powered by the laser pump Verdi V-18, both produced by Coherent®. The specifications relative to the laser source are reported in Fig. 3.4.

For the experiment purposes, the laser pump has been set to produce 14 [W] of coherent light at 532 [nm] in order to power the Mira laser in *mode-locking* configuration, obtaining at the output approximately 1 [W] of pulsed coherent light at 775 [nm].

In Chapter 4 it will be described the entire optical path by means of which the single states are produced.

CW laser source

For the intermediate characterization of the setup, and in general during the entire assembly of both the transmitter and the receiver stations, it has been useful to exploit a tunable laser source operating in CW (Continuous Wave). The device that best has suited this scope has been the `Santec Wavelength Selectable Laser WSL-110`, capable of producing up to 35 [W] of CW horizontally-polarized light in a range between 1527.6 and 1608.7 [nm].

Power Meter

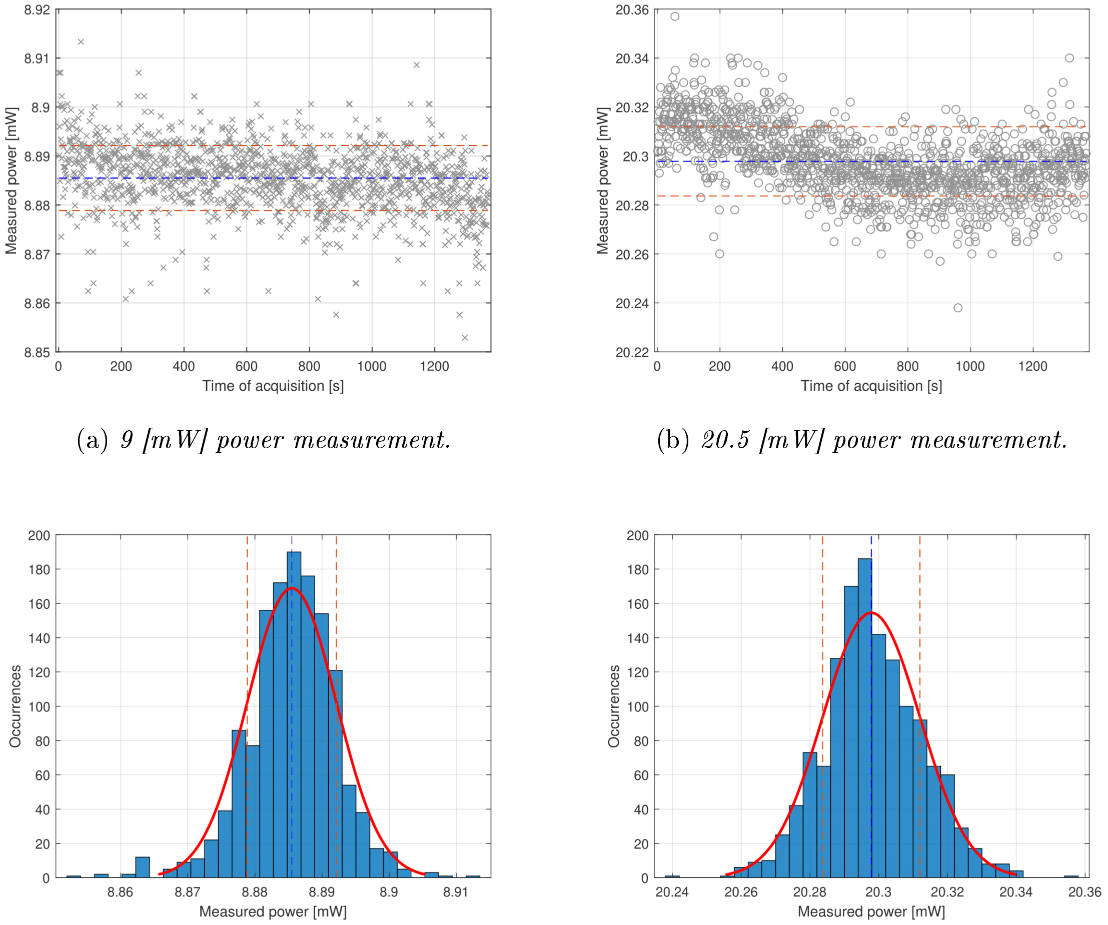
Fundamental during the assembly process has been the `Digital Handheld Optical Power Meter Console` by `Thorlabs`. With this device every operation except for the final characterization has been carried out. Every reference to the measurement of optical power mentioned in this work considers the usage of this type of devices, if no expressly specified.

In order to have an estimate of the error introduced by this device, in Fig. 3.5 it is reported the accuracy of the `Optical Power Meter PM100D` (the one exploited to finalize this experiment) in a graph visualizing the occurrences of power measurements registered in a time interval of 20 minutes. In order to detect any power intensity dependence of this statistics, two measurements have been performed, launching respectively 9 [mW] and 20.5 [mW] of CW optical power directly to the Power Meter sensor by means of 1 meter of single-mode optical fiber.

From these measurements it has emerged that the standard deviation of the two fitted Gaussian functions over the occurrences of the measured powers are respectively

$$\sigma_{9mW} = 0.0066\ [mW] \qquad\qquad \sigma_{20.5mW} = 0.0141\ [mW], \tag{3.7}$$

assumed to be the error introduced by the device in the measuring process.



(a) *9 [mW] power measurement.*

(b) *20.5 [mW] power measurement.*

(c) *9 [mW] occurrences distribution.*

(d) *20.5 [mW] occurrences distribution.*

Figure 3.5: In figure (a) and (b) are shown the two 20 minutes measurements considering respectively 9 [mW] and 20.5 [mW] of optical power. In figures (c) and (d) are reported the relative histograms of occurrences for the two measurements. In all the four figures the blue dashed line represents the mean value while the orange lines indicates the standard deviation with respect to the Gaussian fit computed over each dataset.

Superconducting Nanowire Single Photon Detector

If the source is considered to be a crucial variable in the setup, certainly the photo-detector has the same relevance for the success of the experiment. This device is required in the study in which the pulsed laser source is exploited.

In order to achieve the highest possible resolution in the estimation of the security of the present protocol, the most appropriate choice results to be the `ID281 Superconducting Nanowire` by `ID Quantique` (https://www.idquantique.com/quantum-sensing/products/id281/). This device is a multi-channel SNSPD (Superconducting Nanowire Single Photon Detector) integrated in an automated closed-cycle 0.8 $[K]$ cryostat, capable of guarantee at least 80% of efficiency (at $\lambda = 1550$ $[nm]$). The conversion form an analogue time of arrival to a digital data is accomplished by a `quTAG` *time-to-digital-converter* (TDC), powered by `qutools` (https://qutools.com/qutag/). Further details will be introduced in Chapter 5.

Polarimeter

The polarimeter is an useful device whose main purpose is to give an instantaneous measure of the polarization of the light collected at its aperture, providing effective parameters as the *Degree of Polarization* (DOP) and the *Stokes parameters* s_0, s_1, s_2 and s_3, representable in the *Poincaré Sphere*.

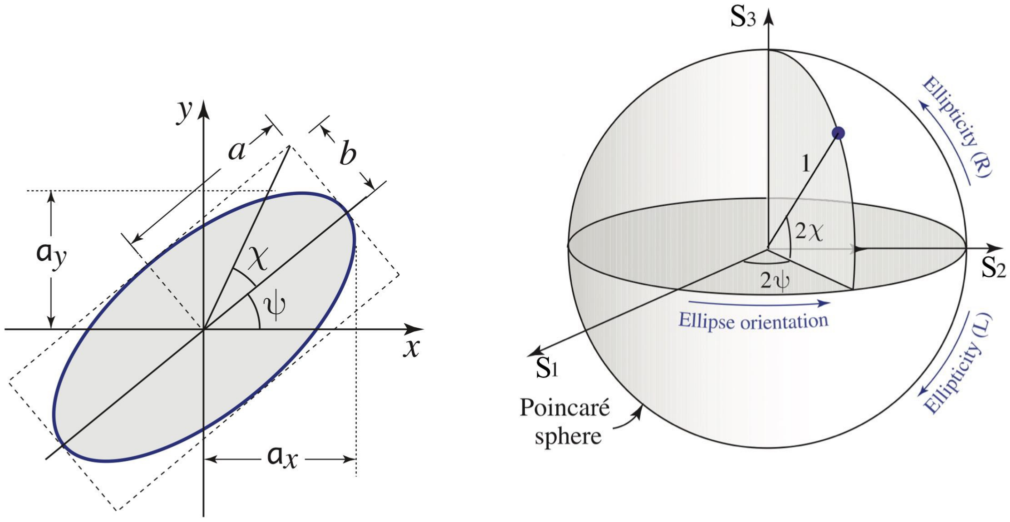
Briefly resuming some basic contents of Polarization Optics, a generic state of polarization can be characterized by two angles ψ and χ, which measure the orientation and the ellipticity of a polarization ellipse, respectively, as defined in Fig. 3.6-(a). According to these parameters, it is possible to depict every state of polarization by a point on the surface of a sphere of unit radius in a spherical coordinate system, namely the Poincarè sphere (see Fig. 3.6-(b)).

In this geometric framework the Stokes parameters can be retrieved as

$$S_1 = cos(2\chi)cos(2\psi) \tag{3.8}$$

$$S_2 = cos(2\chi)sin(2\psi) \tag{3.9}$$

$$S_3 = sin(2\chi) \tag{3.10}$$



(a) *Polarization ellipse.*

(b) *Poincaré Sphere representation.*

Figure 3.6: Polarization ellipse (a) and Poincaré Sphere representation (b) for a generic polarization state.

once the parameter s_0 is normalized.

By means of this device it has been possible to perform a full tomography of the receiver (see Chapter 5), necessary to set the proper orientation of the waveplates thus discriminating the collected photons based on their polarization.
In particular the instrument exploited in the study discussed later during this work is the `Thorlabs PAX1000IR1 polarimeter` (https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=1564) together with the related `Software GUI`.

Kinesis K-Cube$^{\text{TM}}$

In the course of the assembling of the experimental apparatus it has been necessary to properly set some optical components with precise accuracy, in order to retrieve meaningful results. For this reason the adjustment of the most crucial mechanical supports has been performed by means of the `Thorlabs K-Cube`$^{\text{TM}}$ `DC Servo Motor Controller` (https://www.thorlabs.com/thorproduct.cfm?partnumber=KDC101), which is able to finely control the motion of mechanical devices as *rotation stages* or *motorized stages*.
In the next chapters it will be specified the utilization of these devices.

3.2 Configuration of the experimental setup

The design of the configuration exploited to perform the concrete study of this protocol has been developed during the entire period of my trainee-ship. It has undergone numerous modifications, necessary to guarantee the highest possible level of accuracy and robustness, given the available tools provided by the Quantum Future facility.

In this section it follows a general description of the entire apparatus required for the implementation and the characterization of the protocol under study. Detailed discussions regarding the specific stages will be faced in the next chapters.

The qualitative scheme of the final setup is represented in Fig. 3.7. It is subdivided into three main blocks, that are the transmitter (usually named Alice), the quantum channel across which the encoded quantum key is transmitted, and the receiver (Bob for simplicity) at the end of the network.

Starting from the description of the *transmitter stage*, the laser source placed in it is capable of emitting pulses of laser light at 775 [nm] with a frequency of about 76 [MHz]. These pulses are directed through a non-linear crystal performing Spontaneous Parametric Down Conversion with an efficiency around $1/10^6$. Due to the statistic of this non-linear phenomenon it is possible to assume that for each laser pulse an entangled pair of photons is generated and exploited.
For each pair one photon is collected thus entering the iPognac encoder [14]. The topology of this device lets the single photons to be modulated inside a Sagnac interferometer, applying a polarization encoding, before being converted into time-bin encryption and then transmitted across the quantum channel.

The *quantum channel* is clearly the mean across which the cryptographic key is distributed from the transmitter to the receiver. It is in practice realized by an optical network, and in particular it consist in the ether for free space applications, or it is represented by an optical fiber for terrestrial communications. As mentioned before, the present protocol exploits the time-bin encoding for the exchange of the quantum key, and the best solution across which perform this task is the optical fiber. As a matter of fact, standard optical fibers are made by silica, whose crystalline structure

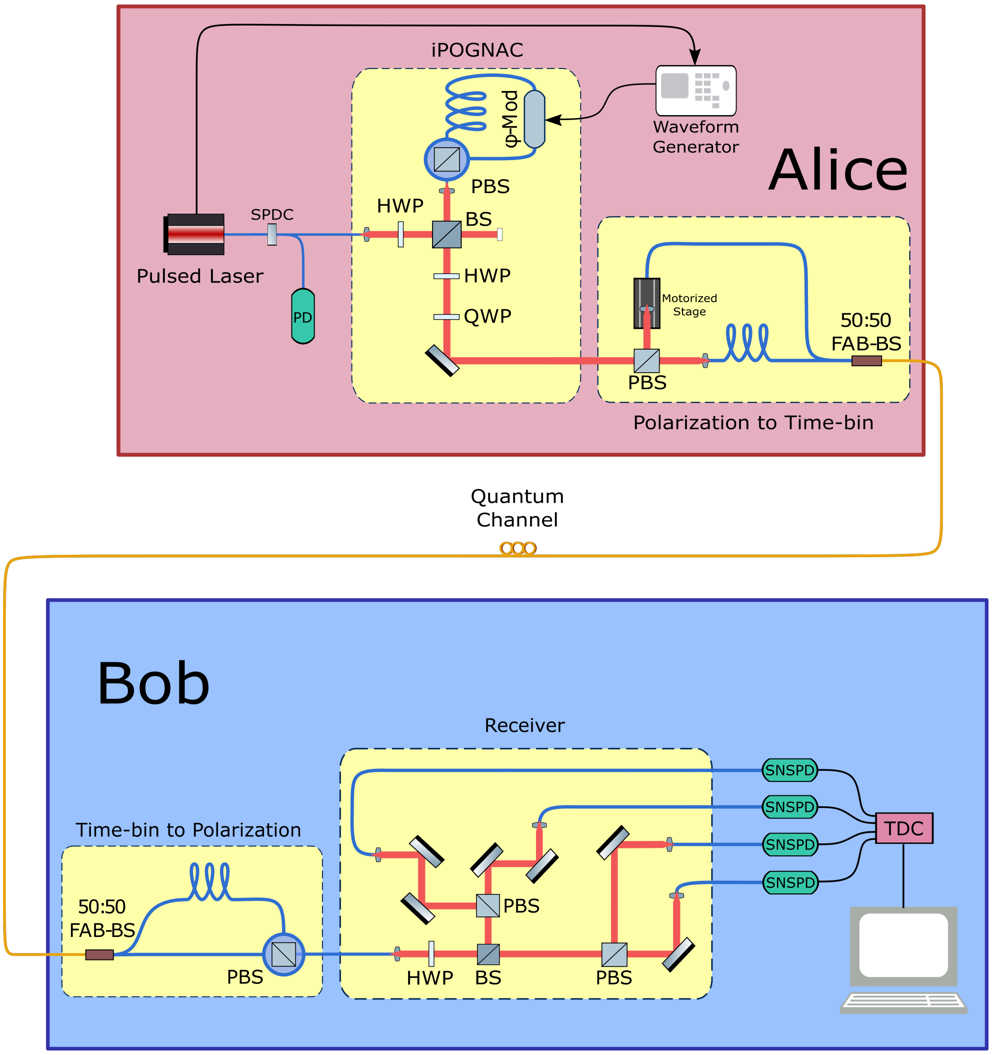


Figure 3.7: Schematic representation of the experimental setup.
BS: beam splitter, FAB-BS: fast-axis-blocking BS, PBS: polarizing BS, ϕ-mod: phase modulator, H/QWP: half/quarter-wave plate, SNSPD: superconducting-nanowire single photon detector, TDC: time-to-digital converter. Single mode fibers are in *yellow*, polarization maintaining fibers are in *blue*.

intrinsically manifests birefringence. This optical property causes the random rotation of the polarization state of each photon traveling through it, causing the complete lost of information encoded in the quantum states. However, exploiting the time of arrival of the single photons circumvents this critical issue.
For the final characterization of the protocol we exploited the 50 meters-long optical fiber that connects the two facilities in which the Alice and Bob are respectively allocated, as quantum channel.

Finally, discussing about the *receiver*, it is composed by the initial encoding conversion device, whose role is to re-transform the information encrypted in the time of arrival of the photons back to the original polarization information. Once the photon has retrieved its original encoding, it is collected by the receiver, whose design has the goal to direct the particle toward the proper photo-detector. At the end of the network four SNSPDs reveal to a Time-to-Digital-Converter the absolute time of arrival of each photon measured at their input ports. The data here collected can be processed by some post-processing programs built *ad hoc* in order to extrapolate information about the security of the communication according to the computation of the C parameter, mentioned in Reference Frame Independence section.

4 Alice Station

Resuming what introduced in the previous chapter, the first fundamental component that has huge impact in the performances of any communication channel is the transmitter stage, here named Alice, wanting to use the formalism introduced in the early studies of Cryptography [22].

As previously mentioned, the Alice station is composed by three main apparati, each one with its specific function: the *pulsed laser source*, the *iPognac polarization encoder* and the *polarization to time-bin converter*.
A detailed scheme of the Alice setup is pictured in Fig. 4.1.

4.1 The Pulsed Laser Source

Starting from what anticipated in Chapter 3, the laser pulses exploited for the distribution of quantum keys in the present protocol are generated by the combination of two devices: the `Mira`™ `HP-P Ti:Sapphire Laser` powered by the laser pump `Verdi V-18` (`Coherent®`). This setup in principle is capable of working both in pulsed regime (*mode-locking*) and in CW regime, emitting photons in a range between 700 $[nm]$ and 1000 $[nm]$.
The actual laser source is set to produce light at the specific wavelength of 775 $[nm]$, that by means of a non-linear crystal performing Spontaneous Parametric Down Conversion (SPDC), it is converted in light with doubled wavelength.
The reason of this choice is simple and lies on the intrinsic properties of the material with which the optical fibers are realized. As a matter of fact, almost the totality of the optical fibers are made of silica, SiO_2, due to its suitable optical properties and simultaneously to its abundance in nature. As it can be observed in Fig. 4.2, the attenuation profile of a pure single-mode optical fiber sees the contribution of different phenomena,

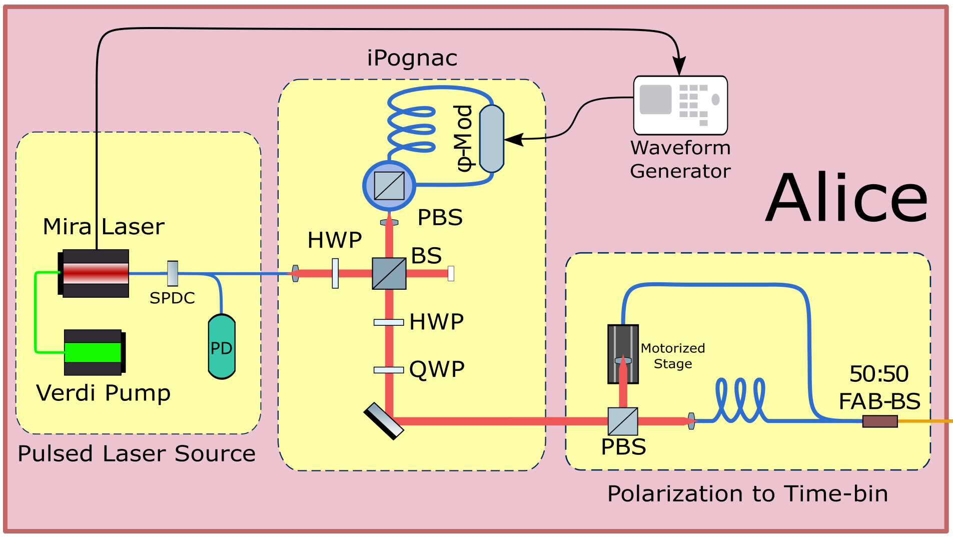


Figure 4.1: Schematic representation of the transmitter setup (Alice). The order from the left to the right represents the cascade with which quantum states at proper wavelength are generated, encoded and converted before being sent through the quantum channel and collected by the receiver (Bob).

