Università degli Studi di Padova

DIPARTIMENTO DI FISICA E ASTRONOMIA "GALILEO GALILEI"
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE
Corso di Laurea Magistrale in Fisica

Space Quantum Communication using Time-bin qubit

Laureando:
Francesco Vedovato

Relatore:
Chiar.mo Prof. Paolo Villoresi

Correlatore:
Chiar.mo Prof. Giuseppe Vallone

Anno Accademico 2014-2015

CONTENTS

INTRODUCTION

The aim of this thesis is to test the feasibility of the *time-bin* encoding technique along a *space quantum link* between a satellite and a ground station.

Quantum Communication represents today the most promising path to ensure *communication security*, a primary necessity for governments, industries and individual citizens.

In this context, *Quantum Key Distribution* (QKD) plays a crucial role allowing to establish a secure communication between two parties. QKD uses the fundamental principles of Nature described by Quantum Mechanics, as Heisenberg's uncertainty principle, to ensure that no one can eavesdrop the communication without being discovered. QKD may be considered the first application of *Quantum Information* available in everyday applications and the time-bin technique is the encoding used for the first commercial realizations based on optical fibers. Free-space optical links are instead more suitable for long-distance QKD among metropolitan areas or even continents.

However, secure quantum communications are nowadays limited to within some hundreds of kilometers due to the physical limits of these two technologies. To overcome these limitations, with a view to a global QKD network, a space quantum channel is required. So far, no orbiting terminals dedicated to quantum communications are available and so experiments try to mimic a quantum transmitter in space by exploiting satellites equipped with corner cube retroreflectors. They are typically used for Laser Ranging activities, even if in the few last years they have been employed for quantum communication tests that have already demonstrated the feasibility of polarization encoding in Space.

Time-bin encoding is another quantum information technique that must be investigated also in the spatial environment. In this case, the information is encapsulated in the *phase* of a photon-wavepacket and this thesis aims to show that the phase holds in the propagation through the space quantum channel. The experiment we will describe here requires the realization of a single photon interferometry at satellite distance involving an orbiting terminal. The feasibility test reported and the obtained results are crucial to extend the frontiers of satellite QKD also to other Quantum Communication protocols such as quantum teleportation and entanglement swapping, never tested in Space so far.

We can now present the chapters description and a small resume of the discussed topics.

The first chapter is about Quantum Communication. We will introduce some basic elements of Quantum Information, the fundamental concepts of

QKD and the main ideas underlying the other Quantum Communication protocols based on entanglement (dense coding, teleportation and entanglement swapping).

In the second chapter we will present two of the main tools of a modern optics laboratory, i.e., the Gaussian optics and the LASER. In particular, we will describe the behavior of a optical 4f-system which role will be fundamental in our experiment, the concept of lineshape function for an atomic transition and the operating principle of a mode-locked laser.

Due to the fact that the experiment is an interferometry one, the third chapter is dedicated to the concept of *coherence*, with particular attention to optics both in the classical and in the quantum description. We will describe the role of coherence in interference experiments and the description of a linear multiport that we will use to predict the detection probabilities in our experiment.

The forth chapter regards Space Quantum Communication by presenting the state of the art of this research field and the experimental steps performed until today. In particular, we will report the single photon exchange between a satellite and a ground station and the first satellite quantum communication realized with polarization encoding.

In the fifth chapter we introduce the time-bin technique and its use to implement the QKD BB84 protocol. Then we will describe the 'Two-Ways" configuration and the idea of the time-bin experiment in Space.

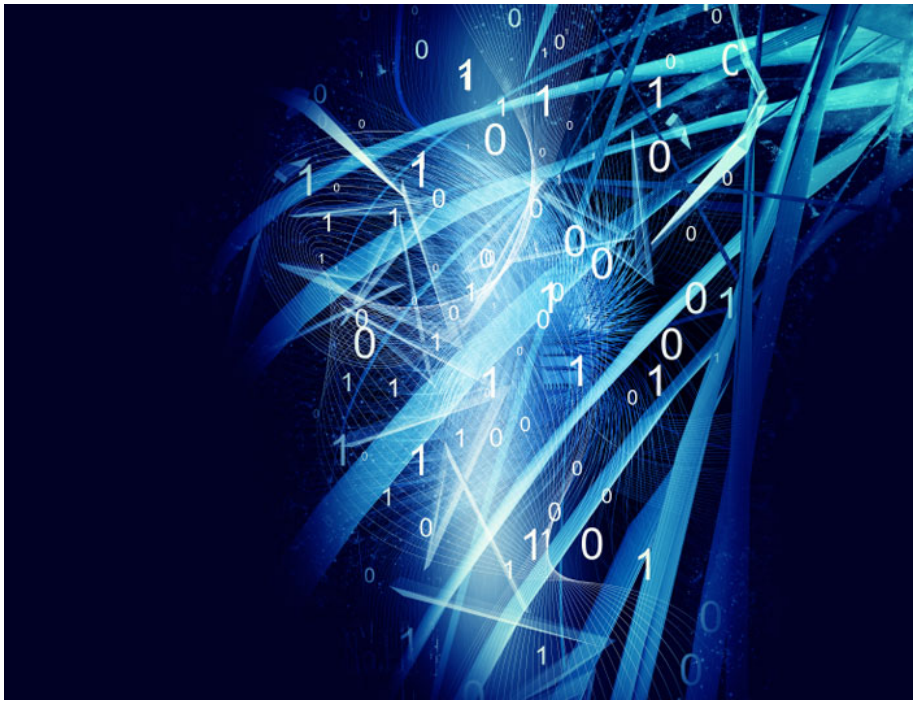
The space time-bin feasibility test is presented with great details in the sixth chapter. We will describe the optical setup used at Matera Laser Ranging Observatory (MLRO) in Matera, the data collection and analysis and the results that show the positive outcome of the test.

1

QUANTUM COMMUNICATION

Quantum Communication is the art of transferring a quantum state from one place to another. It is part of *Quantum Information*, which studies the deep relation between Quantum Mechanics and Information Theory. Quantum Information allows tasks that are impossible using classical information as, for example, secure communications between two parties and teleportation, as we will show in the following.

In this introductory chapter, we report some basic concepts of Quantum Information in order to understand the contents of this thesis. Then, we present the simplest Quantum Communication protocol, *Quantum Cryptography*, that is also the most promising technique for *Space Quantum Communication*. Finally, we show how *entanglement*, the characteristic trait of Quantum Mechanics, can be exploited to realize quantum communications.



1.1 ELEMENTS OF QUANTUM INFORMATION

In this section we review the postulates of Quantum Mechanics and the formalism of *density operator*. Then, we introduce the idea of *qubit*, the quantum analogue to the classical bit. At the end of this section, we demonstrate the *no-cloning theorem* which role is fundamental in all Quantum Communication protocols.

1.1.1 *Postulates of Quantum Mechanics*

There are four basic postulates of Quantum Mechanics which tell you how to represent a physical system and its state, how systems evolve when "not measured", how to carry out measurements and how to describe a composite quantum systems made up of two (or more) distinct physical systems. A complete discussion of these postulates can be found for example in [1], from which we report the four statements:

1. *States*. Associated to any isolated physical system is a *Hilbert space* $\mathcal{H}$. The physical state of the system is completely described by a unit vector ψ in the Hilbert space. The *state vector* is represented by the symbol $|\psi\rangle \in \mathcal{H}$ by using the Dirac notation.
2. *Evolution*. The evolution of a closed quantum system is described by an *unitary transformation*, i.e., an unitary operator acting on the Hilbert space. The state $|\psi_t\rangle$ of the system at time t is related to the state $|\psi_{t'}\rangle$ of the system at time t' by an unitary operator $\hat{U}_{tt'}$ which depends only on the times t and t',
$$|\psi_{t'}\rangle = \hat{U}_{tt'}|\psi_t\rangle \, . \tag{1.1}$$
3. *Measurements*. Quantum measurements are described by a collection $\{\hat{M}_n\}$ of *measurement operators*. These are operators acting on the Hilbert space $\mathcal{H}$ and the index n refers to the measurement outcomes that may occur in the observations.
If $|\psi\rangle$ is the state of the system immediately before the measurement, then the probability that result n occurs is given by
$$\mathcal{P}(n) = \langle\psi|\hat{M}_n^\dagger \hat{M}_n|\psi\rangle \, , \tag{1.2}$$
where $\langle\psi|$ is the vector dual to $|\psi\rangle$ and $\hat{M}_n^\dagger$ is the adjoint of operator $\hat{M}_n$. The state of the system immediately after the measurement is
$$|\psi'\rangle = \frac{M_n|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_n^\dagger \hat{M}_n|\psi\rangle}} \, . \tag{1.3}$$
The measurement operators must satisfy the *completeness equation*
$$\sum_n \hat{M}_n^\dagger \hat{M}_n = \mathbb{1}_{\mathcal{H}} \, . \tag{1.4}$$

4. *Composite systems*. The state space $\mathcal{H}$ of a composite physical system is the tensor product of the state spaces $\mathcal{H}_i$ of the component physical systems

$$\mathcal{H} = \bigotimes_i \mathcal{H}_i \ . \tag{1.5}$$

If the systems are numbered 1 through N and the j-th system is prepared in the state $|\psi_j\rangle$, then the joint state $|\psi\rangle \in \mathcal{H}$ of the total system is

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle \ . \tag{1.6}$$

The third postulate about quantum measurement is often given in terms of *projective measurements*, that are only a special class of measurements. A projective measurement is described by an *observable*, a Hermitian operator $\hat{O} = \hat{O}^\dagger$ acting on the Hilbert space. The observable has a spectral decomposition,

$$\hat{O} = \sum_n n \hat{P}_n \ , \tag{1.7}$$

where $\hat{P}_n$ is the projector onto the eigenspace of $\hat{O}$ with eigenvalue n. The possible outcomes of the measurement correspond to the eigenvalues of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result n is given by

$$\mathcal{P}(n) = \langle\psi|\hat{P}_n|\psi\rangle \tag{1.8}$$

and, given the outcome n occurred, the state after the measurement is

$$|\psi'\rangle = \frac{\hat{P}_n|\psi\rangle}{\sqrt{\mathcal{P}(n)}} \ . \tag{1.9}$$

It is very easy to calculate average values for projective measurements. The average value of the observable $\hat{O}$ is given by

$$\begin{aligned} \langle\hat{O}\rangle &= \sum_n n\mathcal{P}(n) \\ &= \sum_n n\langle\psi|\hat{P}_n|\psi\rangle \\ &= \langle\psi|\hat{O}|\psi\rangle \ . \end{aligned} \tag{1.10}$$

From this formula follows a formula for the variance $\sigma^2_{\hat{O}}$ associated to observations of $\hat{O}$,

$$\sigma^2_{\hat{O}} = \langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2 \ . \tag{1.11}$$

We have formulated the postulates of Quantum Mechanics using the language of state vectors, or *pure states*, assuming that the state of the system is

completely known. However, we can suppose that the system is in one of a number of states $|\psi_i\rangle$ with respective probabilities p_i . The ensemble $\{p_i, |\psi_i\rangle\}$ is an *ensemble of pure states* and the quantum state of the system in this case is called *mixed state* and it is described by the *density operator*

$$\hat{\rho} \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.12}$$

acting on the Hilbert $\mathcal{H}$ of the system.

The formalism of density operator is more general than the formalism of pure states. Indeed, the density operator for a pure state $|\psi\rangle$ has the form $\hat{\rho} = |\psi\rangle\langle\psi|$. All properties of density operator are listed in [1]. We report here only the fact that the trace of the density operator is unitary

$$\mathrm{Tr}\{\hat{\rho}\} = \sum_i p_i \mathrm{Tr}\{|\psi_i\rangle\langle\psi_i|\} = \sum_i p_i = 1 \ , \tag{1.13}$$

where we have used the definition of *trace operation*

$$\mathrm{Tr}\{|\psi_i\rangle\langle\psi_i|\} \equiv \sum_k \langle k|\psi_i\rangle\langle\psi_i|k\rangle = \langle\psi_i| \left(\sum_k |k\rangle\langle k| \right) |\psi_i\rangle = \langle\psi_i|\psi_i\rangle = 1 \ . \tag{1.14}$$

where $\{|k\rangle\}$ is an orthonormal basis for the Hilbert space $\mathcal{H}$ of the system.

Suppose now to take a unit vector $|\psi\rangle$ and an arbitrary operator $\hat{A}$ acting on the Hilbert space. It is useful to evaluate $\mathrm{Tr}\left\{\hat{A}|\psi\rangle\langle\psi|\right\}$ for what we will see in the following. Using the Gram-Schmidt procedure to extend $|\psi\rangle$ to an orthonormal basis $\{|k\rangle\}$ which includes $|\psi\rangle$ as the first element, then we have:

$$\mathrm{Tr}\left\{\hat{A}|\psi\rangle\langle\psi|\right\} = \sum_k \langle k|\hat{A}|\psi\rangle\langle\psi|k\rangle = \langle\psi|\hat{A}|\psi\rangle \ . \tag{1.15}$$

We have to cite here also an important criterion to decide if a state given by a density operator is mixed or pure: $\hat{\rho}$ describe a pure state if and only if $\mathrm{Tr}\left\{\hat{\rho}^2\right\} = 1$ [1].

In the case of the projective measurement $\hat{O}$ given in (1.7), the mean value of its observations if the system is in the mixed state (1.12) is given by

$$\begin{aligned} \langle\hat{O}\rangle &\equiv \sum_i p_i \langle\psi_i|\hat{O}|\psi_i\rangle \\ &= \sum_i p_i \mathrm{Tr}\left\{|\psi_i\rangle\langle\psi_i|\hat{O}\right\} \\ &= \mathrm{Tr}\left\{ \left(\sum_i p_i |\psi_i\rangle\langle\psi_i| \right) \hat{O} \right\} \\ &= \mathrm{Tr}\left\{\hat{\rho}\hat{O}\right\} \ . \end{aligned} \tag{1.16}$$

We will use some of these formulas in the following.

1.1.2 *The qubit*

Here we present the fundamental concept of Quantum Information, the quantum-bit or *qubit*.

The *bit* is the basic object of classical computation and information. It can take two values, 0 or 1, and the value represents the state of the bit. Two possible quantum states for a qubit are the states $|0\rangle$ and $|1\rangle$, which you can think correspond to the stated 0 and 1 for a classical bit. The great difference between bits and qubits is that a qubit can be in a state *other* than $|0\rangle$ or $|1\rangle$. Indeed, any linear combination of these two states (called *superposition*),

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ , \tag{1.17}$$

where $\alpha, \beta \in \mathbb{C}$, is also a possible quantum state, due to the linear structure of the vector quantum space that describe the system.

More precisely, a qubit "lives" in a two-dimensional state space $\mathcal{H}_{1q} \simeq \mathbb{C}^2$ where $\{|0\rangle, |1\rangle\}$ form an orthonormal basis. The condition that an allowed quantum state $|\psi\rangle$ must be a unit vector given in the first postulate is therefore equivalent to the condition

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.18}$$

for the complex coefficients in (1.17).

In Quantum Information, Computation and Communication the qubit is the fundamental quantum mechanical system and we will see in the following that there are physical systems in which practical qubits can be realized.

A useful representation for a generic qubit can be obtained rewriting (1.17) as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.19}$$

using the normalization condition (1.18). The angles θ and φ define a point on the unit three-dimensional sphere, called *Bloch sphere*, that is represented in Figure 1.1.

In (1.17) the qubit is given by a pure state and it is represented by a point on the surface of the Bloch sphere. On the contrary, an arbitrary density matrix for a mixed state one-qubit may be written as

$$\hat{\rho}_{1q} = \frac{\mathbb{1}_{\mathcal{H}_{1q}} + \mathbf{r}\cdot\boldsymbol{\sigma}}{2} \ , \tag{1.20}$$

where $\mathbf{r}$ is a real three-dimensional vector such that $\|\mathbf{r}\| \leqslant 1$ and $\boldsymbol{\sigma}$ is the "vector" with the three *Pauli matrices*

$$\hat{\sigma}_1 = \hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \hat{\sigma}_2 = \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \hat{\sigma}_3 = \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.21}$$

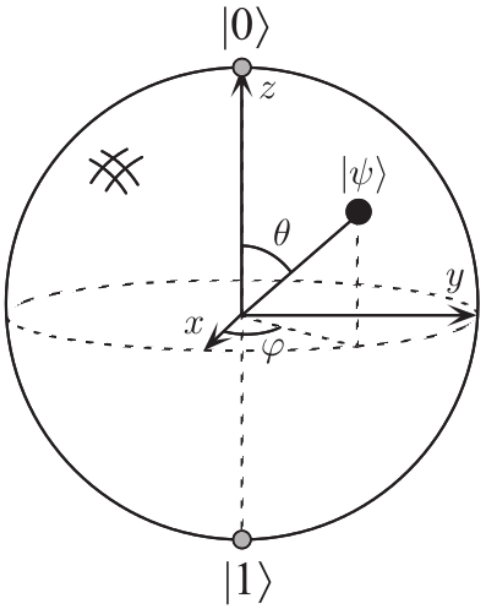


Figure 1.1: Bloch sphere representation of a qubit [1].

as components. The vector $\mathbf{r}$ gives a point on the Bloch sphere and it can be shown that a pure state is characterized by a unit vector $\mathbf{r}$ such that $\|\mathbf{r}\| = 1$ that gives a point on the surface of the sphere, while a true mixed state is represented by a point inside the sphere.

It is possible to use any two-level quantum system in order to create a physical qubit. For example, the spin of an electron or two electronic levels of an atom can be considered for qubit realization. For our purpose, the most important physical system to realize a quantum bit is the *photon*, the light particle. We will see in section 5.1 how to create a *time-bin qubit* using photons.

Now, we concentrate on the simplest way to encode quantum information in a qubit using single photon *polarization*. For example, it is possible to associate the $|0\rangle$ and $|1\rangle$ states, respectively, to the horizontal $|H\rangle$ and vertical $|V\rangle$ states of polarization of a photon. The other photon polarization states often used in Quantum Information realizations are

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) , \tag{1.22}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right) , \tag{1.23}$$

$$|L\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + i|V\rangle\right) , \tag{1.24}$$

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - i|V\rangle\right) , \tag{1.25}$$

where $|\pm\rangle$ represents a photon linearly polarized along a diagonal direction while $|R\rangle$ ($|L\rangle$) represents a right (left) circularly polarized photon. We will use

these state describing the first experimental satellite quantum communication in section 4.2.2.

The polarization encoded qubit can be represent through the Poincaré sphere (Figure 1.2), which is used also in the context of classical polarization [2] and it is quite similar to the Bloch sphere.

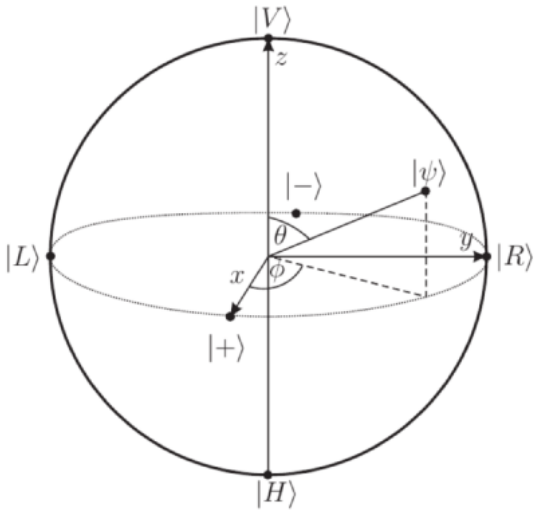


Figure 1.2: Poincaré sphere representation of a polarization encoded qubit.

1.1.3 *The "no-cloning" theorem*

In a classical system the copy of a bit is a simple operation, while in the case of a quantum state a perfect copy of a generic qubit is not allowed. The fact that quantum states cannot be copied is certainly one of the most specific attributes that makes quantum information different from classical information. This negative capability has a great positive counterpart: it prevents a potential enemy from eavesdropping and so it makes Quantum Communication potentially secure, as we will show in the following.

An elementary proof of this theorem can be found in [1]. Suppose that we have a quantum machine with two slots labeled A and B. The A slot starts out in an unknown but pure quantum state $|\psi\rangle$ and the quantum machine has to copy this state into the B slot that starts out in some pure state $|b\rangle$. The initial state of the copying machine is so

$$|\psi\rangle \otimes |b\rangle \ . \tag{1.26}$$

The copying procedure must be effected by an unitary *copying operator* $\hat{U}_C$ that ideally produce

$$|\psi\rangle \otimes |b\rangle \rightarrow \hat{U}_C \left(|\psi\rangle \otimes |b\rangle\right) = |\psi\rangle \otimes |\psi\rangle \ . \tag{1.27}$$

Now, suppose that this copying procedure works for two particular pure states, $|\psi\rangle$ and $|\varphi\rangle$, i.e.,

$$\hat{U}_C\left(|\psi\rangle \otimes |b\rangle\right) = |\psi\rangle \otimes |\psi\rangle \,, \tag{1.28}$$

$$\hat{U}_C\left(|\varphi\rangle \otimes |b\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle \,. \tag{1.29}$$

Taking the inner product of these two equations gives

$$\langle\psi|\varphi\rangle = \left(\langle\psi|\varphi\rangle\right)^2 \tag{1.30}$$

that have only two solutions: either $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. In this way, a copying machine can only clone states which are orthogonal to one another and therefore a general quantum cloning device is impossible.

It can be shown that even if one allows non-unitary copying devices, the cloning of non-orthogonal pure states remains impossible and similar conclusions hold also for mixed states.

1.2 QUANTUM CRYPTOGRAPHY

In this section we describe the first protocol proposed for Quantum Communication, called *Quantum Cryptography* or *Quantum Key Distribution* (QKD) following the clear review [3] by Gisin.

1.2.1 *Basic elements of cryptography*

Cryptography is the art of rendering a message unintelligible to any unauthorized party. To achieve this goal, an algorithm called *cryptosystem* or *cipher* is used to combine a message with a *key* to produce a *cryptogram*. This technique is known as *encryption*. A cryptosystem is secure if it is impossible to unlock the cryptogram (*decryption*) without the key.

The key can be *public*, as in the *RSA cryptosystem* [4]. The security of a public-key cryptosystem is based on computational complexity. For example, the security of RSA is based on the factorization of large integers, a task that Shor has shown could be fastly achieved by using a quantum computer [5], a device that does not yet exist (fortunately in this context!).

On the contrary, the key can be secret and shared by the two communicating parties, traditionally called Alice and Bob. The same key is used for both the encryption and the decryption of the message. The simplest classical secret-key cryptosystem is the *one-time pad*, first proposed by Vernam in 1926 [6] and represented in Figure 1.3.

Alice encrypts her message, a string of bits denoted by the binary number m using a randomly generated key k. She simply adds each bit of the message to the corresponding bit of the key to obtain the encrypted text

$$t = m \oplus k \,, \tag{1.31}$$

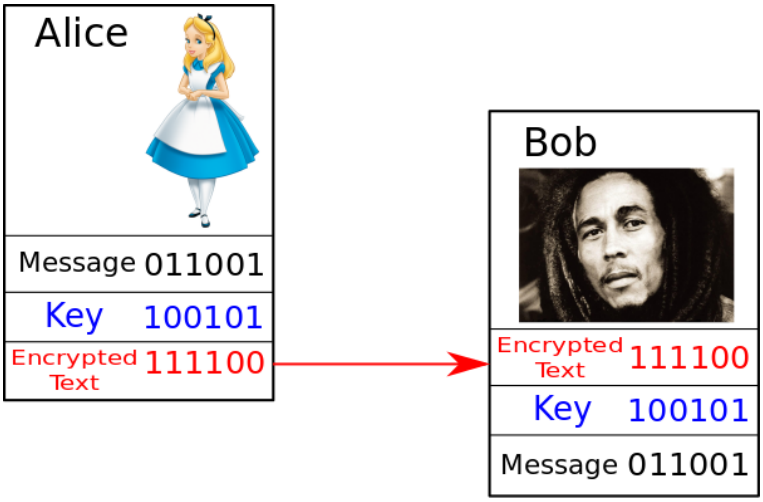


Figure 1.3: One-time pad cryptosystem.

where $\oplus$ denotes the binary addition modulo 2 without carry. The encrypted text t is sent to Bob, who decrypts the message by adding the same key k because

$$t \oplus k = m \oplus k \oplus k = m \,. \tag{1.32}$$

Due to the fact that the bits of the encrypted text t are as random as those of the key, they do not contain any information about the message which Alice and Bob want to share. Shannon in 1949 showed that this cryptosystem is secure according to classical information [7].

The problem of this system is that it is essential for Alice and Bob to possess a common secret key that must be at least as long as the message itself. Further, they can use the key for a single encryption only. They key has to be transmitted by some trusted means, such a courier, or through a personal meeting between Alice and Bob: this is a procedure evidently complex and expensive. As we will show now, Quantum Key Distribution aims to solve the problem of distributing long sequences of key bits in a secure and fascinating way.

1.2.2 *Quantum Key Distribution*

The idea of Quantum Key Distribution is very simple: it turns one of the basic negative statements of Quantum Mechanics *"One cannot take a measurement without perturbing the system"* into a positive resource. Think to this statement applied to a communication between Alice and Bob: it applies also to eavesdroppers, i.e., to a malicious third person, traditionally called Eve, that wants to get information about the communication without introducing perturbations that would reveal her presence. For example, Alice can code information in individual photons which she sends to Bob. If Bob receives the photons unperturbed it means that they were not measured and this

implies that Eve did not get any information about the state of the photons. Alice and Bob can check whether someone was listening and stop their secret conversation.

Actually, Alice and Bob have to complete this nice idea thinking to the one-time pad cryptosystem described above. They do not use photons to transmit information, but only to transmit the random key that contains no information about the message they want to share. If the key is unperturbed, then quantum physics guarantees that no one has gotten any information about this key by eavesdropping and they can safely use it to encode their messages. On the contrary, if the key is perturbed they disregard it and repeat the operation until they are secure to share a secret common key.

The first protocol for QKD was proposed in 1984 by Bennet and Brassard [8] and it is called BB84. We now describe this protocol using the language of photon polarization, but clearly any qubit system would do. BB84 uses four quantum states that constitutes two mutually orthonormal bases, as the horizontal-vertical basis $\{|H\rangle, |V\rangle\}$ and the diagonal-antidiagonal one $\{|+\rangle, |-\rangle\}$ introduced in section 1.1.2.

Conventionally, they attribute the binary value 0 to state $|H\rangle$ and $|+\rangle$ and the value 1 to the other two states $|V\rangle$ and $|-\rangle$. In the first step, Alice sends to Bob individual photons in states *chosen at random* among the four states. Next, Bob measures the incoming photons in one of the two bases, *chosen at random*. In this way, when they use the same basis, they get perfectly correlated results and when they use different bases, they get uncorrelated results, as shown in Figure 1.4.

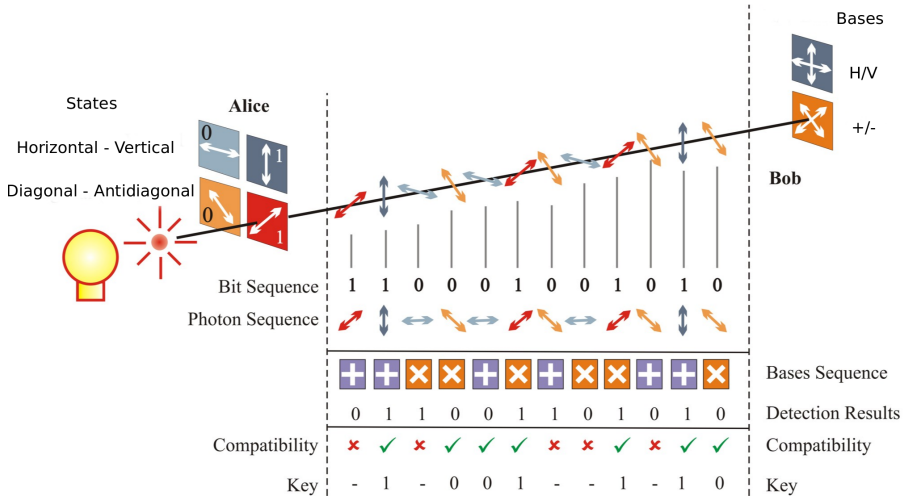


Figure 1.4: BB84 protocol for QKD implemented using photon polarization encoding [http://swissquantum.idquantique.com/IMG/jpg/bb84.jpg].

On average, Bob obtains a string of bits with a 25% error rate, called *raw key*. This error rate is too high to apply standard *error correction schemes*, but Alice and Bob know which bits are perfectly correlates: the ones for which they used the same basis. So, the following procedure for error correction is

possible. For each bit Bob announces publicly in which basis he measured the qubit, without saying the result. Alice then reveals only whether or not the state in which she encoded that qubit is compatible with the basis announced by Bob. They keep the bit if and only if the two bases are compatible and so they discard about 50% of the bit string. The key obtained after this *basis reconciliation* is called *sifted key*. It is to note that to perform the basis reconciliation Alice and Bob use a public channel and so Eve can listen to all the communication.

Now, we have to consider the *security* of this ideal protocol. If Eve intercepts a qubit propagating from Alice to Bob then he does not receive an expected qubit and he will simply tell Alice to disregard it. In this way, Eve only lowers the bit rate, but she does not gain any useful information about the secret key. For real eavesdropping she must send a qubit to Bob in its original state, keeping a copy for herself. But, for the no-cloning theorem shown above, Eve cannot keep a perfect quantum clone and so the no-cloning theorem makes QKD potentially secure.

Another common eavesdropping strategy is called *intercept-resend*. Eve measures each qubit in one of the two bases, precisely as Bob does and then she resends to him another qubit in the state corresponding to her measurement result. In about half of the cases, Eve chooses the basis compatible with the state prepared by Alice and so resends to Bob a qubit in the correct state. In this case, Alice and Bob cannot notice her intervention. But, in the other half of the cases, Eve uses the basis incompatible with Alice's qubit. So, Alice and Bob can discover her intervention in about half of these cases.

At this point of the protocol, Alice and Bob share the sifted key that contains errors that can be caused by technical imperfections as well as possibly by Eve's intervention. The error rate in the sifted key is called *QBER*, for *quantum bit error rate*. This situation in which the two legitimate parties share a classical information with high but not 100% correlation and with possibly some correlation to a third party is common to all quantum and classical cryptosystem. Consequently, the last step in a QKD protocol uses classical algorithms, first to correct the errors (*error correction*) and then to reduce Eve's information on the final key (*privacy amplification*). These two classical algorithms are sketched briefly in [3] and we remand to the extensive literature about them for more details.

We have described the fundamental idea of QKD and the simplest protocol, introducing the fundamental terms used in this context. We will see in section 5.2 how to implement the BB84 protocol using *phase encoding*, but also other protocols were invented in the last thirty years (see [3] for a brief review). Now, we will describe some practical elements that characterize a QKD cryptosystem realized using photons.

1.2.3 *Elements of practical QKD with faint laser pulses*

The first QKD demonstration was experimentally performed at IBM laboratory in the early 1990s over a distance of 30 centimeters [9]. This short distance is clearly of little practical interest, but it marked the start of a series of impressive experimental improvements. Most of the QKD realization so far uses *optical fibers* to guide the photons from Alice to Bob, but also important studies and implementations involve *free-space* quantum channel. Free-space Earth-to-satellite or satellite-to-Earth links are one of the paths to realize a global QKD network and they will be discussed in more details in chapter 4 because they represent one of the main topic of this thesis.