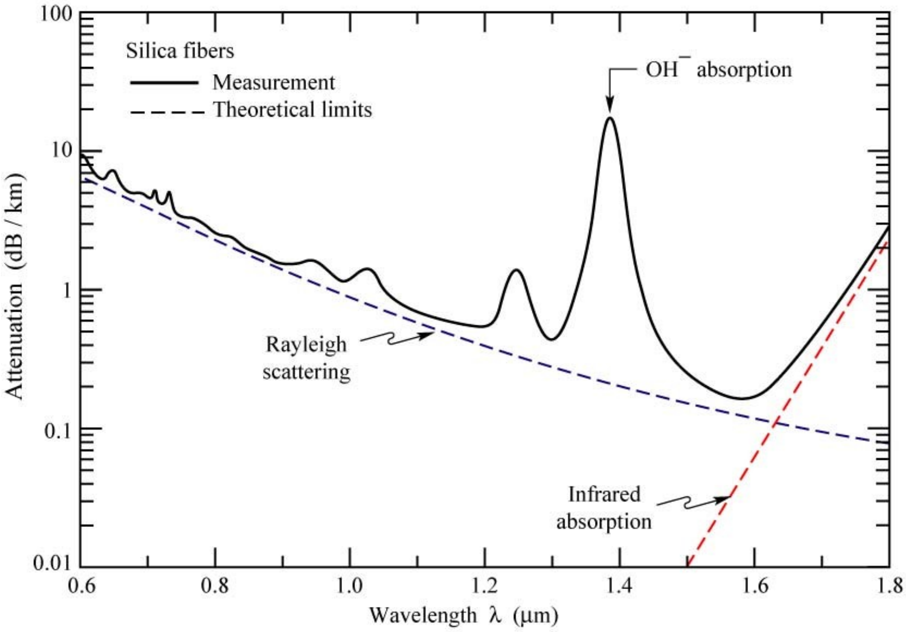


Figure 4.2: Measured attenuation in silica fibers (solid line) and theoretical limits (dashed lines) given by Rayleigh scattering in the short-wavelength region, and by molecular vibration (infrared absorption) in the infrared spectral region.

that increase the losses introduced in specific portions of the spectrum. In particular, due to the Rayleigh scattering phenomenon, light with gradually shorter wavelength is more attenuated passing through the core of a generic optical fiber. For longer wavelengths a different phenomenon, the infrared absorption, enhances the losses inside the silica. Lastly, also the absorption of the free OH^- ions inside the lattice generates attenuation. Among these different regions, portions of intrinsic lower attenuation (commonly named *bands*) find place. These intervals of wavelengths have acquired importance in the study of optical networks, since in general lower attenuation implies longer reachable distances. Probably, the most exploited band in Telecommunications is the so called "C-band" ("Conventional"), whose fortune has grown in the past years due to the diffusion of the Erbium-Doped-Fiber-Amplifiers (EDFA), of which the highest performing gain is encountered exactly at 1550 $[nm]$. At this specific wavelength a generic optical fiber introduces an attenuation of about 0.22 $[dB/km]$.

Thereby, the optical pulses exiting the laser source enter the non-linear crystal with a wavelength of 775 $[nm]$. Here the SPDC process takes place, generating with a conversion efficiency in the order of at most 10^{-6} [23] a pair of photons with exactly half of the energy, and therefore with doubled wavelength (i.e. precisely 1550 $[nm]$). Without entering too much into the details (which is not of interest to this study), in Fig. 4.3 it is pictured the scheme describing the SPDC phenomenon.

It is interesting to mention that the output state of the down-conversion process can be written as

$$|\Psi_{SPDC}\rangle = \sqrt{1-|\lambda|^2}\sum_{n=0}^{\infty}\lambda^n\,|n,n\rangle_{s,i} \tag{4.1}$$

with $\lambda = \eta\tau$, where η represents the overall efficiency parameter and τ is related to the interaction time inside the down-conversion medium [24]. In conclusion, the probability of measuring n photon pairs per pulse is given by

$$P(n) = \left(1-|\lambda|^2\right)|\lambda|^{2n}. \tag{4.2}$$

Before introducing the next component in the chain of generation of the encoded quantum key, it is worth to discuss the characteristic of the produced optical pulses. With the settings currently being adopted in the laser source, the `Verdi V-18` pumps

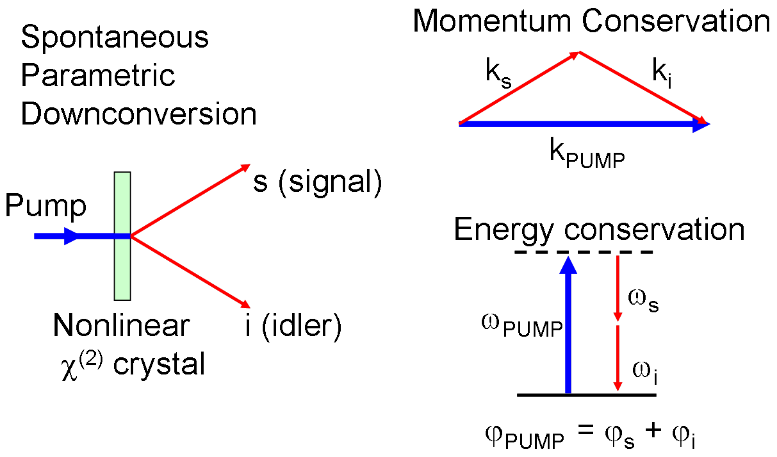


Figure 4.3: Scheme of the SPDC process. The photons exiting the non-linear crystal are usually named *signal photon* and *idler photon*. The first one is the quantum state used for the encryption of the quantum information, while the second one is usually required for heralding the presence of the single photon.
The SPDC is a *second order* non-linear phenomenon (from here comes the symbol $\chi^{(2)}$). Credits to https://en.wikipedia.org/wiki/Spontaneous_parametric_down-conversion#/media/File:Spontaneous_Parametric_Downconversion

14 $[W]$ of optical power inside the Mira™ laser, thus producing about $1[W]$ of pulsed light at 775 $[nm]$. From this amount, just a small portion is injected into the non-linear crystal, usually spanning between 10 $[mW]$ and 20 $[mW]$ of power.

Moreover, the repetition rate of the laser in mode-locking configuration is approximately 76 $[MHz]$. This leads to the computation of the period associated to exactly one pulse, that is approximately

$$T_{pulse} = \frac{1}{f_{pulse}} \approx 13.158 \ [ns] \tag{4.3}$$

Considering instead that the medium across which the signal is transmitted changes along the network, in the assumption that the refractive indices of the air and silica are respectively $n_{air} \approx 1$ and $n_{SiO_2} \approx 1.5$, the temporal width of a single laser pulse has been computed. This value has been measured making use of a Michelson interferometer with movable arm, whose general scheme is depicted for clarity in Fig. 4.4.

The result of the measurement can be observed in Fig. 4.5, where the *visibility* of the measured interference is plotted over the difference of the optical path covered by the pulse. It is appropriate to recall that the *interferometric visibility* expresses a

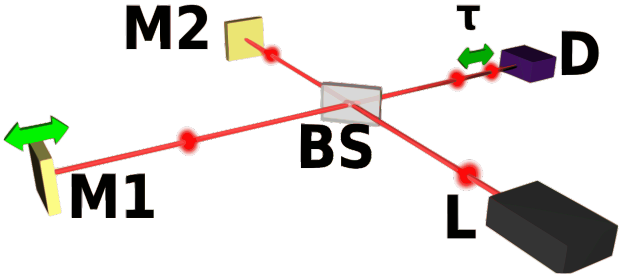


Figure 4.4: Setup for the computation of the field autocorrelation, based on a Michelson interferometer. L: laser in *mode-locking*, BS: beam splitter, M1: moveable mirror providing a *variable delay line*, M2: fixed mirror, D: detector.
Credit to https://en.wikipedia.org/wiki/Optical_autocorrelation#/media/File:Optical-field-autocorrelation-setup.svg

measure of the contrast of interference in a system manifesting wave superposition, and its mathematical formulation ha the following form:

$$v = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}. \tag{4.4}$$

To retrieve this value, here it is briefly introduced the formal expression of the measured intensity as a function of the delay τ between the interfering pulses, that is

$$I(\tau) = \int_{-\infty}^{+\infty} |E(t) + E(t-\tau)|^2 dt. \tag{4.5}$$

Considering to perform a Gaussian fit over the computed visibility, the correspondent standard deviation[1] results to be nearly 1304 $[\mu m]$.
Furthermore, according to the equation

$$\Delta\tau = \frac{\sigma_{fit}}{c\sqrt{2}}, \tag{4.6}$$

where $c \approx 3 \cdot 10^8$ $[m/s^2]$ is the speed of light in vacuum[2] the temporal duration of the

[1] The Gaussian fit function exploited in this computation has the shape $g(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, where the standard deviation σ here does not implies the deviation from the mean value but simply the width of the bell-shaped curve, since the fitted function is performed over acquired data instead of a statistical distribution.

[2] Since the measurement is considered regarding the "optical path difference", the scale with respect to the refractive index of the propagation medium has already been taken into account.

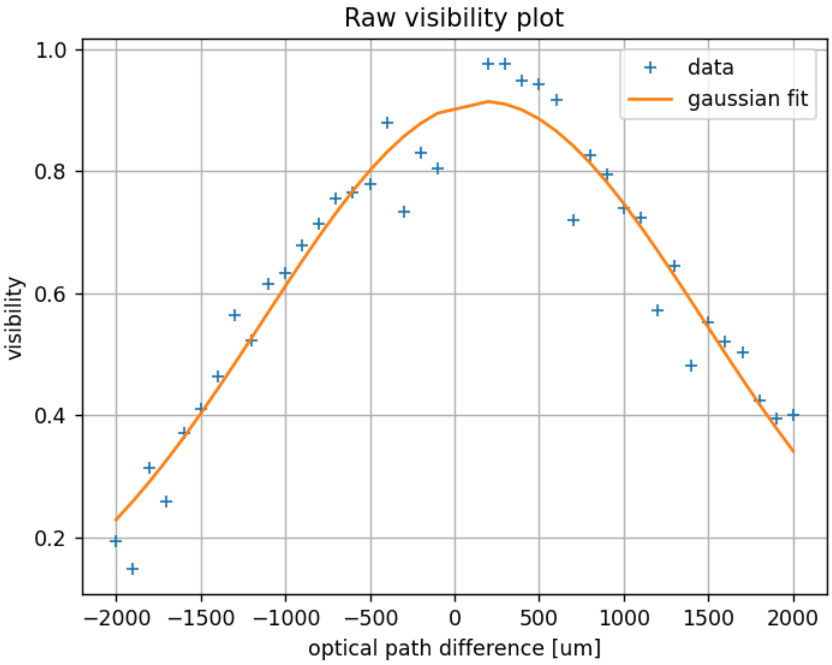


Figure 4.5: Visibility of the interference over the spatial distribution of the laser pulse (blue line), together with the Gaussian fit over the extrapolated data (orange line).

pulse can be computed, returning a value of about 3.08 $[ps]$.

Finally, at the output of the non-linear crystal, from the input pulses single photon states are retrieved with high probability. This can be explained by looking at the Eq. (4.2). As previously mentioned, the probability of generating one couple of entangled photons at the output of a generic non-linear crystal is in the order of $1/10^6$, while the probability of generating more than one pairs is exponentially lower.

According to several observations, it can be assumed that at the output of the crystal approximately single photons are observed.

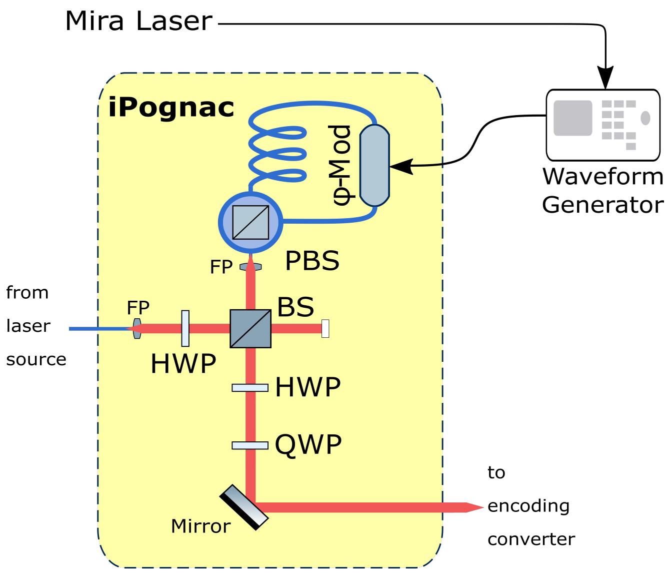


Figure 4.6: Scheme of the iPognac polarization encoder. BS: beam splitter, PBS: polarizing BS, ϕ-mod: phase modulator, H/QWP: half/quarter-wave plate, FP: fiber port. Polarization maintaining fibers are in *blue*, free-space optical path is in *red*.

4.2 iPognac

Following the path covered by the generated quantum states, after passing through some optical components of control the photons enter the polarization encoder stage named iPognac.

This device, which finds a complete schematic representation in Fig. 4.6, is a stable, low-error and calibration-free polarization encoder solution patented by Quantum Future group, which is capable of guarantee long-term temporal stability [14]. During the tests performed by the group it has been assessed that this apparatus is capable to achieve an optimal QBER of 0.05%, corresponding to an extinction ratio between the two bases approximately of 33 $[dB]$.

The purpose of this device is to encode information in the quantum carrier (which is the photon) so that it can be transmitted from the sender to the receiver with a sufficient level of security guaranteed by the laws of Quantum Mechanics.

The cascade of steps by means of which photons are associated with a given information is explained in the following lines.

The single photons originating from the laser source propagates through a polarization-maintaining (PM) fiber until they reach the fiber port (FP) at the input of the encoder.

In this first passage photons have kept an horizontal polarization $|H\rangle$, originated at the output of the non-linear crystal. The fiber port has the goal to collimate in free-space the light entering form the fiber plug and to steer it toward an half-wave plate (HWP), followed by a beam splitter (BS). Photons impinging the BS have diagonal polarization $|D\rangle$ due to the rotation occurred inside the input wave plate. Presumably, any state is thus composed as a superposition of $|H\rangle$ and $|V\rangle$ states, that therefore lay in the Bloch sphere equator. The transmitted light is discarded while the reflected photons are directed toward a second fiber port which inject them into the Sagnac interferometer loop. This portion is composed by a fiber-based polarization beam splitter (PBS), made of PM fibers at its input and output, and a phase modulator connected with a coaxial cable to a *waveform generator*. The output fibers of the PBS close up in the phase modulator creating a closed path for the incoming photons. Photons entering the second FP are injected into the PBS constituting the input of the Sagnac loop, and here their $|H\rangle$ and $|V\rangle$ components are separated into the two output ports, entering the *slow axis* of each branch. This last detail is essential to map the polarization degree of freedom onto the optical path of the photons.

Now what happens is simple but deep. The light with $|H\rangle$ polarization travel in the counterclock-wise (CCW) direction while the $|V\rangle$ polarized light follows the clock-wise (CW) path. In the CW direction each photon encounter a *delay line* before entering the phase modulator, thus acquiring a "late" (L) phase ϕ_L to its original phase state. To complete the loop the photon perform the remaining path entering again in the PBS from the opposite port. Reversely, a photon travelling in the CWW direction crosses the phase modulator, gaining an "early" phase ϕ_E and then enters the delay line before being recollected again at the PBS port.

Photons travelling in the two opposite directions are gathered by the PBS in the opposite axis with respect to the initial ones, and this phenomenon allow to compensate any additional phase introduced in the single branch of the fiber-based PBS. The final state resulting from this transformation is thus expressed as

$$\left|\psi_{out}^{\phi_E,\phi_L}\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i(\phi_L-\phi_E)}|V\rangle\right). \tag{4.7}$$

The interesting feature that can be inferred from Eq. (4.7) is that by properly timing the voltage applied on the phase modulator, it is possible to generate every attainable state in the equator of the Bloch sphere. In particular, the three states of interest can be decoded according to the following choices of phases:

$$\left|\psi_{out}^{0,0}\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{0}|V\rangle\right) = |D\rangle \tag{4.8}$$

$$\left|\psi_{out}^{\frac{\pi}{2},0}\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{-i\frac{\pi}{2}}|V\rangle\right) = |L\rangle \tag{4.9}$$

$$\left|\psi_{out}^{0,\frac{\pi}{2}}\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\frac{\pi}{2}}|V\rangle\right) = |R\rangle \tag{4.10}$$

It is important now to focus the attention on the portion of the transmitter that guarantees the encoding of a secure key to be distributed. It must be premised that in a standard QKD protocol the presence of a Quantum Random Number Generator (QRNG) is essential in order to ensure the highest possible level of security, since the generation of a completely non deterministic sequence of symbols (usually called *randomness seed*) is required to distill an exploitable longer random key. However this condition is not mandatory for the success of this analysis, which scope is to determine the feasibility of a new QKD alternative, and for the sake of simplicity and effectiveness, the random stream has been substituted by a deterministic, predetermined string of symbols, based on the alphabet $\{|H\rangle, |V\rangle, |D\rangle\}$.
This goal is achieved with the help of a *waveform generator*, a machinery that generates a custom voltage function on the basis of specific parameters given at its input. The generated waveform is applied at the control ports of the phase modulator in order to pilot the encoding process.

To be more precise, the sequence of steps is the following. A small fraction of the pulsed signal generated by the light source is fiber coupled and detected by a photodiode, which generates an electric signal at 76 $[MHz]$, given then in input at a Field Programmable Gate Array (FPGA). This device contains an IP (Intellectual Property) Core named *clock wizard* whose role is to convert the 76 $[MHz]$ electric signal into a different one at 10 $[MHz]$, maintaining a constant phase relation between the two envelopes. The signal at 10 $[MHz]$ is therefore used to lock the waveform generator clock via a Phase

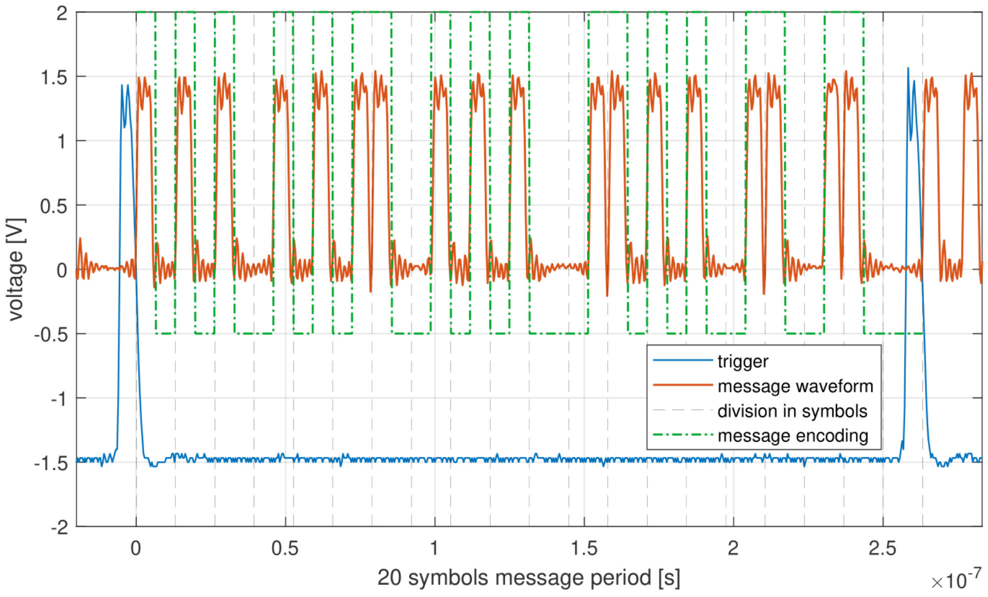


Figure 4.7: Waveform generated encrypting a pseudo-random message in a stream of twenty pulse-period, according to a simple "shape" encoding. The statistics of the choice of the bases are 90% for the basis $\mathbb{Z}$ and 10% for the basis $\mathbb{X}$. In the $\mathbb{Z}$ basis the symbols $|H\rangle \, and \, |V\rangle$ have the same probability to be chosen.

Lock Loop (PLL). Moreover, the FPGA produces an additional signal at 76 $[kHz]$ that behaves has a trigger to the waveform generator to avoid possible relative phase drifts between the pulsed laser source and the waveform generator itself.

The developed system thus designed allows to create the electric signals required to yield the desired encoding with the appropriate timing. Is hence possible to encode the states $\{|L\rangle\,, |R\rangle\,, \text{and } \, |D\rangle\}$ starting from a string whose elements are $\{|H\rangle\,, |V\rangle\,, \text{and } \, |D\rangle\}$.

An example showing the output signal produced by the waveform generator can be observed in Fig. 4.7. In this example it is shown the practical encoded message:

$$|H\rangle\,|H\rangle\,|H\rangle\,|V\rangle\,|V\rangle\,|V\rangle\,|H\rangle\,|V\rangle\,|V\rangle\,|V\rangle\,|D\rangle\,|V\rangle\,|H\rangle\,|H\rangle\,|H\rangle\,|V\rangle\,|H\rangle\,|V\rangle\,|H\rangle\,|D\rangle\,.$$

The strategy chosen to encode the symbols $|H\rangle$, $|V\rangle$ and $|D\rangle$ is based on a simple choice of the position of each laser pulse inside its period. In Fig. 4.8 is represented a detail of the waveform representing the symbols $|H\rangle$ and $|V\rangle$, while for the symbol $|D\rangle$, for which the waveform path is individuated by a low-level voltage in the entire pulse period, is

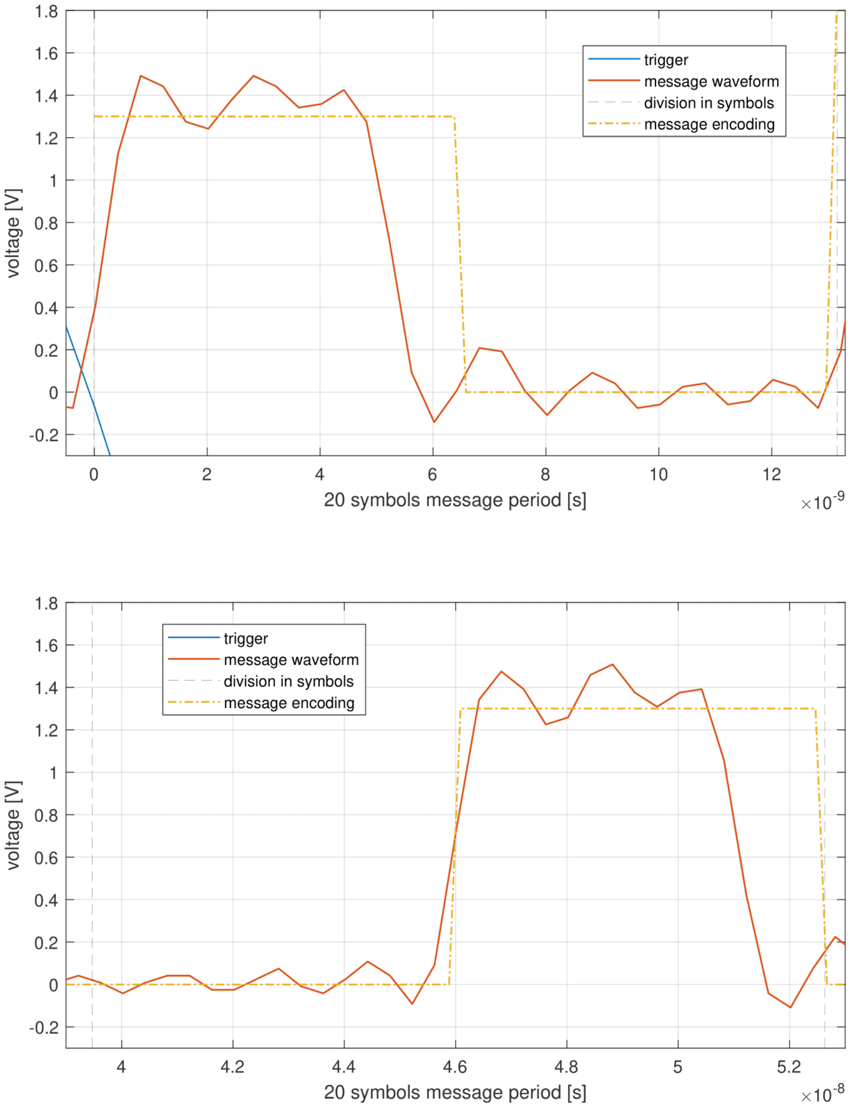


Figure 4.8: Encoding strategy for the two symbols $|H\rangle$ and $|V\rangle$. The entire period of about 13.158 $[ns]$ is divided into two windows. If the pulse is positioned in the first half the encoded symbol is $|H\rangle$ while if the pulse is found in the second half of its period, the associated symbol is $|V\rangle$. It has been omitted for simplicity the $|D\rangle$ state representation, which is simply the absence of the pulse inside its period.

omitted.

Light exiting the Saganc interferometer returns to the initial free-space BS in order to be routed from the output of the transmitted branch to the following steps. Again, the reflected component is discarded, introducing the main limitation of this setup, that is the attenuation of about 6 $[dB]$ of power just in the double crossing of the BS.
After this processing, photons cross a cascade of HWP and QWP properly tuned in order to convert the $|R\rangle$ ($|-j\rangle$) and $|L\rangle$ ($|+j\rangle$) states into $|H\rangle$ and $|V\rangle$. On the contrary, the $|D\rangle$ state remains unchanged after this rotation, enabling the protocol to work properly.

Finally, by means of a *silver mirror* the optical signal is carried through the next stage of the Alice transmitter, that is the encoding converter.

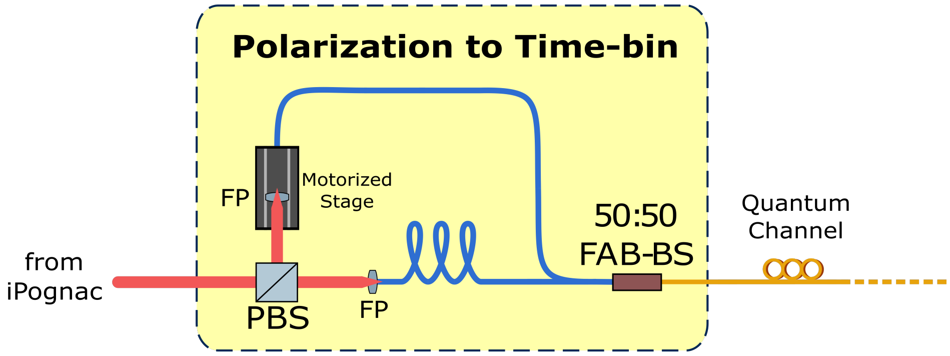


Figure 4.9: Scheme of the encoding converter, from polarization to time-bin. PBS: polarizing BS, FP: fiber port, FAB-BS: Fast-Axis-Blocking BS, Single mode fibers are in *yellow*, polarization maintaining fibers are in *blue*, free-space optical path is in *red*.

4.3 Polarization to Time-Bin Converter

The final node of the Alice apparatus is crucial to guarantee the feasibility of the protocol since, as already anticipated, polarization of quantum states propagating through an optical fiber is altered by mechanical and thermal stress suffered by the fiber along its length, while a strategy based on time-bin encoding is immune to it.

This task is performed by the usage of a PM fiber-based *unbalanced Mach-Zender interferometer* (UMZI), where the input element is constituted by a free-space PBS, which assigns two different paths to the horizontal and vertical components of the input photons. In particular, as can be observed in Fig. 4.9, the horizontally polarized light once transmitted by the PBS is collected by a dedicated steady fiber port, that solves the opposite role with respect to the one seen at the input of the iPognac. The vertically polarized light is instead reflected toward a movable fiber port mounted on a *motorized stage*, whose direction of motion is aligned with the outlet direction of the exiting light.
At this point the two components of light are collected by the respective fiber ports into two separated PM fibers. Before being recombined in a 50:50 Fast-Axis-Blocking BS, one of the two branches, in particular the one collecting the $|H\rangle$ polarized photons, is connected to a delay line of $\Delta L^A = 0.5\ [m]$ of length, therefore introducing an amount of delay of

$$\Delta\tau^A = \frac{\Delta L^A \cdot n}{c} \approx 2.5\ [ns] \tag{4.11}$$

with respect to the $|V\rangle$ polarized particles.

The mapping function resulting by the link of the horizontal and vertical components of light into the early and late time slots of the two dimensional tim-bin encoding can be described as

$$\alpha |H\rangle + \beta |V\rangle \longrightarrow e^{i\phi_A}\alpha |E\rangle + \beta |L\rangle \tag{4.12}$$

where ϕ_A represents the intrinsic (and unavoidable) phase of Alice's UMZI, while $|E\rangle$ and $|L\rangle$ are respectively the "early" and "late" time-bin states in the time-bin encoding. From this setup it is possible to encode also the diagonal state as the superposition of the two time-bin states as

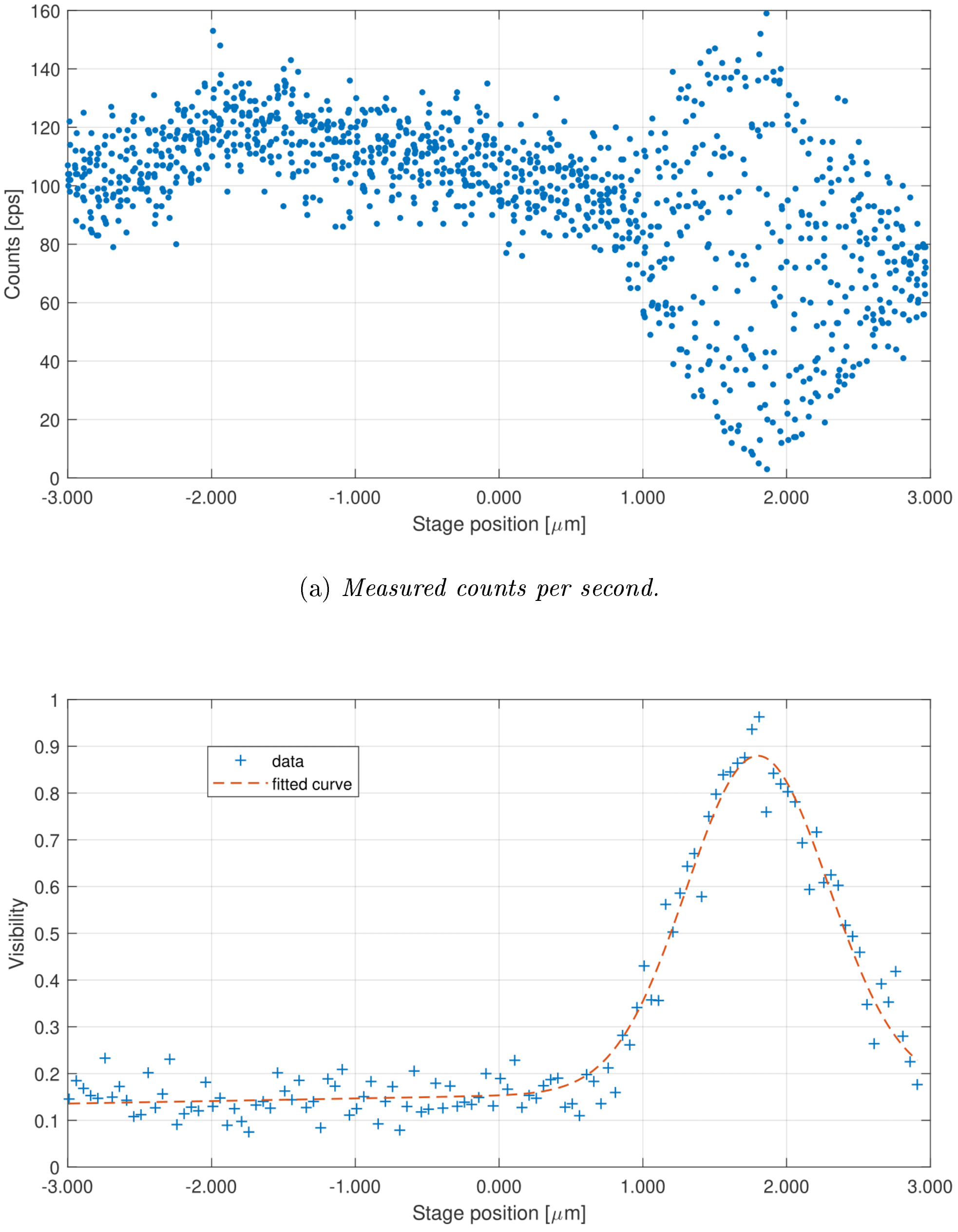
$$|D\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle + e^{i\phi_A}|E\rangle\right). \tag{4.13}$$

With the tools developed so far it is possible to implement the 3-state BB84 protocol, assuming the generation basis to be $\mathbb{Z} = \{|E\rangle, |L\rangle\}$ and the control state as $|D\rangle$.

Returning to the discussion over the implementation of the motorized stage, it has demonstrated of paramount importance in the development of the final setup. As a matter of fact, after some preliminary measurements it has appeared clear that the realization of the encoding converter as it was exploiting two fixed fiber ports was not sufficient to make the two components interfere at the receiver properly. It is our idea that even if the exploited optical components are manufactured to being used in high precision applications, the accuracy in some specific parameters as the length of the fibers or the dimensions of the splices is not enough to achieve micrometric assurance.

The strategy exploited to reach the desired level of precision has been to keep the encoding converter placed at the receiver unchanged, exploiting instead at the transmitter the degree of freedom introduced by the path distance between the $|V\rangle$ output of the BS and the relative fiber port.

This task has been carried out exploiting a *Phyton code* useful to control the motorized stage and simultaneously to measure the interference. The two interfering pulses have been measured at the outputs of a PBS collecting the signal exiting the cascade of both Alice and Bob encoding converters. The result is pictured in Fig. 4.10 and shows the measured interference as the detected number of counts (of the central peak, see Chapter 5 for more details) (a) and the visibility ((b), Eq. (4.4)) as a function of the stage position. Finally the stage has been placed at the position ensuring the maximum possible inter-



(a) *Measured counts per second.*

(b) *Visibility diagram.*

Figure 4.10: Interference studied in a range of 6 [μm] around the initial position of the stage.

ference.

It is worth mentioning that the polarization degree-of-freedom contains no more information once the photons exit the conversion system, passing from polarization to time-bin and gaining the same state of polarization. This is of fundamental importance for the reliability of the protocol, and it is achieved by exploiting the 50:50 FAB-BS. This device has the feature to suppress polarization states that are aligned to the fast axis of the input PM fiber, working similarly to a polarizer.

By way of conclusion, once the message has been encrypted in the time-bin encoding, all that remains is to transmit the key to the receiver (Bob). To have a better estimation of the performances of the protocol, the quantum channel that allows the communication between Alice and Bob is represented by a 50 meters of a single mode optical fiber connecting the two facilities of the Quantum Future laboratory in which are places the source and the receiver.

5 Bob Station

In this chapter it is discussed the setup constituting Bob apparatus, focusing in particular in the concrete realization, optimization and characterization of the passive receiver, necessary to operationalise it.

Bob station is composed by the "time-bin to polarization" encoding converter, followed by the proper receiver, which is able to redirect the four quantum states used for *key generation* and *control* towards the dedicated photon detectors (SNSPDs). As it will be discussed below, the latter is combined with an high-precision time-to-digital converter (TDC), capable of returning accurate information about the time of arrival of each single photon. These data are useful for the required post-processing analysis in order to retrieve an estimation about the security of the protocol. Subsequently, it will be possible to recover the key sent by Alice according to the process of *information reconciliation.*

5.1 Time-bin to Polarization Converter

The first component of Bob apparatus is an UMZI exploited as an encoding converter, formally identical with respect to the one implemented in the Alice setup. The only difference relies in the fact that it is used in reverse configuration, in the sense that light enters the encoding converter through the 50:50 FAB-BS and exits from the PBS. The only difference compared to the previous layout consists in the absence of an extendable delay line, since the adaptation to make the pulses interfere has already been accomplished previously.