Optical QKD, as we have already said, is based on the use of single photons. Theoretically, they are described by a Fock state (see section 3.4 for details) and experimentally these states are difficult to realize. For this reason, practical implementations of QKD rely on *faint laser pulses* in which the photon number distribution obey Poisson statistics, as we will show in section 3.4. The idea is to approximate a single photon Fock state with a coherent pulse with an ultralow mean photon number μ that can be easily realized using standard laser sources and calibrated attenuators.

As we will justify in (3.63), the probability of finding n photons in a coherent state with mean photons number μ is

$$\mathcal{P}(n) = e^{-\mu}\frac{\mu^n}{n!} \tag{1.33}$$

and so the probability that a nonempty weak coherent pulse contains more than one photon is given by the conditional probability

$$\begin{aligned}\mathcal{P}(n > 1|n > 0) &= \frac{1-\mathcal{P}(0)-\mathcal{P}(1)}{1-\mathcal{P}(0)} \\ &= \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}} \approx \frac{\mu}{2}\,.\end{aligned} \tag{1.34}$$

This value can be made arbitrarily small and so weak pulses are very practical and are used in the vast majority of experiments. However, there is a problem: if μ is small, most pulses are empty because

$$\mathcal{P}(0) \approx 1-\mu\,. \tag{1.35}$$

This fact brings to the practical problem of detectors' *dark counts*, i.e., a detection "click" without a photon's arriving. This prevents the use of really low photon numbers and most experiments to date have realized with mean photons number values close to $\mu = 0.1$, meaning that 5% of the nonempty pulses contain more than one photon.

The pseudo-single photon source and the detectors must be connected by a *quantum channel*. It is not especially quantum, except that it is intended to carry information encoded in individual quanta, like individual photons.

One of the experimental parameters used to compare different QKD setups is the quantum bit error rate. The QBER is defined as the ratio of wrong bits N_{wrong} to the total number of bits received $N_{wrong} + N_{right}$ and it is normally of the order of a few percent. An expression for the QBER in terms of the of bit rates is given by [3]:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{err}}{R_{sift} + R_{err}} \approx \frac{R_{err}}{R_{sift}} \, . \tag{1.36}$$

The sifted key rate correspond to the cases in which Alice and Bob made compatible choices of bases and so its rate is half that of the raw key rate R_{raw}

$$R_{sift} = \frac{1}{2} R_{raw} \, . \tag{1.37}$$

Then, the raw key rate can be modeled by the product of the pulse rate f_{rep}, the mean number of photons per pulse μ, the probability t_{link} of a photons arriving at the detector and the probability η of the photon's being detected:

$$R_{raw} = f_{ref} \mu t_{link} \eta \, . \tag{1.38}$$

The error rate R_{err} has two main different contributions. The first one arises from photons that are detected in the wrong detector due to experimental optical imperfections. Its rate R_{opt} is given by the product of the sifted key rate and the probability p_{opt} of a photon's going to the wrong detector

$$R_{opt} = R_{sift} p_{opt} \tag{1.39}$$

and it is an intrinsic error rate of the setup. The second contribution R_{det} arises from detector dark counts and it is proportional to the pulse rate, to the probability p_{dark} of registering a dark count per detector, the number n of detectors according to

$$R_{det} = \frac{1}{4} f_{rep} p_{dark} n \, . \tag{1.40}$$

The proportional factor of $1/4$ arises from the fact that a dark count has a 50% probability of happening when Alice and Bob have chosen incompatible bases and the same chance of occurring in the correct detector.

In this way, the QBER can be splitted in two terms

$$QBER = QBER_{opt} + QBER_{det} \tag{1.41}$$

where

$$QBER_{opt} = \frac{R_{opt}}{R_{sift}} = p_{opt} \tag{1.42}$$

$$QBER_{det} = \frac{R_{det}}{R_{sift}} = \frac{p_{dark} n}{2 t_{link} \eta \mu} \tag{1.43}$$

The "optical" quantum bit error rate $QBER_{opt}$ can be considered as a measure of the optical quality of the setup, depending only on the polarization contrast in the case of polarization encoding. We will see in chapter 6 that in the case of phase encoding the characterizing experimental parameter is the visibility $\mathcal{V}$ of the interference fringes. In the case of phase encoding the optical QBER is estimated according to

$$QBER_{opt} = \frac{1-\mathcal{V}}{2} \,. \tag{1.44}$$

With the QBER, it is possible to estimate the secret key rate R obtainable with the BB84 protocol, defined as the fraction of the length of the fully secure key L and of the length of the raw key M in the asymptotic case of infinitely long keys, i.e.,

$$R = \lim_{N\to\infty} \frac{L}{M} \,, \tag{1.45}$$

where N is the number of exchanged and measured quanta. The QBER and the secret key rate R are related by [10]

$$R = 1 - 2h(QBER) \,, \tag{1.46}$$

where h is the *binary entropy* defined as

$$h(q) = -q\log_2 q - (1-q)\log_2(1-q) \,. \tag{1.47}$$

It is easy to check that the rate (1.46) goes to 0 for $QBER \gtrsim 11\%$.

1.3 QUANTUM COMMUNICATION WITH ENTANGLEMENT

QKD is only one of the protocols for Quantum Communication. Now we discuss other protocols which are based on *entanglement* that is a purely quantum phenomenon: none of the protocols discussed here following [11] are possible classically.

Alice and Bob can share an entangled state and use it for *dense coding*, in which Alice sends to Bob two bits of classical information using one qubit of a entangled pair. Alice and Bob can also use an entangled state for *teleportation*, in which a qubit in an unknown state is teleported from Alice to Bob when Alice sends Bob two classical bits. It is also possible to make entangled two systems that have never interact before using *entanglement swapping*.

All of these Quantum Communications protocols require also a classical communication and for this reason they do not break the laws of Relativity, which says that nothing can travel faster than the speed of light.

1.3.1 *Entanglement*

Entanglement is a property of two or more quantum systems which exhibit *correlations* that cannot be explained by classical physics.

Entanglement is related to the fourth postulate of Quantum Mechanics that rules composite systems. Suppose we have quantum system made up of two subsystems A and B. The Hilbert space $\mathcal{H}$ of the system is given by

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \tag{1.48}$$

where $\mathcal{H}_A$ and $\mathcal{H}_B$ are the Hilbert spaces for the quantum systems A and B respectively. A pure state $|\psi\rangle \in \mathcal{H}$ is called *separable* if there exist two pure states $|a\rangle_A \in \mathcal{H}_A$ and $|b\rangle_B \in \mathcal{H}_B$ such that

$$|\psi\rangle = |a\rangle_A \otimes |b\rangle_B \equiv |a\rangle_A |b\rangle_B \equiv |a_A b_B\rangle \ , \tag{1.49}$$

where in the last equalities we introduced a shorter notation for composite states. If the pure state $|\psi\rangle$ is not separable, it is called *entangled*.

In the following we will consider system made up of two or more qubits system. For example, take the two-qubit Hilbert space

$$\mathcal{H}_{2q} = \mathcal{H}_{1q,A} \otimes \mathcal{H}_{1q,B} = \mathbb{C}^2_A \otimes \mathbb{C}^2_B \ . \tag{1.50}$$

where the canonical basis for each single qubit space $\mathcal{H}_{1q}$ is given by

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ . \tag{1.51}$$

The four states

$$|\Phi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle \pm |1_A 1_B\rangle \right) \ , \tag{1.52}$$

$$|\Psi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}} \left(|0_A 1_B\rangle \pm |1_A 0_B\rangle \right) \tag{1.53}$$

are examples of entangled states because they cannot be expressed as a composition of two qubit states. They are called *Bell states* and form an orthonormal basis for the Hilbert space $\mathcal{H}_{2q}$ of the two-qubit system.

For discussing dense coding it is useful to rewrite the Pauli matrices introduced in (1.21) in terms of the canonical basis $\{|0\rangle, |1\rangle\}$ introduced in (1.51):

$$\hat{\sigma}_1 = |1\rangle\langle 0| + |0\rangle\langle 1| \ , \tag{1.54}$$

$$\hat{\sigma}_2 = i|1\rangle\langle 0| - i|0\rangle\langle 1| \ , \tag{1.55}$$

$$\hat{\sigma}_3 = |0\rangle\langle 0| - |1\rangle\langle 1| \ . \tag{1.56}$$

We can now describe in more details the operation principle for the Quantum Communication protocols based on entanglement announced above.

1.3.2 *Dense coding*

In the dense coding protocol Alice and Bob initially share one of the four Bell states. Alice uses the Pauli matrices to change the shared state and she can send to Bob two bits of classical information by sending him a qubit, which is her half of the entangled Bell state shared. Dense coding provides in this way an example that Quantum Information differs from any sort of classical one, because she encodes two bits into one qubit.

Suppose that Alice and Bob share the Bell state

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle\right) \ . \tag{1.57}$$

Alice would like to send to Bob two bits x and y of classical information. The two parties have agreed in advance some unitary operations that Alice will perform depending on the values of the two bits. Alice reads the first bit x: if $x = 0$, she does not perform any unitary transformation on her qubit; if $x = 1$, she performs a swap operation $\hat{\sigma}_1$ on her qubit

$$x = 0: \quad |\Phi^+\rangle \to (\mathbb{1}_2 \otimes \mathbb{1}_2)|\Phi^+\rangle = |\Phi^+\rangle \ , \tag{1.58}$$

$$x = 1: \quad |\Phi^+\rangle \to (\hat{\sigma}_1 \otimes \mathbb{1}_2)|\Phi^+\rangle = |\Psi^+\rangle \ . \tag{1.59}$$

Then, she reads the second bit y: if $y = 0$, she does not perform any transformation; if $y = 1$, she performs a phase shift $\hat{\sigma}_3$ on her qubit. The phase shift changes $|\Phi^+\rangle$ and $|\Psi^+\rangle$ to $|\Phi^-\rangle$ and $|\Psi^-\rangle$ respectively. Using the Pauli matrices, one can easily check that

$$\hat{\sigma}_3 \hat{\sigma}_1 = i\hat{\sigma}_2 \ . \tag{1.60}$$

Summarizing, the transformations Alice applies to her qubit depending on the values of the two bit are

$$x = 0, y = 0: \quad |\Phi^+\rangle \to (\mathbb{1}_2 \otimes \mathbb{1}_2)|\Phi^+\rangle = |\Phi^+\rangle \ , \tag{1.61}$$

$$x = 1, y = 0: \quad |\Phi^+\rangle \to (\hat{\sigma}_1 \otimes \mathbb{1}_2)|\Phi^+\rangle = |\Psi^+\rangle \ , \tag{1.62}$$

$$x = 0, y = 1: \quad |\Phi^+\rangle \to (\hat{\sigma}_3 \otimes \mathbb{1}_2)|\Phi^+\rangle = |\Phi^-\rangle \ , \tag{1.63}$$

$$x = 1, y = 1: \quad |\Phi^+\rangle \to (i\hat{\sigma}_2 \otimes \mathbb{1}_2)|\Phi^+\rangle = |\Psi^-\rangle \ . \tag{1.64}$$

In this way, after the Alice's transformation, Alice and Bob share of of the four Bell states. But, they cannot deduce from measurements on their own system which Bell state they share. However, Alice can send to Bob her qubit, in which case Bob has one of the four orthonormal Bell states. Performing a *Bell state measurement*, he can measure which Bell state he has and so deduce the values of the two bit x and y transmitted by Alice.

1.3.3 *Quantum teleportation*

Quantum teleportation is a process by which Alice can send to Bob one qubit in an *unknown state* $|\psi\rangle$ by sending Bob two classical bits. Alice and Bob must initially share an entangled Bell state. When classical bits are sent over a classical channel, it is then possible for Alice to retain a copy. But, the no-cloning theorem says that it is impossible for Alice to copy an unknown quantum state. Indeed, when she sends $|\psi\rangle$ to Bob, she retains no information about the state of $|\psi\rangle$. It is as if the state $|\psi\rangle$ moves from Alice to Bob, hence the name teleportation. It is to note that not the entire object, but only its quantum state is transferred from Alice to Bob without ever existing at any intermediate location.

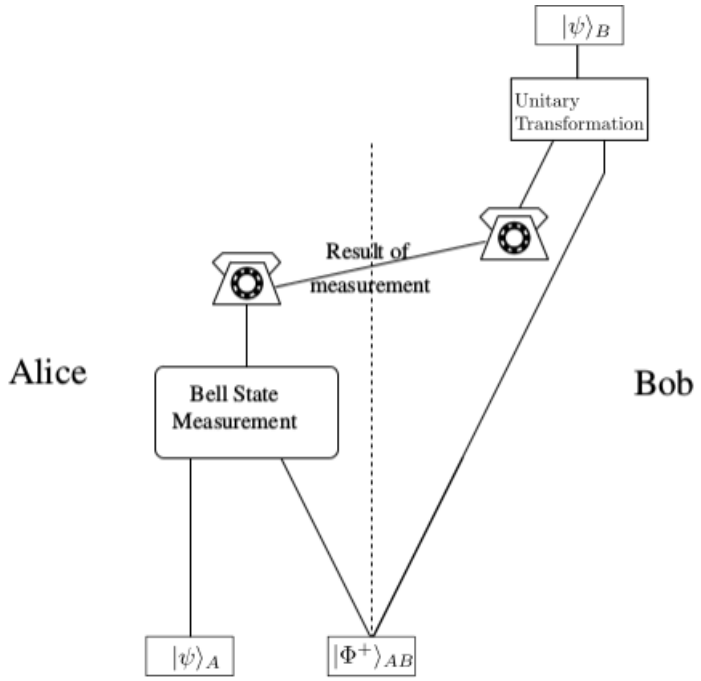


Figure 1.5: Quantum teleportation protocol for Quantum Communication [11].

Initially, Alice and Bob share the entangled Bell state

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right) \ . \tag{1.65}$$

Suppose that Alice also has a qubit $|\psi\rangle_A$ in an unknown quantum state

$$|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A \ . \tag{1.66}$$

This is the state she wants to teleport to Bob, as shown in Figure 1.5. The state must be unknown to her, because otherwise she can just phone Bob up and tell him all details of the state to let him recreate it.

The initial state of the system is so a three-qubits state

$$|\psi\rangle_A|\Phi^+\rangle_{AB} = (\alpha|0\rangle_A + \beta|1\rangle_A) \otimes \frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right) \tag{1.67}$$

that can be expanded as

$$\begin{aligned}|\psi\rangle_A|\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(\alpha|0_A0_A0_B\rangle + \alpha|0_A1_A1_B\rangle + \beta|1_A0_A0_B\rangle + \beta|1_A1_A1_B\rangle\right)\\ &= \frac{1}{2}\left[|\Phi^+\rangle_{AA}(\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_{AA}(\alpha|0\rangle_B - \beta|1\rangle_B) + \right.\\ &\quad \left. + |\Psi^+\rangle_{AA}(\alpha|1\rangle_B + \beta|0\rangle_B) + |\Psi^-\rangle_{AA}(\alpha|1\rangle_B - \beta|0\rangle_B)\right] . \end{aligned} \tag{1.68}$$

The two qubits of Alice are now written in terms of the four Bell states, while the state of Bob's qubit in all four cases is very similar to the original qubit that Alice has to teleport to him.

Alice now performs a Bell state measurement on her part of the system, to deduce which Bell state she has. Then, she uses two bits of classical information to communicate (classically) to Bob the result of her measurement. In this way, now Bob knows which of the four states $\alpha|0\rangle_B \pm \beta|1\rangle_B$, $\alpha|1\rangle_B \pm \beta|0\rangle_B$ he has and can apply a defined unitary transformation to his system to obtain the teleported state

$$|\psi\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B . \tag{1.69}$$

Indeed, it is easy to check that there exists such an unitary transformation for each one of Alice's outcomes:

$$|\Phi^+\rangle_{AA} \Rightarrow \quad \mathbb{1}_2(\alpha|0\rangle_B + \beta|1\rangle_B) = |\psi\rangle_B , \tag{1.70}$$

$$|\Phi^-\rangle_{AA} \Rightarrow \quad \hat{\sigma}_3(\alpha|0\rangle_B - \beta|1\rangle_B) = |\psi\rangle_B , \tag{1.71}$$

$$|\Psi^+\rangle_{AA} \Rightarrow \quad \hat{\sigma}_1(\alpha|1\rangle_B + \beta|0\rangle_B) = |\psi\rangle_B , \tag{1.72}$$

$$|\Psi^-\rangle_{AA} \Rightarrow \quad \hat{\sigma}_1\hat{\sigma}_3(\alpha|1\rangle_B - \beta|0\rangle_B) = |\psi\rangle_B . \tag{1.73}$$

1.3.4 *Entanglement swapping*

What does it happen if one photon from an entangled pair is teleported, that is, if entanglement itself is teleported? This process, know as entanglement swapping, allows one to entangle particles that have no common past. If Alice and Bob have never interacted, it is enough that Alice is entangled with Charlie and also Bob is entangled with Charlie to make Alice and Bob entangled.

Suppose that Alice and Charlie share an entangled pair $|\Psi^-\rangle_{Ac}$ and that Charlie and Bob share the pair $|\Psi^-\rangle_{CB}$. The initial state of the four-qubits system is given by

$$|\Psi^{swapp}\rangle = |\Psi^-\rangle_{Ac} \otimes |\Psi^-\rangle_{CB} \tag{1.74}$$

that can be expanded as [12]

$$\begin{aligned}|\Psi^{swapp}\rangle = \frac{1}{2}\left[|\Psi^+\rangle_{AB} \otimes |\Psi^+\rangle_{cC} - |\Psi^-\rangle_{AB} \otimes |\Psi^-\rangle_{cC}\right.\\ \left. - |\Phi^+\rangle_{AB} \otimes |\Phi^+\rangle_{cC} + |\Phi^-\rangle_{AB} \otimes |\Phi^-\rangle_{cC}\right] . \end{aligned} \tag{1.75}$$

Charlie can perform a Bell state measurement on his two qubits, c and C, and so they become entangled. Suppose, for example, that Charlie performs his Bell measurement and finds the result corresponding to the state $|\Phi^+\rangle_{cC}$. The resulting state of Alice's and Bob's qubits is then proportional to

$$\left(\mathbb{1}_{AB} \otimes \hat{P}^{\Phi^+}_{cC}\right) |\Psi^{swapp}\rangle = \left(\mathbb{1}_{AB} \otimes |\Phi^+\rangle_{cC}\langle\Phi^+|_{cC}\right) |\Psi^{swapp}\rangle \propto |\Phi^+\rangle_{AB}|\Phi^+\rangle_{cC} \,. \tag{1.76}$$

Consequently Alice and Bob also become entangled and entanglement swapping is achieved. Depending on the outcome, Charlie tells Bob to apply to his qubit one of the four Pauli matrices to transform the state he shared with Alice in one well defined Bell state.

The entanglement swapping protocol itself has been experimentally demonstrated with various physical systems. It is at the heart of Quantum Information applications and the foundations of quantum physics and is a crucial ingredient for *quantum repeaters*, third-man quantum cryptography, loophole-free Bell tests and other fundamental tests of Quantum Mechanics [12].

2

BEAM OPTICS AND LASER THEORY

Classically, light is described by *electromagnetic waves* that satisfy the *wave equation* derived from Maxwell's equations. Many solutions of the wave equation are available, for example light can be confined in the form of *beams*, i.e., waves that are spatially localized and non diverging. The *Gaussian beam* exhibits these characteristics and it is a particularly important solution of the wave equation because it is the beam produced by the common *laser oscillator*, the most important tool of modern experiments involving classical or quantum optics.

In this chapter we present the *Gaussian Optics* and a brief review of *laser theory*, including the description of the effects of simple optical elements, as thin lenses, on a Gaussian beam, some aspects of light-matter interaction that are important to characterize the properties of the laser light and some elements of *non-linear optics* that we will use in the following.

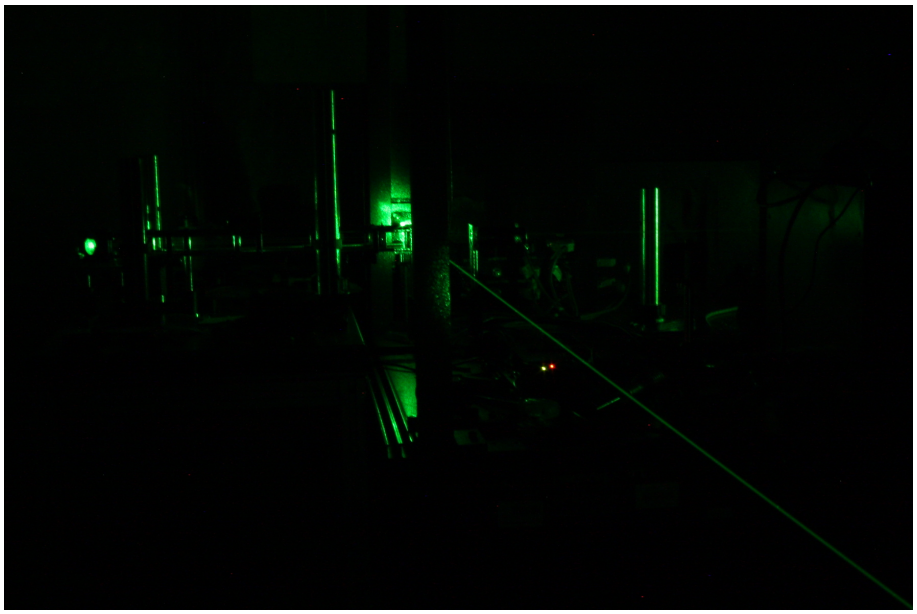


Figure 2.1: A picture of the laser beam used at MLRO in Matera.

2.1 CLASSICAL THEORY OF ELECTROMAGNETIC FIELDS

In this section we present a brief review of the classical theory of electromagnetic field that we use in the following to introduce the Gaussian beam in the next section and the *formalism of the second quantization* to achieve a quantum mechanical description of light in the next chapter.

A classical electromagnetic field is described by two related vectors fields that are real functions of position and time: the electric field $\mathbf{E}(\mathbf{r}, t)$ and the magnetic field $\mathbf{B}(\mathbf{r}, t)$. In the vacuum the Maxwell's equations in absence of sources reduce to

$$\nabla^2\mathbf{E} - \frac{1}{c^2}\frac{\partial^2\mathbf{E}}{\partial t^2} = 0, \tag{2.1}$$

$$\nabla^2\mathbf{B} - \frac{1}{c^2}\frac{\partial^2\mathbf{B}}{\partial t^2} = 0, \tag{2.2}$$

where c is the speed of light in the vacuum. Since the common detectors are usually sensitive to the electric rather then the magnetic field, in the following we discuss only the field $\mathbf{E}(\mathbf{r}, t)$. We also assume that the field is *polarized* along a fixed direction given by a unit real constant vector $\mathbf{u}$ such that $\mathbf{E}(\mathbf{r}, t) = u(\mathbf{r}, t)\mathbf{u}$ and we can use the scalar description of light waves given by the real classical *wavefunction* $u(\mathbf{r}, t)$ to simplify the treatment. Due to equation (2.1) the wave function satisfies the *wave equation*

$$\nabla^2 u(\mathbf{r}, t) - \frac{1}{c^2}\frac{\partial^2 u(\mathbf{r}, t)}{\partial t^2} = 0\ . \tag{2.3}$$

This equation is linear and so the *principle of superposition* applies: given two or more solutions of the wave equation, also their sum is a solution of the same wave equation.

The wave equation takes a simpler form if the wave is monochromatic, i.e., its wavefunction has harmonic time dependence:

$$u(\mathbf{r}, t) = a(\mathbf{r}) \cos\left(\varphi(\mathbf{r}) + \omega t\right) \tag{2.4}$$

where $a(\mathbf{r})$ is a positive real function that describe wave amplitude, $\varphi(\mathbf{r})$ is a real function describing the *phase* of the field and ω is the angular frequency (related to the frequency ν by $\omega = 2\pi\nu$). In the classical treatment it is common to represent the real wavefunction $u(\mathbf{r}, t)$ of a monochromatic wave in terms of a complex function

$$U(\mathbf{r}, t) = a(\mathbf{r})e^{i\varphi(\mathbf{r})}e^{i\omega t} \tag{2.5}$$

so that

$$u(\mathbf{r}, t) = \mathrm{Re}\left[U(\mathbf{r}, t)\right]\ . \tag{2.6}$$

We can write also

$$U(\mathbf{r}, t) = U(\mathbf{r})e^{i\omega t} \tag{2.7}$$

defining the *complex amplitude* $U(\mathbf{r}) \equiv a(\mathbf{r})e^{i\varphi(\mathbf{r})}$, whose magnitude $|U(\mathbf{r})| = a(\mathbf{r})$ is the amplitude of the wave. Inserting (2.7) into the wave equation (2.3) we get the *Helmholtz equation*

$$\nabla^2 U(\mathbf{r}) + k^2 U(\mathbf{r}) = 0 \,, \tag{2.8}$$

where

$$k \equiv \omega/c \tag{2.9}$$

is called the *wavenumber*.

The *optical intensity* of a classical monochromatic wave is defined as the square modulus of its complex wavefunction

$$I(\mathbf{r}) = |U(\mathbf{r})|^2, \tag{2.10}$$

and for a monochromatic wave it does not vary with time.

The simplest example of solution for the Helmholtz equation (2.8) is the *plane wave*

$$U(\mathbf{r}) = Ae^{-i\mathbf{k}\cdot\mathbf{r}} \tag{2.11}$$

where A is a complex constant and $\mathbf{k}$ is a real three-dimensional vector, called *wavevector*, that gives the direction of propagation with magnitude equal to the wavenumber k to respect (2.8). This solution is called plane wave because the surfaces of constant phase, called *wavefronts*, describe parallel planes perpendicular to the wavevector $\mathbf{k}$ separated by the *wavelength*:

$$\lambda = \frac{2\pi}{k} = \frac{c}{\nu} \,. \tag{2.12}$$

Another example of solution is the *spherical wave*

$$U(\mathbf{r}) = \frac{A_0}{r} e^{-ikr} \,, \tag{2.13}$$

where we have use spherical coordinates so $r = |\mathbf{r}|$ and A_0 is a complex constant. In this case the wavefronts are concentric spheres separated by a radial distance $\lambda = 2\pi/k$ that advance radially at velocity c.

The plane wave and the spherical wave represent the two extremes of angular and spatial confinement, respectively. The normals to the wavefronts of a plane wave are parallel to the direction of propagation given by the wavevector so there is no angular spread, but the wave is completely delocalized because it extends over all of space. Conversely, the normals to the wavefronts of a spherical wave diverge in all angular directions, but the wave originates from a single spatial point.

There is also light that can be confined in the form of beams, i.e., waves with Gaussian intensity distribution in any transverse plane to the direction of propagation so that the power is concentrated within a small cylinder around the beam axis and with angular divergence of the wavefront normals that assumes the minimum value permitted by the wave equation for a given width. Such type of light is described in the following section and it is product by an ideal laser source, as we will show in the following.

2.2 GAUSSIAN OPTICS

In this section we describe the main properties of a Gaussian beam and its behavior when it is transmitted through a lens or it is confined in a *optical resonator*, as in the case of the common laser oscillator.

2.2.1 *The Gaussian Beam*

A light wave is called *paraxial wave* when its wavefront normals are paraxial, i.e., when they make small angles with the direction of propagation. One way to construct a paraxial wave is to take a plane wave Ae^{-ikz} propagating in the z direction and modify its *complex envelope* A making it a slowly varying function of position, i.e., $A \to A(\mathbf{r})$, so the complex amplitude becomes

$$U(\mathbf{r}) = A(\mathbf{r})e^{-ikz} \, . \tag{2.14}$$

The envelope must be approximately constant within a neighborhood of size $\lambda = 2\pi/k$ to have a wave that is locally like a plane wave with paraxial wavefront normals.

The complex amplitude (2.14) must satisfies the Helmholtz equation (2.8) and this implies that the envelope $A(\mathbf{r})$ respects the *paraxial Helmholtz equation* [2]:

$$\nabla_T^2 A(\mathbf{r}) - 2ik\frac{\partial A(\mathbf{r})}{\partial z} = 0 \, , \tag{2.15}$$

where $\nabla_T^2 = \partial^2/\partial x^2 + \partial^2/\partial y^2$ is the transverse part of the Laplacian operator.

The simplest solution of equation (2.15) is given by the *paraboloidal wave*

$$A(\mathbf{r}) = \frac{A_1}{z}e^{-ik\frac{\rho^2}{2z}} \, , \tag{2.16}$$

where

$$\rho^2 = x^2 + y^2 \tag{2.17}$$

and A_1 is a complex constant. This wave is the paraxial approximation of the spherical wave (2.13) if $\rho = \sqrt{x^2+y^2} \ll z$.

The *Gaussian beam* is another solution of the paraxial Helmholtz equation obtained from (2.16) with a transformation of the z coordinate. Replacing z with $q(z) \equiv z + iz_0$, where z_0 is a real parameter called *Rayleigh range*, we get a shifted version of the paraboloidal wave in the form

$$A(\mathbf{r}) = \frac{A_0}{q(z)}e^{-ik\frac{\rho^2}{2q(z)}} \tag{2.18}$$

that is also a solution of (2.15).

We can define two real function $R(z)$ and $W(z)$ such that

$$\frac{1}{q(z)} = \frac{1}{R(z)} - i\frac{\lambda}{\pi W^2(z)} \tag{2.19}$$

and substitute (2.18) in (2.14) to obtain the *Gaussian beam complex amplitude*

$$U(\mathbf{r}) = \frac{A_0}{iz_0}\frac{W_0}{W(z)} e^{-\frac{\rho^2}{W^2(z)}} e^{-i\left[kz+k\frac{\rho^2}{2R(z)}-\zeta(z)\right]}, \tag{2.20}$$

where

$$W(z) = W_0\sqrt{1+\left(\frac{z}{z_0}\right)^2} \tag{2.21}$$

$$R(z) = z\left[1+\left(\frac{z_0}{z}\right)^2\right] \tag{2.22}$$

$$\zeta(z) = \tan^{-1}\left(\frac{z}{z_0}\right) \tag{2.23}$$

and W_0 is related to the Rayleigh range z_0 by

$$\pi W_0^2 = \lambda z_0 \,. \tag{2.24}$$

The expression (2.20) is the most important result of this section. It shows that the Gaussian beam is characterized by the two parameter A_0 and z_0 which are determined from the boundary condition of the wave equation, while all the other parameters are related to the Rayleigh range z_0 and to the wavelength λ.

We can now discuss some properties of the Gaussian beam that will be use in the following.