Basically, photons entering the 50:50 FAB-BS are split equally between the two arms constituted by two PM fibers. One of these two branches is directly linked to a fiber-based PBS, while the other one is extended by means of a delay line introducing the

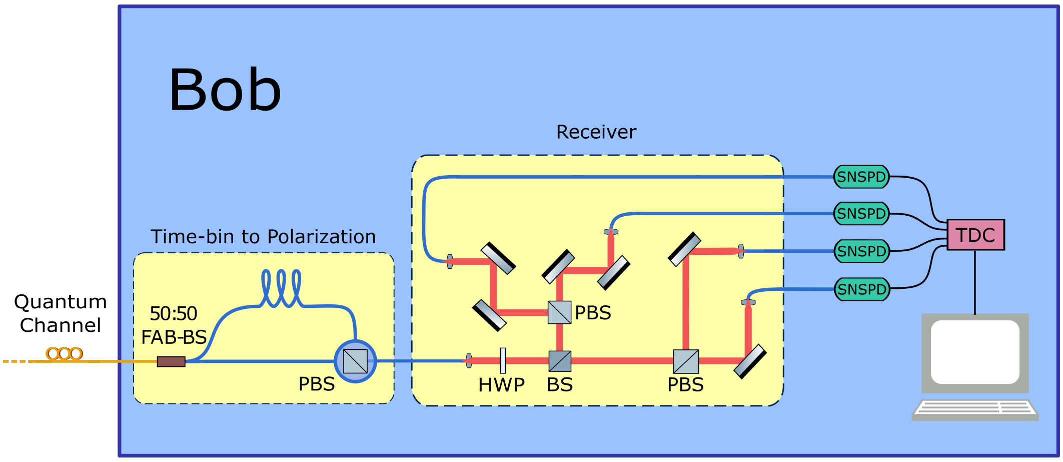


Figure 5.1: Schematic representation of the receiver setup (Bob). The apparatus is composed by the encoding converter (from time-bin to polarization) and the passive receiver together with the detection system.

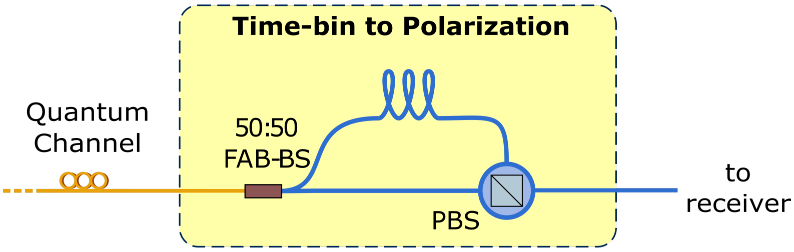


Figure 5.2: Scheme of the encoding converter, from time-bin to polarization. PBS: polarizing BS, FAB-BS: Fast-Axis-Blocking BS, Single mode fibers are in *yellow*, polarization maintaining fibers are in *blue*.

same amount of temporal delay as in Alice case, formally

$$\Delta L^B = 0.5\ [m] \implies \Delta\tau^B \approx 2.5\ [ns], \tag{5.1}$$

before being routed to the same PBS. A the PBS downstream, used in this case in a reverse configuration, light distributes inside the output PM fiber with horizontal or vertical states of polarization according to the path covered inside the UMZI. A detail of the scheme is pictured in Fig. 5.2.

It is interesting to notice that the temporal unbalance introduced progressively first from Alice's UMZI and then from Bob's, temporally distributes the light in the three-peaks configuration characteristic of the time-bin encoding, as can be seen for example in [25, 26, 27].

Therefore, the states exiting the Bob encoding converter have the following shape

$$|E\rangle \quad \longrightarrow \quad |\Psi_E\rangle = \frac{1}{\sqrt{2}}\big(|EE\rangle \otimes |V\rangle + e^{i\phi_B}\,|EL\rangle \otimes |H\rangle\big) \tag{5.2}$$

$$|L\rangle \quad \longrightarrow \quad |\Psi_L\rangle = \frac{1}{\sqrt{2}}\big(|LE\rangle \otimes |V\rangle + e^{i\phi_B}\,|LL\rangle \otimes |H\rangle\big) \tag{5.3}$$

$$\begin{aligned} |D\rangle \quad \longrightarrow \quad |\Psi_D\rangle = \frac{1}{\sqrt{2}}(&|EE\rangle \otimes |V\rangle + e^{i\phi_B}\,|EL\rangle \otimes |H\rangle \\ &+ e^{i\phi_A}\,|LE\rangle \otimes |V\rangle + e^{i(\phi_A+\phi_B)}\,|LL\rangle \otimes |H\rangle) \end{aligned} \tag{5.4}$$

where the two states in Eq. (5.2) and Eq. (5.3) are obtained when Alice transmits respectively "Early" and "Late", while Eq. (5.4) refers to the result of Alice sending the $|D\rangle$ state. Obviously, ϕ_B represents the intrinsic phase introduced by the Bob's encoding converter.

An expressive representation of the states before and after the passage through the Bob's UMZI is pictured in Fig. 5.3.

With reference to Eq. (5.2), Eq. (5.3), Eq. (5.4) and Fig. 5.3 the writings $|EE\rangle$ and $|LL\rangle$ indicates the laterals peaks correspondent to photons travelling along respectively short and long paths of both Alice's ans Bob's UMZI. The arrival time of the these outer

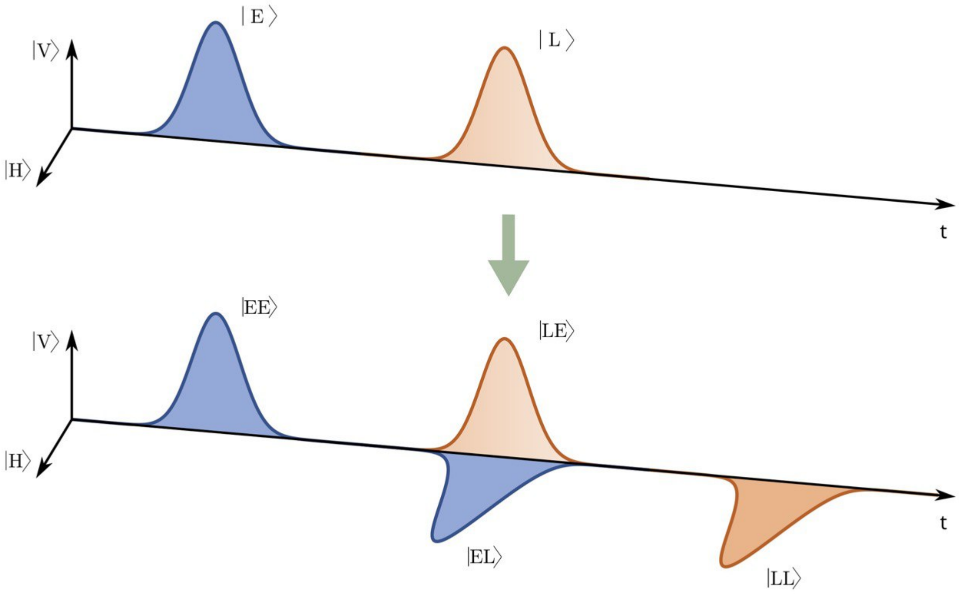


Figure 5.3: States at the input and output of the Bob's time-bin to polarization encoding converter (UMZI). Blue and orange curves represent the two possible time-bin encoding chosen at the Alice side. Visualizing the pulses in the two polarization planes ($|H\rangle$,$|V\rangle$) in just one plane allows to retrieve the pulses associated with the key basis (lateral peaks) and the ones for the control basis (central peak).
By kind permission of Scalcon D., Agnesi C. [25].

peaks is measured in the $\mathbb{Z}$ basis and therefore they are used for the secret key generation. The probability of measuring in this basis is 50% since approximately half of the light contributes to create the lateral peaks.

On the contrary the central peak contains the superposition of the two indiscernible states $|LE\rangle$ and $|EL\rangle$, and the information about the relative phase between them is encrypted in their polarization state.

Of great importance in the future analysis is the state of polarization of this central peak once Alice transmits the $|D\rangle$ state, described as

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle + e^{i\theta} |V\rangle \right), \tag{5.5}$$

where $\theta = \phi_A - \phi_B$ represents the phase difference between the transmitter and receiver UMZIs. As a matter of fact, the central peak is indispensable to control the level of secrecy of the shared key. As anticipated, this work discusses a three-states protocol, even if this appellation refers only to the strategy of encoding chosen by Alice. On the Bob side all the three bases in the Bloch sphere are exploited. In particular, the $\mathbb{Z}$ basis is used to extract the key by the observations performed over the lateral peaks of each triad, while the $\mathbb{X}$ and $\mathbb{Y}$ bases are required for the estimation of the security parameter C considering the central peaks. These two procedures can be performed in parallel, enhancing the versatility of this protocol.

At this point photons have retrieved their information about the polarization, and they are suited to be collected by the passive receiver.

5.2 The Receiver

The receiver discussed in this section and placed at the end of the communication link is the spearhead of this innovative protocol since it has been assembled to merge the versatility of a RFI system together with the robustness typical of the hybrid encoding, firstly proposed in [25]. As it has been already anticipated, it is fully passive, thus not requiring any effort in performing active control over the communication channel in order to collect interpretable data.

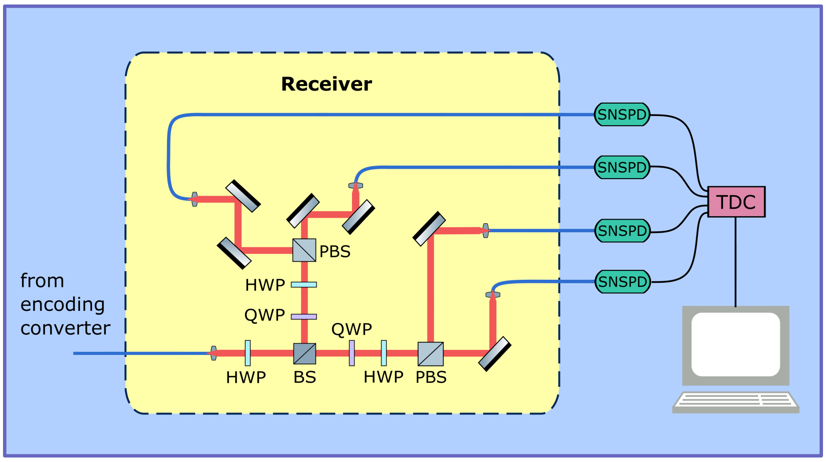


Figure 5.4: Scheme of the encoding converter, from polarization to time-bin. BS: beam splitter, PBS: polarizing BS, HWP: half-wave plate, QWP: quarter-wave plate, SNSPD: superconducting nanowire single photon detectors, TDC: time-to-digital converter. Polarization maintaining fibers are in *blue*, free-space optical path is in *red*.

Since this component has been fully designed and built during this traineeship, involving a great deal of effort, it is worth to describe both the layout and the characterization that give this device the robustness that shows to have.

5.2.1 Layout

A schematic representation of the receiver is displaced in Fig. 5.4. In its core it is based on a free space optical circuit that has the goal to route every photon toward the proper receiver, in order to build the right statistics concerning the encoded polarization.

Light exiting the Bob's interferometer is coupled in the fast and slow axes of the PM fiber, according to the amount of $|H\rangle$ and $|V\rangle$ components that superimposing represent it, in relation to the formal description given in Eq. (5.5). The PM fiber connecting the UMZI and the receiver is fundamental in order to guarantee the maintenance of the information, that now it is kept in the polarization state of each photon.

Once entered inside the receiver light is rotated in its polarization by a HWP in order to compensate the relative rotation between the slow and fast axes of the PM fiber and the $|H\rangle$ and $|V\rangle$ axes of the receiver[1].

At this point the beam enters a free space BS that randomly divides it in two different paths. This object plays a key role in the implementation of the BB84 protocol: it

[1] This HWP could be simply substituted by an input collimator mounted on a rotatable holder.

describes the attempt of randomly selecting the measurement basis in order to provide the intrinsic security of a *prepare and measure* procedure. To be more precise, the RFI approach requires the necessity to accumulate enough statistics in both the $\mathbb{X}$ and $\mathbb{Y}$ bases, and this is achieved exploiting this BS. Transmitted photons are thus steered towards the branch of the receiver responsible to measure the photons in the $\mathbb{X}$ basis, while the reflected photons are directed to the other side of the setup where the $\mathbb{Y}$ basis is exploited as a measurement basis.

Each section of the receiver in which the measurement is performed is constituted by the concatenation of a QWP, a HWP and a free space PBS, which allows to retrieve any quantum states in the surface of the Bloch sphere. In particular, if proper adjusted, the combination of these two wave plates together with the polarizing BS grants to perform a projective measurement on the incoming photons. As a matter of fact, each of the output branches of the two PBSs will be associated to a specific *projector* $\hat{\Pi}_j$ (more details will be provided below).

At the end of these four paths light is then collected by variable focus collimators, that help the beams to be injected in the respective single mode optical fibers in order to be driven to the SNSPDs. At this point the optical network formally ends. The next few steps belong to the analysis process.

Each SNSPD behaves as a trigger device, heralding the presence of a single photon with a *detection efficiency* grater than 80%, a *timing jitter* at most of 50 $[ps]$ (see Fig. 5.5), a *dark count rate* smaller than 1 $[Hz]$ and a *recovery time* not exceeding 80 $[ps]$[2].

The voltage signals associated with the measured arrivals are then collected by the TDC, which assigns at each detection the absolute time in which each measured photon has been spotted.

From the data collected at this step it is possible to perform any desired post-processing algorithm.

[2] See https://marketing.idquantique.com/acton/attachment/11868/f-023b/1/-/-/-/-/ID281_Brochure for more details.

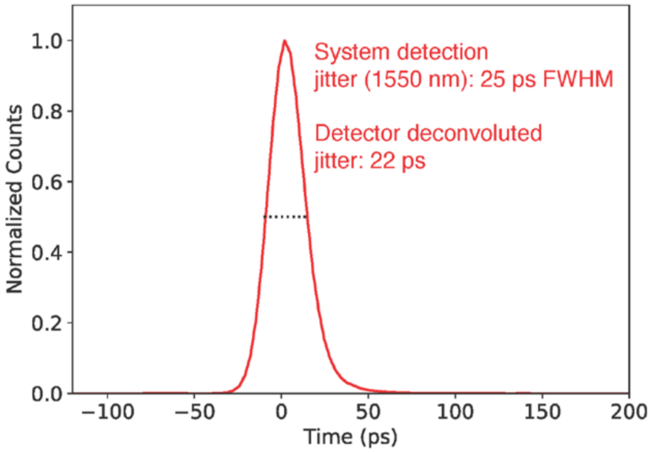


Figure 5.5: Jitter retrieved from the Gaussian fit over the detected counts (normalized) per picosecond.

5.2.2 Characterization

Once the setup has been assembled, an important passage that must be accomplished in order to make the receiver work properly consists in its characterization, and in particular in the derivation of the four projectors associated to its measurement arms.
This procedure is organized in two steps, and for both of them the usage of a polarimeter (see Chapter 3) is required, since it is capable of returning the specific polarization parameters related to the measured photons, and therefore giving a useful reference for the calibration of the device.

Firstly, it is necessary to position the wave plates downstream the first BS such that they rotate properly an input horizontally polarized light in the desired state of polarization. To do so the calibration has to be made in backward direction for each branch, injecting a light beam into the output collimator and rotating the correspondent wave plates such that at the polarimeter (positioned in place of the input collimator) it is measured the expected state of polarization.

Secondly, once the wave plates positions are set, two additional wave plates are required in between the input HWP and the BS. These two consist of a QWP followed by a HWP mounted on two *motorized rotators* and driven by an electromechanical actuator, in order to retrieve any desired state of polarization with high precision and fine positioning. Essentially, the idea is to take trace of certain combination on the positions of the two motorized wave plates, monitoring their adjustments by means of the polarimeter placed next to them and recording the related angular positions, such that the specific input polarization states can be retrieved smoothly. Once the settings are registered for each input polarization state, the polarimeter can be removed and the receiver can be characterized. The following step is indeed to inject every polarization state, one at a time, and for each case to measure with the four SNSPDs the amount of photons collected at each output in order to retrieve a correlation between the probability a photon enters a specific detector and the state of polarization injected at the input of the receiver.

5.2.3 Computation of the Projectors

The *modus operandi* by means of which the four projectors are reconstructed makes use of a procedure similar to the optimization problem introduced in Reference Frame Independence, exploiting the same `CVX` tool offered by `MATLAB`, with some corrections with respect to the minimization utilized for the computation of the C parameter.

Unlike what was done previously in [17], where *a priori* known statistics of the compatible POVM of Alice and Bob was assumed, in this work the goal has been to retrieve these parameters directly from the designed setup, acquiring more detailed information about the developed apparatus and simultaneously providing an accurate description of the situation under study.

For this purpose, measurements on both polarization and photon counts have been taken, in the same procedure explained above.

The minimization problem can be computed considering ten different input states of polarization, as

$$|H\rangle\,, \quad |V\rangle\,, \quad |D\rangle\,, \quad |A\rangle\,, \quad |L\rangle\,, \quad |R\rangle\,, \quad |\phi_1\rangle\,, \quad |\phi_2\rangle, \quad |\phi_3\rangle, \quad |\phi_4\rangle \tag{5.6}$$

where the last four are generic states in the surface of the Bloch sphere chosen at random, represented in Fig. 5.6 for clarity. By means of Eq. (2.10) it is possible to retrieve the density matrices of the ten input states exploiting the Bloch coordinates s_1, s_2, s_3, whose values are obtained computing the mean over the measures taken for each of these parameters.

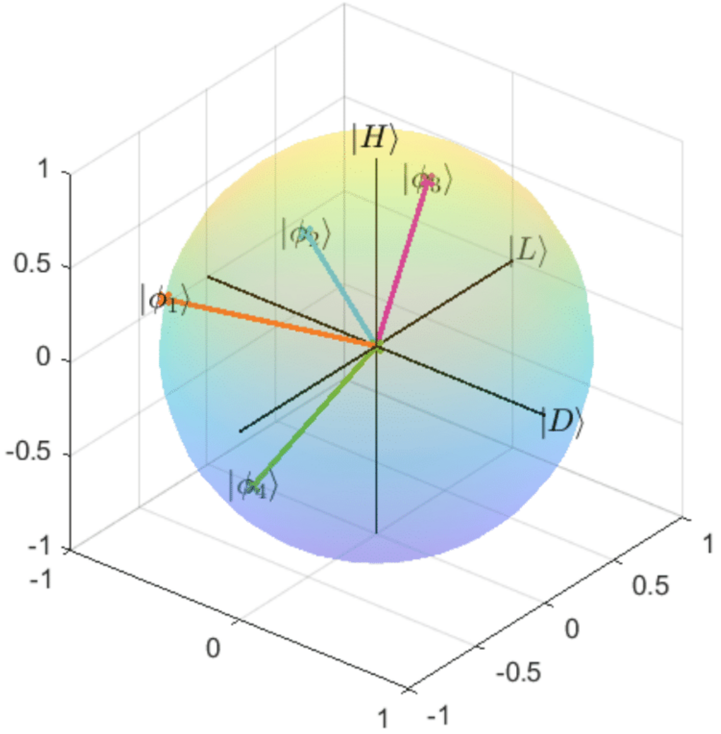


Figure 5.6: 3D representation of the discussed vectors $|\phi_1\rangle$, $|\phi_2\rangle$, $|\phi_3\rangle$, $|\phi_4\rangle$ in the Bloch sphere.

The next step is the adjustment and the estimation of the four output collimators in the receiver setup such that the highest possible value can be reached. This is achieved by measuring the optical power before and after the device, according to the formula

$$\eta_{collimator} = \frac{P_{out}}{P_{in}} \tag{5.7}$$

where the notation is not misunderstandable. The measured value of the coupling efficiency at the four collimators has been $\eta \approx 0.75$. From the knowledge of this parameter it is possible to retrieve the amount of losses intrinsic in the coupling of light from the free space path to the core of the optical fibers headed to the photon detectors, and therefore estimate the intensity of the photon flux travelling the receiver as

$$\tilde{P}_{in} = \frac{P_{out}}{\eta}. \tag{5.8}$$

Finally, the output probabilities of measuring the ten input states at each SNSPD can be simply calculated as follows

$$p_{|\psi\rangle,\hat{\Pi}} = \frac{P_{|\psi\rangle,\hat{\Pi}}}{\sum_{k}^{L,R,D,A} P_{|\psi\rangle,\hat{\Pi}_k}} \tag{5.9}$$

where $|\psi\rangle$ stands for the $n-th$ generic transmitted state received by Bob, while $\hat{\Pi}$ indicates the chosen projector on which measure the received state.
According to the Born rule, that for this specific approach can be rewritten as

$$Tr\left[\hat{\rho}_n \hat{\Pi}_k\right] = p_{|\psi_n\rangle,\hat{\Pi}}, \tag{5.10}$$

it is now possible to perform a minimization computation to retrieve the POVMs.

Indeed, the problem translates as

$$\underset{\hat{\Pi}_k}{\texttt{minimize}}: \quad \sum_n \sum_k \left(Tr\left[\hat{\rho}_n \hat{\Pi}_k\right] - p_{|\psi_n\rangle,\hat{\Pi}} \right) \tag{5.11}$$

$$\texttt{subject to} : \begin{cases} \hat{\Pi}_L + \hat{\Pi}_R + \hat{\Pi}_D + \hat{\Pi}_A = \hat{\mathbb{1}} \\ \hat{\Pi}_k^\dagger = \hat{\Pi}_k \quad \forall k \\ Tr\left[\hat{\Pi}_k\right] \geq 0 \quad \forall k \\ det\left[\hat{\Pi}_k\right] \geq 0 \quad \forall k \end{cases}$$

that describes the intent of computing the POVMs that minimize the difference between the theoretical probability derived by Eq. (5.10) and the experimental one (Eq. (5.9)) considering four different constraints. Firstly, the four POVMs must respect the normalization condition in order to empower the physical meaning. Secondly, they must be Hermitian in order to be an *observable*. Furthermore, the POVMs must be *semidefinite positive*, and this is guaranteed by the last two constraints.

This procedure will at the end return a mathematical description of the four projectors $\hat{\Pi}_L$, $\hat{\Pi}_R$, $\hat{\Pi}_D$ and $\hat{\Pi}_A$.

The passive receiver is thus fully characterized, giving a detailed description of the behaviour of the post-selection measurement performed by Bob in the estimation of the secrecy of the distribute quantum key.

6 Experimental Tests

The calibration of the setup analysed in Chapter 4 and Chapter 5 has required several time and continuous adjustments during the last months. Basically, the absence of isolated test rooms and the constant presence of personnel in the laboratory facilities for the executions of parallel experiments have not guaranteed a secluded environment. However this approach of refinement has allowed to better understand the criticalities and the weak points of this protocol, giving in some cases the possibility to directly improve it.
In this connection, an example can be represented by the substitution of the pulsed laser source. Initially the choice fell on an integrated DFB (Distributed Feedback) laser source (`AA0701 Series` by `G&H`), pulsed by a cascade of three operational amplifiers and driven by a dedicated FPGA. This architecture allowed to generate pulses of hundreds of picoseconds of width at a repetition rate of $R \approx 50\ [MHz]$.
Taking advantage of a failure of the DFB laser, some measurements have been thus taken with the `Mira` laser, and this has revealed indeed that a higher accuracy could be reached with pulses about two orders of magnitude shorter. This change in the choice of the laser source has required a modification in the Alice's UMZI setup, like the introduction of the movable stage as discussed previously.
A general framework of the approach followed to conclude this study is explained in the following pages.

This chapter is subdivided into two blocks. In the first one it will be presented the first relevant experimental test, performed exploiting a CW light source. This experience has returned the most promising results in terms of feasibility of the protocol, assessing the correctness of the pursued methodology. The second part will treat the final data-taking, executed utilizing the formerly mentioned pulsed laser source. This last observation has led to some less satisfactory results, which will be adequately handled in the next chapter.

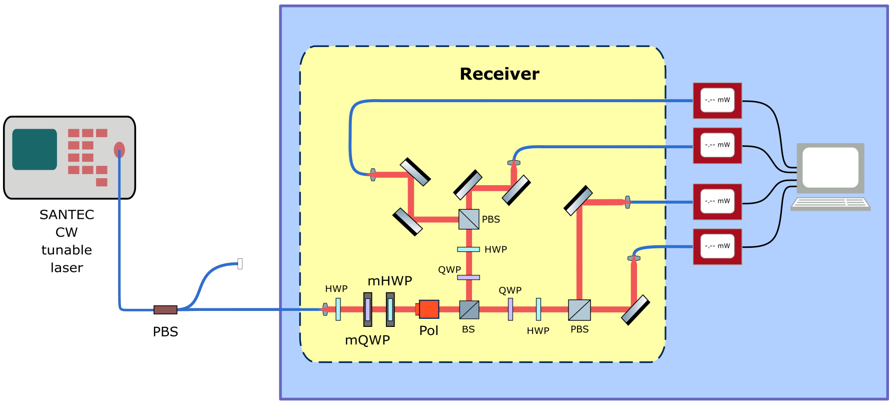


Figure 6.1: Scheme of the characterization setup considering a CW signal. BS: beam splitter, PBS: polarizing BS, HWP: half-wave plate, QWP: quarter-wave plate, mQWP/mHWP: mortorized-QWP/HWP, Pol: polarimeter. Polarization maintaining fibers are in *blue*, free-space optical path is in *red*. The four devices depicted at the outputs of the receiver, connected to the external computer, are Thorlabs power meters (Chapter 3).

6.1 CW laser source

The first phase of the experimentation consists in the characterization of the POVMs of the receiver, with the same procedure listed in Section 2.2 and Section 2.3. A useful schematic representation is depicted in Fig. 6.1.

A cw signal emitted from the Santec laser (Chapter 3) at 1550 $[nm]$ is made pass through an external PBS, which guarantees that its polarization is completely horizontal, before being injected in the input collimator of the passive receiver. The initial HWP is already positioned at the proper orientation that makes a generic $|H\rangle$ state entering the receiver to acquire exactly 50% of probability to be transmitted or reflected at the first BS. With respect to the original configuration, a QWP and a HWP are mounted in this order in two motorized rotators, that enables a fine tuning in their rotation. These two devices are then followed by a polarimeter that, as already anticipated, performs instantaneous visualization and measurements on the polarization states of the impinging photons. At this point it is sufficient to derive the proper orientation of the two rotatable wave plates in order to generate each desired input state.

For this study the chosen states are the one listed in Eq. (5.6), and the corresponding density matrices associated with these quantum states are

$$\hat{\rho}_{|H\rangle} \approx \begin{pmatrix} 1.000+0.000i & 0.000+0.000i \\ 0.000+0.000i & 0.000+0.000i \end{pmatrix}, \quad \hat{\rho}_{|V\rangle} \approx \begin{pmatrix} 0.000+0.000i & 0.000+0.000i \\ 0.000+0.000i & 1.000+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|D\rangle} \approx \begin{pmatrix} 0.500+0.000i & 0.500+0.000i \\ 0.500+0.000i & 0.500+0.000i \end{pmatrix}, \quad \hat{\rho}_{|A\rangle} \approx \begin{pmatrix} 0.500+0.000i & -0.500+0.000i \\ -0.500-0.000i & 0.500+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|L\rangle} \approx \begin{pmatrix} 0.452+0.000i & 0.001+0.498i \\ 0.001-0.498i & 0.548+0.000i \end{pmatrix}, \quad \hat{\rho}_{|R\rangle} \approx \begin{pmatrix} 0.465+0.000i & 0.000-0.499i \\ 0.003+0.499i & 0.535+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|\phi_1\rangle} \approx \begin{pmatrix} 0.881+0.000i & 0.281-0.161i \\ 0.281+0.161i & 0.119+0.000i \end{pmatrix}, \quad \hat{\rho}_{|\phi_2\rangle} \approx \begin{pmatrix} 0.269+0.000i & 0.372-0.242i \\ 0.372+0.242i & 0.731+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|\phi_3\rangle} \approx \begin{pmatrix} 0.395+0.000i & -0.321+0.369i \\ -0.321-0.369i & 0.605+0.000i \end{pmatrix}, \quad \hat{\rho}_{|\phi_4\rangle} \approx \begin{pmatrix} 0.387+0.000i & -0.273+0.403i \\ -0.273-0.403i & 0.613+0.000i \end{pmatrix}$$

computed considering the Stokes coordinates s_1, s_2, s_3 derived as the mean of a 30 seconds measurement for each input state[1]. These results are in line with the expected results, demonstrating that the receiver is finely calibrated.

The probabilities associated with these input states considering the four possible projective measurements that Bob can performs are reported in Table 1.

With these information the last step is essentially the acquisition of the power at the four photon detectors while they measure the light at the end of the receiver, for each set of the two motorized wave plates, and therefore for each input state. A graphical description of the procedure here proposed is sketched in Fig. 6.2.

[1] The conversion from Stokes vectors to Jones vectors, useful for the Bloch sphere representation, has been performed after a change of reference frame, from Cartesian to spherical.

	Measurement POVM			
Input states	$\hat{\Pi}_L$	$\hat{\Pi}_R$	$\hat{\Pi}_D$	$\hat{\Pi}_A$
$\|H\rangle$	0.226	0.276	0.245	0.274
$\|V\rangle$	0.211	0.256	0.264	0.269
$\|L\rangle$	0.447	0.001	0.263	0.289
$\|R\rangle$	0.000	0.482	0.246	0.272
$\|D\rangle$	0.207	0.265	0.528	0.000
$\|A\rangle$	0.200	0.244	0.001	0.554
$\|\phi_1\rangle$	0.154	0.260	0.365	0.122
$\|\phi_2\rangle$	0.110	0.289	0.431	0.070
$\|\phi_3\rangle$	0.379	0.067	0.096	0.458
$\|\phi_4\rangle$	0.387	0.049	0.123	0.442

Table 1: Probabilities for each combination of input states and applied POVMs, computed considering Eq. (5.9).

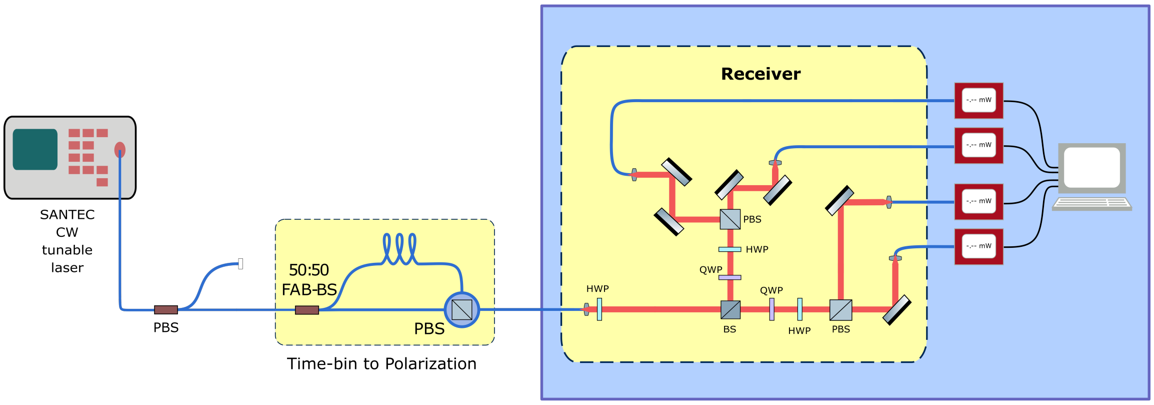


Figure 6.2: Scheme of the measurement setup considering a CW signal.

From the power data is thus trivial to compute the statistics, as it has been explained in Eq. (5.9).

Finally it is possible to retrieve the accurate description of the four POVMs distinctive of the passive receiver thus configured, applying the mathematical minimization outlined in Eq. (5.11). The results obtained after this process are therefore

$$\hat{\Pi}_{|L\rangle} = \begin{pmatrix} 0.253+0.000i & -0.003+0.259i \\ -0.003+0.259i & 0.265+0.000i \end{pmatrix} \tag{6.1}$$

$$\hat{\Pi}_{|R\rangle} = \begin{pmatrix} 0.282+0.000i & -0.006+0.264i \\ -0.006-0.264i & 0.254+0.000i \end{pmatrix} \tag{6.2}$$

$$\hat{\Pi}_{|D\rangle} = \begin{pmatrix} 0.225+0.000i & 0.236+0.022i \\ 0.236-0.022i & 0.265+0.000i \end{pmatrix} \tag{6.3}$$

$$\hat{\Pi}_{|A\rangle} = \begin{pmatrix} 0.240+0.000i & -0.227+0.017i \\ -0.227-0.017i & 0.216+0.000i \end{pmatrix} \tag{6.4}$$

with the `MATLAB` code returning an optimal value of the difference between the theoretical and the experimental result of ≈ 0.0039.

As before, also these results satisfy the expectations about the theoretical projectors up to a scaling factor introduced by the presence of the initial BS, which have the following shape

$$\hat{\Pi}_{|L\rangle} = \frac{1}{2}\left|L\right\rangle\left\langle L\right| = \begin{pmatrix} 0.250+0.000i & 0.000-0.250i \\ 0.000+0.250i & 0.250+0.000i \end{pmatrix} \tag{6.5}$$

$$\hat{\Pi}_{|R\rangle} = \frac{1}{2}\left|R\right\rangle\left\langle R\right| = \begin{pmatrix} 0.250+0.000i & 0.000+0.250i \\ 0.000-0.250i & 0.250+0.000i \end{pmatrix} \tag{6.6}$$

$$\hat{\Pi}_{|D\rangle} = \frac{1}{2}\left|D\right\rangle\left\langle D\right| = \begin{pmatrix} 0.250+0.000i & 0.250+0.000i \\ 0.250+0.000i & 0.250+0.000i \end{pmatrix} \tag{6.7}$$

$$\hat{\Pi}_{|A\rangle} = \frac{1}{2}\left|A\right\rangle\left\langle A\right| = \begin{pmatrix} 0.250+0.000i & -0.250+0.000i \\ -0.250+0.000i & 0.250+0.000i \end{pmatrix}. \tag{6.8}$$

The results obtained after measuring the power collected at the input of the four photon detector, once the aforementioned calibration has been completed, are shown for completeness in Fig. 6.3.

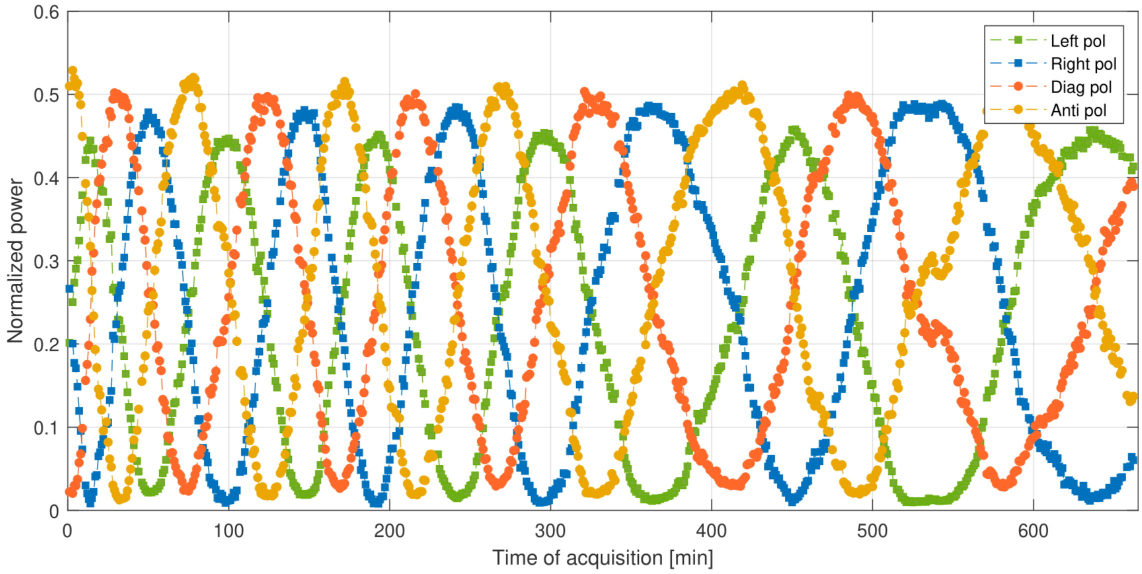


Figure 6.3: 12 hours power measurement showing the intrinsic interference between the couple of states in each respective basis. $|L\rangle$ polarized light is in *green*, $|R\rangle$ polarized light is in *blue*, $|D\rangle$ polarized light is in *orange* and $|A\rangle$ polarized light is in *yellow*. The acquisition frequency is 1 $[spm]$. The normalization is performed taking the ratio between each measured power and the total amount of power collected at the four receiver outputs in the same instant.