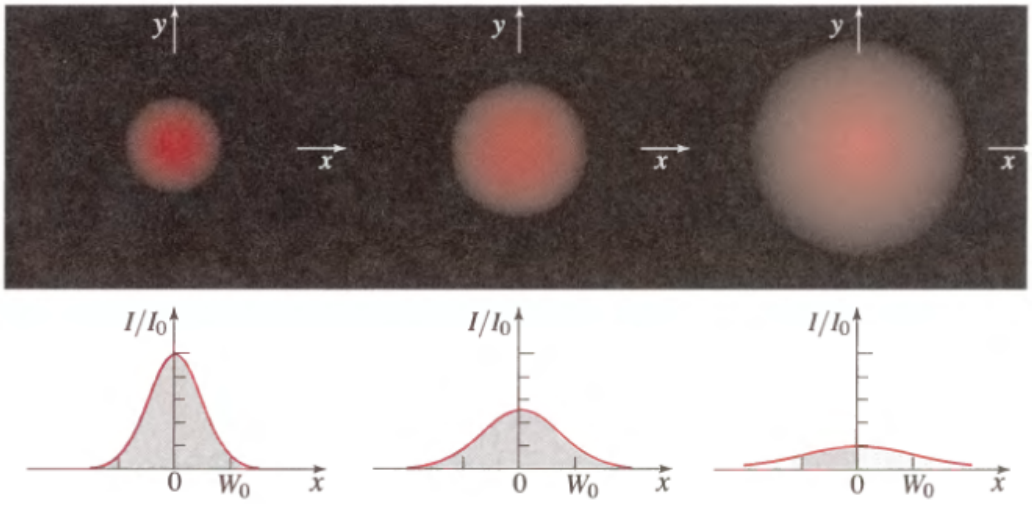


Figure 2.2: Normalized intensity I/I_0 as function of the radial distance ρ at different points: $z = 0$, $z = z_0$ and $z = z_0$ [2].

The optical intensity results a Gaussian function of the distance ρ at each fixed value of z:

$$I(\rho, z) = I_0\left[\frac{W_0}{W(z)}\right]^2 e^{-\frac{2\rho^2}{W^2(z)}}, \tag{2.25}$$

where $I_0 = |A_0/iz_0|^2$, as shown in Figure 2.2. Within any transverse plane, the beam intensity assumes its peak value on the beam axis and drops by the factor $1/e^2$ at the radial distance $\rho = W(z)$. For this reason, $W(z)$ is called *beam radius* and its explicit form is given in (2.21) and represented in Figure 2.3. It assumes its minimum value W_0, called *beam waist*, in the $z = 0$ plane

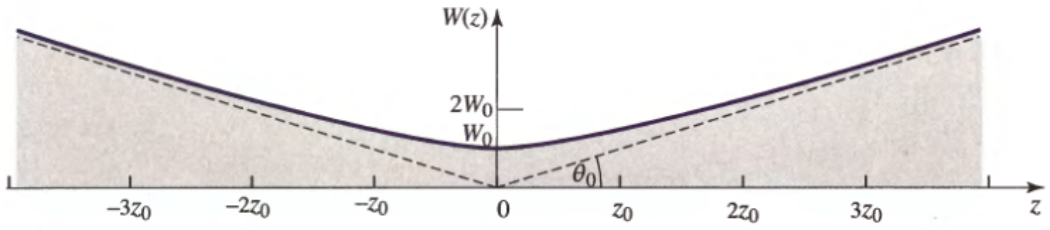


Figure 2.3: Beam radius $W(z)$ as function of the radial distance [2].

and the waist diameter $2W_0$ is called *spot size*. Due to the linear increase of the beam radius far from the beam center when $z \gg z_0$, typically one define the *divergence angle* as

$$\theta_0 = \frac{\lambda}{\pi W_0} \, . \tag{2.26}$$

The wavefronts of the Gaussian beam are the surfaces of constant phase $\varphi(\rho, z)$, i.e., they are defined by

$$\varphi(\rho, z) \equiv kz + k\frac{\rho^2}{2R(z)} - \zeta(z) = \text{constant} \, . \tag{2.27}$$

This is the equation of a paraboloidal surface of radius of curvature $R(z)$ and so $R(z)$ given in (2.22) and plotted in Figure 2.4 is the curvature of the wavefront at position z.

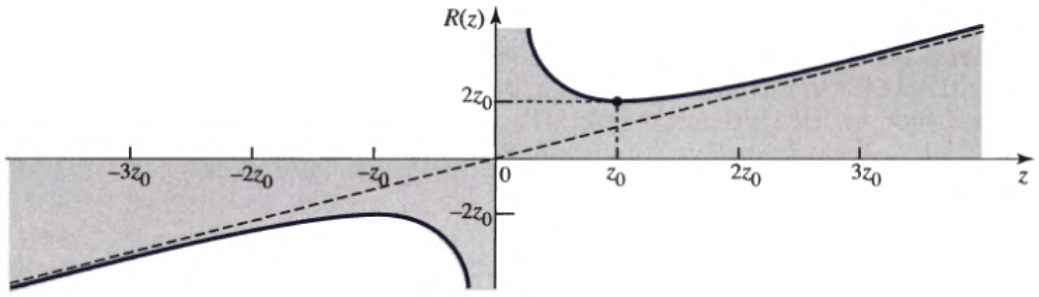


Figure 2.4: Radius of curvature of the Gaussian beam $R(z)$ as function of the radial distance [2].

We can now summarize the characteristics of the Gaussian beam represented in Figure 2.5. Near the beam center for $|z| \ll z_0$ at points within the beam waist $\rho \ll W_0$ the intensity is approximately constant and the phase $\varphi \approx kz$ because $\zeta(z) \approx 0$ and $R(z) \approx +\infty$. The Gaussian beam may therefore be approximated near its center by a plane wave. On the contrary, far from the beam waist when $|z| \gg z_0$ the beam radius $W(z)$ increases linearly with the

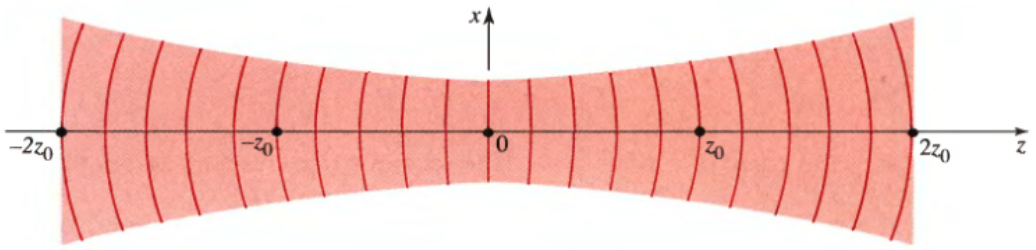


Figure 2.5: Wavefronts of a Gaussian beam [2].

distance z and so the beam intensity is approximately uniform. Since $R(z) \approx z$ the wavefronts are spherical except for an excess phase $\zeta(z) \approx \pi/2$ and so the wave is similar to a spherical one.

2.2.2 *Beam shaping through thin lenses*

In this section we present the effects of a *thin lens* on a Gaussian beam. We will show that it is transmitted maintaining its Gaussian nature and that only the beam waist and curvature are altered so that the beam is only reshaped. The results of this section are important for designing the time-bin optical setup that we will describe in chapter 6.

The *complex amplitude transmittance* of a thin lens of focal length f ($f > 0$ for convex lens, $f < 0$ for concave lens) is proportional to [2]

$$e^{ik\frac{\rho^2}{2f}}, \tag{2.28}$$

so that the complex amplitude (2.20) is multiplied by this phase factor: in this way the wavefronts are modified, but the beam radius does not change. Figure 2.6 represents the effects of the thin lens of focal length f on the beam.

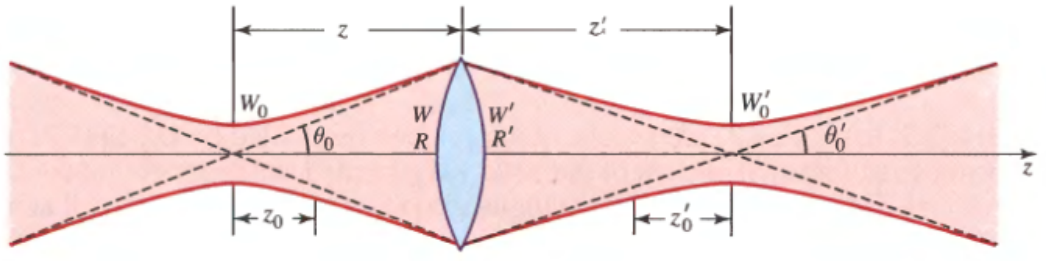


Figure 2.6: Transmission of a Gaussian beam through a thin lens [2].

We see that the transmitted wave is also a Gaussian beam with $W' = W$ at lens position and curvature R' that satisfies

$$\frac{1}{R'} = \frac{1}{R} - \frac{1}{f}. \tag{2.29}$$

The parameters of the emerging beam may be determined from the parameter of the incident one and they can be found in [2].

In the limiting case in which $(z - f) \gg z_0$ the beam can be approximated by a spherical wave so that

$$W_0' \approx \left| \frac{f}{z - f} \right| W_0 \,, \tag{2.30}$$

$$\frac{1}{z'} + \frac{1}{z} \approx \frac{1}{f} \,. \tag{2.31}$$

These two relations are the same relations provided by *ray optics* for the location and size of a patch of light of diameter $2W_0$ located at the distance z to the left of a thin lens, as show in Figure 2.7.

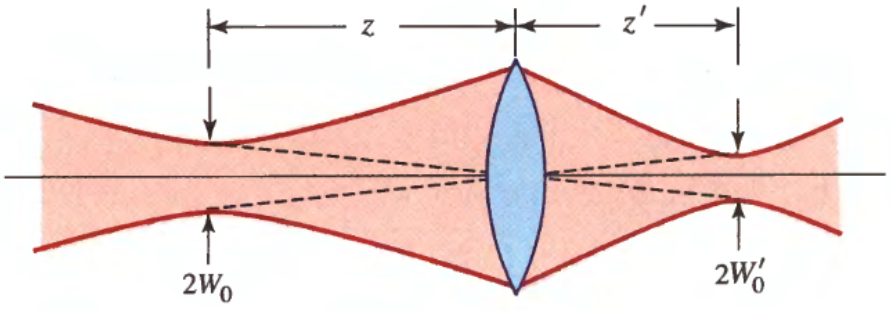


Figure 2.7: Gaussian beam imaging in the ray-optics limit [2].

Knowing the behavior of a thin lens on a Gaussian beam one can derive the effects of a optical system composed by two or more lens on the beam. This is typically done within the formalism of *matrix optics*, i.e., a technique for tracing paraxial rays. A *light ray* is described by its position and by the angle it makes respect to the optical axis, as shown in Figure 2.8. In the paraxial approximation, i.e., if the angles are small, the positions and angles at the input and output planes of an optical system are related by a 2×2 matrix M called *ABCD-matrix* according to

$$\begin{pmatrix} y_2 \\ \theta_2 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} y_1 \\ \theta_1 \end{pmatrix} \,. \tag{2.32}$$

The matrix that describe the behavior of a simple optical elements can be found in [2]. We report here only the two matrix that we will use in the following. The matrix that described the *ray propagation in free space* for a distance d is given by

$$M_d = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \,, \tag{2.33}$$

while the matrix for a *thin lens of focal length* f is

$$M_f = \begin{pmatrix} 1 & 0 \\ -\frac{1}{f} & 1 \end{pmatrix} \,. \tag{2.34}$$

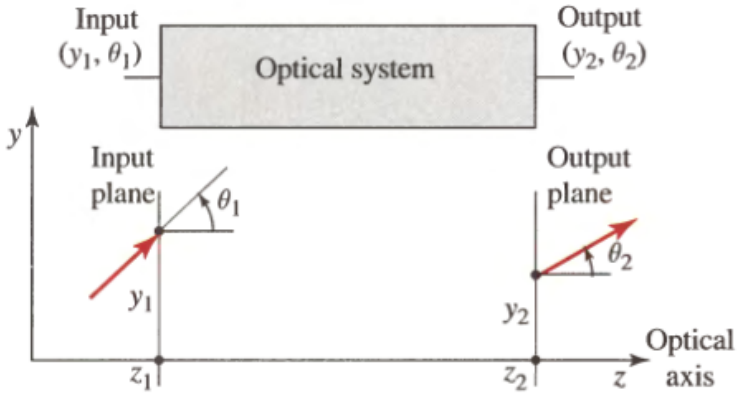


Figure 2.8: Ray-tracing coordinates for a generic optical system [2].

If a system is composed of N optical elements whose ABCD matrices are $M_1, M_2, \ldots, M_N$, it is equivalent to a single optical system described by the matrix

$$M = M_N \cdots M_2 M_1 \, . \tag{2.35}$$

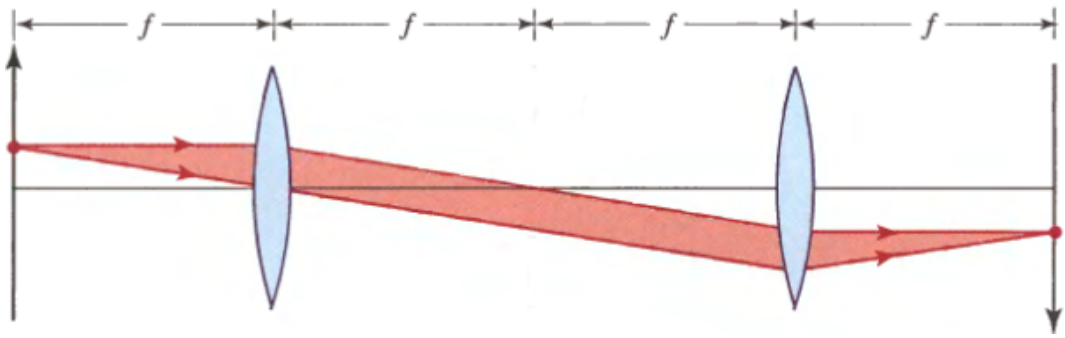


Figure 2.9: The 4f image system and ray-tracing [2].

For example, we consider here the 4f-*system* shown in Figure 2.9. This system serves as a focused imaging system with unity *magnification*. It is composed by a propagation in free space for a distance f, two lenses of focal length f at the distance 2f and a final propagation of distance f. Its ABCD-matrix is given by

$$M_{4f} = M_{d=f} M_f M_{d=2f} M_f M_d = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbb{1}_2 \, . \tag{2.36}$$

It is so clear that the image at the input plane is replicated at the output plane with unity magnification $\mathcal{M}$, but reversed because

$$y_2 = -y_1 \rightarrow \mathcal{M} = \frac{y_1}{y_2} = -1 \tag{2.37}$$

$$\theta_2 = -\theta_1 \tag{2.38}$$

The effects of a 4f-system on a Gaussian beam can be found applying the matrix formalism to Gaussian beam, but for simplicity we give only the result, shown in Figure 2.10, obtained using the correct formalism in the MATLAB script given in [13]. We can see that the impinging beam is focused and then

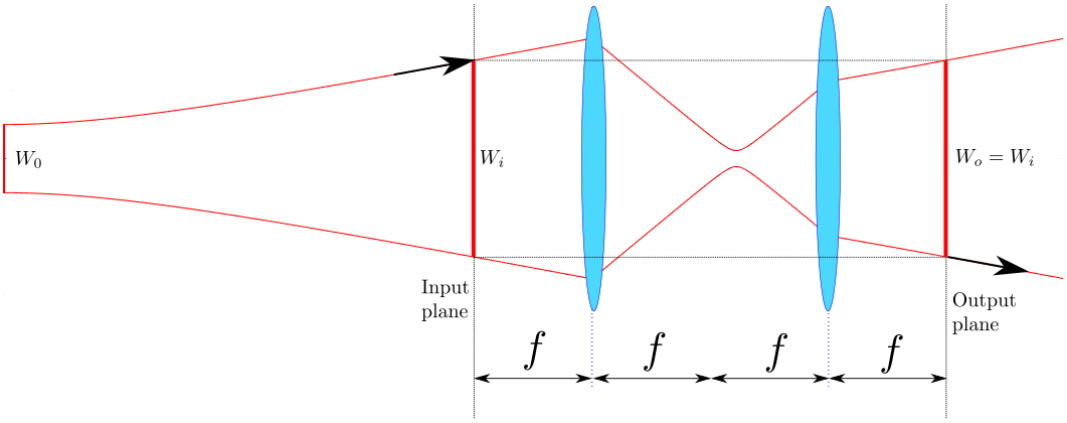


Figure 2.10: The effects of a 4f-system on a Gaussian beam calculated with the MATLAB script [13].

reshaped by this optical system and its only effect is to reverse the wavefront of the input beam maintaining the beam radius equal at the input and at the output planes ($W_i = W_o$). The black arrows show the ray-tracing accordingly to (2.32) using the ABCD-matrix (2.36).

We will use a modified 4f-system in our optical setup in Matera to control the spatial confinement of the beam as we will show in section 5.3.

2.2.3 *The spherical mirror resonator*

The effect of a mirror on a Gaussian beam is similar to the effect of a lens except for a reversal direction of propagation. In fact, the *complex amplitude reflectance* of a mirror of curvature R ($R > 0$ for convex mirror, $R < 0$ for concave mirror) is proportional to

$$e^{ik\frac{\rho^2}{R}} \tag{2.39}$$

and so the mirror modifies the phase of the beam. The reflected beam therefore remains Gaussian, with radius of curvature R_2 at the mirror related to the radius of curvature of the original beam R_1 by [2]

$$\frac{1}{R_2} = \frac{1}{R_1} + \frac{2}{R}\,, \tag{2.40}$$

that is the equation (2.29) with the identification $f = -R/2$.

We can consider some particular cases. If the mirror is planar ($R = +\infty$) we have $R_1 = R_2$ and so the mirror reverses the direction of the beam without altering its curvature.

If the impinging beam has the same curvature, at the mirror, of the mirror itself, i.e., if $R_1 = -R$ (the sign is due to the convention adopted) then $R_2 = R$. The wavefront of the incident and the reflected beams so coincide with the shape of the mirror and the wave retraces its path as shown in Figure 2.11.

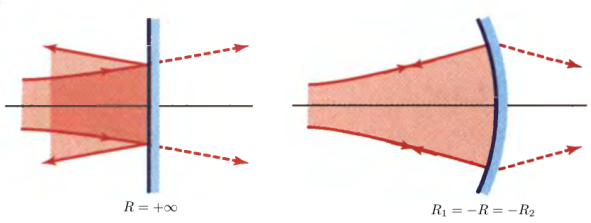


Figure 2.11: Reflection of a Gaussian beam at a mirror [2].

Now, we can think that the radii of curvature of the wavefronts of a Gaussian Beam at planes separated by a distance d match the radii of two mirrors separated by the same distance, as in Figure 2.12. The beam reflects on the first mirror, retraces itself to the second one where it once again reflects and retrace itself back to the first mirror. The two mirror form a *spherical resonator* and the beam can exists within it satisfying the boundary conditions imposed by the two mirrors.

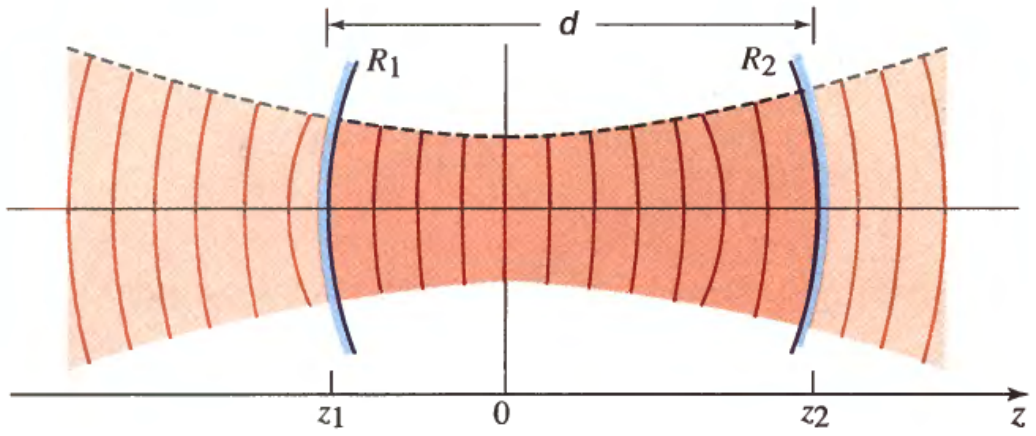


Figure 2.12: The Gaussian beam as a mode of the *spherical mirror resonator* [2].

The Gaussian beam is so a *mode* of the spherical mirror resonator. We can now find the allowed resonator frequencies. All points on each mirror share the same phase because the mirror surfaces coincide with the beam wavefronts. As the beam propagates from the first mirror to the second one, its phase (2.27) on the beam axis changes by

$$\varphi(0, z_2) - \varphi(0, z_1) = k(z_2 - z_1) - [\zeta(z_2) - \zeta(z_1)] \equiv k\Delta z - \Delta\zeta \, . \tag{2.41}$$

In a *resonator round-trip*, i.e., in a complete propagation from mirror 1 to mirror 2 and return, the phase changes by

$$\Delta\varphi_{rt} = 2(k\Delta z - \Delta\zeta) \, , \tag{2.42}$$

and this change must be a multiple of 2π to have a truly retracing of the beam. The distance of the two mirror d is equal to Δz,

$$d = \Delta z \,, \tag{2.43}$$

and so the condition of resonance is

$$\begin{aligned} \Delta\varphi_{rt} &= 2(k\Delta z - \Delta\zeta) \\ &= 2\left(\frac{2\pi}{\lambda}d - \Delta\zeta\right) = 2\pi n \end{aligned} \tag{2.44}$$

with $n = 0, \pm 1, \pm 2 \ldots$. Writing $\lambda = c/\nu$ we get the allowed frequencies ν_n

$$\begin{aligned} \frac{2\pi\nu_n}{c}d - \Delta\zeta &= \pi n \\ \nu_n &= n\nu_F + \frac{\Delta\zeta}{\pi}\nu_F \,, \end{aligned} \tag{2.45}$$

where

$$\nu_F \equiv \frac{c}{2d} \,. \tag{2.46}$$

The frequency spacing of adjacent modes of different frequencies is equal to ν_F and it is independent of the curvature. The allowed frequencies of the resonator will play an important role in the theory of laser oscillation that we will describe in the following.

2.3 LIGHT-MATTER INTERACTION

In this section we present some aspects of the theory of optical absorption and emission in atoms that we will use to describe the principle of laser operation. Firstly, we begin with a discussion of the *Einstein coefficients* that describe the concepts of absorption and emission and then we move to a brief description of the shape of the spectral lines that plays an important to determine the characteristics of the light emitted by a laser.

2.3.1 *Einstein coefficients*

The quantum atomic theory predicts that light is emitted or absorbed whenever an electron in an atom makes a jump between two quantum levels, as shown in Figure 2.13. Due to conservation of energy, the angular frequency ω of the light must be around the value ω_0 fixed by

$$\hbar\omega_0 = E_2 - E_1, \tag{2.47}$$

where E_2 and E_1 are respectively the energies of the upper and the lower level of the electron.

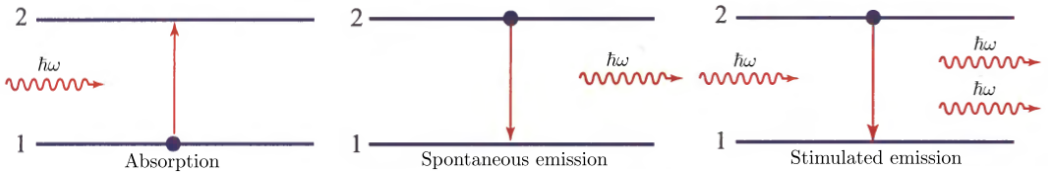


Figure 2.13: Atomic transitions [2].

The radiative process by which an electron in a lower level is promoted to an upper level by absorbing the required energy from the incoming field is called *absorption*. The process by which an electron in an upper level drops to a lower level is called *emission* and can be of two types: *spontaneous*, because the electron in the excited state has a natural tendency to de-excite and lose its excess energy, or *stimulated*, when the incoming field stimulates the downward emission.

The rules that govern these processes are described by quantum electrodynamics, but can be found also following the Einstein treatment [14] as we do now. Let us assume that we have a ensemble of N atoms with two possible atomic levels 1 and 2 with energies E_1 and E_2 respectively and $E_1 < E_2$. If we indicate with $N_1(t)$ the number of atoms in the first level at time t and with $N_2(t)$ the number of atoms in the second one, their sum must satisfies for all times t

$$N = N_1(t) + N_2(t) \tag{2.48}$$

and consequently

$$\frac{dN_1}{dt} = -\frac{dN_2}{dt} \, . \tag{2.49}$$

If we suppose that the atoms are exposed to an electromagnetic radiation of energy density per unit of frequency $\rho(\omega)$, the rate of change of the number of atoms in the first level must be

$$\frac{dN_1}{dt} = A_{21}N_2 + B_{21}\rho(\omega_0)N_2 - B_{12}\rho(\omega_0)N_1 \, , \tag{2.50}$$

where A_{21}, B_{21} and B_{12} are the *Einstein coefficients* that describe the *transition rates* for the spontaneous emission and the stimulated emission from level 2 to level 1 and the absorption from level 1 to level 2 respectively.

Einstein derived an explicit formula for its coefficients supposing that at *thermal equilibrium* the transition rated must satisfy

$$\frac{dN_1}{dt} = -\frac{dN_2}{dt} = 0 \, . \tag{2.51}$$

He finally obtained

$$A_{21} = \frac{\hbar\omega_0^3}{\pi^2 c^3} B_{21} \tag{2.52}$$

$$B_{12} = B_{21} \, , \tag{2.53}$$

from which we can see that one has to calculate only one coefficient with the full quantum mechanical treatment, for example the coefficient B_{21} that rules the stimulated emission, to have the rates for all the atomic transitions.

2.3.2 *Lineshape function for atomic transitions*

We have to note that the radiation emitted in atomic transitions is not perfectly monochromatic. The shape of the emission line is described by the *spectral lineshape function* $g_\omega(\omega)$ [15]. It has a peak at the central frequency $\omega = \omega_0$ of the transition given by (2.47) and it is normalized to have

$$\int g_\omega(\omega)\, d\omega = 1 \,. \tag{2.54}$$

The lineshape function is characterized by its *Full Width at Half Maximum* (FWHM) $\Delta\omega$ that gives a measure of the width of the spectral line.

The broadening of the line is due to various mechanisms and the most important are the natural broadening, the collisional broadening and the Doppler broadening. The broadening mechanism can be homogeneous, if all the individual atoms behave in the same way and produce the same spectrum, or inhomogeneous, if the individual atoms behave differently and contribute to different parts of the spectrum.

The rate at which light is emitted by spontaneous emission is determined by the Einstein coefficient A_{21}. It determine the *radiative lifetime* τ_l defined as

$$\tau_l \equiv \frac{1}{A_{21}} \,. \tag{2.55}$$

This finite lifetime lead to a broadening of the spectral line accordingly to the *energy-time uncertainty principle*:

$$\Delta E \Delta t \gtrsim \hbar \,. \tag{2.56}$$

This kind of line broadening, called *natural*, is intrinsic to the transition and it affects all the atoms in the same way and so it is homogeneous. Its spectral lineshape function has *Lorentzian shape*

$$g^L_\omega(\omega) = \frac{\Delta\omega/2\pi}{(\omega - \omega_0)^2 + (\Delta\omega/2)^2} \,, \tag{2.57}$$

its FWHM is given by

$$\Delta\omega = \frac{\Delta E}{\hbar} \approx \frac{1}{\tau_l} \,, \tag{2.58}$$

and it is plotted in Figure 2.14 on the left.

An example of inhomogeneous broadening is given by the *Doppler broadening*. It originated from the random motion of the atoms that gives rise to Doppler shifts in the observed frequencies. Without giving the details of the

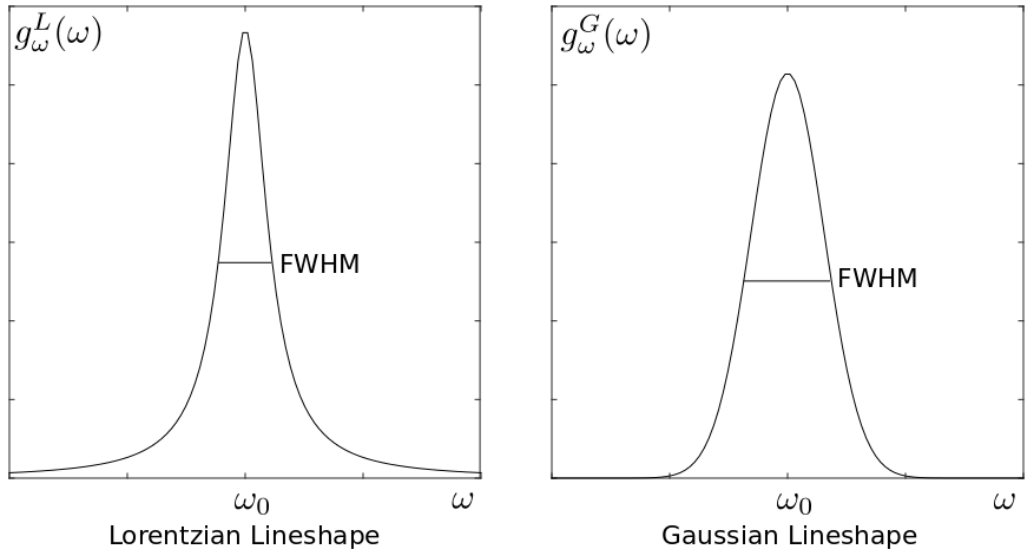


Figure 2.14: Lorentzian and Gaussian lineshape functions.

calculation that can be found in [14, 15], the lineshape function for Doppler broadening is a Gaussian

$$g^G_\omega(\omega) = \frac{1}{\sqrt{2\pi\Delta\omega^2}} e^{-\frac{(\omega-\omega_0)^2}{2\Delta\omega^2}} \tag{2.59}$$

as shown in Figure 2.14 on the right. Its FWHM $\Delta\omega$ is given by [15]

$$\Delta\omega = 2\omega_0\sqrt{\frac{2\ln 2 k_B T}{mc^2}}\,, \tag{2.60}$$

where k_B is the Boltzmann constant, T is the temperature, m is the mass of the atoms and c is the speed of light. In some cases the dominant broadening mechanism can be the Doppler broadening, as in low-pressure gases at room temperature and so the effective lineshape function is closer to Gaussian than Lorentzian.

2.4 LASERS

The laser is the fundamental tool of modern optics laboratories and, of course, of our time-bin experiment. The acronym laser stands for *Light Amplification by Stimulated Emission of Radiation* and it was invented in the 1960s. In this section we present briefly the physical principles of laser operation and then we give a short description of the properties of light emitted from a laser following [15].

2.4.1 *Theory of laser oscillation*

In Figure 2.15 there is a schematic model of a *laser oscillator*. It consists of a cavity given by a spherical resonator with mirrors of reflectivity $\mathcal{R}_1$ and $\mathcal{R}_2$

that contains an *active medium* (or *gain medium*). The light bounces between the two mirrors and it is amplified each time it passes through the active medium. If the amplification is sufficient to balance the losses during a round-trip, the oscillation can occur and the laser operates. The length of the cavity d determine the allowed modes of oscillation and the shape of the mirrors determine the form of the laser output that can be clearly a Gaussian beam.