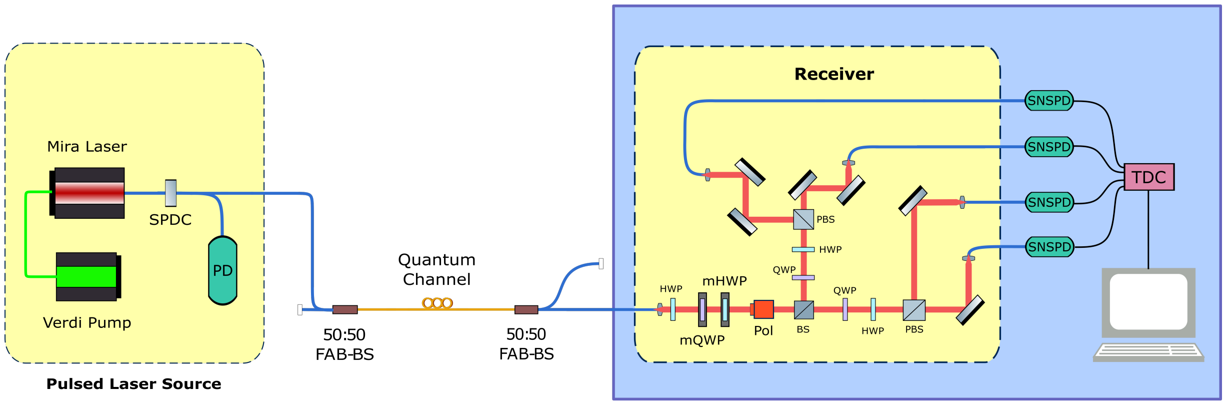


Figure 6.4: Scheme of the characterization setup considering a pulsed signal. BS: beam splitter, PBS: polarizing BS, HWP: half-wave plate, QWP: quarter-wave plate, mQWP/mHWP: mortorized-QWP/HWP, Pol: polarimeter, SPDC: spontaneous parametric down conversion, PD: photon detector, SNSPD: superconducting nanowire single PD, FAB-BS: fast-axis blocking BS, TDC: time-to-digital converter. Polarization maintaining fibers are in *blue*, single mode fibers are in *yellow*, free-space optical path is in *red*.

6.2 Pulsed laser source

Similarly to what pursued for the case of the cw laser source, the characterization of the receiver demands a proper setup, illustrated in Fig. 6.4. Also in this case the first step to perform the calibration is the computation of the density matrices related to the states injected in the receiver, that are

$$\hat{\rho}_{|H\rangle} \approx \begin{pmatrix} 0.999+0.000i & 0.010+0.000i \\ 0.010+0.000i & 0.000+0.000i \end{pmatrix}, \quad \hat{\rho}_{|V\rangle} \approx \begin{pmatrix} 0.000+0.000i & 0.003-0.003i \\ 0.003+0.003i & 1.000+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|D\rangle} \approx \begin{pmatrix} 0.492+0.000i & 0.499-0.001i \\ 0.499+0.001i & 0.508+0.000i \end{pmatrix}, \quad \hat{\rho}_{|A\rangle} \approx \begin{pmatrix} 0.503+0.000i & -0.500+0.002i \\ -0.500-0.002i & 0.497+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|L\rangle} \approx \begin{pmatrix} 0.505+0.000i & -0.001+0.500i \\ -0.001-0.500i & 0.495+0.000i \end{pmatrix}, \quad \hat{\rho}_{|R\rangle} \approx \begin{pmatrix} 0.499+0.000i & 0.003-0.500i \\ 0.003+0.500i & 0.501+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|\phi_1\rangle} \approx \begin{pmatrix} 0.109+0.000i & -0.291+0.114i \\ -0.291-0.114i & 0.891+0.000i \end{pmatrix}, \quad \hat{\rho}_{|\phi_2\rangle} \approx \begin{pmatrix} 0.078+0.000i & 0.267-0.022i \\ 0.267+0.024i & 0.922+0.000i \end{pmatrix}$$

$$\hat{\rho}_{|\phi_3\rangle} \approx \begin{pmatrix} 0.308+0.000i & 0.427-0.177i \\ 0.427+0.177i & 0.692+0.000i \end{pmatrix}, \quad \hat{\rho}_{|\phi_4\rangle} \approx \begin{pmatrix} 0.242+0.000i & -0.131+0.408i \\ -0.131-0.408i & 0.758+0.000i \end{pmatrix}$$

which shows some alterations with respect to the values computed in the previous case, underling the fact that even slight modification in the environment (i.e. temperature fluctuations, mechanical stress, etc.) can in some cases cause the optical components of the receiver to move, hence changing the performances of the apparatus.
For these states the associated probabilities are reported in Table 2

	Measurement POVM			
Input states	$\hat{\Pi}_L$	$\hat{\Pi}_R$	$\hat{\Pi}_D$	$\hat{\Pi}_A$
$\|H\rangle$	0.212	0.340	0.156	0.292
$\|V\rangle$	0.165	0.297	0.398	0.139
$\|L\rangle$	0.443	0.019	0.364	0.175
$\|R\rangle$	0.015	0.520	0.312	0.153
$\|D\rangle$	0.155	0.284	0.549	0.013
$\|A\rangle$	0.209	0.372	0.018	0.400
$\|\phi_1\rangle$	0.275	0.303	0.087	0.335
$\|\phi_2\rangle$	0.122	0.352	0.499	0.027
$\|\phi_3\rangle$	0.274	0.219	0.439	0.068
$\|\phi_4\rangle$	0.456	0.034	0.298	0.213

Table 2: Probabilities for each combination of input states and applied POVMs, computed considering Eq. (5.9).

In a similar manner as the one introduced previously, the computation of the POVMs requires the measurement of the number of photons collected at the four SNSPDs for each state that enters the receiver.

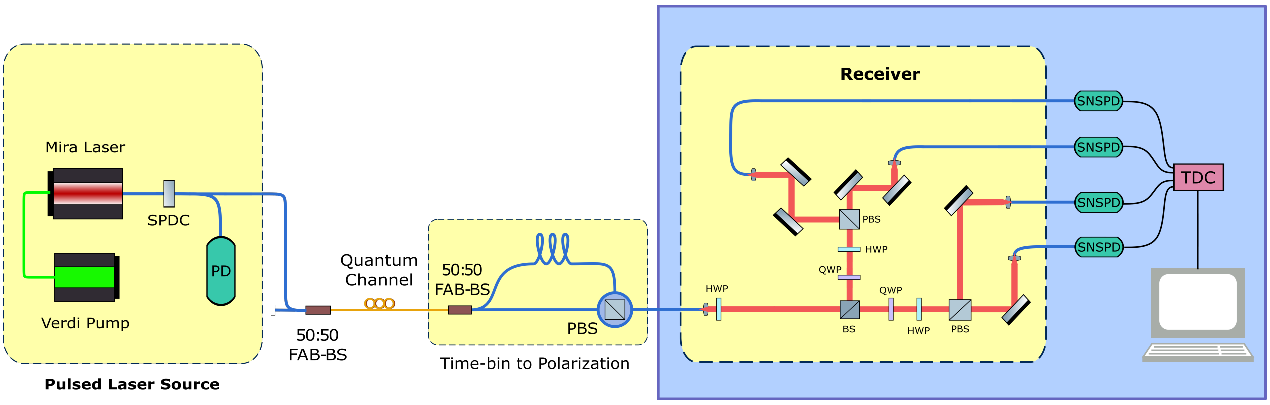


Figure 6.5: Scheme of the measurement setup considering a pulsed signal.

The scheme is the one proposed in Fig. 6.5, and the corresponding outcomes are

$$\hat{\Pi}_{|L\rangle} = \begin{pmatrix} 0.221 + 0.000i & -0.022 + 0.205i \\ -0.022 - 0.205i & 0.235 + 0.000i \end{pmatrix} \tag{6.9}$$

$$\hat{\Pi}_{|R\rangle} = \begin{pmatrix} 0.318 + 0.000i & -0.043 - 0.248i \\ -0.043 + 0.248i & 0.259 + 0.000i \end{pmatrix} \tag{6.10}$$

$$\hat{\Pi}_{|D\rangle} = \begin{pmatrix} 0.195 + 0.000i & 0.259 + 0.051i \\ 0.259 - 0.051i & 0.358 + 0.000i \end{pmatrix} \tag{6.11}$$

$$\hat{\Pi}_{|A\rangle} = \begin{pmatrix} 0.266 + 0.000i & -0.195 + 0.008i \\ -0.195 - 0.008i & 0.148 + 0.000i \end{pmatrix} \tag{6.12}$$

In this case the optimal value yielded by the MATLAB script is ≈ 0.1974.

With the characterization so far retrieved, before running the experiment, a last calibration should be done. In particular by means of some fiber based polarization controllers it is possible to compensate some potential losses or misalignment in the polarization in the entire optical circuit that may penalize one side peak, increasing the other. The same type of device is utilized also at the input of each SNSPD, since by fabrication these instruments have sensitivity varying as a function of the input polarization.

Finally, before moving on to the analysis of the data collected so far, it is worth to

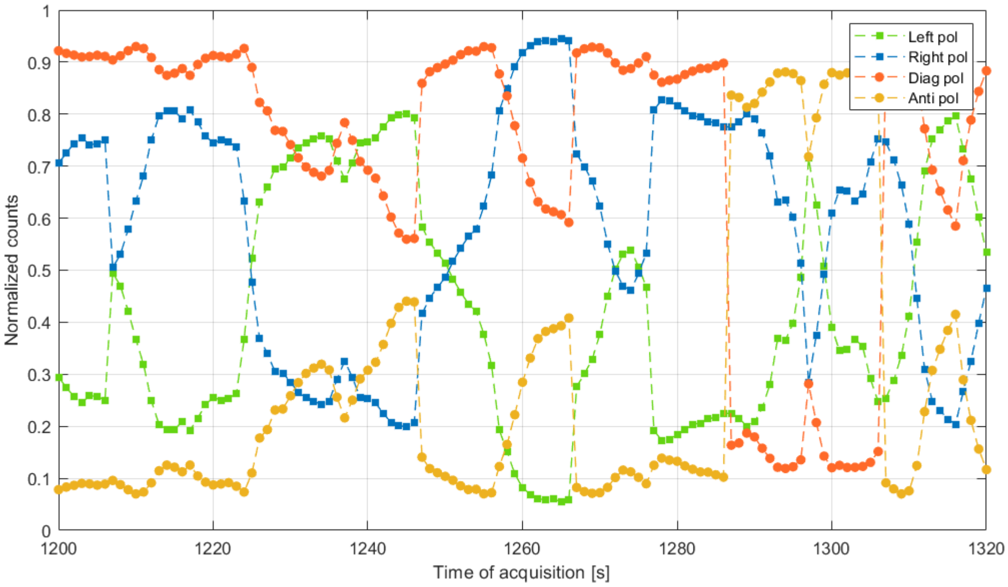


Figure 6.6: 2 minutes window among the entire measurement showing the intrinsic interference between the couple of states in each respective basis and between the two bases. $|L\rangle$ polarized light is in *green*, $|R\rangle$ polarized light is in *blue*, $|D\rangle$ polarized light is in *orange* and $|A\rangle$ polarized light is in *yellow*.

show the diagram relating the measured photons (normalized) as a function of time. In Fig. 6.6 it is represented just a detail of the entire measurement, considering a two minute window (minutes 25′ and 26′), while in Fig. 6.7 it is reported the entire data-take just for the sake of exhaustiveness.

In Fig. 6.3, Fig. 6.6 and Fig. 6.7 the vertical axis refers to the normalized power (number of counts) collected at each detector. Since it has been normalized with respect to the total optical power per second (for the cw experiment) or the total number of counts per second (for the pulsed experiment), this value can be considered as a direct estimate of the probability of detecting a well-polarized photon at each performed measure. With this assumption it is possible to compare the two experiments even if they are exploiting two different source strategies.

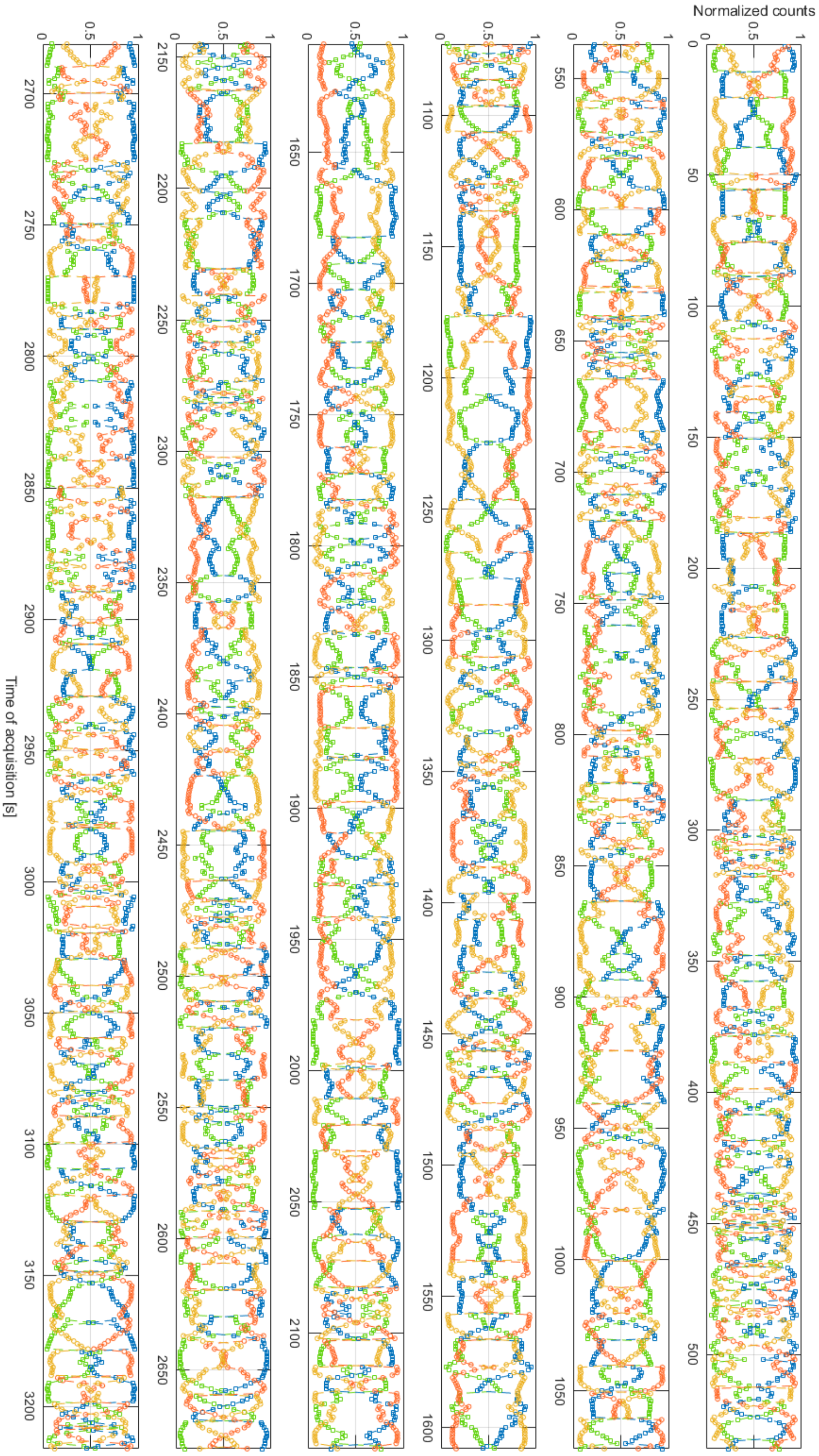


Figure 6.7: 2 hours data acquisition. $|L\rangle$ polarized light is in *green*, $|R\rangle$ polarized light is in *blue*, $|D\rangle$ polarized light is in *orange* and $|A\rangle$ polarized light is in *yellow*.

7 Data Analysis

It is now possible to exploit the results so far derived with the aim to estimate the level of secrecy of the proposed RFI protocol in the assumption of both the cw laser source and the pulsed laser source.
As already outlined in Chapter 2, in order to retrieve the fraction of trustful key that Alice and Bob can exploit in order to successfully encrypt their future conversations (the SKR), an estimation of the C parameter (Eq. (2.22)) must be made.
Eventually, the minimization problem expressed in Eq. (2.31) can therefore be applied and the resulting outcomes are here discussed.

First of all, it is convenient to focus on the graphical and numerical derivations extrapolated from the first experience, the one considering a cw laser source.
From the observations of Fig. 6.3 and Fig. 6.7 it is clear the presence of an interfering phenomenon occurring in the envelope of the power (number of photons) measured at each power meter (photon detector). Firstly, it must be emphasized that each detector observes a pace in the incoming photon flux that oscillates in a sinusoidal behaviour. This is easily attributable to the constant fluctuation of the phase inside the two UMZIs placed at Alice's and Bob's stations. As a matter of fact, these delicate devices suffer from temperature variation and mechanical stress, that slightly modify the path difference covered by the photons in the two branches, inducing a changing in their interference.
Furthermore, it can be stated that the variation of the amount of recorder photons at the receiver calibrated to measure the $|L\rangle$ polarized light is in *antiphase* with respect to the envelope registered at the detector responsible to meter the $|R\rangle$ polarized light. A similar reasoning can be applied to the $\mathbb{X}$ basis, considering thereby the $|D\rangle$ and $|A\rangle$ states, which display an inversion of phase between the two of them too.
On the contrary, by observing each envelope and those of the two states belonging to the

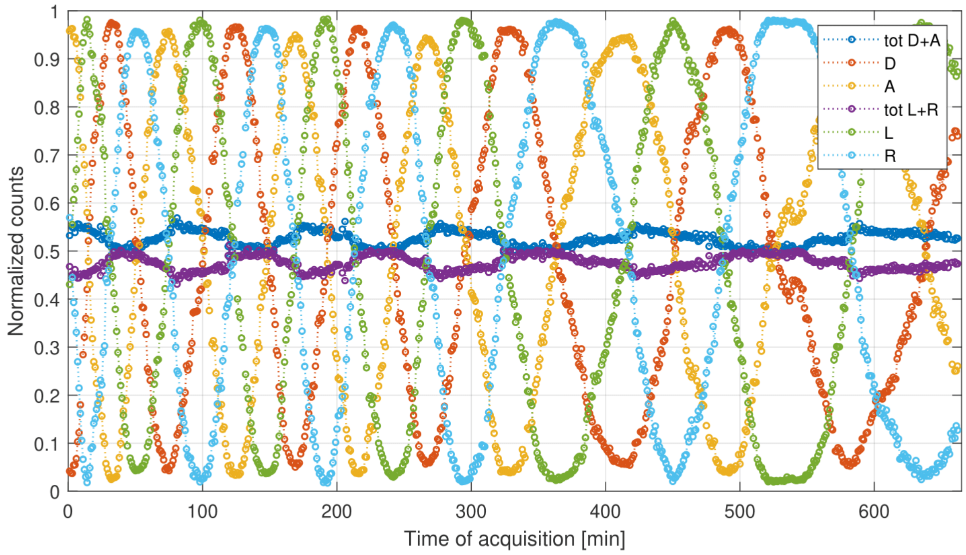


Figure 7.1: 12 hours cw power measurement (normalized) in which the interference between the four polarization states is shown, together with the envelope of the detected power (normalized) for each measurement basis (*blue* for the $\mathbb{X}$ basis and *purple* for the $\mathbb{Y}$ basis). The detection in each basis is computed as the sum of the detections recorded in the two states belonging to the basis. The normalization in this case is computed as the ratio between the measured power and the sum of the power collected at the two receiver outputs belonging to the same basis.

opposite basis, it can be declared that the signals are *in quadrature*. All these considerations demonstrate the statistics of the current experiment, in which the probability of measuring one photon at a specific polarization at the receiver arranged to detect it is extremely high. On the contrary, the probability of detecting a photon in the opposite polarization state is very low, since the envelopes in such situation extinguish, while for the remaining two possibilities the probability is one half. This behaviour demonstrates that the two control bases are thus mutually unbiased, as can be noticed also by observing the trade of the detections in the two bases, pictured in Fig. 7.1.