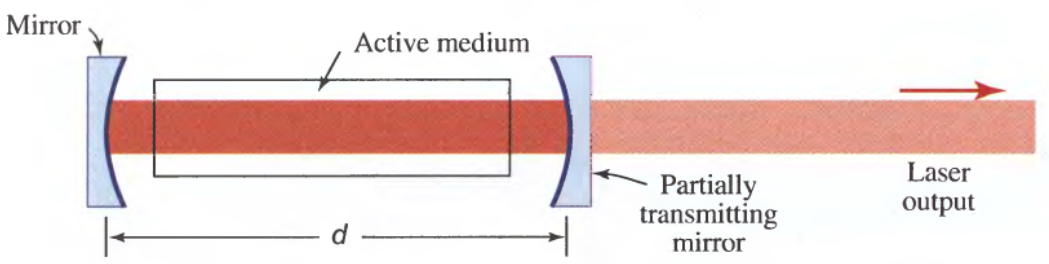


Figure 2.15: A schematic model of a laser oscillator [2].

The light amplification is quantified by the *gain coefficient* $\gamma(\omega)$, defined by

$$\frac{dI(z)}{dz} = \gamma(\omega)I(z) \ , \tag{2.61}$$

where I is the optical intensity, z is the direction of propagation of the beam and ω is the angular frequency of the light. Integrating (2.61) we obtain

$$I(z) = I_{z=0}e^{\gamma(\omega)z} \tag{2.62}$$

that shows that the intensity grows exponentially inside the active medium.

We will consider that the light beam inside the cavity has frequency ω close to the resonance frequency ω_0 of the atoms of the active medium. We require that the stimulated emission rate should exceed the absorption rate to have amplification: in this way the number of photons in the beam increases as it propagates through the active medium. From the treatment of the Einstein coefficients given in section 2.3.1, this situation occurs when

$$B_{21}N_2\rho(\omega_0) > B_{12}N_1\rho(\omega_0) \ , \tag{2.63}$$

i.e, when we have a non-equilibrium condition called *population inversion*

$$N_2 > N_1 \ . \tag{2.64}$$

In thermal equilibrium at temperature T is never possible to satisfy (2.64), because the ratio of N_2 to N_1 is given by the Boltzmann factor

$$\frac{N_2}{N_1} = e^{-(E_2-E_1)/k_BT} < 1 \ . \tag{2.65}$$

The population inversion condition (2.64) can be achieved, for example, in a *four-level pumping system*, like that shown in Figure 2.16. Electrons of the

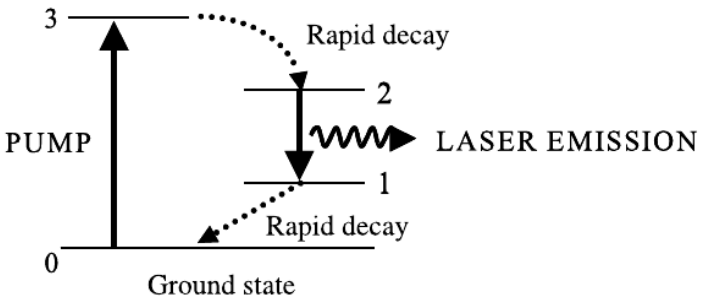


Figure 2.16: The four-level pumping system used to achieve population inversion in the active medium [15].

atoms of active medium are pumped from the ground state to level 3 by a pumping process that can be optical or electrical. From level 3 they decade rapidly to level 2, creating a population inversion with respect to level 1, from which atoms decade back rapidly to the ground state. The transition used to obtain the laser light involve the level 2 and 1 and it is characterized by the lineshape function $g_\omega(\omega)$ centered at $\omega_0 = (E_2 - E_1)/\hbar$.

Assuming that the frequency dependence of the Einstein coefficient $B_{21} = B_{12}$ follows the spectral lineshape function $g_\omega(\omega)$ of the transition [15], the gain coefficient that is achieved for a population inversion

$$\Delta N = N_2 - N_1 \tag{2.66}$$

is given by

$$\gamma(\omega) = \frac{\lambda^2}{4n^2\tau_l}\Delta N g_\omega(\omega)\ , \tag{2.67}$$

where λ is the vacuum wavelength of radiated light, n is the refractive index of the active medium and τ_l is the radiative lifetime of the level 2.

In condition of normal operation the population inversion will be proportional to the pumping rate R and so to the power supplied by the pump external source. The behavior of the gain coefficient in the active medium as a function of the pumping rate is shown in Figure 2.17. When the gain is sufficient to initiate laser operation, i.e., for a value of the pumping rate $R = R_{th}$ called *laser threshold*, the oscillator begins to emit light and the gain coefficient gets clamped at the threshold value γ_{th}.

Neglecting the effect of gain-saturation, in stable oscillation conditions the increase of the intensity due to amplification must balance the losses due to imperfect reflectivity of the two mirrors and the other losses due, for example, to scattering of light in the active medium. This condition for laser oscillation can be written as

$$\mathcal{R}_1\mathcal{R}_2\sigma e^{2\gamma L} = 1\ , \tag{2.68}$$

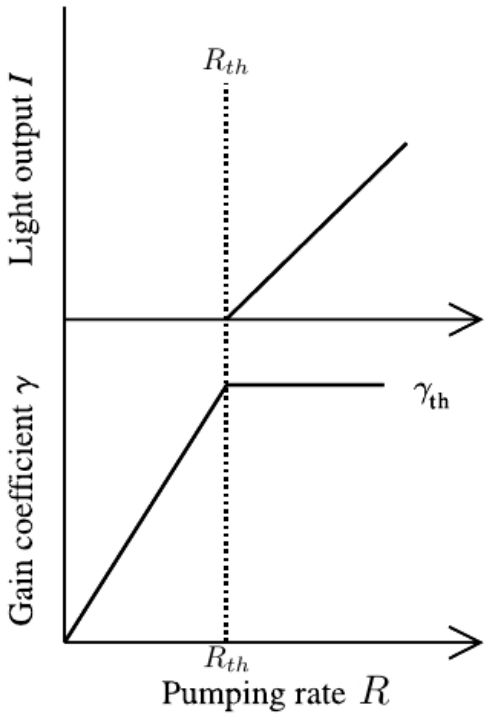


Figure 2.17: The dependence of the gain coefficient γ and of the intensity of light output I on the pumping rate R [15].

where L is the length of the gain medium and σ accounts for the other losses. The equation (2.68) define the threshold gain

$$\gamma_{th} = -\frac{1}{2L}\ln(\mathcal{R}_1\mathcal{R}_2) - \frac{1}{2L}\ln\sigma \tag{2.69}$$

required to make the laser oscillates. For pumping rates larger than R_{th} the gain can not increase further because it is clamped by the oscillation condition. The extra energy given by the pumping process thus increases the intensity of the laser output as shown in Figure 2.17.

The cavity and the medium are the essential part of the laser and determine the properties of the laser beam, as we describe now.

2.4.2 *Properties of laser beam*

The *spectral distribution* of the generated laser light is determined both by the atomic lineshape of the active medium and by the modes allowed by the cavity. The intracavity field is a standing wave and the allowed frequencies are those of the spherical resonator we find in (2.45) and are separated in angular frequency by

$$\omega_F = 2\pi\nu_F = 2\pi\frac{c}{2d} = \frac{\pi c}{d}\ . \tag{2.70}$$

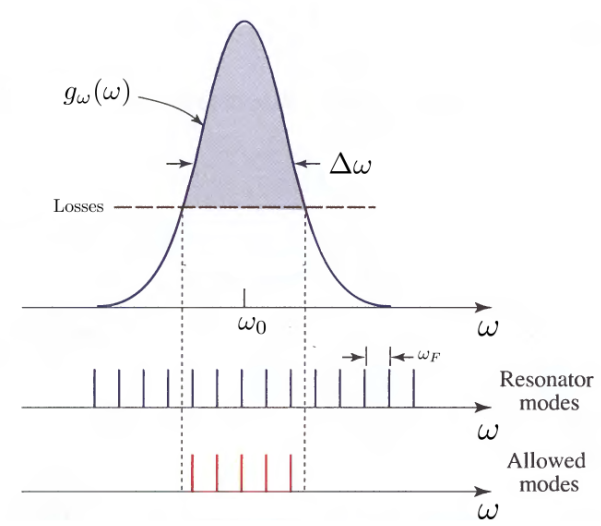


Figure 2.18: Longitudinal modes selection [2].

The length of the cavity determine all the possible *longitudinal modes*, but only the modes whose angular frequencies lie within the linewidth $\Delta\omega$ of the laser transition described by the lineshape function $g_\omega(\omega)$ are amplified by the active medium, as shown in Figure 2.18. A *single-mode* laser, i.e., a laser in which only one longitudinal mode can oscillate, is typically achieved by introducing a frequency-selective element into the cavity.

The *spatial distribution* of the emitted laser light depends on the geometry of the resonator and on the shape of the active medium that determine the *transverse mode* structure of the beam. As we have shown in section 2.2.3 the spherical resonator supports, for example, the Gaussian beam and so it gives rise to an output that takes the form of a Gaussian beam. More complicated modes supported by the spherical resonator lead to the Hermite-Gaussian beam, other solution of the paraxial Helmholtz equation (2.15) that reduce to the Gaussian beam in the simplest case.

The last important property of the laser beam regards the mode of operation. Often is desirable to operate lasers in a *pulsed mode* since the optical power can be greatly increased when the output pulse has a limited duration. Efficient pulsing schemes are based on turning the laser itself on and off using an internal modulation process and common methods used are *gain switching*, *Q-switching* and *mode-locking* [2].

In the mode-locking method pulsed laser action is obtained by coupling together more modes of the laser and locking their phases to each other: in this way they behave like the Fourier components of a periodic function of time of period

$$T_F = 1/\nu_F = \frac{2d}{c} \tag{2.71}$$

and therefore form a periodic pulse train. The light in a mode-locked laser can be regarded as a single narrow pulse of photons reflecting back and forth between the mirrors of the resonator, as shown in Figure 2.19. At each

reflection from the output mirror, a fraction of the photons is transmitted in the form of a pulse of light. The frequencies spacing $\nu_F = 1/T_F$ gives the *repetition rate* of the pulsed laser.

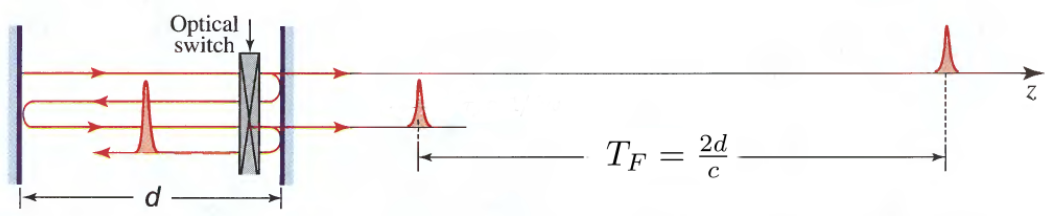


Figure 2.19: Scheme for the *mode-locking* operation of a laser to product pulses [2].

The question remains open is how the modes can be locked together so that they have the same phase. This can be achieved using an active or passive modulator (switch) placed inside the resonator.

We can think to a optical active switch controlled by an external applied signal that blocks the light inside the cavity at all times, except when the pulse is about to cross it, whereupon it opens for the duration of the pulse. The pulse is not affected by the switch and so it is permitted to pass. When the condition of phase locking is not satisfied the individual modes have different phases determined by the random condition at the onset of their oscillation. It can happen, by accident, that the phases take on equal values and so the sum of the modes will form a pulse that would not be affected by the modulator. Any other combination of phases would be blocked by the switch and only when the modes have equal phases lasing can occur and they continue to be locked together. Mathematically, the optical switch determine the boundary condition of the wave equation that the field must satisfy. The different modes of the field inside the cavity respect the wave equation, but only if the modes have equal phases they respect also the boundary condition and so the mode-locked pulse train is the unique solution.

Alternatively, if we put a passive switch like a saturable absorber inside the cavity we can also achieve mode locking. The absorption coefficient of the absorber decreases as the intensity of light passing through it increases and so it transmits only intense pulses, i.e., light passes when the phases of the modes are locked together to form an intense pulse.

A mode-locking oscillator is the master oscillator that we will use in the experimental realization in Matera and the temporal characteristics of the output pulses will play a fundamental role to test time-bin encoding method along a space channel as we will explain in section 6.3.

2.5 NON-LINEAR OPTICS AND SECOND HARMONIC GENERATION

In this section we present some aspects of non linear optics, introducing in particular the effect called *Second Harmonic Generation* (SHG) that we have used in the experimental test in Matera.

Previously the invention of the laser, it was thought that all optical media were linear, but now it is clear that optical media can exhibit *nonlinear* behavior. For example, the refractive index of a medium depends on light intensity and the principle of superposition is violated in a nonlinear optical medium because the wave equation is not linear.

The most important nonlinear effect that we will use in the experimental realization of time-bin setup is the fact that frequency of light can be altered by passing through a nonlinear medium; the light can change from red to green, for example, in a SHG crystal, as we will describe in the following.

The nonlinearity resides in the medium and not in the light itself. A linear dielectric medium is characterized by a linear relation between the polarization density **P** and the electric field **E**. If the medium is isotropic, these two vectors are parallel and the relation can be written using the components as

$$P = \epsilon_0 \chi E \, , \tag{2.72}$$

where ϵ_0 is the permittivity of free space and χ is the electric susceptibility of the medium, defined as

$$\chi = n^2 - 1 \tag{2.73}$$

where n is the refractive index of the medium.

The nonlinearity can have microscopic or macroscopic origin. The polarization density is the product of the individual dipole moments induced by the applied electric field and the density of dipole moments. The relation between P and E is linear when the electric field is small and becomes non linear when E takes values comparable to interatomic electric fields ($\sim 10^5 - 10^8$ V/m). The external applied optical fields are typically smaller than the interatomic fields and so, for non linear media, the relation between the polarization density and the field can be expanded in a Taylor series about $E = 0$ as

$$P = \epsilon_0 \chi E + \epsilon_0 \chi^{(2)} E^2 + \epsilon_0 \chi^{(3)} E^3 + \dots \, . \tag{2.74}$$

The propagation of light in a non linear medium is described by the wave equation derived from Maxwell's equations for an arbitrary homogeneous isotropic dielectric medium:

$$\nabla^2 E - \frac{n^2}{c^2} \frac{\partial^2 E}{\partial t^2} = -S \, , \tag{2.75}$$

where

$$S \equiv -\mu_0 \frac{\partial^2 P_{NL}}{\partial t^2} \tag{2.76}$$

is the *radiation source* with μ_0 the magnetic permeability of free space and

$$P_{NL} \equiv P - \epsilon_0 \chi E = \epsilon_0 \chi^{(2)} E^2 + \epsilon_0 \chi^{(3)} E^3 + \dots \tag{2.77}$$

is the non linear part of the polarization density.

An iterative solution of equation (2.75) can be found by noting that the radiation source $S = S(E)$ is a function of the field that, itself, radiates. If an electric field E_0 engraves on a non linear medium it creates a radiation source $S(E_0)$ that radiates another field E_1 and so on, as shown in Figure 2.20. The first step of the iterative solution is called *first Born approximation*:

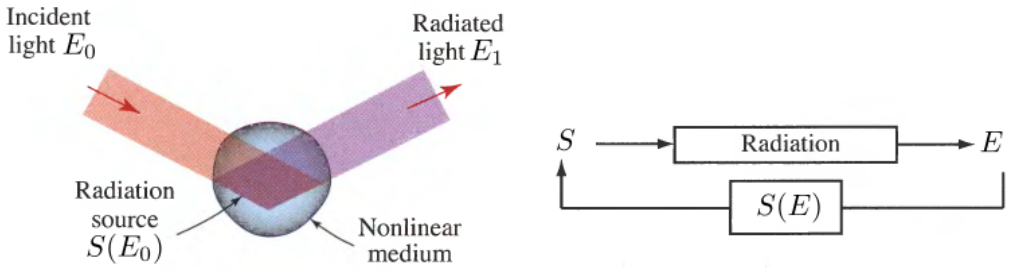


Figure 2.20: The first Born approximation [2].

light propagation through the non linear medium is described as a scattering process in which the scattered field is determined from the incident light. We can use the incident field E_0 to determine the non linear polarization density P_{NL} that gives the frequency components of the radiation source and so of the scattered field.

For example, we take a non linear medium for which only the second order of the expansion (2.74) is important, i.e.,

$$P_{NL} = \epsilon_0 \chi^{(2)} E^2 \,. \tag{2.78}$$

If the incident light is an harmonic field of angular frequency ω and wavelength $\lambda_0 = 2\pi c/\omega$ where c is the speed of light in the vacuum

$$E(t) = \mathrm{Re}\left[\tilde{E}_\omega e^{i\omega t}\right] \,, \tag{2.79}$$

the corresponding polarization density is obtained by substituting (2.79) in (2.78). In this way we get [2]

$$P_{NL} = \frac{\epsilon_0 \chi^{(2)}}{2} |\tilde{E}_\omega|^2 + \mathrm{Re}\left[\tilde{E}_\omega^2 e^{i(2\omega)t}\right] \,, \tag{2.80}$$

and so the radiation source and the radiative field have optical frequencies 0 and 2ω.

The scattered field has a component at the second harmonic of the incident field, or, in other words, with a half wavelength $\lambda = \lambda_0/2$; for this reason this non linear effect is called *second harmonic generation*.

The intensity of the second harmonic scattered field $I_{2\omega}$ results proportional to the square of the intensity I_ω of the incident field and the efficiency of the second harmonic generation can be defined as

$$\eta_{SHG} = \frac{I_{2\omega}}{I_\omega} \propto \frac{L^2}{A} P \,, \tag{2.81}$$

where L is the length of the interaction volume, P is the incident power and A is the cross-sectional area of the interaction volume. To have the maximum efficiency the incident light must have the largest possible power, the incident wave must be focused to the smallest possible area A and provide the longest possible interaction length L.

In our setup we will focalize an intense pulsed laser with 1064 nm of wavelength into a SHG crystal to generate the 532 nm green pulsed lasers used in the experiment, as described in section 6.1.

3

COHERENCE AND INTERFERENCE PHENOMENA

When two or more electromagnetic waves are simultaneously present in the same region of space and time, accordingly to the *principle of superposition*, the resultant wave is the sum of the individual waves. Conversely, the optical intensity does not respect such a principle: the intensity of the sum of two waves is not necessarily the sum of their intensities. The disparity is associated classically with the phenomenon of *interference* and it depends on the *phase* relationship between the superimposed waves. The concept of *coherence* plays an essential role in all classical and quantum *interference phenomena* and so also in the time-bin experiment that is the central topic of this thesis.

For this reason, we introduce in this chapter the *statistical optics* that studies the properties of random light and then we present the classical and the quantum description of optical coherence. We finally present the description of a *linear optical multiport* that we will use to predict the detection probabilities in our time-bin setup.

Figure 3.1: Wave interference [https://soundpossibilities.wordpress.com/2013/08/11/the-coherence-of-interference].

3.1 INTRODUCTION TO STATISTICAL OPTICS

Randomness in light arises from unpredictable fluctuations of light sources or of the medium through which light propagates. The study of random fluctuations of light is also called *theory of optical coherence*. In order to describe the quantum theory of optical coherence we have to perform the quantization of electromagnetic field. For these reasons, we start describing a classical electromagnetic random field inside a volume of finite dimension V, following the treatment in [16].

We can think to the field inside the cavity as a sum of monochromatic waves that oscillate at the frequencies imposed by the boundary conditions given by the cavity. Taken the general form of a monochromatic complex wave $U(\mathbf{r},t) = U(\mathbf{r})e^{i\omega t}$ given by (2.7) we get a discrete set of *mode functions* $\{U_k(\mathbf{r})\}$, requiring that the complex amplitude $U(\mathbf{r})$ obey the Helmholtz equation (2.8) and the set of boundary conditions of the cavity. In this way we define a set of allowed angular frequencies $\{\omega_k\}$ and have a complete and orthonormal set of mode functions $\{U_k(\mathbf{r})\}$, i.e.,

$$\int_V U_k^*(\mathbf{r})U_l(\mathbf{r})d^3r = \delta_{kl}. \tag{3.1}$$

The general form of the time dependent wave function is so a sum over all the allowed frequencies of the monochromatic functions $U_k(\mathbf{r})e^{\pm i\omega k}$. In the classical treatment, it is convenient to express the real field $E(\mathbf{r},t)$ inside the volume as the sum of two complex conjugate terms

$$E(\mathbf{r},t) = E^{(+)}(\mathbf{r},t) + E^{(-)}(\mathbf{r},t)\ , \tag{3.2}$$

where $E^{(+)}(\mathbf{r},t)$ is the positive frequency part of the field, i.e., the sum of all the terms varying with time as $e^{-i\omega_k t}$ for $\omega_k > 0$, and $E^{(-)}(\mathbf{r},t)$, on the contrary, is the negative frequency part and contain all terms varying as $e^{i\omega_k t}$ for $\omega_k < 0$ and

$$\left(E^{(\pm)}(\mathbf{r},t)\right)^* = E^{(\mp)}(\mathbf{r},t)\ . \tag{3.3}$$

The use of this complex field in classical context is a mathematical convenience rather than a physical necessity since classical measuring devices tend to respond only to the real field $E = 2\mathrm{Re}\left[E^{(\pm)}\right]$.

In terms of the set mode function $\{U_k(\mathbf{r})\}$, the positive frequency part of the field can be written as

$$E^{(+)}(\mathbf{r},t) = \sum_k A_k U_k(\mathbf{r})e^{-i\omega_k t}\ , \tag{3.4}$$

where $\{A_k\}$ is the set of complex constants that represent the Fourier amplitudes of the field $E^{(+)}(\mathbf{r},t)$.

In practice, we rarely know the set of numbers A_k with more than limited certainty because the fields we examine are radiated by systems whose

behavior can be described only in statistical terms. We must regard these coefficient as *random variables* in general, and the most we can say about them can be expressed through a probability distribution $\mathcal{P}(\{A_k\}) = \mathcal{P}(A_1, A_2, \dots)$. The field itself is so random and its characteristics can be formulated only in statistical terms. If we measure some function $\mathcal{F}$ of $E^{(+)}(\mathbf{r}, t)$, we can predict only its mean value, i.e., the *statistical average*

$$\langle \mathcal{F}(E^{(+)}) \rangle = \int \mathcal{P}(\{A_k\}) \mathcal{F}(E^{(+)}(\{A_k\})) \prod_k d^2 A_k \, , \tag{3.5}$$

where $d^2 A_k = d(\mathrm{Re} A_k) d(\mathrm{Im} A_k)$ and the normalization condition on the distribution of A_k is

$$\int \mathcal{P}(\{A_k\}) \prod_k d^2 A_k = 1 \, . \tag{3.6}$$

The average (3.5) is an *ensemble average* and so, in principle, to measure it we must repeat the experiment many times by using the same procedure for preparing the field. The theory of optical coherence deals with the definitions of these statistical averages, with the laws that govern them and with the measures by which light is classified as coherent, partially coherent or incoherent as we will see describing the Young experiment in the next section.

If the statistical description of the field is *time-invariant*, we say that the field is *stationary*. This term does not mean that nothing is happening; it means that our knowledge about the field does not change with time. In other words, stationarity does not mean constancy, but it signifies constancy of the average properties. When the field is stationary, the statistical averaging operation (3.5) can usually be carried out by *time averaging* over a long time duration

$$\langle \mathcal{F}(E^{(+)}) \rangle = \lim_{T \to +\infty} \frac{1}{2T} \int_{-T}^{T} \mathcal{F}(E^{(+)}(\mathbf{r}, t)) dt \tag{3.7}$$

by virtue of the *ergodic hypothesis* that ensure that, in this hypothesis, the two averages are equivalent.

We will see in the next section that the classical correlation functions used to describe interference phenomena is a function like $\mathcal{F}(E^{(\pm)})$ and so the statistical description is necessary to explain coherence properties.

3.2 CLASSICAL COHERENCE FUNCTIONS

The most famous experiment that exhibits the coherence properties of light is the Young's two slits experiment shown in Figure 3.2. A plane monochromatic wave obtained focalizing a spherical wave impinges on a screen Σ where there are two parallel slits at the positions P_1 and P_2. The two waves emerging from the slits, neglecting diffraction effects, give raise to an interference pattern on the screen Σ'. We want to give the classical description of such a interference phenomenon.

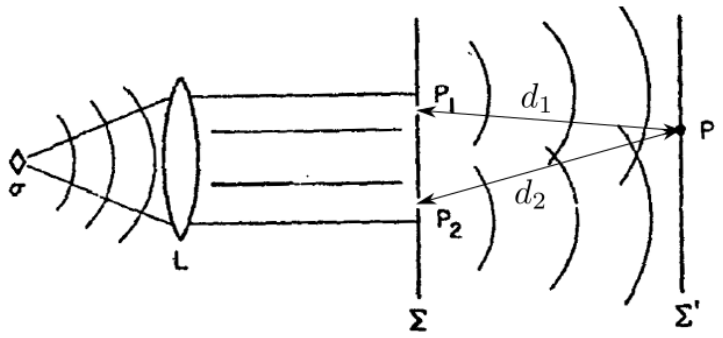


Figure 3.2: Young's two slits experiment [16].

The field at point P (at position $\mathbf{r}$ from the origin) at time t may be approximated by a certain linear superposition of the fields present at the two slits at positions $\mathbf{r}_1$ and $\mathbf{r}_2$ at earlier time

$$E^{(+)}(\mathbf{r}, t) = K_1 E^{(+)}(\mathbf{r}_1, t_1) + K_2 E^{(+)}(\mathbf{r}_2, t_2) \,, \tag{3.8}$$

where the times are given by $t_{1,2} = t - d_{1,2}/c$ and K_1, K_2 are two geometrical coefficients independent of the properties of the field.

In the classical treatment, a classical detector placed in P measure the squared absolute value of some component of the complex field strength, i.e., the intensity of light on the detector is proportional to

$$\begin{aligned} |E^{(+)}(\mathbf{r}, t)|^2 = {} & |K_1|^2 E^{(-)}(\mathbf{r}_1, t_1) E^{(+)}(\mathbf{r}_1, t_1) + |K_2|^2 E^{(+)}(\mathbf{r}_2, t_2) E^{(+)}(\mathbf{r}_2, t_2) \\ & + 2\mathrm{Re}\{K_1^* K_2 E^{(-)}(\mathbf{r}_1, t_1) E^{(+)}(\mathbf{r}_2, t_2)\} \,. \end{aligned} \tag{3.9}$$

The intensity is a function of field $E^{(+)}$ and so, for what we have seen in the last section, the only thing we can predict is its ensemble average $I(\mathbf{r}, t)$ taken over the set of random coefficients $\{A_k\}$, i.e.,

$$\begin{aligned} I(\mathbf{r}, t) \equiv {} & \left\langle |E^{(+)}(\mathbf{r}, t)|^2 \right\rangle \\ = {} & |K_1|^2 \left\langle |E^{(+)}(\mathbf{r}_1, t_1)|^2 \right\rangle + |K_2|^2 \left\langle |E^{(+)}(\mathbf{r}_2, t_2)|^2 \right\rangle \\ & + 2\mathrm{Re}\left\{ K_1^* K_2 \left\langle E^{(-)}(\mathbf{r}_1, t_1) E^{(+)}(\mathbf{r}_2, t_2) \right\rangle \right\} . \end{aligned} \tag{3.10}$$

The first two terms are just the intensities associated with the fields from each of the slits while the third term gives rise to interference. We set now

$$I_1 \equiv |K_1|^2 \left\langle |E^{(+)}(\mathbf{r}_1, t_1)|^2 \right\rangle \,, \tag{3.11}$$

$$I_2 \equiv |K_2|^2 \left\langle |E^{(+)}(\mathbf{r}_2, t_2)|^2 \right\rangle \,, \tag{3.12}$$

and introduce the *first order normalized mutual coherence function* [17] between two points $(\mathbf{r}, t)$ and $(\mathbf{r}', t')$ defined by

$$g^{(1)}(\mathbf{r}, t; \mathbf{r}', t') = \frac{\left\langle E^{(-)}(\mathbf{r}, t) E^{(+)}(\mathbf{r}', t') \right\rangle}{\sqrt{\left\langle |E^{(+)}(\mathbf{r}, t)|^2 \right\rangle \left\langle |E^{(+)}(\mathbf{r}', t')|^2 \right\rangle}} \,. \tag{3.13}$$

The function $g^{(1)}(\mathbf{r}, t; \mathbf{r}', t')$ describe the correlation coefficient of the random variables $E^{(-)}(\mathbf{r}, t)$ and $E^{(+)}(\mathbf{r}', t')$. Its absolute value is bounded

$$0 \leqslant |g^{(1)}(\mathbf{r}, t; \mathbf{r}', t')| \leqslant 1 \, , \tag{3.14}$$

and it is a measure of the degree of correlation between the fluctuations of the field $E^{(+)}$ at $(\mathbf{r}, t)$ and those at $(\mathbf{r}', t')$.

We can now rewrite (3.10) in terms of component intensities plus a coherence term

$$\begin{aligned} I(\mathbf{r}, t) &= I_1 + I_2 + 2\mathrm{Re}\left\{ K_1^* K_2 g^{(1)}(\mathbf{r}_1, t_1; \mathbf{r}_2, t_2) \sqrt{\langle |E^{(+)}(\mathbf{r}_1, t_1)|^2 \rangle} \sqrt{\langle |E^{(+)}(\mathbf{r}_2, t_2)|^2 \rangle} \right\} \\ &= I_1 + I_2 + \sqrt{I_1 I_2}\; 2\; \mathrm{Re}\left\{ g^{(1)}(\mathbf{r}_1, t_1; \mathbf{r}_2, t_2) \right\} \\ &= I_1 + I_2 + 2\; \sqrt{I_1 I_2}\; |g_{12}^{(1)}|\; \cos \phi_{12} \end{aligned} \tag{3.15}$$

where we have assumed equal the two geometrical coefficients $K_1 = K_2$ and written the first order coherence function as

$$g^{(1)}(\mathbf{r}_1, t_1; \mathbf{r}_2, t_2) \equiv |g_{12}^{(1)}| e^{i\phi_{12}} \, . \tag{3.16}$$

The equation (3.15) is the *interference equation*: it shows that the optical intensity of the sum of two waves is not the sum of their optical intensities. The disparity is associated with the first order normalized mutual coherence function and depends on the phase relationship ϕ_{12} between the two superimposed waves. Because of it changes from point to point it forms the interference pattern on the screen Σ' and we are able to predict such a pattern knowing the coherence function $g^{(1)}(\mathbf{r}_1, t_1; \mathbf{r}_2, t_2)$.

When $|g_{12}| = 1$ the two superimposed waves are completely coherent; on the contrary, when $|g_{12}| = 0$ the waves are completely incoherent and there is no interference; in the intermediate case, the two waves are partially coherent.

It is important to give an experimental criterion to measure the coherence of two superimposed waves. In general, the intensity versus the phase ϕ_{12} assumes the form of a sinusoidal pattern. The strength of the interference is measured by the *visibility*, defined as

$$\mathcal{V} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}, \tag{3.17}$$

where I_{max} and I_{min} are the maximum and the minimum values the intensity takes as ϕ_{12} is varied, i.e., when $\cos \phi_{12} = 1$ or -1 respectively

$$\begin{aligned} I_{max} &= I_1 + I_2 + 2\sqrt{I_1 I_2} |g_{12}| \, , \\ I_{min} &= I_1 + I_2 - 2\sqrt{I_1 I_2} |g_{12}| \, . \end{aligned}$$

The visibility results

$$\mathcal{V} = \frac{2\sqrt{I_1 I_2}}{I_1 + I_2} |g_{12}| \tag{3.18}$$

and so it is proportional to the absolute value of the first order normalized mutual coherence function.

The visibility is one of the most important parameter to be determined in a interference experiment and we will estimate it in the interferometry satellite time-bin experiment in chapter 6.

3.3 TEMPORAL COHERENCE AND INTERFEROGRAMS

In this section we present the concept of temporal coherence that leads to the definition of *coherence time* and we present an experimental method to measure it that we will use in section 6.2 applied to the laser beam used at MLRO Observatory.

We consider now the fluctuations of a stationary light $E^{(+)}(\mathbf{r}, t)$ at a fixed position $\mathbf{r}$ as a function of time. The random fluctuations of $E^{(+)}(\mathbf{r}, t)$ are characterized by a time-scale that represents the memory of the random function. After this time, the process "forgets" itself, i.e., fluctuations at temporal points separated by a time delay longer than this memory time are independent.

A quantitative measure of this temporal behavior is given by valuating the coherence function $g^{(1)}(\mathbf{r}, t; \mathbf{r}', t')$ given in (3.13) at the same spatial point $\mathbf{r} = \mathbf{r}'$ and at two temporal points separated by a time delay $t' \equiv t + \tau$.

$$g^{(1)}(\mathbf{r}, t; \mathbf{r}, t' = t + \tau) = \frac{\left\langle E^{(-)}(\mathbf{r}, t) E^{(+)}(\mathbf{r}, t + \tau) \right\rangle}{\sqrt{\left\langle |E^{(+)}(\mathbf{r}, t)|^2 \right\rangle \left\langle |E^{(+)}(\mathbf{r}, t + \tau)|^2 \right\rangle}} . \tag{3.19}$$

Due to stationarity, the statistical description of the beam under displacements of the time variable must be invariant and this implies that the temporal coherence function can only depend on the time difference τ and so we can define the *temporal coherence function*, neglecting the spatial dependence on $\mathbf{r}$, as

$$\begin{aligned} g(\tau) &\equiv g^{(1)}(\mathbf{r}, t; \mathbf{r}, t' = t + \tau) \\ &= \frac{\left\langle E^{(-)}(t) E^{(+)}(t + \tau) \right\rangle}{\sqrt{\left\langle |E^{(+)}(t)|^2 \right\rangle \left\langle |E^{(+)}(t + \tau)|^2 \right\rangle}} \\ &= \frac{\left\langle E^{(-)}(t) E^{(+)}(t + \tau) \right\rangle}{\sqrt{\left\langle |E^{(+)}(t)|^2 \right\rangle \left\langle |E^{(+)}(t)|^2 \right\rangle}} \\ &= \frac{\left\langle E^{(-)}(t) E^{(+)}(t + \tau) \right\rangle}{\left\langle E^{(-)}(t) E^{(+)}(t) \right\rangle} \end{aligned} \tag{3.20}$$

where we used the ergodic property that implies

$$\left\langle |E^{(+)}(t+\tau)|^2 \right\rangle = \lim_{T\to+\infty} \frac{1}{2T} \int_{-T}^{T} |E^{(+)}(t+\tau)|^2 d(t+\tau)$$
$$= \lim_{T\to+\infty} \frac{1}{2T} \int_{-T}^{T} |E^{(+)}(t)|^2 dt = \left\langle |E^{(+)}(t)|^2 \right\rangle \ . \tag{3.21}$$

The absolute value of the temporal coherence function gives a measure of the degree of temporal correlation between $E^{(+)}(t)$ and $E^{(+)}(t+\tau)$ and cannot exceed the unity

$$0 \leqslant |g(\tau)| \leqslant 1 \ . \tag{3.22}$$

For example, when the light is deterministic and monochromatic it is described by $E^{(+)}(t) = E_0 e^{-i\omega t}$ with E_0 a complex constant and the temporal coherence function is

$$g(\tau) = \frac{\left\langle E_0 e^{i\omega t} E_0 e^{-i\omega(t+\tau)} \right\rangle}{\langle E_0 e^{i\omega t} E_0 e^{-i\omega t} \rangle} = e^{-i\omega\tau} \tag{3.23}$$

and so $|g(\tau)| = 1$ for all τ and $E^{(+)}(t)$ and $E^{(+)}(t+\tau)$ are completely correlated for all τ.

For most sources of light, $|g(\tau)|$ decreases from its maximum value $|g(0)| = 1$ as τ increases. If it decreases monotonically, the value τ_c at which it drops to a prescribed value (i.e. $1/2$ or $1/e$) gives a measure of the memory time of the fluctuations and it is called *coherence time*. In other words, the coherence time is a measurement of the width of $|g(\tau)|$. Another definition of the coherence time is given by

$$\tau_c \equiv \int_{-\infty}^{+\infty} |g(\tau)|^2 d\tau \ . \tag{3.24}$$

The coherence time is determined primarly by the spectral width of the light $\Delta\omega$ [15] according to

$$\tau_c \approx \frac{1}{\Delta\omega} \ . \tag{3.25}$$

A perfectly monochromatic source with $\Delta\omega = 0$ has an infinite coherence time, while the coherence time for a spectral broadened source is inversely related to the spectral width.

For example, for light with a Lorenztian lineshape of half width $\Delta\omega$ given by (2.57) the temporal coherence function results [15, 18]

$$g^L(\tau) = e^{-i\omega_0\tau} e^{-|\tau|/\tau_c} \tag{3.26}$$

where in this case $\tau_c = 1/\Delta\omega$. Instead, for a Gaussian lineshape function (2.59) we have [15, 18]

$$g^G(\tau) = e^{-i\omega_0\tau} e^{-\frac{\pi}{2}\left(\frac{\tau}{\tau_c}\right)^2} \tag{3.27}$$

where $\tau_c = \sqrt{8\pi \ln 2}/\Delta\omega \approx 4/\Delta\omega$.

Associated to the concept of coherence time is the *coherence length*, defined as

$$l_c \equiv c\tau_c \ . \tag{3.28}$$

In an optical system, the light can be treated as effectively coherent if the coherence length is much greater than all optical path-length differences encountered. We will see the importance of coherence time and length in the description of the time-bin encoding technique.

We now present an experimental method to measure the coherence time of a light source. The idea is to superimpose to the field $E^{(+)}(t)$ a replica of itself delayed by the time τ, i.e., $E^{(+)}(t+\tau)$. We can use the interference equation that we obtain for the sum of the two waves (at a fixed position $\mathbf{r}$) at two temporal point $t_1 = t$ and $t_2 = t + \tau$ given by

$$E_1^{(+)}(t_1) \equiv E^{(+)}(t) \ , \tag{3.29}$$

$$E_2^{(+)}(t_2) \equiv E^{(+)}(t+\tau) \ . \tag{3.30}$$

These two waves have the same optical intensities I_0

$$I_1 = \left\langle |E_1^{(+)}(t_1)|^2 \right\rangle = \left\langle |E^{(+)}(t)|^2 \right\rangle = I_0 \ , \tag{3.31}$$

$$I_2 = \left\langle |E_2^{(+)}(t_2)|^2 \right\rangle = \left\langle |E^{(+)}(t+\tau)|^2 \right\rangle = \left\langle |E^{(+)}(t)|^2 \right\rangle = I_0 \ , \tag{3.32}$$

where we used again the stationarity of the field.

The total field is

$$E_{tot}^{(+)}(t) = E_1^{(+)}(t_1) + E_2^{(+)}(t_2) = E^{(+)}(t) + E^{(+)}(t+\tau) \tag{3.33}$$

and so, repeating the calculations that led to (3.15), we obtain

$$\begin{aligned} I &= \left\langle |E_{tot}^{(+)}(t)|^2 \right\rangle \\ &= \left\langle |E_1^{(+)}(t_1) + E_2^{(+)}|^2 \right\rangle \\ &= I_1 + I_2 + 2\sqrt{I_1 I_2}|g^{(1)}(\mathbf{r}, t_1; \mathbf{r}, t_2)| \cos\phi_{12} \\ &= 2I_0 \left(1 + |g(\tau)| \cos\phi_{12}\right) \end{aligned} \tag{3.34}$$

where $|g(\tau)|e^{i\phi} \equiv |g^{(1)}(\mathbf{r}, t_1; \mathbf{r}, t_2)| \cos\phi_{12}$ is the first order normalized mutual coherence function that reduces to the temporal coherence function because the total wave is the sum of a wave and an its delayed replica. The interference term is governed by the temporal coherence function that describes the ability of a wave to interfere with a delayed replica of itself.

Experimentally, this kind of superposition may be achieved using a *Michelson interferometer* (see Figure 3.3). A stationary wave impinges on a beam

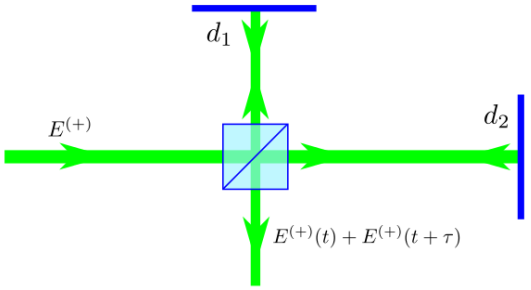


Figure 3.3: The Michelson interferometer used to measure the coherence time of a light source.

splitter (a semi-reflecting mirror, see section 3.7 for more details) that generates two identical waves that propagate in the two orthogonal directions shown.

The two optical paths can have different lengths d_i with $i = 1, 2$ and so the two waves recombe them at the beam splitter after the reflection at the mirrors having a time delay one respect to the other. We can think to keep one mirror fixed at the distance d_1 from the beam splitter and move the other mirror at some distance d_2. The time delay between the two waves is so

$$\tau = \frac{2(d_2 - d_1)}{c} \tag{3.35}$$

and we can obtain, changing the distance d_2, the value of the intensity given by (3.34) for different value of τ.

If we represent the normalized intensity $I/2I_0$ as a function of the time delay τ we obtain the *interferogram* (see Figure 3.4), from which we can extract $|g(\tau)|$.

We will use this procedure to measure the coherence time of the pulsed laser used in the experimental realization of time-bin experiment at MLRO Observatory (see section 6.2).

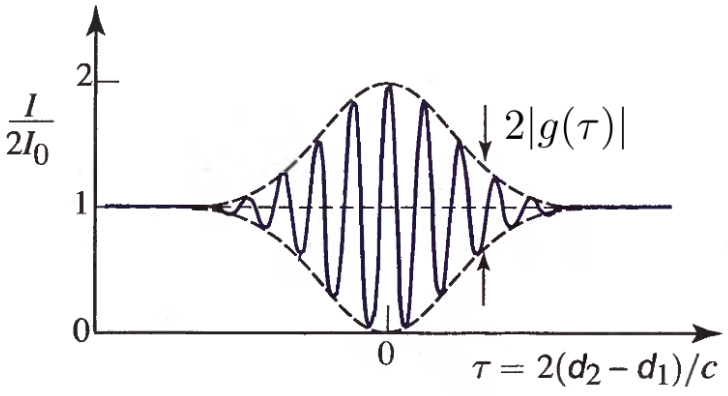


Figure 3.4: The interferogram shows the normalized intensity $I/2I_0$ as a function of the time delay τ for the Michelson interferometer [2].

3.4 QUANTIZATION OF ELECTROMAGNETIC FIELD

In this section we will introduce the quantization of the electromagnetic field and the coherent states by using the formalism of creation and annihilation operators that we will use also in the following to describe some aspects of quantum optics.

The quantization of electromagnetic field in the vacuum is obtain promoting the classical real field $E(\mathbf{r},t)$ and $B(\mathbf{r},t)$ to hermitian operators $\hat{E}(\mathbf{r},t)$ and $\hat{B}(\mathbf{r},t)$. We will focalize only to the electric field as before.

The field operator $\hat{E}(\mathbf{r},t)$ can be separated into its positive and negative frequency parts

$$\hat{E}(\mathbf{r},t) = \hat{E}^{(+)}(\mathbf{r},t) + \hat{E}^{(-)}(\mathbf{r},t) \tag{3.36}$$

The two parts are mutually adjoint

$$\hat{E}^{(\pm)}(\mathbf{r},t) = \left(\hat{E}^{(\mp)}(\mathbf{r},t)\right)^{\dagger} \tag{3.37}$$

to ensure that $\hat{E}(\mathbf{r},t)$ is hermitian $\hat{E}(\mathbf{r},t) = \hat{E}^{\dagger}(\mathbf{r},t)$.

We can expand the operator $\hat{E}(\mathbf{r},t)$ in terms of the set of mode function discussed earlier. Now, the classical Fourier coefficients $\{A_k\}$ must be replace by *quantum mechanical mode operators* that are generally written as $\{\hat{a}_k\}$ and are normalized to have [16]

$$\hat{E}^{(+)}(\mathbf{r},t) = i\sum_k \sqrt{\frac{\hbar\omega_k}{2}}\hat{a}_k u_k(\mathbf{r})e^{-i\omega_k t}\ . \tag{3.38}$$

The operators $\{\hat{a}_k\}$ and their adjoints $\{\hat{a}_k^{\dagger}\}$ satisfy the *canonical commutation relations*

$$\left[\hat{a}_k, \hat{a}_l^{\dagger}\right] = \delta_{kl}\ , \tag{3.39}$$

$$\left[a_k, a_l\right] = \left[\hat{a}_k^{\dagger}, \hat{a}_l^{\dagger}\right] = 0\ . \tag{3.40}$$

These relations are the familiar algebraic relations used for the simple harmonic oscillator and so they define the amplitude operators for an infinite set of oscillators, one for each mode of the field.

The Hamiltonian operator for the electromagnetic field can be written in the form

$$\hat{H} = \sum_k \hbar\omega_k \hat{a}_k^{\dagger}\hat{a}_k + constant \tag{3.41}$$

and so it is evident that the electromagnetic field in the vacuum is so equivalent in its dynamical properties to an infinite sequence of harmonic oscillators.

The product

$$\hat{n}_k \equiv \hat{a}_k^{\dagger}\hat{a}_k \tag{3.42}$$

defines the *number operator* for the k-th mode. This operator has eigenvalues $n_k = 0, 1, 2, \ldots$ and eigenstates $|n_k\rangle$ and represent the *number of photons* in the k-th mode. The operators $\hat{a}_k$ and $\hat{a}_k^\dagger$ act in the Fock space, i.e. the infinite dimensional Hilbert space of "number representation" where a generic state with n_{k_1} photons in the mode k_1, n_{k_2} photons in the mode k_2 and so on has the form

$$|n_{k_1} n_{k_2} \cdots\rangle \equiv |n_{k_1}\rangle \otimes |n_{k_2}\rangle \otimes \cdots \ . \tag{3.43}$$

The operators $\hat{a}_k^\dagger$ and $\hat{a}_k$ are called creation and annihilation operators because they respectively create and destroy one photon in the k-th mode, i.e.

$$\hat{a}_k^\dagger |\cdots n_k \cdots\rangle = \sqrt{n_k + 1}\,|\cdots n_k + 1 \cdots\rangle \ , \tag{3.44}$$

$$\hat{a}_k |\cdots n_k \cdots\rangle = \sqrt{n_k}\,|\cdots n_k - 1 \cdots\rangle \ . \tag{3.45}$$

The ground state of the electromagnetic field is the *vacuum state* where there are no photons

$$|\text{vac}\rangle \equiv |\{0_k\}\rangle \ . \tag{3.46}$$

Applying each one of the annihilation operators to the vacuum state we obtain

$$\hat{a}_k |\text{vac}\rangle = 0 \tag{3.47}$$

because there are no photons to destroy. We can also generate the quantum state $|\{n_k\}\rangle$ that has $n = \sum_k n_k$ photons by applying the creation operators $\hat{a}_k^\dagger$ to the vacuum state,

$$|\{n_k\}\rangle = \prod_k \frac{\left(\hat{a}_k^\dagger\right)^{n_k}}{\sqrt{n_k!}} |\text{vac}\rangle \ . \tag{3.48}$$

The state vectors $|\{n_k\}\rangle$ for all values of the integers $\{n_k\}$ form a complete orthonormal set and span the whole Fock space.

But, they are only one set of basis vectors available in the Fock space and now we construct another important set. Let use define for the k-th mode alone the state $|\alpha_k\rangle$ with the property

$$\hat{a}_k |\alpha_k\rangle = \alpha_k |\alpha_k\rangle \ . \tag{3.49}$$

The state $|\alpha_k\rangle$ is so the eigenstate of the annihilation operator $\hat{a}_k$ and it is called *coherent state*. We now derive the form of a coherent state in terms of the states of "number representation". Firstly we drop the index k for brevity because the problem is the same for all modes k: we want to find the coherent state $|\alpha\rangle$ that satisfies

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle \ . \tag{3.50}$$

We assume that there exists a unitary operator $\hat{D}(\beta)$, called *displacement operator*, which carries out the translation

$$\hat{D}^{-1}(\beta)\,\hat{a}\,\hat{D}(\beta) = \hat{a} + \beta \tag{3.51}$$

$$\hat{D}^{-1}(\beta)\,\hat{a}^\dagger\,\hat{D}(\beta) = \hat{a}^\dagger + \beta^* \tag{3.52}$$

on the operators $\hat{a}$ and $\hat{a}^\dagger$. We can now write starting from (3.50) and using (3.51)

$$\begin{aligned}
\hat{D}^{-1}(\alpha)\ \hat{a}\ \mathbb{1}|\alpha\rangle &= \hat{D}^{-1}(\alpha)\ \alpha|\alpha\rangle \\
\hat{D}^{-1}(\alpha)\ \hat{a}\ \hat{D}(\alpha)\hat{D}^{-1}(\alpha)|\alpha\rangle &= \hat{D}^{-1}(\alpha)\ \alpha|\alpha\rangle \\
(\hat{a}+\alpha)\ \hat{D}^{-1}(\alpha)|\alpha\rangle &= \hat{D}^{-1}(\alpha)\ \alpha|\alpha\rangle \\
\hat{a}\hat{D}^{-1}(\alpha)|\alpha\rangle &= 0
\end{aligned}$$

from which it follows that the coherent state is just a displaced form of the vacuum state

$$|\alpha\rangle = \hat{D}(\alpha)|\text{vac}\rangle\ . \tag{3.53}$$

It can be checked using the commutation relations (3.39) and (3.40) that a suitable form for the operator $\hat{D}(\beta)$ is given by

$$\hat{D}(\beta) = e^{\beta\hat{a}^\dagger - \beta^*\hat{a}} \tag{3.54}$$

because it respect (3.51) and (3.52) and it is unitary.

So, the coherent state can be written as

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{\alpha}}|\text{vac}\rangle\ . \tag{3.55}$$

Using the theorem that state that for two operator $\hat{A}$ and $\hat{B}$ whose commutator $[\hat{A},\hat{B}]$ commutes with each of them one has

$$e^{\hat{A}}e^{\hat{B}} = e^{\hat{A}+\hat{B}+\frac{1}{2}[\hat{A},\hat{B}]}\ , \tag{3.56}$$

choosing $\hat{A} = \alpha\hat{a}^\dagger$ and $\hat{B} = -\alpha^*\hat{a}$ we have

$$\begin{aligned}
e^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{\alpha}} &= e^{\alpha\hat{a}^\dagger - \alpha^*\hat{\alpha} - \frac{1}{2}|\alpha|^2[\hat{a}^\dagger,\hat{a}]} = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{\alpha} + \frac{1}{2}|\alpha|^2\mathbb{1}} \Rightarrow \\
\Rightarrow \hat{D}(\alpha) &= e^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{\alpha}}e^{-\frac{1}{2}|\alpha|^2} = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{\alpha}}\ .
\end{aligned}$$

The operator $\hat{D}(\alpha)$ is written in *normal order*, i.e., the annihilation operators all stand to the right of the creation operators. This form is convenient because we have

$$e^{-\alpha^*\hat{a}}|\text{vac}\rangle = 1|\text{vac}\rangle = |\text{vac}\rangle \tag{3.57}$$

and so we can write finally

$$\begin{aligned}
|\alpha\rangle &= \hat{D}(\alpha)|\text{vac}\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2}e^{\alpha\hat{a}^\dagger}|\text{vac}\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{(\alpha\hat{a}^\dagger)^n}{n!}|\text{vac}\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|\text{vac}\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle
\end{aligned} \tag{3.58}$$

where we used the state with n photons in the selected mode

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|\text{vac}\rangle \ . \tag{3.59}$$

The coherent state (3.58) can be rewritten in a more expressive way. If we calculate the expectation value of the number operator $\hat{n} = \hat{a}^\dagger\hat{a}$ for the coherent state (3.58) we find

$$\langle n\rangle = \langle\alpha|\hat{n}|\alpha\rangle = |\alpha|^2 \ . \tag{3.60}$$

So, it is clear that

$$\mu \equiv |\alpha|^2 \tag{3.61}$$

is the average number of photon in the coherent state $|\alpha\rangle$ that we can write as

$$|\alpha\rangle \equiv |\sqrt{\mu}e^{i\phi}\rangle = \sum_{n=0}^{\infty}\sqrt{e^{-\mu}\frac{\mu^n}{n!}}e^{in\phi}|n\rangle \ . \tag{3.62}$$

The probability that the coherent state contains exactly m photons is given by

$$\mathcal{P}(m) = |\langle m|\alpha\rangle|^2 = e^{-\mu}\frac{\mu^m}{m!} \ , \tag{3.63}$$

that is the *Poisson distribution* with a mean of μ that we used in section 1.2.3 to describe optical implementations of QKD system with faint laser pulses.

We have found the form of the coherent state for a single mode. The state vectors given by products of the coherent states of all modes

$$|\{\alpha_k\}\rangle \equiv \prod_k |\alpha_k\rangle \tag{3.64}$$

span the Fock space and are another important set of basis vectors. The name coherence states characterized these vectors because they are the states with full quantum coherence, as we will show in the next section.

3.5 QUANTUM COHERENCE FUNCTIONS

In this section we introduce the concept of *quantum coherence* following the treatment presented in [16]. We will describe briefly a quantum model of a ideal detector and then we will introduce the quantum coherence functions that lead to the definition of quantum coherence.

The quantum theory of coherence is mostly due to Glauber (see for example [16]). He constructed this theory in a manner that closely parallels the classical theory of coherence. The fundamental idea is that the intensity of a light must be measured by devices that attenuate the beam by absorbing photons in one or another way. The use of any absorption process means in effect that the

field we are measuring is the one associated with photon annihilation, i.e., the quantum field $\hat{E}^{(+)}(\mathbf{r}, t)$.

It is not necessary to discuss the details of the photoabsorption process to find its the matrix element. If the field makes a transition from the initial (pure) state $|i\rangle$ to a final state $|f\rangle$ in which one photon has been absorbed, the matrix element must be proportional to

$$\langle f|\hat{E}^{(+)}(\mathbf{r}, t)|i\rangle \ . \tag{3.65}$$

We now define an *ideal photon detector* as a system like a *single-atom counter* with a frequency-independent photoabsorption probability. In this way, the rate, that we will continue to indicate with I and call "intensity", at which it records a photon is proportional to the sum over all final states of the field $|f\rangle$ of the squared absolute values of the probability amplitude (3.65). So, we have that the probability per unit time that a photon is absorbed by the detector at position $\mathbf{r}$ and time t is proportional to

$$\begin{aligned}\sum_f |\langle f|\hat{E}^{(+)}(\mathbf{r}, t)|i\rangle|^2 &= \sum_f \langle i|\hat{E}^{(-)}(\mathbf{r}, t)|f\rangle\langle f|\hat{E}^{(+)}(\mathbf{r}, t)|i\rangle \\ &= \langle i|\hat{E}^{(-)}(\mathbf{r}, t)\hat{E}^{(+)}(\mathbf{r}, t)|i\rangle \end{aligned} \tag{3.66}$$

where we have used the fact that the set of final states may be regarded as complete and it is to note the normal ordering of the operators.

If the field is initially not in a pure state $|i\rangle$ but in a mixed state described by

$$\hat{\rho} = \sum_i p_i|i\rangle\langle i| \ , \tag{3.67}$$

the expectation value in (3.66) is replaced, following the rules stated in section 1.1.1, by

$$\mathrm{Tr}\left\{\hat{\rho}\hat{E}^{(-)}(\mathbf{r}, t)\hat{E}^{(+)}(\mathbf{r}, t)\right\} = \sum_i p_i\langle i|\hat{E}^{(-)}(\mathbf{r}, t)\hat{E}^{(+)}(\mathbf{r}, t)|i\rangle \ . \tag{3.68}$$

This field average determines the counting rate of an ideal photodetector and it is a particular form of a more general type of expression where the fields $\hat{E}^{(-)}$ and $\hat{E}^{(+)}$ are valuated at different space space-time points. These more general expressions are statistical averages that measure the quantum correlation of fields at separated positions and times. For this reason, in analogy with the classical treatment, we define a *first order (quantum) correlation function* [16, 17] as

$$G^{(1)}(\mathbf{r}, t; \mathbf{r}', t') \equiv \mathrm{Tr}\left\{\hat{\rho}\hat{E}^{(-)}(\mathbf{r}, t)\hat{E}^{(+)}(\mathbf{r}', t')\right\} \ . \tag{3.69}$$

Recording photon intensities with single-atom counter does not exhaust the measurements we can make upon the field. For example, we can use two single-atom detector at different positions $\mathbf{r}$ and $\mathbf{r}'$ to count photon

coincidences or we can use a detector where not just one atom acts as a detector, but two atoms at positions $\mathbf{r}$ and $\mathbf{r}'$. If the initial field state is pure, the matrix element used to calculate the probability that the two atoms undergo detected photoabsorption process must be proportional to

$$\langle f|\hat{E}^{(+)}(\mathbf{r}',t')\hat{E}^{(+)}(\mathbf{r},t)|i\rangle \tag{3.70}$$

that gives a total probability per unit time

$$\sum_f |\langle f|\hat{E}^{(+)}(\mathbf{r}',t')\hat{E}^{(+)}(\mathbf{r},t)|i\rangle|^2 = \langle i|\hat{E}^{(-)}(\mathbf{r},t)\hat{E}^{(-)}(\mathbf{r}',t')\hat{E}^{(+)}(\mathbf{r}',t')\hat{E}^{(+)}(\mathbf{r},t)|i\rangle \ . \tag{3.71}$$

We can now generalize the last relation defining a *second order quantum correlation function*, i.e.,

$$\begin{aligned} &G^{(2)}(\mathbf{r}_1,t_1;\mathbf{r}_2,t_2;\mathbf{r}_3,t_3;\mathbf{r}_4,t_4) = \\ &\quad = \mathrm{Tr}\left\{\hat{\rho}\hat{E}^{(-)}(\mathbf{r}_1,t_1)\hat{E}^{(-)}(\mathbf{r}_2,t_2)\hat{E}^{(+)}(\mathbf{r}_3,t_3)\hat{E}^{(+)}(\mathbf{r}_4,t_4)\right\} \ . \end{aligned} \tag{3.72}$$

It is now natural to define an infinite succession of correlation functions $G^{(n)}$ in view of the possibility of discussing n-photon coincidence experiments, or the behavior of a n-atoms photon detector. Commonly, the pair of coordinates $(\mathbf{r}_i,t_i)$ is replaced by a single symbol $x_i=(\mathbf{r}_i,t_i)$ for brevity. We can define the *n-th order correlation function* as

$$\begin{aligned} &G^{(n)}(x_1;\ldots;x_n;x_{n+1};\ldots;x_{2n}) = \\ &\quad = \mathrm{Tr}\left\{\hat{\rho}\hat{E}^{(-)}(x_1)\cdots\hat{E}^{(-)}(x_n)\hat{E}^{(+)}(x_{n+1})\cdots\hat{E}^{(+)}(x_{2n})\right\} \ . \end{aligned} \tag{3.73}$$

The coherence functions have many important properties that are listed in [16] for example.

We can now define the concept of *quantum coherence*. Let us assume that the first n correlation functions $G^{(1)},\ldots,G^{(n)}$ all factorize in the form

$$G^{(m)}(x_1;\ldots;x_m;x_{m+1};\ldots;x_{2m}) = \mathcal{E}^*(x_1)\cdots\mathcal{E}^*(x_m)\mathcal{E}(x_{m+1})\cdots\mathcal{E}(x_{2m}) \tag{3.74}$$

for $1\leqslant m\leqslant n$, where $\mathcal{E}$ is the same function in all cases and it is a complex solution of the wave equation for the field. A field which obeys the condition (3.74) for the first n correlation functions will be called *n-th order coherent*. If the condition (3.74) holds for all n we speak of *full coherence*.

We can find the quantum mechanical states for which the fields have the property of full coherence. We shall consider for brevity the case of a pure normalized state $|\Psi\rangle$ for which the density operator have the form $\hat{\rho}=|\Psi\rangle\langle\Psi|$ and so the the n-th order correlation function takes the form

$$\begin{aligned} &G^{(n)}(x_1;\ldots;x_n;x_{n+1};\ldots;x_{2n}) = \\ &\quad = \langle\Psi|\hat{E}^{(-)}(x_1)\cdots\hat{E}^{(-)}(x_n)\hat{E}^{(+)}(x_{n+1})\cdots\hat{E}^{(+)}(x_{2n})|\Psi\rangle \ . \end{aligned} \tag{3.75}$$

We have to find what kind of pure state leads to the factorization of this expression. Since the operators $\hat{E}^{(+)}$ and $\hat{E}^{(-)}$ do not commute it is impossible to diagonalize them simultaneously and have a common eigenstate. However, the products are normally ordered and so is sufficient to find the eigenstate for the operator $\hat{E}^{(+)}$. If the tried state $|\Psi\rangle$ satisfies

$$\hat{E}^{(+)}(x)|\Psi\rangle = \mathcal{E}(x)|\Psi\rangle \tag{3.76}$$

where the eigenvalue $\mathcal{E}(x)$ is an ordinary complex function that must satisfy the same wave function of $\hat{E}^{(+)}(x)$, then the correlation function $G^{(n)}$ factorize accordingly to

$$\begin{aligned} G^{(n)}(x_1;\ldots;x_n;x_{n+1};\ldots;x_{2n}) &= \\ &= \mathcal{E}^*(x_1)\cdots\mathcal{E}^*(x_n)\mathcal{E}(x_{n+1})\cdots\mathcal{E}(x_{2n})\langle\Psi|\Psi\rangle \end{aligned} \tag{3.77}$$

and so the state $\hat{\rho} = |\Psi\rangle\langle\Psi|$ is fully coherent.