Same considerations can be made also for the single photon alternative of the protocol, with regards to Fig. 6.6, in which a similar behaviour is evident.

What has just been discussed can indeed be encountered also observing the histograms of the photon detected at the four SNSPDs, as pictured in Fig. 7.2.

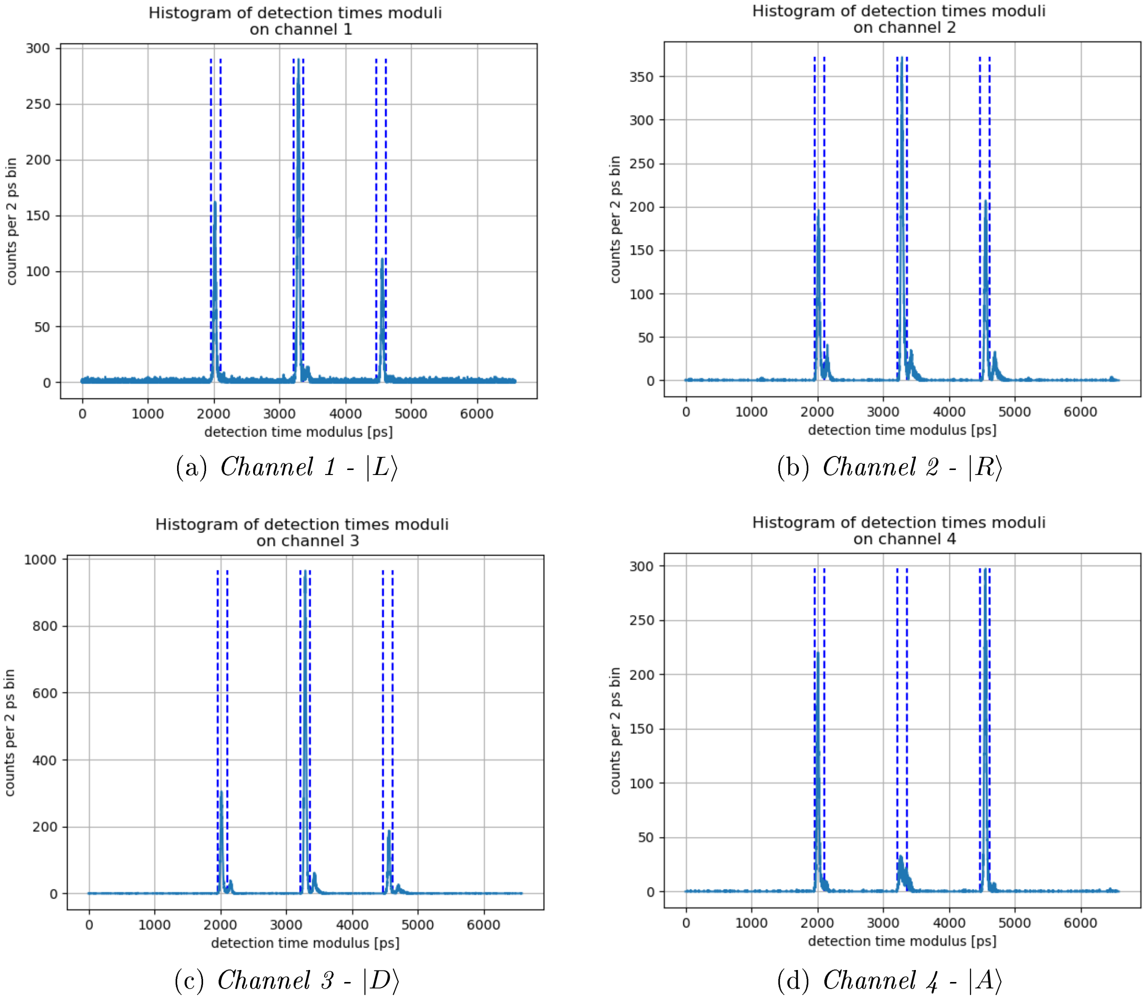
The plots here presented show the histograms of the time of arrival of the detected photons in each channel, corresponding to the outcome of the four projective measurements performed by the receiver. To be more precise, each histogram is built considering the amount of detections that are recorded at each instant of time inside the pulse period of 13.158 $[ns]$, exploiting 9579 bins. The number of bins has been chosen just to guarantee a precise scaling between the pulse period and the construction of histograms with a width of the bins of about 2 $[ps]$. In addiction it is important to mention that the *modulus* operation has been taken into account in order to precisely position each detection in the proper time inside the period of the pulse. As a matter of fact, the remainder of the division between the time of arrival t_{arr} and the pulse period T_{pulse} can be considered to be the "offset" from the beginning of the period to t_{arr} itself, allowing to re-scale the time of arrival into a new reference frame:

$$t^{mod}_{detection} = t_{arr} \quad \% \quad T_{pulse}. \tag{7.1}$$

With this simple computation it is possible to construct the typical three-peaks histogram characteristic of the time-bin encoding. As a final comment before proceeding in the data analysis, it may be reasonable to mention that the study performed for the computation of the security parameter in the case of the pulsed laser source is based on the number of detections measured in an integration window of 150 $[ps]$ around the central peak of each histogram. This value has been decided after considering some different alternatives of the integration intervals, as the best trade off that guarantees an appropriate extinction ratio between the central peak and the fluctuation of the background noise outside the three lobes.

Resuming the discussion left unsettled about Fig. 7.2, it is clear that also in the use of the pulsed laser source the protocol works properly, manifesting interference at the output of the four measurement branches. The data displayed in the figure are related to the counts measured at second 1207”. Considering the central peak of each histogram, the magnitude of the peaks associated with the $|L\rangle$ and $|R\rangle$ polarization states are comparable. In this situation the diagonal polarization reaches a local maximum, while instead the anti-diagonal polarization is quite suppressed.

From the data concerning the measured photons at each temporal instant it is now available to study the C parameter as a function of time.



(a) *Channel 1* - $|L\rangle$

(b) *Channel 2* - $|R\rangle$

(c) *Channel 3* - $|D\rangle$

(d) *Channel 4* - $|A\rangle$

Figure 7.2: Histogram of the modulus of the detected time of arrival for the pulsed-based protocol. The detections refer to (a) the channel 1 in which $|L\rangle$ polarized light is measured, (b) the channel 2 in which $|R\rangle$ polarized light is measured, (c) the channel 3 in which $|D\rangle$ polarized light is measured, (d) the channel 4 in which $|A\rangle$ polarized light is measured.

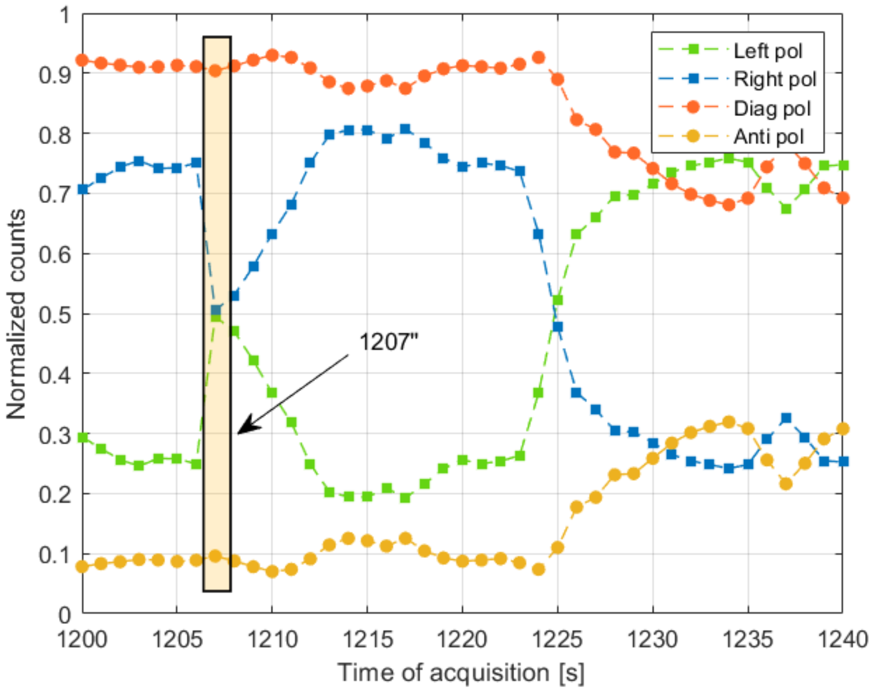


Figure 7.3: Detail of the samples recorded at the second 1207”. It can be seen the amount of photons collected at the four SNSPDs, showing interference with high extinction ratio.

Applying the convex optimization algorithm already mentioned in Eq. (2.31) with the constraints imposed by the derived POVMs, the computed results are the one shown in Fig. 7.4. As it can be seen, the derived results for the cw scenario are quite promising, showing a security parameter spanning from a lowerbound of ≈ 0.95 and an upperbound of ≈ 1.65. It must be recalled that from the experience discussed in [17], the maximum value achievable in Eq. (2.22) is $C = 2$, under the condition of utilizing two maximally entangled states, and therefore in the best case scenario of unconditional security.

Another interesting study about the security parameter can be mentioned, that refers to the computation of C as a function of the phase of the polarization state entering the receiver. Considering the formulation of a quantum state as a superposition of the two pure states $|H\rangle$, $|V\rangle$ expressed in Eq. (5.5), it is possible to perform the convex optimization analysis considering several different superpositions of the horizontal and vertical polarization states, each one with its specific phase ϕ. The resulting three-dimensional diagram picturing the pace of each considered input polarization as a function of time is displaced in Fig. 7.5.

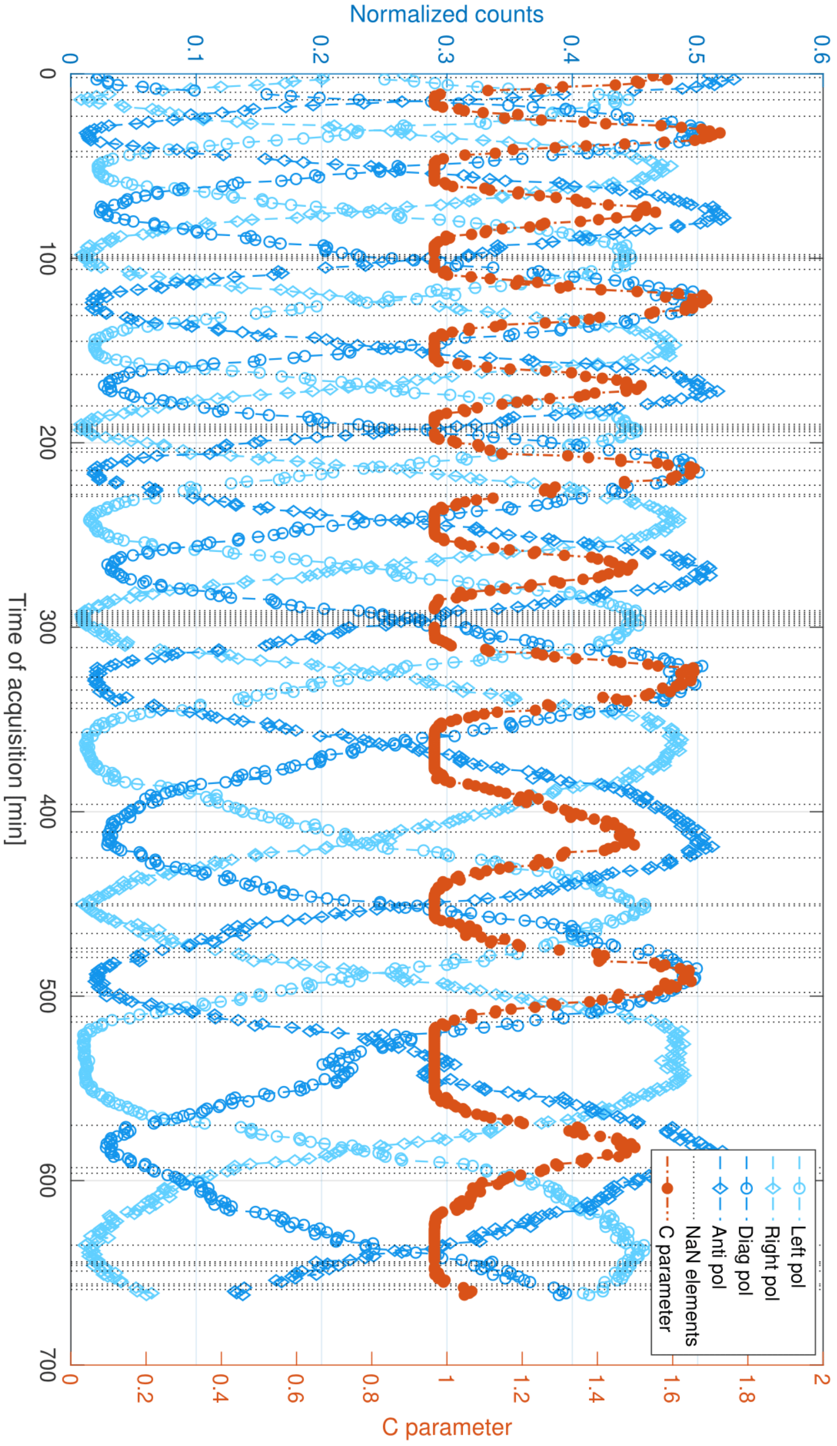


Figure 7.4: Computed C parameter (in *dark orange*, on the right side) and normalized measured optical power (in *blue* and *white-blu*, left side) as a function of time, in the configuration exploiting a cw laser source. The black dashed lines indicate the samples for which the minimization algorithm does not find a feasible result.

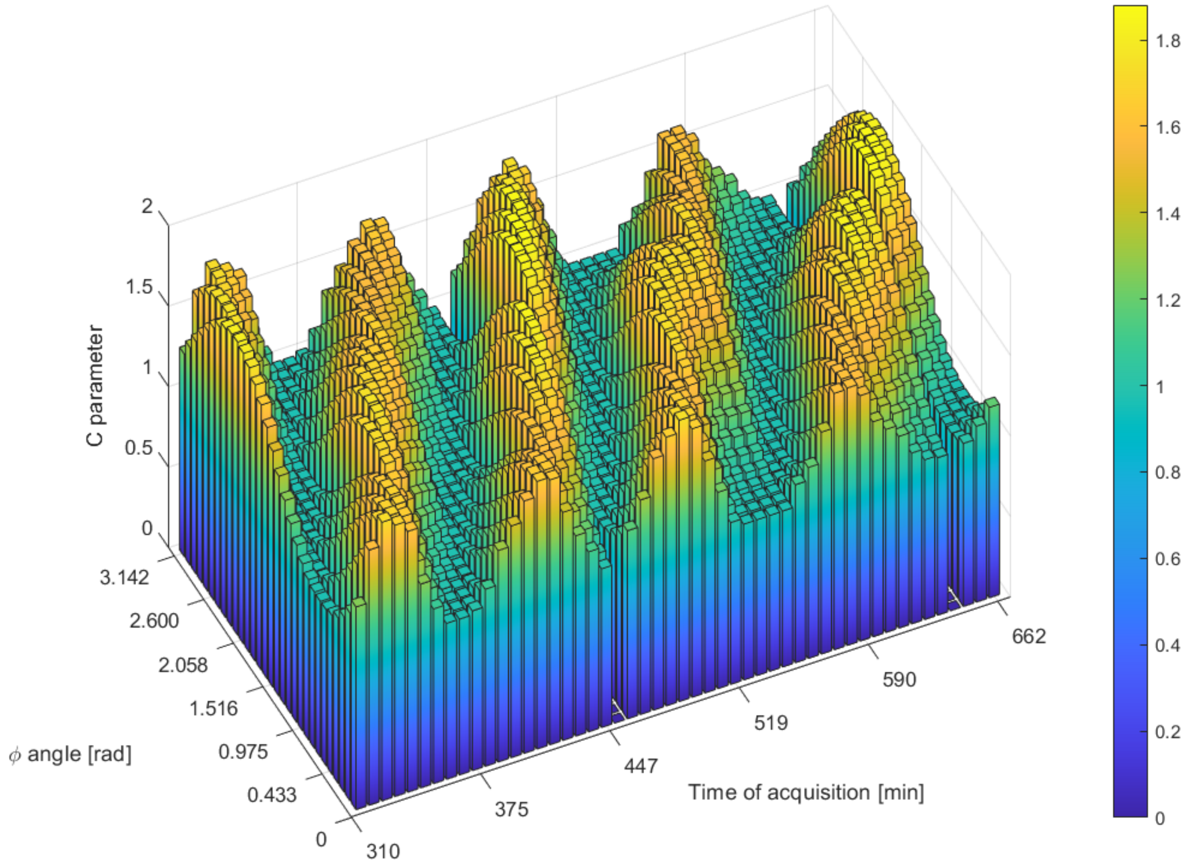


Figure 7.5: Three-dimensional histogram reproducing the envelope of the C parameter as a function of time and phase ϕ. For the considered analysis only a portion of samples have been used for the computation of the security parameter inside the interval belonging to the second half of the data-take. The phase has been chosen among the interval $\phi \in [0; \pi]$ since it has been observed that the periodicity of C is π. The histogram is formed by a grid of 50x30 bars.

It is interesting to notice the presence of a periodicity in the fluctuation of the C parameter, strictly related to the variation of the phase suffered from the received state.

Also in this case, as previously noticed, the security parameter spans from a minimum around 1 (more precisely $C_{min} = 0.968$) up to a maximum value of $C_{max} = 1.881$, proving the feasibility of the proposed RFI protocol.