To have the explicit form of $|\Psi\rangle$ we have to solve equation (3.76). We note that $|\Psi\rangle$ cannot have a fixed number of photons because $\hat{E}^{(+)}$ is an annihilation operator and so the number of photons must be undefined. We can use the expansion (3.38) for the field operator and the corresponding expansion that must be available for the eigenvalue function

$$\mathcal{E}(\mathbf{r},t) = i\sum_k \sqrt{\frac{\hbar\omega_k}{2}}\alpha_k u_k(\mathbf{r})e^{-i\omega_k t}\,. \tag{3.78}$$

In this way, the eigenvalue equation (3.76) implies that the state $|\Psi\rangle$ satisfies

$$\hat{a}_k|\Psi\rangle = \alpha_k|\Psi\rangle\,, \tag{3.79}$$

i.e., the equation (3.49) that holds for the coherent state $|\alpha_k\rangle$ and so the tried state $|\Psi\rangle$ has the form

$$|\Psi\rangle = |\{\alpha_k\}\rangle = \prod_k |\alpha_k\rangle = \prod_k \left[e^{-\frac{1}{2}|\alpha_k|^2}\sum_{n_k=0}^{\infty}\frac{\alpha_k^{n_k}}{\sqrt{n_k!}}|n_k\rangle\right] \tag{3.80}$$

that we derived in the last section. This is the motivation for the name *coherent state* given to the eigenstate of the annihilation operator.

So, the full coherence conditions impose very stringent restrictions on the density operator for the fields, but electromagnetic fields which satisfy this condition quite accurately in large space-time volumes is no longer difficult to generate in practice. For example, the beam generated by a laser operating well above its threshold, like them we have discussed section 2.4, possesses full coherence because its density operator may be written ([16], section 2.13.1) in the form $\hat{\rho} = |\alpha_{k_0}\rangle\langle\alpha_{k_0}|$ where $|\alpha_{k_0}\rangle$ is the coherent state for the single excited mode k_0 corresponding to the frequency ω_0.

3.6 QUANTUM MECHANICAL INTERPRETATION OF INTERFERENCE

In this section we will see how coherence functions emerge in interference phenomena and we will give a quantum mechanical interpretation of such phenomena that will help us in the description of time-bin protocol.

We start with the quantum treatment of Young's interference of Figure 3.2. As we make in section 3.2, we assume that the source of light is monochromatic and we assume that the two slits have dimensions of the order of the wavelength of the light. This latter assumption lets us to ignore diffraction effects. The field at the screen at position $\mathbf{r}$ at time t is the sum of the operators at the two slits

$$\hat{E}^{(+)}(x) = K_1 \hat{E}^{(+)}(x_1) + K_2 \hat{E}^{(+)}(x_2) \, . \tag{3.81}$$

We assume that the two slits are equal in size to have $K_1 = K_2 = K$ and that our observations of the interference pattern on the screen are made with an ideal photon detector now. We have seen that the probability per unit time that a photon is absorbed by the detector at position $\mathbf{r}$ and time t is proportional to the "intensity"

$$\begin{aligned} I(\mathbf{r}, t) \equiv G^{(1)}(x, x) &= \mathrm{Tr}\left\{ \hat{\rho} \hat{E}^{(-)}(x) \hat{E}^{(+)}(x) \right\} = \\ &= |K|^2 \left\{ G^{(1)}(x_1, x_1) + G^{(1)}(x_2, x_2) + 2\mathrm{Re} G^{(1)}(x_1, x_2) \right\} \, . \end{aligned} \tag{3.82}$$

If we write

$$G^{(1)}(x_1, x_2) = |G^{(1)}(x_1, x_2)| e^{i\Phi_{12}} \tag{3.83}$$

the probability becomes

$$I(\mathbf{r}, t) = |K|^2 \left\{ G^{(1)}(x_1, x_1) + G^{(1)}(x_2, x_2) + 2|G^{(1)}(x_1, x_2)| \cos \Phi_{12} \right\} \, . \tag{3.84}$$

and the oscillation of the cosine term led to the familiar interference fringes.

This quantum description of Young's experiment is so close to the classical one that it may not be clear in what way the interference phenomenon is a quantum mechanical one. Interference phenomena occur in quantum mechanics whenever the probability amplitude for reaching a given final state for a system from a given initial state is the sum of two or more partial amplitude with well defined phase relations one between the other. Each partial amplitude represent an alternative way in which the system can evolve from the initial state to the final one.

In the quantum description of Young's experiment, the correlation function depend on the state $\hat{\rho}$ of the field before the absorption of a photon by the photodetector. This state can be any quantum mechanical allowed state.

For example, we may consider as the initial state of the field a single-photon state $|\gamma\rangle$ incident on the slits. The final state of the field will be the vacuum state $|\mathrm{vac}\rangle$, where the photon has been absorbed. The amplitude for reaching this final state is the sum of two amplitudes, each associated with the passage

of the photon through one of the two slits. The existence of the interference fringes is related to our inability to tell which of the possible paths the photon actually takes: any attempt to determine which of the two paths the photon has followed will cancel the interference fringes and this fact is essentially due to the *Heisenberg principle*. The different paths by which a system may evolve will contribute to the total amplitude with partial amplitudes with well-defined phase relationship and this idea is the fundamental idea of *Feynman path integral method* to calculate the transition probability in a quantum system.

3.7 LINEAR OPTICS AND INTERFERENCE WITH SINGLE PHOTONS

In this section we present the description of *linear optics*, i.e., of the optical components largely used in all optical experimental realizations of quantum information. Firstly, we will describe the classical treatment and secondly the quantum one following [19]. Finally, we will see how linear optics can bring to interference phenomena with single photons.

An optical component is linear if the output fields are linearly related to the input fields. We consider the component like a *multiport* (see Figure 3.5) with N input fields and N output fields. In the conventional treatment of linear optical networks the fields are usually assumed to be monochromatic, but in all practical realizations the optical signals have finite duration so a time-domain formulation is necessary and we will present it in the following.

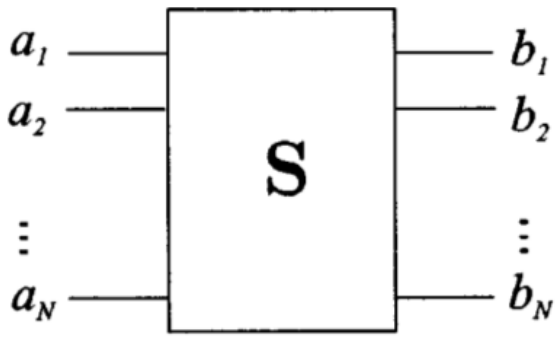


Figure 3.5: A linear multiport with N input and output modes [19].

We do not pay attention to the complete description of the field's dependence on space and time, as we made in the previous sections, and so we denote the complex classical fields in the input and output ports with their mode coefficients a_i and b_i respectively ($i = 1, \ldots, N$). Input and output modes with the same index may share the same physical port if they propagate in different directions, but they also may share the same physical port if

they are separated for example in frequency or polarization. Input and output fields are related by the linear relation

$$b_i = \sum_{j=1}^{N} S_{ij} a_j \tag{3.85}$$

where S_{ij} are the element of a N x N matrix S called *scattering matrix*. In a vector notation

$$\mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_N \end{pmatrix}, \quad \mathbf{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} \tag{3.86}$$

and the relation (3.85) is

$$\mathbf{b} = S\mathbf{a} \, . \tag{3.87}$$

We assume that the multiport is *lossless* so that the output intensity must be equal to the input intensity. We can write the complex conjugate of (3.85)

$$b_i^* = \sum_{j=1}^{N} S_{ij}^* a_j^* \, . \tag{3.88}$$

Defining the row vectors

$$\mathbf{b}^\dagger = (b_1^* \cdots b_N^*), \quad \mathbf{a}^\dagger = (a_1^* \cdots a_N^*) \tag{3.89}$$

the equation (3.88) becomes in a matrix form

$$\mathbf{b}^\dagger = \mathbf{a}^\dagger S^\dagger = (S\mathbf{a})^\dagger, \tag{3.90}$$

and so we have for the conservation of intensity that

$$I_a = \sum_{j=1}^{N} |a_j|^2 = \mathbf{a}^\dagger \mathbf{a} = I_b = \mathbf{b}^\dagger \mathbf{b} = (S\mathbf{a})^\dagger (S\mathbf{a}) = \mathbf{a}^\dagger S^\dagger S \mathbf{a} \tag{3.91}$$

for any input vector $\mathbf{a}$ and it follows that the scattering matrix S for a lossless multiport must be unitary

$$S^\dagger S = \mathbb{1}_N \, . \tag{3.92}$$

For example, we consider the *50:50 beam splitter* (BS) of Figure 3.6. The beam splitter is a optical component that has two input ports and two outputs ports so its scattering matrix is a 2 x 2 matrix. Physically, it is a semireflecting mirror with equal transmission and reflection coefficients. The phase shift between the reflected and transmitted fields depend on the construction of the beam splitter and if it is constructed as a single dielectric layer, the reflected and transmitted beams will differ in phase by a factor of $e^{i\pi/2} = i$. Assuming that

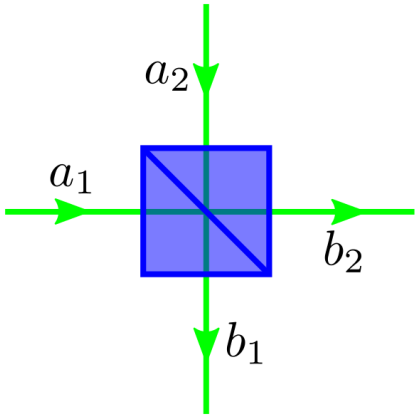


Figure 3.6: Input-output modes representation of a beam splitter.

the reflected field suffers a $\pi/2$ phase shift, the input **a** and output **b** modes are related according to the matrix

$$S_{BS} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} . \tag{3.93}$$

We conclude this classical description of linear optics noting that a cascade of M multiport whose scattering matrix are $S_1, S_2 \dots S_M$ is equivalent to a single multiport of scattering matrix $S = S_M \cdots S_2 S_1$.

Now, we consider the lossless multiport from a quantum mechanical perspective. This description is based on the field quantization presented in section 3.4 where we used the discrete frequency domain, but in the following we will see how the theory can be formulated for time-localized photons so that modes separation in time is possible as well.

The N input and N output monochromatic fields of the multiport are described quantum mechanically replacing the a_i and b_i fields with the quantum annihilation operators $\hat{a}_i$ and $\hat{b}_i$ respectively. Input operators respect the commutation relations

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{ij}, \quad \left[\hat{a}_i, \hat{a}_j\right] = 0 , \tag{3.94}$$

because modes with different index are independent. We have replaced the classical fields with annihilation operators, but the relation between $\hat{b}_i$ and $\hat{a}_i$ still can be written using (3.85) as

$$\hat{b}_i = \sum_{j=1}^{N} S_{ij} \hat{a}_j . \tag{3.95}$$

We have also to replace the complex conjugates field a_i^* and b_i^* with creation operators $\hat{a}_i^\dagger$ and $\hat{b}_i^\dagger$ and use the analogue of equation (3.88)

$$\hat{b}_i^\dagger = \sum_{j=1}^{N} S_{ij}^* \hat{a}_j^\dagger . \tag{3.96}$$

Using the commutation relations (3.94) we have

$$\left[\hat{b}_i, \hat{b}_j^\dagger\right] = \left[\sum_{k=1}^{N} S_{ik}\hat{a}_k, \sum_{l=1}^{N} S_{jl}^* \hat{a}_l^\dagger\right] = \sum_{k,l=1}^{N} S_{ik}S_{jl}^* \left[\hat{a}_k, \hat{a}_l^\dagger\right] = \sum_{k,l=1}^{N} S_{ik}S_{jl}^* \delta_{kl} = \delta_{ij} \tag{3.97}$$

where in the last passage we used also the fact that the scattering matrix is unitary. It is to note that the scattering matrix used in the quantum description is the same of the classical description and this simplify the transition between the two treatments.

In the context of quantum linear multiport is commonly used the *Heisenberg picture*, where the vector states are constant and the operators evolve. It is very simple to write the constant state of the system using the input or the output operators because we have

$$\hat{\mathbf{b}}^\dagger = \hat{\mathbf{a}}^\dagger S^\dagger \Rightarrow \hat{\mathbf{a}}^\dagger = \hat{\mathbf{b}}^\dagger S \tag{3.98}$$

that explicitly reads

$$\hat{a}_i^\dagger = \sum_{j=1}^{N} \hat{b}_j^\dagger S_{ji} \ . \tag{3.99}$$

The constant state of the system, i.e., the input state that is in the form

$$|\text{in}\rangle = \mathcal{F}(\{\hat{a}_i^\dagger\})|\text{vac}\rangle \ , \tag{3.100}$$

where $|\text{vac}\rangle$ is the vacuum state of the linear multiport and $\mathcal{F}$ indicates a generic combination of input photons, can be rewritten in terms of the output operators as

$$|\text{out}\rangle = |\text{in}\rangle = \mathcal{F}(\{\hat{a}_i^\dagger\})|\text{vac}\rangle = \mathcal{F}\left(\left\{\sum_{j=1}^{N} \hat{b}_j^\dagger S_{ji}\right\}\right)|\text{vac}\rangle \ . \tag{3.101}$$

This state can be used to determine the probabilities for detecting a certain number n of photons at certain outputs b_j. The general procedure described in section 3.5 gives the behavior of a n-photon counter. The treatment described above must be adapted for the formalism of the linear multiport. In our description we do not pay attention to the spatial and temporal dependence of fields because we have described the system in terms of input and output fields. In this way, the field $\hat{E}^{(+)}(\mathbf{r}, t)$ that appears in (3.65) and annihilates a photon at position $\mathbf{r}$ and time t must be replaced by the annihilation operator at output port b_j, i.e., the field operator $\hat{b}_j$. So, we can write the probability of detection of n photons at the j-th port as

$$I_{b_j}^n = \langle \text{out}| \underbrace{\hat{b}_j^\dagger \cdots \hat{b}_j^\dagger}_{n \text{ times}} \underbrace{\hat{b}_j \cdots \hat{b}_j}_{n \text{times}} |\text{out}\rangle \tag{3.102}$$

because the state $\hat{\rho}$ of the field before the detection is the pure constant state $|out\rangle$.

Let us make an example to explain this point. We can think to a single-photon input state impinging at port a_1 of the 50:50 beam splitter of Figure 3.6. The input state is

$$|in\rangle = |1\rangle_{a_1} = \hat{a}_1^\dagger |vac\rangle \tag{3.103}$$

We rewrite it using (3.101)

$$|in\rangle = |out\rangle = \sum_{j=1}^{N} \hat{b}_j^\dagger S_{j1} |vac\rangle. \tag{3.104}$$

In terms of the output operators it becomes

$$|1\rangle_{a_1} = \hat{a}_1^\dagger |vac\rangle = \frac{1}{\sqrt{2}} \left(i\hat{b}_1^\dagger |vac\rangle + \hat{b}_2^\dagger |vac\rangle \right) = \frac{1}{\sqrt{2}} \left(i|1\rangle_{b_1} + |1\rangle_{b_2} \right) . \tag{3.105}$$

We can now calculate the probability to detect the photon at one of the two output ports, for example b_1 using (3.102)

$$\begin{aligned} I_{b_1}^1 &= \langle out|\hat{b}_1^\dagger \hat{b}_1 |out\rangle \\ &= \langle out|\hat{n}_{b_1} \left[\frac{1}{\sqrt{2}} (i|1\rangle_{b_1} + |1\rangle_{b_2}) \right] \\ &= \frac{1}{2}(-i)(i)_{b_1}\langle 1|1\rangle_{b_1} = \frac{1}{2} , \end{aligned} \tag{3.106}$$

where we used the properties of number operator $\hat{n}_{b_j} = \hat{b}_j^\dagger \hat{b}_j$ and the orthonormality of the states

$${}_{b_k}\langle m|l\rangle_{b_j} = \delta_{ml}\delta_{kj} . \tag{3.107}$$

So, we can detect the single input photon in each of the two output ports b_1 and b_2 with equal probability 1/2.

A more interesting calculation bring to a quantum interference phenomena with single-photon. We consider the *balanced Mach-Zender interferometer* of Figure 3.7. This interferometer is composed by two 50:50 beam splitter and a phase shift in one of the arms. The scattering matrix for this optical system is given by

$$\begin{aligned} S &= S_{BS} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} S_{BS} \\ &= \frac{1}{2} \begin{pmatrix} e^{i\theta} - 1 & i(1 + e^{i\theta}) \\ i(1 + e^{i\theta}) & 1 - e^{i\theta} \end{pmatrix} \end{aligned} \tag{3.108}$$

where we use the rule that states that the total scattering matrix of a composed system is the product of the scattering matrix of its components.

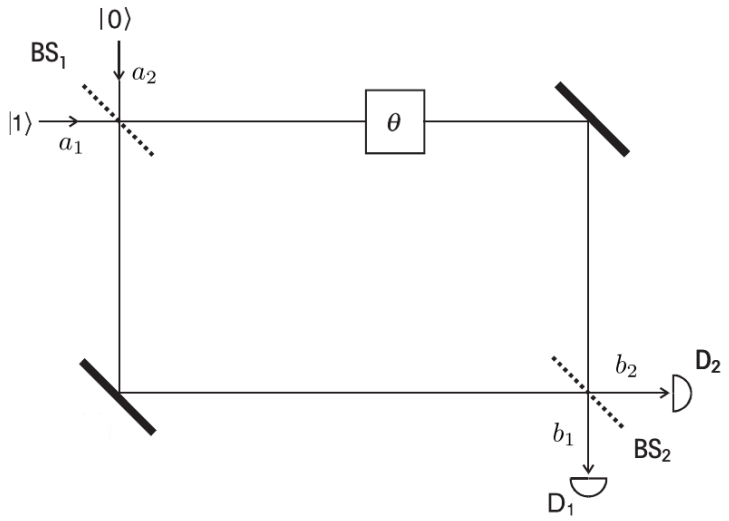


Figure 3.7: The balanced Mach-Zender interferometer [17].

We consider as input state a single-photon entering at port a_1

$$|in\rangle = |1\rangle_{a_1} = \hat{a}_1^\dagger |vac\rangle \tag{3.109}$$

that becomes, in terms of the output operator,

$$\begin{aligned} |out\rangle &= \frac{1}{2}\left[(e^{i\theta}-1)\hat{b}_1^\dagger + i(e^{i\theta}+1)\hat{b}_2^\dagger\right]|vac\rangle \\ &= \frac{1}{2}\left[(e^{i\theta}-1)|1\rangle_{b_1} + i(e^{i\theta}+1)|1\rangle_{b_2}\right] . \end{aligned} \tag{3.110}$$

We can calculate the probability to get the photon at the output ports, for example for b_1 we have

$$\begin{aligned} I^1_{b_1} &= \langle out|\hat{b}_1^\dagger \hat{b}_1|out\rangle \\ &= \frac{1}{4}|1-e^{i\theta}|^2 = \sin^2\frac{\theta}{2} \end{aligned} \tag{3.111}$$

and for b_2 we have correctly

$$I^1_{b_2} = \cos^2\frac{\theta}{2} . \tag{3.112}$$

We note that $I^1_{b_1} + I^1_{b_2} = 1$ gives correctly the total probability to detect the input photon at one of the two output ports. Moreover, we can see that, if the additional phase shift θ between the two arms of the interferometer is null $\theta = 0$ the input photon can be detected only at port b_2.

This is an quantum mechanical interference phenomena realized with single photons. In fact, to arrive at one of the two detectors D_1 or D_2 the photon can take one on the two paths given by each of the two arms of the interferometer. We cannot say which of the possible paths the photon actually takes and so the two quantum amplitude related to the two different path have a well-defined phase relationship and interfere.

3.7.1 *Time-domain formulation for linear quantum optics*

In all practical experiments the photons are more or less localized in time. We now analyze the effect of the linear multiport on a localized input pulse to give the machinery to calculate the photon-detection probabilities in time-bin like experiments.

A *pulse*, such the coherent laser pulse we have described in section 2.4, contains necessarily a continuous band of (angular) frequencies ω centered about a central frequency ω_0. Generalizing the the case of discrete frequencies described above we can define continuous frequency creation $\hat{a}_i^\dagger(\omega)$ and annihilation $\hat{a}_i(\omega)$ operators ($i = 1, \ldots, N$) for each one of the N input modes of a linear lossless multiport.

Similarly to equation (3.94), we can fix the normalization to be:

$$\left[\hat{a}_i(\omega), \hat{a}_j^\dagger(\omega')\right] = \delta_{ij}\delta(\omega - \omega') \,, \tag{3.113}$$

where $\delta(\omega - \omega')$ is the delta function.

To create localized photons in a pulse centered about time t_0 we use the *photon-wavepacket creation operator* [18]:

$$\hat{a}_{i,t_0}^\dagger = \int d\omega \; \xi^{t_0}(\omega)\hat{a}_i^\dagger(\omega) \,, \tag{3.114}$$

where the function $\xi^{t_0}(\omega)$ describes the *pulse amplitude* in the frequency domain that is strictly related to the *lineshape function* $g_\omega(\omega)$ of the source and has the form

$$\xi^{t_0}(\omega) \equiv e^{i(\omega-\omega_0)t_0}\sqrt{g_\omega(\omega)} \tag{3.115}$$

where ω_0 is the central (angular) frequency of the pulse spectrum and t_0 to is the time at which the peak of the pulse passes the coordinate origin. The lineshape function $g_\omega(\omega)$, given by the square modulus of $\xi^{t_0}(\omega)$, has bandwidth $\Delta\omega$ (see section 2.3.2) assumed throughout to be small relative to the central frequency, i.e., $\Delta\omega \ll \omega_0$ and so the integration domain in (3.114) can be extended from $-\infty$ to ∞. For a pulsed light, the bandwidth $\Delta\omega$ and the coherence time τ_c are inversely related as we have seen in (3.25)

$$\tau_c \equiv \frac{1}{\Delta\omega} \,. \tag{3.116}$$

With the definition (3.115), the pulse amplitude is correctly normalized to 1:

$$\int d\omega |\xi^{t_0}(\omega)|^2 = \int d\omega g_\omega(\omega) = 1 \tag{3.117}$$

for what we have seen in section 2.3.2.

We can find the commutation rules for the photon wave-packet operators:

$$\left[\hat{a}_{i,t_0}, \hat{a}_{j,t_1}^\dagger\right] \propto \delta_{ij}e^{i\omega_0(t_2-t_1)}g_t(t_2 - t_1) \,, \tag{3.118}$$

where we have indicated with g_t the Fourier transform of the lineshape function, that corresponds substantially to the temporal coherence function for the pulse that is null for times greater than the coherence time, i.e., $|g_t(t)|$ is zero for $t \gtrsim \tau_c$. So, two pulses in the same j-th input mode at time t_1 and t_2 with $|t_2 - t_1| \gtrsim \tau_c$ can be treated as independent because their separation in time is greater than the coherence time.

For concreteness, a *Gaussian pulse* is described in the frequencies-domain by

$$\xi^{t_0}(\omega) = \frac{1}{(2\pi\Delta\omega^2)^{1/4}} e^{i(\omega-\omega_0)t_0 - \frac{(\omega-\omega_0)^2}{4\Delta\omega^2}}, \tag{3.119}$$

The formalism that follows is valid for any square-normalized functions $\xi^{t_0}(\omega)$ but the Gaussian form is used to illustrate the results in the following. Using (3.119), (3.116) and (3.113) we find, for the photon wave-packet operators, the following commutation rules

$$\left[\hat{a}_{i,t_0}, \hat{a}^\dagger_{j,t_1}\right] = \delta_{ij} e^{-\frac{(t_1-t_0)^2}{2\tau_c^2}} \tag{3.120}$$

ans so, if $|t_1 - t_0| \gg \tau_c$, two Gaussian pulses in the same j-th input mode can be treated as we have already seen.

If we take two independent Gaussian pulses centered about t_1 and t_2 respectively entering the first port a_1 of the multiport

$$|t_1^{a_1}\rangle = \hat{a}^\dagger_{1,t_1}|\text{vac}\rangle \,, \tag{3.121}$$

$$|t_2^{a_1}\rangle = \hat{a}^\dagger_{1,t_2}|\text{vac}\rangle \,, \tag{3.122}$$

$$\tag{3.123}$$

we can see using (3.113) and the properties of annihilation operators that their quantum states are orthogonal because

$$\langle t_1^{a_1}|t_2^{a_1}\rangle = \langle \text{vac}|\hat{a}_{1,t_1}\hat{a}^\dagger_{1,t_2}|\text{vac}\rangle = e^{-\frac{(t_2-t_1)^2}{2\tau_c^2}} \tag{3.124}$$

that reduces to zero if the two pulses are separated in time more than the coherence time.

We note that, generalizing equation (3.95) and (3.97), also the output continuous operators of the linear multiports respect the same commutation relations

$$\left[\hat{b}_{i,t_0}, \hat{b}^\dagger_{j,t_1}\right] = \delta_{ij} e^{-\frac{(t_1-t_0)^2}{2\tau_c^2}} \,, \tag{3.125}$$

and so two pulses in the same j-th output mode can be treated as independent and orthogonal if their separation in time is greater than the coherence time. It is this type of separation used time-bin qubit encoding, as we will see in chapter 5.

Finally, generalizing (3.99) we have

$$\hat{a}^{\dagger}_{i,t_0} = \sum_{j=1}^{N} \int d\omega \; \xi^{t_0}(\omega) S_{ji} \hat{b}^{\dagger}_{j}(\omega). \tag{3.126}$$

This last equation let us calculate the detection probabilities at output ports of an optical system as we will show in section 5.1 applied to time-bin qubits.

4

TOWARD SPACE QUANTUM COMMUNICATIONS

Communications security is today a primary necessity in the life of governments, businesses and individual citizens. QKD, as we have seen, represents the most promising resource to ensure secure communications because it is based on the fundamental principles of Nature, described by the theory of Quantum Mechanics. Although it is already available in commercial products, at present the QKD can guarantee links that do not exceed few hundreds of kilometers. For this reason, it is very important to be able to extend QKD on global scale and one of the most important approaches to achieve this purpose is represented by Satellite Quantum Communications (SQCs).

In this chapter we present SQCs describing the motivations and the state of the art of this challenging field of research. Then we analyze more in detail the most relevant experiments that have shown the feasibility of SQCs testing the exchange of single photons along a quantum link between a satellite and a ground station and the preservation of single photon polarization that makes polarization encoding possible along a quantum space channel.

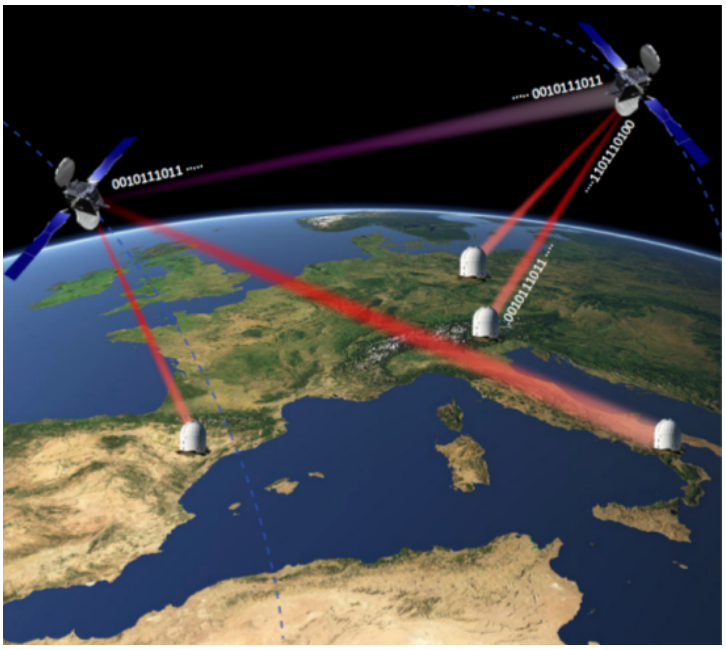


Figure 4.1: Future scenario of Space Quantum Communication.

4.1 MOTIVATIONS AND STATE OF THE ART

The aim of SQCs is to extend the frontiers of Quantum Communications (QCs) to satellite distances, by exploiting novel methods and techniques for qubit transmission. The main objective of SQCs is to develop a global network aimed at provide secure communications by means of satellite-to-ground, ground-to-satellite and satellite-to-satellite quantum links. This objective is crucial particularly in this moment, in which large scale violations of the privacy in the exchange of confidential informations were perpetrated against governmental, industrial and individual customers and then discovered and exposed to the public. The risk of neglecting the development of Quantum Communication technologies is that future secret communications will not be possible, because, for example, a new classical fast algorithm for factorization or the implementation of a quantum computer would render current secure communications instantaneously vulnerable.

First demonstrations of QKD performed out of laboratories were mainly implemented in optical telecommunication fiber networks via light pulses containing one photon on average as we have discussed in section 1.2.3, where either the *polarization* or the *phase* of the photon is used to encode the qubit. Quantum communication in a metropolitan area in optical fibers was already shown in the United States [20] and in Europe [21]. A remarkable use of QKD has been demonstrated in 2007 for ensuring the integrity of the dedicated line used for counting the voting ballots of the Swiss national elections on October of that year [21]. It has been shown [22] that free space optical links are more suitable for long distance QCs among metropolitan areas or even continents. Within this two technologies it has been possible to achieve a maximum quantum link distances of few hundreds kilometers (307 km with optical fibers [23] and 144 km in free space [24]). Nevertheless, further improvements seem to be unrealistic due mostly to photon absorption in fiber optic long cables and to obstruction of objects in the line of sight or to the Earth's curvature in free space links.

To overcome these limitations, focusing on the realization of a *global QKD network*, there are two possible solutions. The first one consists in the use of several ground stations that connect Alice and Bob. To have a trusted server scheme, a third figure called Charlie shares via QKD a key both with Alice and Bob. The problem is that Charlie has full access to the cryptographic key and therefore he could eavesdrop any information. Because of the presence of many intermediate ground stations, to reach long distance quantum communications this approach may bring to a severe security weakening. To have an untrusted scheme, it is necessary to use a quantum entangled state to share the key without disclosing it to Charlie. Even though entanglement based protocols are very promising, they need the use of a quantum memory that is still under study.

Figure 4.2: Future scenario of QKD network: dedicated quantum terminals orbiting around the Earth exchanging keys with optical ground station.

The second solution relies on the use of *satellites* as trusted nodes. The feasibility of exchanging single photons from-and-to a ground station via a satellite was already demonstrated by two experiments [25, 26]. These experiment were aimed at showing that a photon could be detected at the expected time and its properties, like polarization, measured for Quantum Communication purpose. In 2014, the *QuantumFuture Group* of the University of Padua realized the first experimental satellite quantum communication [27] by exploiting the photon polarization as carrier of quantum information. We will dedicate particular attention to this last experiment, because its setup is the basis of the *satellite time-bin feasibility test* that we will describe in the following chapters.

Satellite Quantum Communications are part of the European road map for Quantum Information Processing and Communication [28], but also outside Europe the are a lot of projects about satellite QKD. In Japan a collaboration between JAA (Japan National Spatial) and the University of Tokyo wants to demonstrate and improve actual quantum and classical optical communications [29]. In the month of May 2014 it had been launched the first satellite of the project that is able to send polarized weak coherent pulse between Space and an optical ground station. Then, it should demonstrate the possibility to generate a single qubit into Space and send it to the Earth, a realization that has yet to be proven with an orbiting satellite. In China there is a bigger project called *Quantum Science Satellite* [30]. The first satellite will be launched in the January 2016 and it will be equipped with a decoy state BB84 source and will be visible and trackable for a lot of optical ground stations. This satellite should also have an entangled source to perform experiments like

Bell's violation and teleportation protocol. Also the Canadian Space Agency has a project in collaboration with Canadian universities, like IQC of Waterloo, to realize a satellite for quantum communications [31].

An important aspect of SQCs is the implementation of QKD with moving terminals, something not possible with fiber based links. Furthermore, a satellite terminal is visible only for some minutes from the ground and one is therefore faced with a *finite key* that cannot approach its asymptotic limit (1.45) and mathematical criteria were developed to address this problem [32].

Then, the methodology developed for SQCs is also suitable for the investigation of very fundamental questions of Nature. Quantum Mechanics was developed to describe the behavior of the smallest dimensions in Physics. Quantum channels over several thousand of kilometers can pave the way for future tests of Quantum Mechanics on an entirely different scale. The fact that this theory was not meant for this scale raises the question as to whether all predictions are still valid at these distances or in strong gravitational fields (e.g., the gravitational field of the Sun).

The extension to Space of QCs is motivated by the vision of a network of quantum terminals on satellites that may provide the exchange of cryptographic key in the first place, but later also the teleportation of states and the distributed quantum computation via quantum repeaters. The most realistic scenario of global QKD system will consist of short distance fiber based quantum key exchanges supported by long distance quantum key exchanges between states or continent via satellite quantum links. Furthermore, communications among a flotilla of dedicated quantum terminals orbiting around the Earth exchanging keys with optical ground station (as in Figure 4.1 and 4.2) is not a too distance.

4.2 EXPERIMENTAL STEPS TOWARDS SATELLITE QUANTUM COMMUNICATIONS

In this section we present the early experimental works that have demonstrated the feasibility of SQCs. As we have already noted, at the moment no orbiting satellites dedicated specifically to quantum communications are in operation. The three works that we present ([25, 26, 27]) are all characterized by the idea of mimicking a quantum transmitter in orbit exploiting low orbit satellites equipped with *corner-cube retroreflectors* (CCRs), devices that reflect back the incident light in the origin direction. The power of the incoming light can be set to mimic a pseudo single photon source at the satellite that plays in this way the role of Alice, while Bob is at the ground station where the retroreflected photons are detected and analyzed.

Firstly, we will describe the two works [25, 26] that demonstrate the feasibility of the exchange of single photons between a satellite and a Earth-based station and then we will preset the recent work [27] where is shown that polarization encoding is possible along such type of quantum channel.

4.2.1 *Exchange of single photons between a satellite and a Earth-based station*

Villoresi and colleagues in [25] report the first experimental investigations on the exchange of single photon between a low Earth orbiting (LEO, orbits ranging in amplitude 0 - 2000 km) satellite transmitter and a ground-based receiver, the Matera Laser Ranging Observatory (MLRO) in Matera.

Their experiment is based on the exploitation of the *Satellite Laser Ranging* (SLR) technique. Typically, satellite laser-ranging systems are used for geodynamical studies (crustal dynamics, polar motion, time-varying geopotential monitoring) by means of a series of measurements of the *round trip time* (rtt) of optical laser pulses that propagate from a station on the Earth, are then retroreflected at the satellite and are finally detected at the ground station. From the measure of the flying time (rtt) of the pulse they can obtain the distance of the satellite with great resolution. The International Laser Ranging Service (ILRS) network provides to the various stations the *trajectory's previsions* that are used to follow the orbiting satellite during its passage.

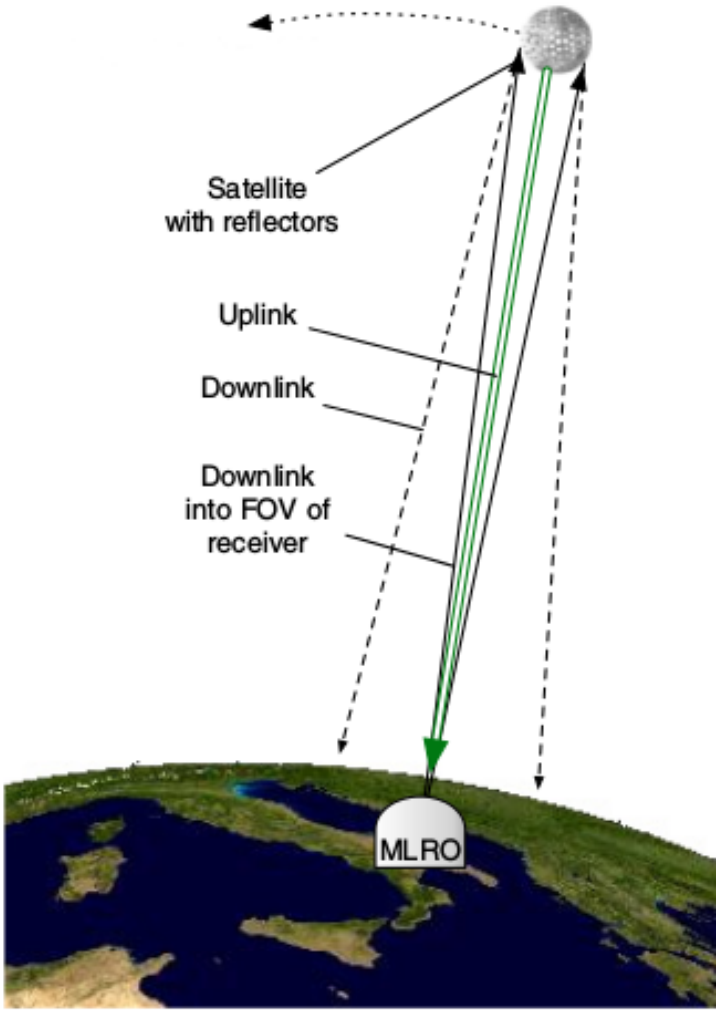


Figure 4.3: The scheme of the satellite single photon link [25].

The operating principle of the experiment is to use the excellent satellite tracking system of the MLRO station to perform precise measurements of single photons returns. They mimic a single photons source on a satellite using the retroreflection of a weak laser pulse from a SLR satellite, as shown in Figure 4.3. A laser pulse (wavelength 532 nm, repetition rate 17 kHz) is directed toward the satellite (uplink). A fraction of the beam in the uplink is retroreflected into the field-of-view (FOV) of the telescope of MLRO, whose primary mirror has 1.5 m aperture. The radiation in the downlink constitutes the single photons channel because, by means of *link budget calculation*, they show that the number of photons in the downlink is of the order of one.

To achieve this result, differently from the SLR technique, they are not interested in measuring the round trip time, but they measure the number of detected photons per second, the detector count rate (DCR), and compare it with the expected value given by the *Degnan radar link-budget equation* [33] that we will explain in the following (section 4.2.2).

Exploiting the SLR tracking system they correlate the detection events with the transmitted laser pulses and computed the deviation $D = t_{exp} - t_{ref}$ between the expected return time t_{exp} and the detection event time stamp t_{ref}. The values of the deviation D, grouped in several bins of varying widths (from 1 to 20 ns), were accumulated over short arcs of the total satellite pass.

Figure 4.4 shows the histogram of the deviations D for the Ajisai satellite obtained with bin size of 5 ns. The evidence of the single photon exchange is given by the peak centered at $D = 0$ that is larger the mean value of the background counts by 4.5 standard deviations.

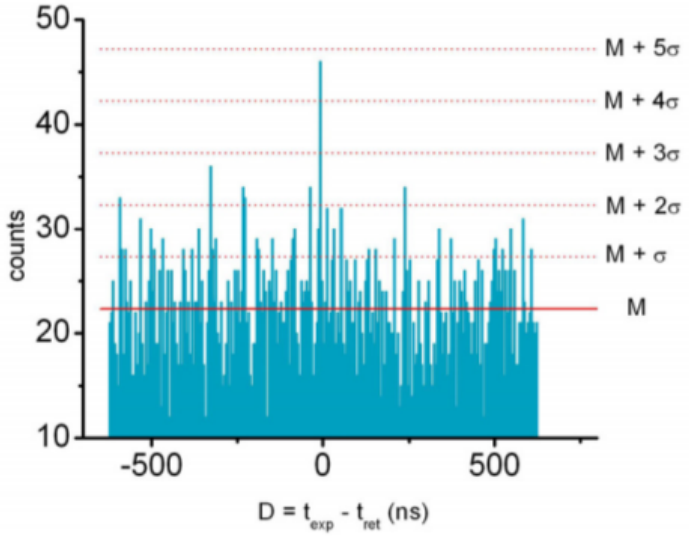


Figure 4.4: Histogram of the differences D between expected and observed detections for Ajisai satellite [25].

According to the link-budget equation they estimated that, for each laser shot, about $1.2 \cdot 10^5$ photons leave the satellite in the whole solid angle subtended by the downlink FOV, while an average of 0.4 photon per pulse are

directed in the downward channel, thus realizing the condition of the single photon channel and attesting the feasibility of a satellite-based quantum channel.

The other work about the single photon exchange between a satellite and a ground station is due to Yin and colleagues [26]. Their setup for single photon link from satellite to ground was installed at the Shangai Observatory. Differently from the previous work, the telescope employed a binocular structure with a transmitting and a receiving telescope. In their setup they couple the beam of the SLR of Shangai Observatory with a laser beam (wavelength 702 nm, repetition rate 76 MHz) used for the single photon exchange. This coupled beams were transmitted to the CHAMP satellite that reflected them to the receiving telescope and the acquisition system where photons are detected.

About the temporal synchronization, the quantum system and the SRL one are independent. They estimate the deviation D between the experimental and the theoretical transmitting time and represent the histogram the D values, as shown in Figure 4.5. The peak of the histogram is centered at 0 ns, as expected and the time accuracy is given by the full width at half maximum (FWHM) of the Gaussian fit (1.35 ± 0.03 ns).

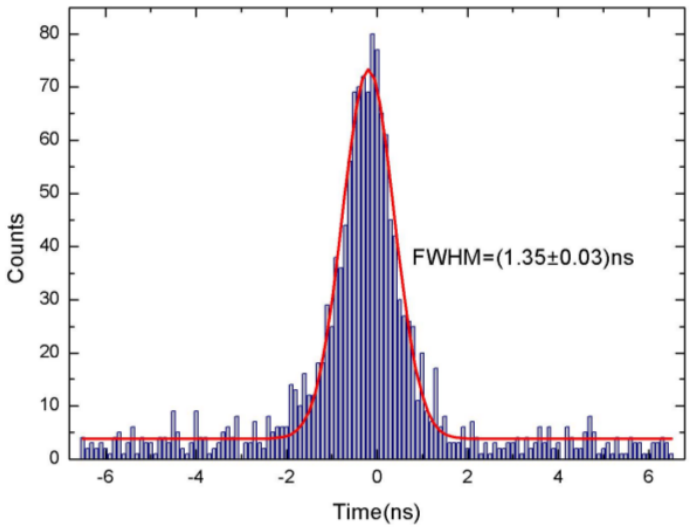


Figure 4.5: Histogram of the differences D between the experimental and the theoretical transmitting time [26].

Then, analyzing the data with 2 ns of bin size they estimate the effective echo signals counts $\overline{N'} = 1000$ and the effective dark counts of the detector $\overline{N'_b} = 58$, from which they obtain the *signal to noise ratio* (SNR)

$$\mathrm{SNR} = \frac{\overline{N'} - \overline{N'_b}}{\overline{N'_b}} = 16.2 \,, \tag{4.1}$$

which is good enough to generate quantum links for unconditionally secure QKD [34].

4.2.2 *Satellite Quantum Communication with polarization encoding*

The last important work about experimental Satellite Quantum Communication is due again to the group of Villoresi [27] and can be viewed as the continuation of the previous works: they not only realized the single photon exchange between a satellite and a ground station, but also demonstrate that single photon polarization preservation and discrimination between different polarization encoded quantum states can be realized.

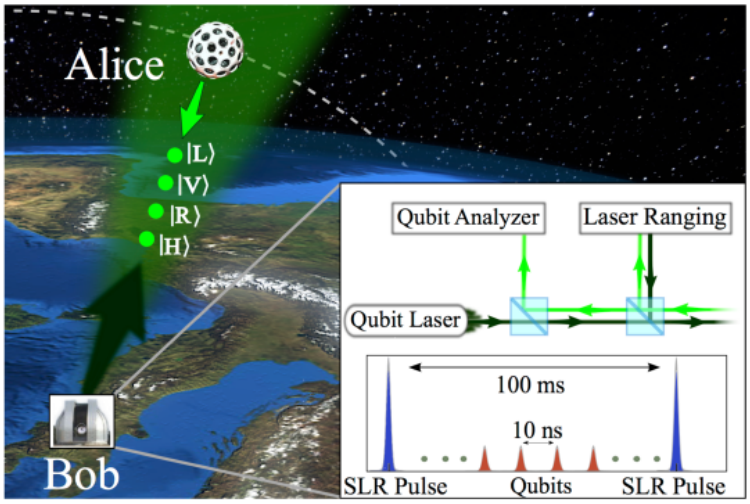


Figure 4.6: Scheme of the satellite quantum communication demonstration with polarization encoding [27].

They exploit the same laser ranging station in Matera of the previous work, but with a modified synchronization system: it lets them to collect the SLR data and the "quantum data" at the same time with two separated detection systems well synchronized with the MLRO atomic clock. Figure 4.6 sketched the operation of the quantum transmitter, Alice, and of the quantum receiver, Bob: Alice is simulated by CCRs of a LEO orbiting satellite while the discrimination of the different polarization states is done by Bob at the ground station.

Alice qubit stream is realized from a 100 MHz (temporal separation 10 ns) train of polarized pulses (532 nm, horizontal, vertical, left or right circular polarization) synchronized with the 10 Hz (temporal separation 100 ms) train of strong SLR pulses. The two beams are coupled at a beam splitter and sent upward from the ground to the satellite and then they are reflected to the ground. Estimating the uplink attenuation, they set the pulse energy for the qubit stream such that the pulses reflected from satellites have an average photon number close to one. At Bob, they measure a Quantum Bit Error Rate (QBER) typically lower than 5%, a level suitable for several quantum information protocols, like QKD as we have discussed in section 1.2.3.

The setup of this experiment is very similar to the setup of the satellite time-bin experiment that we will present in the following with great details. It

is important to note that the retroreflected qubit stream is collected by Bob's qubit state analyzer that can change between two receiving mutually unbiased bases, horizontal-vertical $\{|H\rangle, |V\rangle\}$ and left-right circular $\{|L\rangle, |R\rangle\}$. In this experiment is essential that CCRs can preserve the polarization state during the reflection. They use four different LEO satellites with such polarization preserving CCRs (Jason-2, Larets, Starlette and Stella) and one satellite (Ajisai) that does not preserve the polarization for comparison.

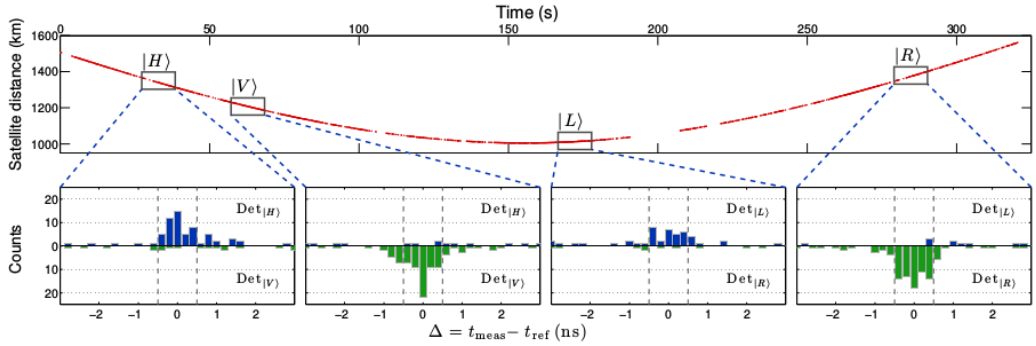


Figure 4.7: The passage of Larets satellite used to demonstrate polarization preservation along the quantum channel [27].

Figure 4.7 shows a passage of Larets satellite they collected: the whole passage is divided into four interval of 10 seconds corresponding to four different polarized input states: horizontal $|H\rangle$, vertical $|V\rangle$, left circular $|L\rangle$ and right circular $|R\rangle$. At the receiver, they used two single photon detectors measuring two orthogonal polarizations: the four histograms in the figure report the obtained counts at the receiver for each single photon detector in function of the measured detection time. So, they estimate the QBER as

$$Q = \frac{n_{wrong} + 1}{n_{corr} + n_{wrong} + 2}, \tag{4.2}$$

where n_{corr} and n_{wrong} are the number of detections in the transmitted and orthogonal polarization respectively. For the passage in the figure they estimated $n_{corr} = 199$, $n_{wrong} = 13$ that give a QBER of $6.5\% \pm 1.7\%$ that is suitable for QKD with polarization encoding.

Then, they demonstrate the feasibility of polarization encoding also with other satellites as shown in Figure 4.8. They divide the detection period in 5 seconds intervals. They fix the sent polarization to $|V\rangle$ and measure in two orthogonal polarization $|H\rangle$ and $|V\rangle$. For each satellite, they show the bare QBER (blue dots) and QBER calculated after background subtraction (red dots) and their average values for the whole passage that result below 11% for satellite with coated CCRs, demonstrating the feasibility of the BB84 protocol from satellite to ground. As expected, for Ajisai, having non polarization preserving CCRs, the QBER is above 40%.

In the figure is reported also the number of photons per pulse leaving the satellite μ_{sat} that is estimated dividing the the average number of photons

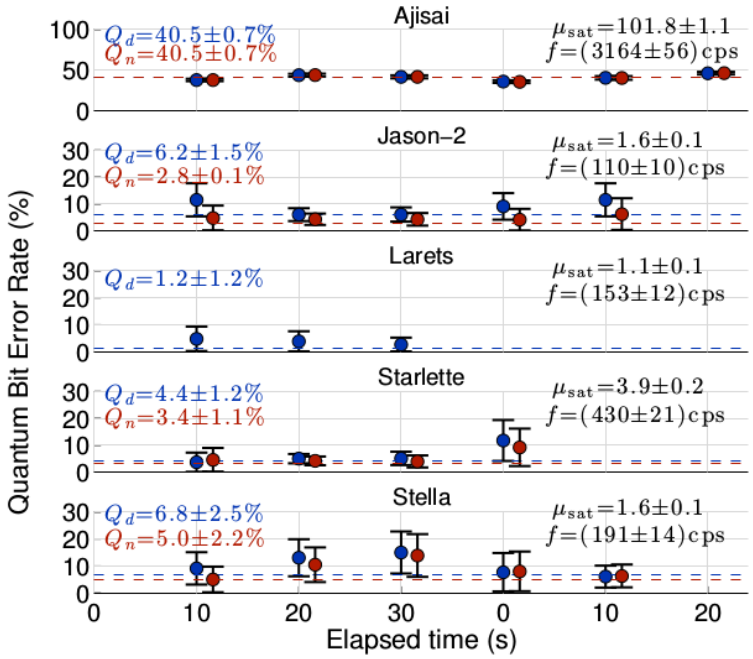


Figure 4.8: Feasibility of polarization encoding with satellites using coated CCRs [27].

per pulse detected at the receiver μ_{rx}, by the transmittivity of the quantum channel. To predict the detected number of photons per pulse they use the *Degnan link-budget radar equation* [33]

$$\mu_{rx} = \mu_{tx}\eta_{tx}G_t\Sigma\left(\frac{1}{4\pi R^2}\right)^2 T_a^2 A_t \eta_{rx}\eta_{det}\,, \tag{4.3}$$

where μ_{tx} is the source mean photon per pulse, η_{tx} is the optical transmission efficiency, G_t is the transmission gain, Σ and R are the satellite cross-section and slant distance, T_a is the atmospheric transmittivity, A_t is the telescope area, η_{rx} is the optical receiving efficiency and η_{det} is the single photon detector efficiency. They factorize (4.3) into uplink and downlink contributions:

$$\text{uplink: } \mu_{sat} = \mu_{tx}\eta_{tx}G_t\rho A_{eff}\left(\frac{1}{4\pi R^2}\right)T_a\,, \tag{4.4}$$

$$\text{downlink: } \mu_{rx} = \mu_{sat}G_{down}\left(\frac{1}{4\pi R^2}\right)T_a A_t\eta_{rx}\eta_{det}\,, \tag{4.5}$$

where they have splitted the satellite cross-section according to $\Sigma = \rho A_{eff} G_{down}$ where ρ and A_{eff} correspond to the CCR reflectivity and to the effective satellite retroreflective area and they contribute to the uplink, while G_{down} expresses the effective downlink gain and so it contributes to the downlink term.

Using these expressions they extrapolate the transmitter gain G_t and use it to predict the number of received photons to compare it with the measured one. They show in Figure 4.9 that the Degnan radar equation and equations (4.4)-(4.5) provide a precise fit for the measured counts so that the estimated

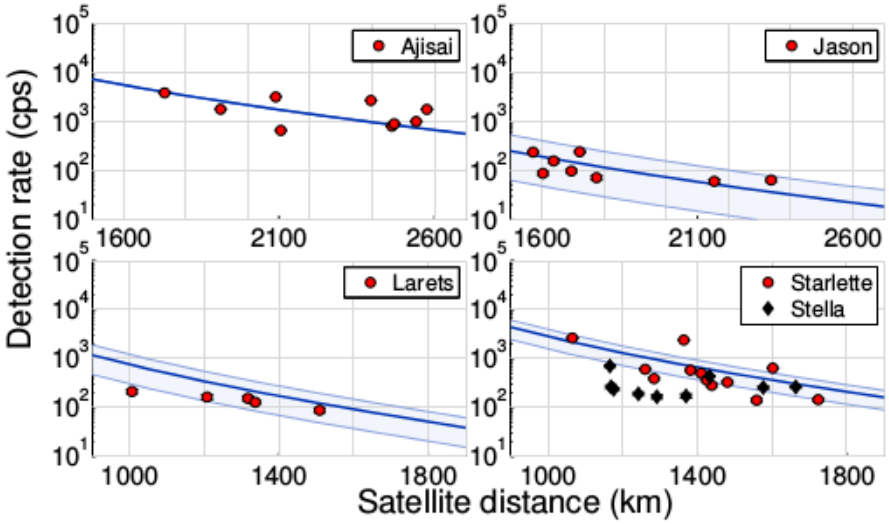


Figure 4.9: Fit of the measured detection rate realized with the link-budget equation for the different satellites used in the experiment [27].

μ_{sat} values reported in Figure 4.8 for different satellites are correct and of the order of one, as required by realistic QKD scenario.

In this way, they experimentally demonstrate the preservation of single photon polarization over a satellite-to-ground channel, covering an unprecedented length (more than 1000 kilometers) compared to ground experiments and showing the feasibility of quantum information protocols such as QKD along a space channel. In this test-experiment the information is encoded in the polarization of the photon. However, it is necessary to study other protocols and encoding techniques along space channel, like the *time-bin* encoding that we will present in the next chapter.

5

TIME-BIN ENCODING FOR SPACE QUANTUM COMMUNICATION

In this chapter we describe the *time-bin encoding* for Quantum Communication: a weak laser pulse is brought through interferometry technique in a quantum superposition of states characterized by the propagation time. The relative *phase* between the two states can be controlled and used to encapsulate the information that Alice and Bob want to share.

Firstly, we will show how to realize a *time-bin qubit* and how to calculate the detection probabilities in the typical setup used for this encoding technique. Then, we will present the simplest experimental configuration that one can use to implement the QKD-BB84 protocol with *phase encoding*. Finally, we will describe how the time-bin encoding technique can be exploited in a space quantum channel between an orbiting satellite and a ground station, as it is pictorially represented in Figure 5.1.

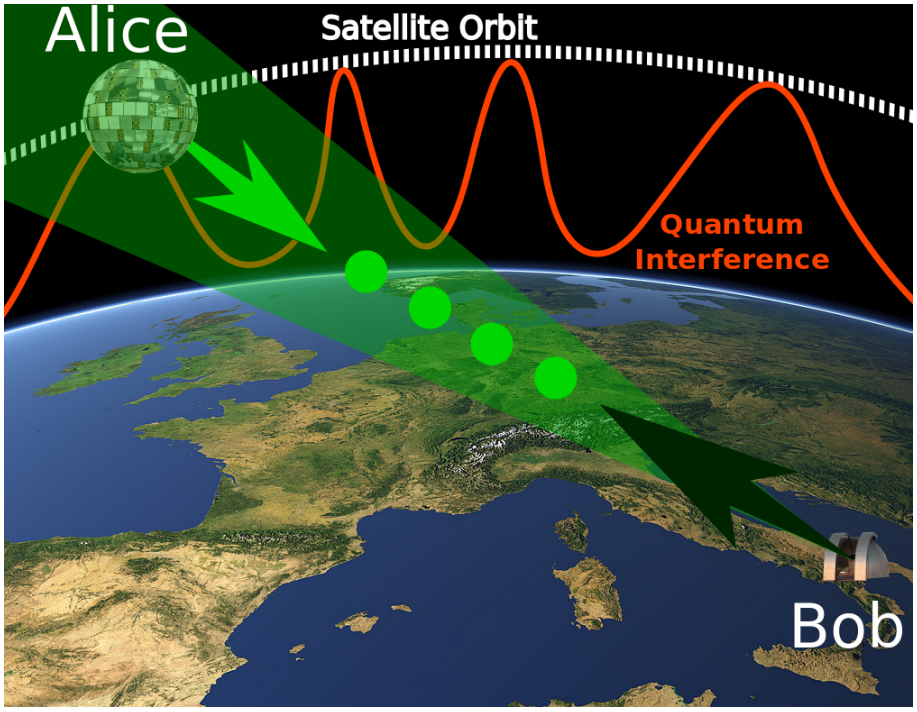


Figure 5.1: The exploitation of the satellite orbit using the *time-bin* encoding technique.

5.1 TIME-BIN QUBIT AND QUANTUM INTERFERENCE

In this section we use the results of section 3.7 to study the dynamics of a linear multiport with localized photons as input state to calculate the detection probabilities for the optical setup typically used in time-bin experiments.

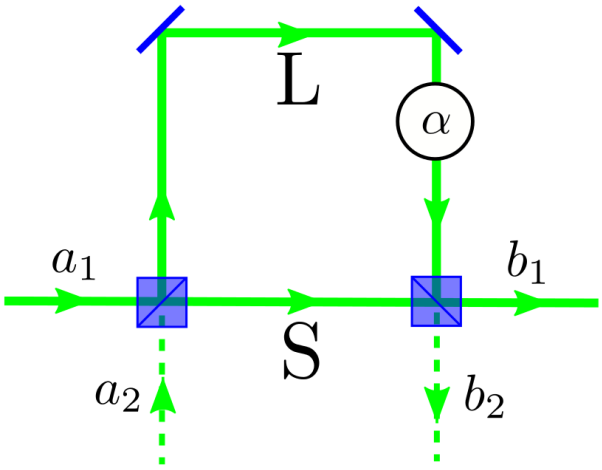


Figure 5.2: Input-output modes representation for a Mach-Zender unbalanced interferometer.

We consider an input pulse entering a *Mach-Zender unbalanced interferometer* as show in Figure 5.2. We can describe the interferometer as a linear filter consisting of a delay element (the long arm) and a phase modulator of value α sandwiched between two 50:50 beam splitters. The two arms short S and long L are unbalanced, i.e., the *path difference* $l = L - S$ is not null, so that at the output ports we will get two well separated pulses, as we will show now.

The difference between the two arms l is set to avoid single photon interference: this can be achieved taking the path difference greater than the coherence length l_c (see section 3.3) of the pulse that is related to the bandwidth $\Delta\omega$:

$$l \gg l_c = c\tau_c = \frac{c}{\Delta\omega} \,. \tag{5.1}$$

Setting

$$l \equiv c\Delta t \,, \tag{5.2}$$

$$S \equiv ct_S \,, \tag{5.3}$$

the scattering matrix of the interferometer (viewed as a cascade of three multiports) is given by

$$\begin{aligned} S^A &= S_{BS} \begin{pmatrix} e^{i\phi_A} & 0 \\ 0 & 1 \end{pmatrix} S_{BS} e^{i(\omega-\omega_0)t_S} \\ &= \frac{1}{2} \begin{pmatrix} 1 - e^{i\phi_A} & i(e^{i\phi_A}+1) \\ i(e^{i\phi_A}+1) & e^{i\phi_A}-1 \end{pmatrix} e^{i(\omega-\omega_0)t_S} \end{aligned} \tag{5.4}$$

where $e^{i(\omega-\omega_0)t_S}$ represents the propagation of the pulse in the short path within the time $t_S = S/c$ and

$$e^{i\phi_A} \equiv e^{i(\omega-\omega_0)\Delta t + i\alpha} \tag{5.5}$$

is the *delay parameter* [19] relative to the short arm that represents the delay Δt introduced by the long one and a possible supplementary phase α introduced by the phase modulator.

Now, we take as input state of the interferometer a single photon pulse[1] entering the first port a_1 centered about t_0 as shown in Figure 5.3:

$$|in\rangle = \hat{a}^\dagger_{1,t_0}|vac\rangle \ . \tag{5.6}$$

Setting

$$t_1 = t_0 + t_S \ , \tag{5.7}$$
$$t_2 = t_1 + \Delta t = t_0 + t_S + \Delta t \ , \tag{5.8}$$
$$\tag{5.9}$$

and using (3.126), we can get the output state of the unbalanced Mach-Zender interferometer described by the scattering matrix S^A in (5.4),

$$\begin{aligned}
|out\rangle = |in\rangle &= \hat{a}^\dagger_{1,t_0}|vac\rangle \\
&= \sum_{j=1}^{2} \int d\omega \xi^{t_0}(\omega) S^A_{j1} \hat{b}^\dagger_j(\omega)|vac\rangle \\
&= \int d\omega \ \xi^{t_0}(\omega) S^A_{11} \hat{b}^\dagger_1(\omega)|vac\rangle + \int d\omega \xi^{t_0}(\omega) S^A_{21} \hat{b}^\dagger_2(\omega)|vac\rangle \\
&= \int d\omega \ \xi^{t_0}(\omega) \frac{1}{2}(1 - e^{i\phi_A}) e^{i(\omega-\omega_0)t_S} \hat{b}^\dagger_1(\omega)|vac\rangle \\
&\qquad + \int d\omega \ \xi^{t_0}(\omega) \frac{i}{2}(e^{i\phi_A} + 1) e^{i(\omega-\omega_0)t_S} \hat{b}^\dagger_2(\omega)|vac\rangle \\
&= \int \frac{d\omega}{2} \ \left[\xi^{t_1}(\omega)\hat{b}^\dagger_1(\omega) - e^{i\alpha}\xi^{t_2}(\omega)\hat{b}^\dagger_1(\omega)\right]|vac\rangle \\
&\qquad + \int \frac{d\omega}{2} \ \left[ie^{i\alpha}\xi^{t_2}(\omega)\hat{b}^\dagger_2(\omega) + i\xi^{t_1}(\omega)\hat{b}^\dagger_2(\omega)\right]|vac\rangle \\
&= \frac{1}{2}\left(\hat{b}^\dagger_{1,t_1} - e^{i\alpha}\hat{b}^\dagger_{1,t_2} + ie^{i\alpha}\hat{b}^\dagger_{2,t_2} + i\hat{b}^\dagger_{2,t_1}\right)|vac\rangle \ ,
\end{aligned} \tag{5.10}$$

where we have used

$$\xi^{t_0}(\omega)e^{i(\omega-\omega_0)t_S} = \xi^{t_0+t_S}(\omega) = \xi^{t_1}(\omega) \ , \tag{5.11}$$
$$e^{i\phi_A}\xi^{t_0}(\omega)e^{i(\omega-\omega_0)t_S} = e^{i(\omega-\omega_0)\Delta t}e^{i\alpha}\xi^{t_0}(\omega)e^{i(\omega-\omega_0)t_S} = e^{i\alpha}\xi^{t_2}(\omega) \tag{5.12}$$

and the definition (3.114) applied to the output operators.