It should be mentioned that in the considered histogram two slices of data along the phase direction are set to zero by the computation of the convex optimization (for $t = 454$ $[min]$ and $t = 641$ $[min]$). The reason is due to the presence of some results in the derivation of the density matrix $\hat{\rho}_{AB}$ that the MATLAB code has not managed to calculate. It should be reminded that this operator represents the *two qubit* density matrix associated with the

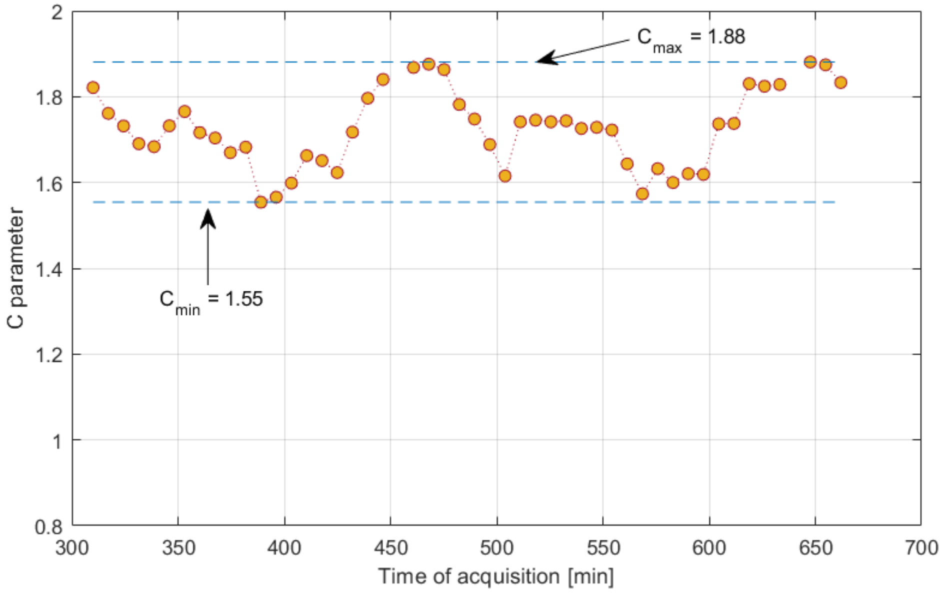


Figure 7.6: Security parameter in function of the acquisition time. Data are extracted from the the histogram in Fig. 7.5 in the assumption of independence from the phase ϕ.

key distributed between Alice and Bob.

Since the amount of infeasible data are a small percentage among the total, they can be ignored, without any degradation of the overall study.

Finally, imaging to follow the ridges of the histogram in Fig. 7.5 considering hence the hypothesis of a phase invariant quantum channel, the retrieved pace of the C parameter is the one depicted in Fig. 7.6.

A similar proof of concept has been pursued in the experience that considers the single photons as a light source. Nevertheless the results have shown a lower degree of security, underlining some imperfections strictly related to the calibration of the receiver apparatus. In particular, the findings returned by the `CVX MATLAB` minimization tool in terms of the density matrix $\hat{\rho}_{AB}$ provides some *infeasible* results. As a consequence the security parameter C cannot be computed and for this reason this last experiment has not yielded the expected level of security achieved in the cw scenario.

After some further analysis it is reasonable to affirm that the main cause that has led to this inconvenience is the extreme susceptibility of the receiver apparatus thus realized. Actually, a different simulation involving the utilization of the POVMs computed for the cw method (Eq. (6.1), Eq. (6.2), Eq. (6.3), Eq. (6.4)) applied to the data collected in the

pulsed laser source configuration has brought to a different outcome, always exhibiting infeasible matrices, with however a greater fraction of numerical (and therefore meaningful) results.
It is probable that in the lapse of time that has passed between the calibration of the receiver and the effective execution of the measurement of the distribution of the quantum key, for a total interval of about three days, the setup suitable to measure the received states sent by the transmitter has suffered some slight misalignments that has modified the algebraic projectors used to carry out the convex minimization procedure. This, in the end, has made the convex optimization routine to not being able to find physical solutions, returning thus infeasible results.

Although the data-take recorded for the pulsed source configuration has proved to be compromised by the inaccuracy of the exploited POVMs, it is still interesting to show the estimation of the security parameter from the collected data, exploiting this time the ideal POVMs reported in Eq. (6.5). The result is pictured in Fig. 7.7
As it can be noticed, the computation of the security parameter has derived reasonable values for a good portion of the collected data, proving once again the correctness of the protocol proposed in this work. The presence of several infeasible results (represented in the graph as dashed vertical lines) reveal however the limitations introduced by a suboptimal characterization of the Bob's apparatus, that has led to inaccuracies in the acquisition of the experimental statistics. This last part demonstrates the importance of achieving a high standard of calibration in each step of the exploited communication system.

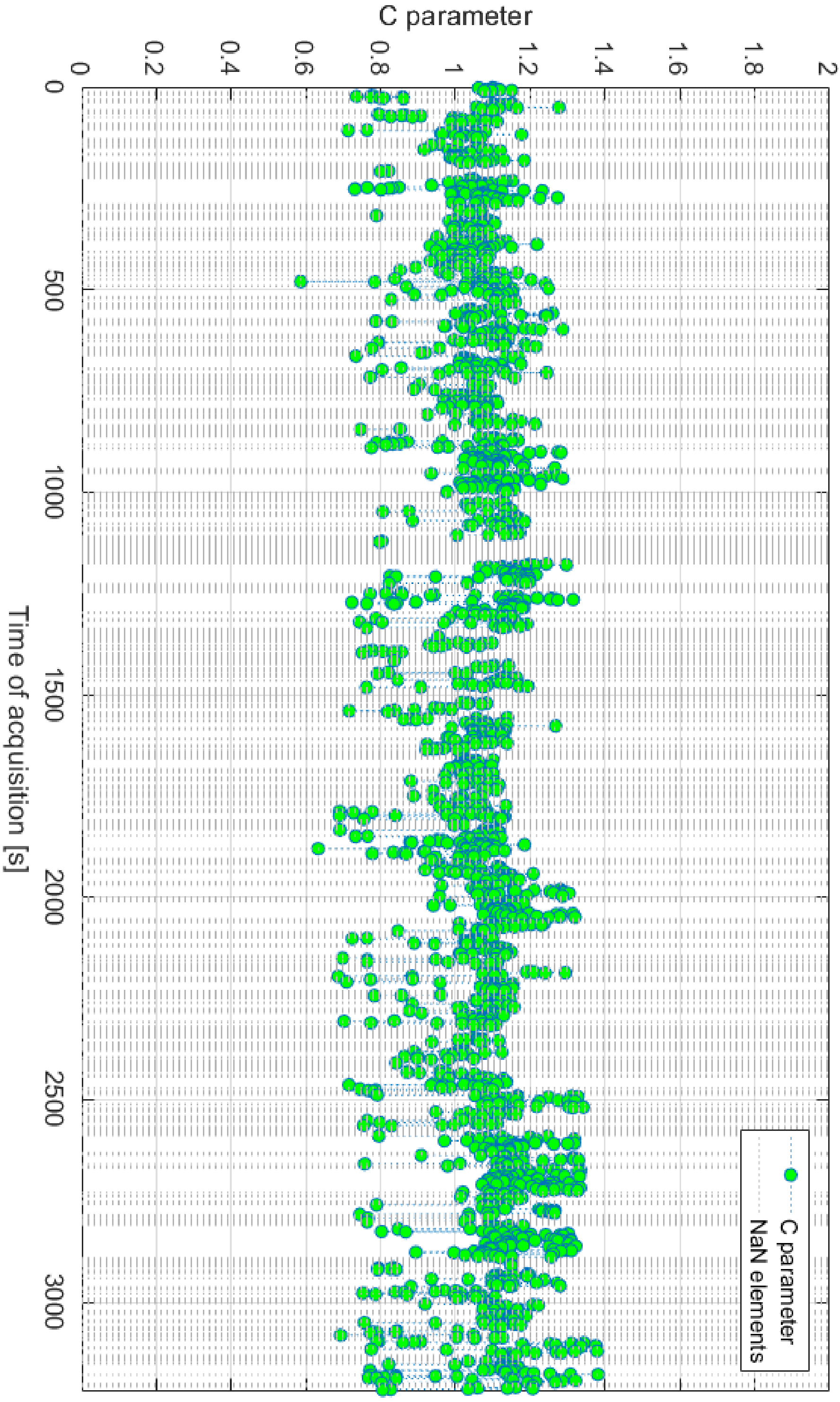


Figure 7.7: Simulation of the C parameter exploiting the ideal POVMs of Eq. (6.5). The dashed *grey* lines represent the infeasible results returned from the `MATLAB CVX` program, which reveal the low reliability of the measured data.

8 Conclusions

In this thesis the feasibility of a Reference Frame Independent protocol based on Cross-encoding has been determined and the required communication apparatus demanded to implement this Quantum Key Distribution procedure has been characterized.

By the realization of a fully passive receiver it has been demonstrated the possibility to achieve high level of security in the distribution of a cryptographic key, according to the computation of the C parameter [17], without loosing the condition of independence from any reference frame, making this strategy extremely beneficial in practical applications in which an active control on the phase fluctuation of the communication channel is not implementable.

Two studies have been proposed in order to give credit to present work.

The first has exploited a cw laser source and standard power meters for the detection of the received message, demonstrating the feasibility of the protocol. Promising results have been shown allowing this protocol to be potentially considered a valid alternative among the QKD possibilities developed in the last years.

The upgrade to this experiment has been the development of an improved version of the previous setup, exploiting a pulsed laser source for the generation of the quantum states to be distributed between Alice and Bob. This passage has required the adaptation of the pre-existing communication system in order to fulfill the constraints introduced by more accurate devices. In particular the improvements have regarded the encoding stage, in order to acquire the desired level of interference, and the receiver station, which has seen the implementation of highly accurate Superconducting-Nanowire-Single-Photon-Detectors.

For both the experiences appropriate softwares have been deployed, capable of attaining concrete post-processing results.

Furthermore, for each configuration a complete calibration of the receiver has been performed, resulting in the derivation of the algebraic description of the related POVMs, exploited in the measurement process.

From the data collected in the study of the first setup it has been possible to prove the correctness of the developed theoretical model, demonstrating the feasibility of the protocol in the implementation of actual distribution of a quantum key for cryptographic purposes.
The proof of concept has returned satisfactory results also in the study performed on the second apparatus, that although has shown grater sensitivity to the dependence on the calibration of the fostered scheme. However, we have not been able to take further trials to derive better results since in the last days of data analysis the temperature controller of the SNSPDs has broken down. This will require few weeks of stabilization to make it operational again.

Albeit this last experience has not provided results as good as the first one, the feasibility of the proposed protocol has been shown. We are confident that with few more calibration attempts and additional data-takes it will be possible to apply the same procedure utilized in the first study, acquiring enough data to establish similar successful results, that in few months will lead to a complete publication in a relevant scientific journal.

Finally, it is possible to state that this study may represents the catalyst to a new generation of Reference-Frame-Independent QKD studies, whose target is the development of entirely polarization-based RFI QKD protocols for free-space and satellite-based communications.

Bibliography

[1] McKinsey and Company. *Quantum Technology Monitor.* URL: https://www.mckinsey.com/featured-insights/the-rise-of-quantum-computing.

[2] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179. DOI: https://doi.org/10.1016/j.tcs.2014.05.025.

[3] S. Pirandola et al. "Advances in quantum cryptography". In: *Adv. Opt. Photon.* 12.4 (Dec. 2020), pp. 1012–1236. DOI: 10.1364/AOP.361502. URL: http://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012.

[4] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* 10th. USA: Cambridge University Press, 2011. ISBN: 1107002176.

[5] M. G. A. Paris. "The modern tools of quantum mechanics". In: *The European Physical Journal Special Topics* 203.1 (Apr. 2012), pp. 61–86. DOI: 10.1140/epjst/e2012-01535-1. URL: https://doi.org/10.11402Fepjst2Fe2012-01535-1.

[6] "The Measuring Process". In: *Quantum Theory: Concepts and Methods.* Ed. by Asher Peres. Dordrecht: Springer Netherlands, 2002, pp. 373–429. ISBN: 978-0-306-47120-9. DOI: 10.1007/0-306-47120-5_12. URL: https://doi.org/10.1007/0-306-47120-5_12.

[7] Simon Singh. *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography.* Anchor Books, 2000. ISBN: 978-1-85702-879-9.

[8] Anthony Laing et al. "Reference-frame-independent quantum key distribution". In: *Phys. Rev. A* 82 (1 July 2010), p. 012304. DOI: 10.1103/PhysRevA.82.012304. URL: https://link.aps.org/doi/10.1103/PhysRevA.82.012304.

[9] Yun-Hong Gong et al. "Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror". In: *Opt. Express* 26.15 (July 2018), pp. 18897–18905. DOI: 10.1364/OE.26.018897. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-26-15-18897.

[10] Heasin Ko et al. "Experimental filtering effect on the daylight operation of a free-space quantum key distribution". In: *Scientific Reports* 8.1 (2018), p. 15315. ISSN: 2045-2322. DOI: 10.1038/s41598-018-33699-y. URL: https://doi.org/10.1038/s41598-018-33699-y.

[11] M. Avesani et al. "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics". In: *npj Quantum Information* 7.1 (2021), p. 93. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00421-2. URL: https://doi.org/10.1038/s41534-021-00421-2.

[12] Sheng-Kai Liao et al. "Satellite-Relayed Intercontinental Quantum Network". In: *Phys. Rev. Lett.* 120 (3 Jan. 2018), p. 030501. DOI: 10.1103/PhysRevLett.120.030501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

[13] Cristian Bonato et al. "Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link". In: *Opt. Express* 14.21 (Oct. 2006), pp. 10050–10059. DOI: 10.1364/OE.14.010050. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-14-21-10050.

[14] Marco Avesani et al. *Stable, low-error, and calibration-free polarization encoder for free-space quantum communication.* Sept. 2020. DOI: 10.1364/OL.396412.

[15] Yu-Yang Ding et al. "Polarization variations in installed fibers and their influence on quantum key distribution systems". In: *Opt. Express* 25.22 (Oct. 2017), pp. 27923–27936. DOI: 10.1364/OE.25.027923. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-25-22-27923.

[16] Charles H. Bennett. “Quantum cryptography using any two nonorthogonal states”. In: *Phys. Rev. Lett.* 68 (21 May 1992), pp. 3121–3124. DOI: 10.1103/PhysRevLett.68.3121. URL: https://link.aps.org/doi/10.1103/PhysRevLett.68.3121.

[17] Hongwei Liu et al. “Reference-Frame-Independent Quantum Key Distribution Using Fewer States”. In: *Phys. Rev. Applied* 12 (3 Sept. 2019), p. 034039. DOI: 10.1103/PhysRevApplied.12.034039. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.12.034039.

[18] Kiyoshi Tamaki et al. “Loss-tolerant quantum cryptography with imperfect sources”. In: *Phys. Rev. A* 90 (5 Nov. 2014), p. 052314. DOI: 10.1103/PhysRevA.90.052314. URL: https://link.aps.org/doi/10.1103/PhysRevA.90.052314.

[19] Can Wang et al. “Reference-frame-independent quantum key distribution with source flaws”. In: *Phys. Rev. A* 92 (4 Oct. 2015), p. 042319. DOI: 10.1103/PhysRevA.92.042319. URL: https://link.aps.org/doi/10.1103/PhysRevA.92.042319.

[20] Michael Grant and Stephen Boyd. *CVX: Matlab Software for Disciplined Convex Programming, version 2.1*. http://cvxr.com/cvx. Mar. 2014.

[21] Michael Grant and Stephen Boyd. “Graph implementations for nonsmooth convex programs”. In: *Recent Advances in Learning and Control*. Ed. by V. Blondel, S. Boyd, and H. Kimura. Lecture Notes in Control and Information Sciences. http://stanford.edu/~boyd/graph_dcp.html. Springer-Verlag Limited, 2008, pp. 95–110.

[22] R. L. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342.

[23] Matthias Bock et al. “Highly efficient heralded single-photon source for telecom wavelengths based on a PPLN waveguide”. In: *Opt. Express* 24.21 (Oct. 2016), pp. 23992–24001. DOI: 10.1364/OE.24.023992. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-24-21-23992.

[24] M. A. Broome et al. “Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing”. In: *Opt. Express* 19.23 (Nov. 2011), pp. 22698–22708. DOI: 10.1364/OE.19.022698. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-19-23-22698.

[25] Davide Scalcon et al. *Cross-encoded quantum key distribution exploiting time-bin and polarization states with qubit-based synchronization*. Nov. 2021.

[26] John M. Donohue et al. “Coherent Ultrafast Measurement of Time-Bin Encoded Photons”. In: *Phys. Rev. Lett.* 111 (15 Oct. 2013), p. 153602. DOI: 10.1103/PhysRevLett.111.153602. URL: https://link.aps.org/doi/10.1103/PhysRevLett.111.153602.

[27] P. Kurpiers et al. “Quantum Communication with Time-Bin Encoded Microwave Photons”. In: *Phys. Rev. Applied* 12 (4 Oct. 2019), p. 044067. DOI: 10.1103/PhysRevApplied.12.044067. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.12.044067.

Ringraziamenti

Desidero ringraziare innanzitutto il mio relatore Prof. Giuseppe Vallone per avermi dato la possibilità di svolgere il tirocinio e la tesi all'interno di una realtà stimolante com'è il gruppo di ricerca Quantum Future. Lo ringrazio sopratutto per la passione che mi ha trasmesso negli ultimi due anni per lo studio della Meccanica Quantistica.

Non posso non ringraziare il mio co-relatore PhD Costantino Agnesi, che per tutto il periodo di tirocinio si è dimostrato instancabilmente disponibile nel colmare ogni mio dubbio e risolvere qualsiasi problema riscontrassimo durante il percorso. Un supporto fondamentale per raggiungere degli obiettivi tanto ambiziosi.

Ringrazio tutti i membri del LUXOR, ed in particolare Francesco Santagiustina, Matteo Padoan e Davide Scalcon per essersi sempre resi disponibili ad aiutarmi ad affrontare i problemi più disparati.

Un ringraziamento lo rivolgo in particolare ad Aura, senza la quale le giornate di studio e le nottate davanti a Matlab sarebbero state sicuramente più difficili e meno efficaci.

Ringrazio i miei genitori, Laura e Franco, per il costante e smisurato supporto con il quale, fin da piccolo, mi hanno accompagnato nelle mie vittorie e nei fallimenti. Questo traguardo è anche vostro.

Ringrazio mio fratello Alessandro, che da quando ne ho memoria mi ha sempre mostrato la strada migliore, spianandola per me ad ogni passo. E ringrazio i miei amici del dell'università e del Q8, ed i miei colleghi di lavoro, uno ad uno, per essermi stati vicini ed avermi aiutato a crescere.

Ed infine desidero ringraziare Gaia, per i suoi continui sacrifici e per la pazienza dimostrata nell'appoggiare le mie scelte più difficili. Sei il mio punto di riferimento, e di questo te ne sarò sempre grato.