1 We use the formalism of single photons even if practical implementations use attenuated pulsed laser to mimic single photon states as described in section 1.2.3

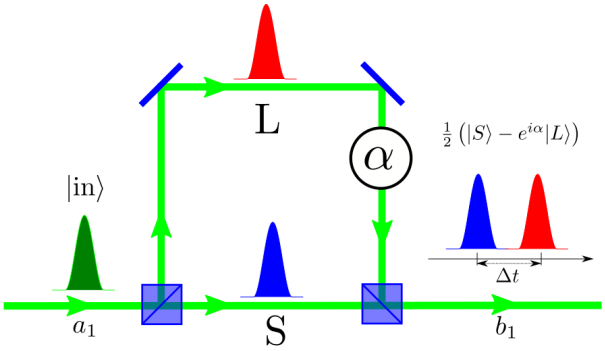


Figure 5.3: The *time-bin qubit*.

We can now explain the idea of *time-bin qubit*. We neglect the output port b_2 and consider only the output state $|\Psi\rangle$ at the port b_1 (see Figure 5.3). This state is a superposition of the states that give the two pulses well separated emerging from port b_1 and we can write it as

$$|\Psi\rangle = \frac{1}{2}\left(\hat{b}^{\dagger}_{1,t_1} - e^{i\alpha}\hat{b}^{\dagger}_{1,t_2}\right)|vac\rangle \ . \tag{5.13}$$

We define

$$|S\rangle \equiv \hat{b}^{\dagger}_{1,t_1}|vac\rangle \tag{5.14}$$

and

$$|L\rangle \equiv \hat{b}^{\dagger}_{1,t_2}|vac\rangle \tag{5.15}$$

to indicate the pulses that have taken the short and the long path respectively and so the state can be written as:

$$|\Psi\rangle = \frac{1}{2}\left(|S\rangle - e^{i\alpha}|L\rangle\right) \ . \tag{5.16}$$

The idea of *time-bin qubit* is that each pulse is brought into a superposition of two time-bins, an early one, $|S\rangle$, corresponding to time t_1 and a delayed one, $|L\rangle$, relative to time t_2. The probability amplitude of each time-bin and their relative phase allow one to prepare any possible qubit state. The relative phase between the two pulses can be measured by using interferometry technique, as we will do in our experiment (see section 5.4). This possibility of qubit encoding was called *time-bin* for the first time in [35], but the idea was presented in various works: in [36] where Franson used a similar setup to test a *Bell inequality* for position and time, in [37] and in [38] where Rarity and Bennet respectively applied the idea to quantum key distribution.

We now consider the output state at port b_1 as a new input state of another Mach-Zender interferometer (see Figure 5.4) with the same path lengths S and L, but with scattering matrix S^B that is in the form of (5.4) with delay parameter

$$e^{i\phi_B} \equiv e^{i(\omega-\omega_0)\Delta t + i\beta} \ , \tag{5.17}$$

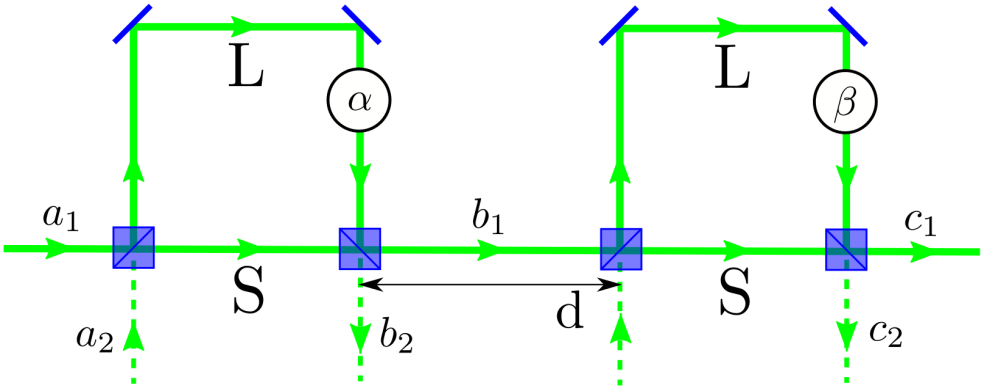


Figure 5.4: Double Mach-Zender configuration for time bin encoding technique.

i.e., the two interferometers are characterized by two different phase modulators.

The input state of the second interferometer is made up of the two pulses emerging from port b_1 of the first one and entering the second one centered at time T_1 and T_2 determined by the distance d of the two interferometers

$$T_1 = t_1 + d/c \,, \tag{5.18}$$
$$T_2 = t_2 + d/c \,, \tag{5.19}$$

and so we can write it as

$$|in'\rangle = \frac{1}{2}\left(\hat{b}^\dagger_{1,T_1} - e^{i\alpha}\hat{b}^\dagger_{1,T_2}\right)|vac\rangle \,. \tag{5.20}$$

This state is a linear superposition of two pulse states that are well separated in time if the time difference

$$T_2 - T_1 = t_2 - t_1 = \Delta t \tag{5.21}$$

is longer than the coherence time of the pulse, i.e., $\Delta t \gg \tau_c$ as we have assumed in (5.1).

We can get the output state after the second Mach-Zender interferometer that has scattering matrix S^B writing the input state in terms of the output operators $\hat{c}_i$ ($i = 1, 2$) using the result in (5.10). Now, we have two entry times T_1 and T_2 and so we expect four exit times

$$\tau_{SS} = T_1 + t_S \,, \tag{5.22}$$
$$\tau_{SL} = \tau_{SS} + \Delta t \,, \tag{5.23}$$
$$\tau_{LS} = T_2 + t_S \,, \tag{5.24}$$
$$\tau_{LL} = \tau_{LS} + \Delta t \tag{5.25}$$

to obtain:

$$\begin{aligned}|\text{out}'\rangle = \frac{1}{2}\frac{1}{2}\left(\hat{c}^{\dagger}_{1,\tau_{SS}} - e^{i\beta}\hat{c}^{\dagger}_{1,\tau_{SL}} + ie^{i\beta}\hat{c}^{\dagger}_{2,\tau_{SL}} + i\hat{c}^{\dagger}_{2,\tau_{SS}}\right)|\text{vac}\rangle \\ - \frac{1}{2}e^{i\alpha}\frac{1}{2}\left(\hat{c}^{\dagger}_{1,\tau_{LS}} - e^{i\beta}\hat{c}^{\dagger}_{1,\tau_{LL}} + ie^{i\beta}\hat{c}^{\dagger}_{2,\tau_{LL}} + i\hat{c}^{\dagger}_{2,\tau_{LS}}\right)|\text{vac}\rangle \\ = \frac{1}{4}\left[\hat{c}^{\dagger}_{1,\tau_{SS}} - e^{i\beta}\hat{c}^{\dagger}_{1,\tau_{SL}} - e^{i\alpha}\hat{c}^{\dagger}_{1,\tau_{LS}} + e^{i(\alpha+\beta)}\hat{c}^{\dagger}_{1,\tau_{LL}}\right]|\text{vac}\rangle \\ + \frac{i}{4}\left[\hat{c}^{\dagger}_{2,\tau_{SS}} + e^{i\beta}\hat{c}^{\dagger}_{2,\tau_{SL}} - e^{i\alpha}\hat{c}^{\dagger}_{2,\tau_{LS}} - e^{i(\alpha+\beta)}\hat{c}^{\dagger}_{2,\tau_{LL}}\right]|\text{vac}\rangle\ . \end{aligned} \tag{5.26}$$

We can define, for each exit port c_i, a state with a pulse centered at one of the four final times:

$$|SS\rangle_i \equiv \hat{c}^{\dagger}_{i,\tau_{SS}}|\text{vac}\rangle \tag{5.27}$$

$$|SL\rangle_i \equiv \hat{c}^{\dagger}_{i,\tau_{SL}}|\text{vac}\rangle \tag{5.28}$$

$$|LS\rangle_i \equiv \hat{c}^{\dagger}_{i,\tau_{LS}}|\text{vac}\rangle \tag{5.29}$$

$$|LL\rangle_i \equiv \hat{c}^{\dagger}_{i,\tau_{LL}}|\text{vac}\rangle \tag{5.30}$$

and write the output state after the second interferometer as

$$\begin{aligned}|\text{out}'\rangle = \frac{1}{4}\left(|SS\rangle_1 - e^{i\beta}|SL\rangle_1 - e^{i\alpha}|LS\rangle_1 + e^{i(\alpha+\beta)}|LL\rangle_1\right) \\ + \frac{i}{4}\left(|SS\rangle_2 + e^{i\beta}|SL\rangle_2 - e^{i\alpha}|LS\rangle_2 - e^{i(\alpha+\beta)}|LL\rangle_2\right)\ . \end{aligned} \tag{5.31}$$

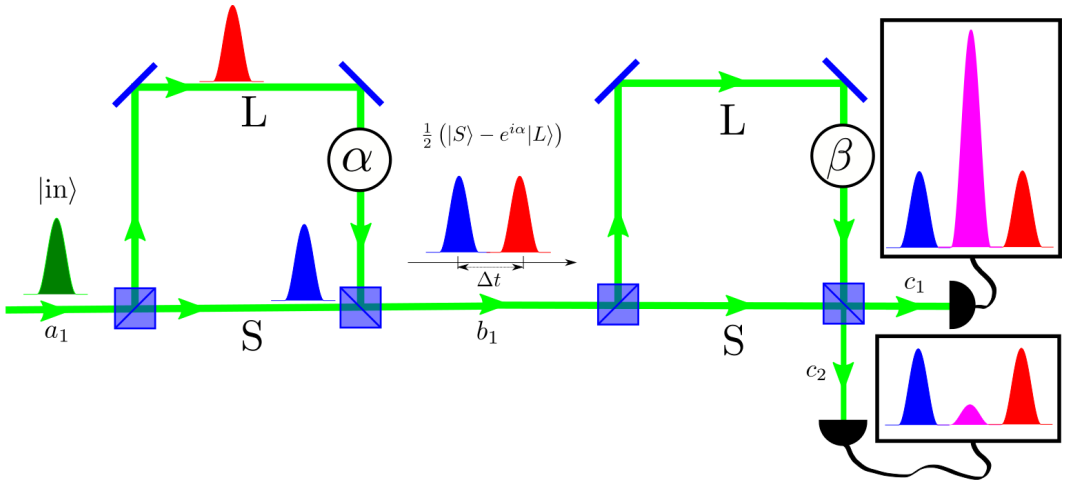


Figure 5.5: Representation of the pulse propagation in the double Mach-Zender configuration that leads to quantum interference.

We can interpret this final state in a simple way, referring to Figure 5.5. The input pulse $|\text{in}\rangle$ enters the interferometer at port a_1. It can arrive at one of the output ports of the second interferometer following one the four different

paths described by the four finale state. By monitoring detector counts as a function of the time since the emission of the photons, you obtain a *three-peaks histogram* as shown in the figure. Indeed, each pulse can pass through the short arm in both the interferometers ($|SS\rangle_i$ path), or through the long arm in both the interferometers ($|LL\rangle_i$ path). But it also can pass the first time through the short and the second one through the long ($|SL\rangle_i$ path) and vice versa ($|LS\rangle_i$ path). These two last possibilities are characterized by close arriving times if the interferometers are stable for the duration of the time of flight. So, the *superposition* between $|SL\rangle_i$ and $|LS\rangle_i$ leads to *quantum interference* because we can not distinguish between the two paths. A timing window can be used to discriminate between interfering and non-interfering events as we explain now.

Suppose we want to detect the pulse in the final state $|out'\rangle$ at a specified time τ at the output port c_j ($j = 1, 2$). Its probability can be calculated in the same way we followed in section (3.7) generalizing formula (3.102) and the number operator for discrete annihilation operators to *pulse number operator*

$$\hat{n}_{c_{j,\tau}} = \hat{c}^{\dagger}_{j,\tau}\hat{c}_{j,\tau} \tag{5.32}$$

and write the detection probability at the port c_j at time τ as:

$$I_{c_j}(\tau) = \langle out'|\hat{c}^{\dagger}_{j,\tau}\hat{c}_{j,\tau}|out'\rangle \ . \tag{5.33}$$

If we want to detect the pulse in a temporal window $\Delta\tau$ centered at time $\tau = \tau_{SL} \approx \tau_{LS}$ at exit port c_2, its probability is given by

$$\begin{aligned}
I_{c_2}(\Delta\tau) &= \langle out'|\hat{c}^{\dagger}_{2,\Delta\tau}\hat{c}_{2,\Delta\tau}|out'\rangle \\
&= \langle out'|\hat{n}_{c_{2,\Delta\tau}}|out'\rangle \\
&= \langle out'|\left[\frac{i}{4}\left(e^{i\beta}|SL\rangle_2 - e^{i\alpha}|LS\rangle_2\right)\right] \\
&= \left(\frac{-i}{4}\right)\left(\frac{i}{4}\right)\left[e^{-i\beta}|SL\rangle_2 - e^{-i\alpha}|LS\rangle_2\right]\left[e^{i\beta}|SL\rangle_2 - e^{i\alpha}|LS\rangle_2\right] \\
&= \frac{1}{16}\left(1 - \mathcal{V}_Q e^{-i(\alpha-\beta)} - \mathcal{V}_Q e^{i(\alpha-\beta)} + 1\right) \\
&= \frac{1}{8}\left[1 - \mathcal{V}_Q \cos(\alpha-\beta)\right] \ ,
\end{aligned} \tag{5.34}$$

where we have defined the *quantum visibility* that characterizes quantum interference as

$$\mathcal{V}_Q = \langle SL|LS\rangle \ , \tag{5.35}$$

i.e., it is the overlap between the two pulses $|SL\rangle_i$ and $|LS\rangle_i$ and it is a real number in $[0, 1]$ by using (3.124). We introduce this definition of visibility to emphasize the importance of the interferometer stability: the two arriving times of the interfering pulses are close one to each other only if the temporal

unbalance Δt of the interferometers is stable for the duration of the pulse propagation from the source to the detector. We will estimate the quantum visibility obtained in our experiment in the last chapter.

In the following of this chapter we will suppose that interferometer stability holds so that the visibility is unitary. In this case, the detection probability (5.34) reduces to

$$\frac{1}{4}\sin^2\left(\frac{\alpha-\beta}{2}\right). \tag{5.36}$$

If the phase difference $\Delta\varphi \equiv \alpha - \beta$ imposed by the two modulators is null we get destructive interference at port c_2 and constructive interference at port c_1 (see Figure 5.5). We obtain this situation in the preliminary tests we realized at Luxor Laboratory that we will describe in section 5.3. The interference effect described in this double Mach-Zender configuration can be achieved also with a simpler implementation that we will present in the next section.

5.2 "TWO WAYS" SETUP AND BB84 PROTOCOL

As we have seen in section 1.2.3 practical implementations of QKD rely on faint laser pulses that approximate single-photon Fock space. In the time-bin encoding protocol information is encoded in the *phase* of the transmitted pulse using an interferometry setup like that we have described in the last section, hence the name *phase encoding*.

We can think that the first interferometer of Figure 5.5 belongs to Alice and the second one to Bob and that they want to share a secret key. However, to prevent the practical and difficult necessity to align two interferometers the double-interferometer configuration can be changed into a simpler one, called "Two-ways" (or "Plug&Play") [39], where it is used one interferometer, as in Figure 5.6.

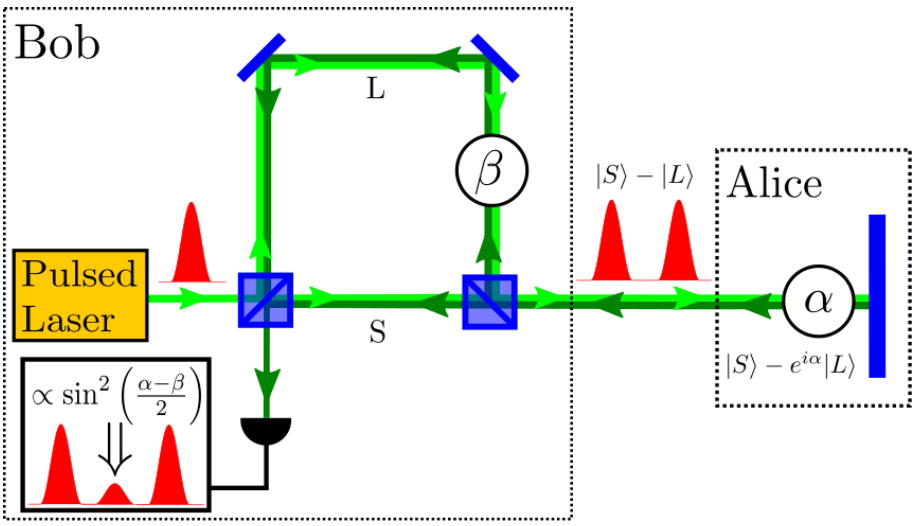


Figure 5.6: "Two-Ways" interferometry setup for QKD.

Alice's setup consists of a sending-back mirror and a phase modulator, while Bob's setup is composed by a pulsed laser source, the interferometer with a phase modulator and two single-photon detector connected to the output ports even if for practical purpose only one detector is sufficient as shown in the figure.

Bob can send pulses to Alice: due to the unbalance $l = L - S$ between the two arms of the interferometer (greater then the coherence length l_c of the laser source), after the Bob's interferometer the state of the pulse is a linear superposition of two different states characterized by the followed path, as described above. In the first passage through the interferometer Bob does not impose an additional phase β with its modulator. The pulse propagates to Alice and the losses along the channel can be controlled to reach a mean number of *one photon per pulse* when the pulse bounces back at Alice's mirror. Alice can add with her modulator the relative phase α between the two quantum states and the pulse propagates to Bob's side after the reflection. So, the pulse enters in the Bob's interferometer for the second time and it is finally detected at the exit port. In the second passage through the interferometer Bob can add the phase β with his modulator.

With this configuration we have simplified the situation of Figure 5.5 but the results for the detection probabilities are the same. The photon in its travel from the laser source to the detector can follow four different paths: short-short (SS), long-long (LL), short-long (SL) or long-short (LS). This last two paths are quantum mechanically indistinguishable and so we find the same quantum interference phenomenon of the last section.

The detection probability at central time τ_{SL}^{LS} at the exit port with the detector depends on the phase difference $\alpha - \beta$ and it is proportional to

$$\sin^2 \frac{\alpha - \beta}{2} , \tag{5.37}$$

because it corresponds to the c_2 output port of Figure 5.5.

This setup can be used to implement BB84 QKD protocol ([3, 8] and section 1.2.2) based on single photon interference as we explain now. Alice chooses to apply one of four phase shifts $\alpha = 0, \pi/2, \pi, 3\pi/2$. She associates 0 and $\pi/2$ with bit 0, and $\pi/2$ and $3\pi/2$ with bit 1. On the contrary, Bob randomly applies a phase shift of either 0 or $\pi/2$. He associates to a detected pulse the bit 1 and to a transmitted but not detected pulse the bit 0.

After they have exchanged a big number of pulses, the two parties can determine a shared key. For each transmitted pulse, Bob tells his phase shift to Alice which calculates the phase difference $\alpha - \beta$ (modulo 2π) and tells to Bob to keep only the pulses with phase difference equal to 0 or π. In this way, she can predict the result of the detection on Bob' side and the bit encoding procedure ensure the same results, as shown in Table 5.1.

This QKD configuration is advantageous because the pulse passes through the same interferometer twice, simplifying the problems connected to alignment and stability. The latter must kept only for the flying time of the pulse

Alice's Bit	α	β	$\alpha - \beta$	Detection's probability	Bob's bit	To keep?
0	0	0	0	0	0	Yes
0	0	$\pi/2$	$3\pi/2$	1/2	?	No
1	π	0	π	1	1	Yes
1	π	$\pi/2$	$\pi/2$	1/2	?	No
0	$\pi/2$	0	$\pi/2$	1/2	?	No
0	$\pi/2$	$\pi/2$	0	0	0	Yes
1	$3\pi/2$	0	$3\pi/2$	1/2	?	No
1	$3\pi/2$	$\pi/2$	π	1	1	Yes

Table 5.1: Implementation of the BB84 protocol with phase encoding.

and this brings to the idea of a a satellite implementation of Two-Ways system, as we will describe in the following.

The Two-Ways configuration is an important milestone in fiber-based practical QKD. Most real systems for long-distance QKD uses the Plug&Play setup (or similar) [40, 23]. In particular, the first commercial QKD systems are based on it [41].

We will test the feasibility of the phase encoding technique with a optical setup similar to the Two-Ways one along a free-space quantum channel between a Low Earth Orbit satellite and a ground station in the last chapter.

5.3 PRELIMINARY TESTS AT LUXOR LABORATORY

We tested the Two-Ways setup at LUXOR Laboratory (CNR - IFN Padua) in the preliminary studies for the experimental satellite realization at Matera Laser Ranging Observatory (MLRO) of the Italian Space Agency (ASI) in Matera.

Due to the repetition rate of the laser beam used at MLRO ($\nu_F = 100$ MHz, corresponding to $T_F = 10$ ns) and to the single photon detector timing resolution (~ 1 ns), the temporal separation between the two pulses long $|L\rangle$ and short $|S\rangle$ must be approximately of 3 ns to distinguish the three-peaks in the counts histogram. So, the unbalance between the two arms of the interferometer must be of the order of one meter.

This strong unbalance implies that the beam propagating in the long arm must be reshaped for being well superimpose to the beam propagating in the short arm. To obtain such a good condition we have implemented in the long arm a *double* 4f*-system*, like that described in section 2.2 and shown in in Figure 5.7.

In this way, the propagation in both the arms of the interferometer is the same. Indeed, the first 4f-system reverses the image at the first beam splitter BS_1 on the first mirror M_1, then there is a propagation for a distance equal to the short arm and finally the image at the second mirror M_2 is reverted at the second beam splitter BS_2.

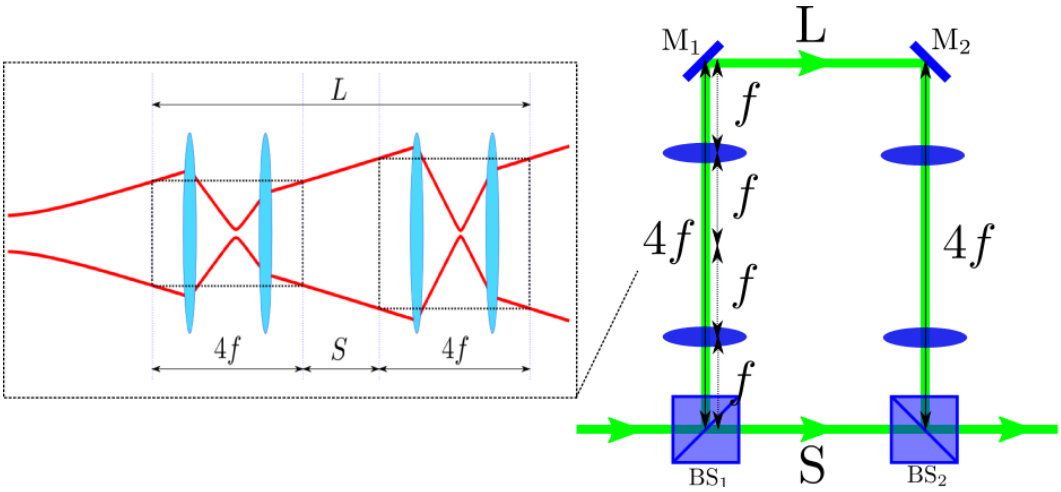


Figure 5.7: The implementation of the double 4f-system in the unbalanced Mach-Zender interferometer.

Experimentally, the interferometer is realized using two-inches Thorlabs® optical elements. The two beam splitters are 50 : 50 plate beam splitter model BSW16 and the model of the two mirrors is BB2-E02.

Regarding the four lenses, due to the unbalance of the order of one meter, their focal length must be about 125 mm. More precisely, each lens is a doublet (250 mm meniscus plus 250 mm plano-convex lens) of equivalent focal length 125 mm. We chose to use the doublet to correct the *spherical aberration*.

To avoid problems related to *defocus aberration* the two mirrors of the interferometer were mounted on a micrometer sled to adjust the nominal unbalance to the practical one. To guarantee the stability and the alignment of the interferometer the two beam splitters and the four lenses were mounted rigidly.

The laser source used at LUXOR Laboratory was a pulsed laser ($\lambda = 532$ nm, $\nu_F = 17$ kHz) with a coherence length less than one meter to avoid single pass interference.

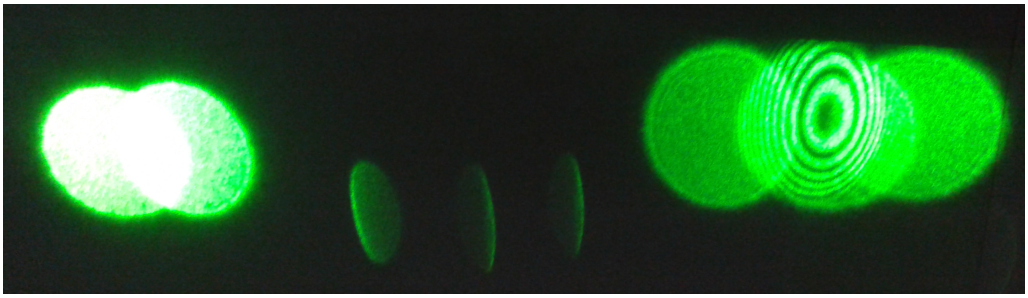


Figure 5.8: Interference fringes obtained in the preliminary test at Luxor Laboratory.

At one port of the interferometer we placed a sending back mirror to realize the Two-Ways configuration shown in Figure 5.6. In this way, at the exit port corresponding to the first beam splitter BS_1 we obtained the interference fringes shown in Figure 5.8 on the right. More precisely, on the left we can see the two beam spots corresponding to the unused port of the interferometer in

the single pass: they are deliberately not well superimposed. However, on the right the interference fringes due to the interfering path are self-evident. The fringes are very narrow and circular and this fact indicates that the optical system is not well aligned, as it is clear by looking at the two spots on the left. The spots at the center of the image are due to the retro-reflections of the lenses and they do not matter.

Once optimized the interferometer, we collected the intensity of the interfering spot with a fast photo-diode. This let us to visualize, using an oscilloscope, the expected image of the three-peaks. If the phase introduced in the interferometer is null, we will expect destructive interference. Indeed, in Figure 5.9 on the left you can see only two peaks, corresponding to the non-interfering paths SS and LL, while the interfering peak is well extinct. Then, we introduced a phase shift in the interferometer and we collected an image for the constructive interference, as you can see in Figure 5.9 on the right.

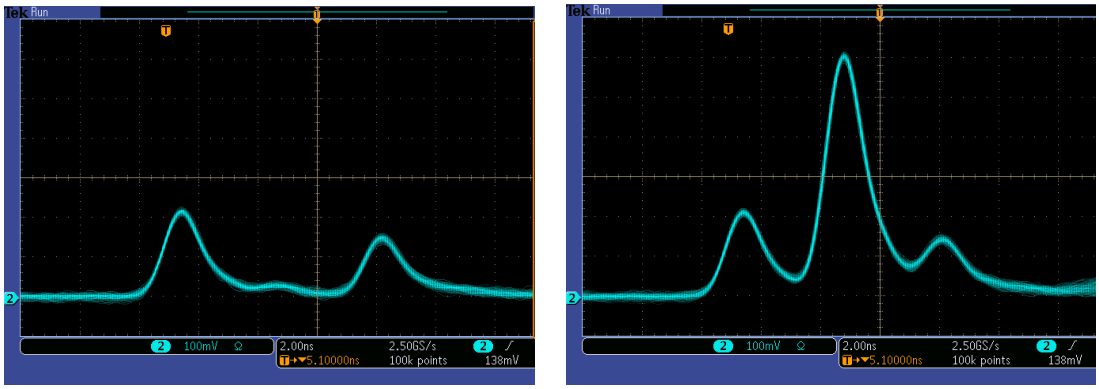


Figure 5.9: Image of destructive (on the left) and constructive (on the right) interference obtained with a fast photo-diode at Luxor Laboratory.

5.4 TIME-BIN EXPERIMENT IN SPACE: THE IDEA

As we have shown in chapter 4, experimental feasibility tests for Space Quantum Communication have been realized by exploiting corner cube retroreflectors of satellites used for geodynamical studies. The idea of a time-bin feasibility test in Space is very simple: corner cube retroreflectors can play the role of the sending-back mirror of the Two-Ways setup of Figure 5.6. As shown in Figure 5.10, the satellite plays the role of Alice and the ground station where there is the interferometer is Bob.

A great difference compared to the standard Two-Ways setup, as well the use of a satellite at thousands of kilometers from the interferometer, is given by the fact that the satellite moves. Thus, the sending-back mirror it is not fixed, but it moves and its motion implies that the satellite introduces a phase shift φ between the two quantum states $|S\rangle$ and $|L\rangle$. As we have shown above, the losses in the quantum channel guarantee that the mean photon number

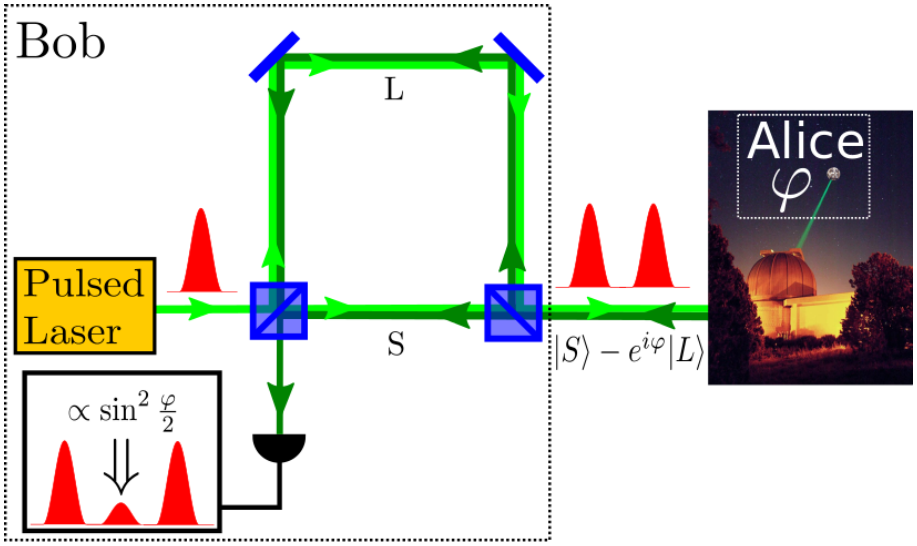


Figure 5.10: The idea of time-bin experiment using moving satellites.

per retroreflected pulse is close to one. So, the phase shift φ rules the detection probability that, at the exit port represented in the figure, is proportional to

$$\sin^2 \frac{\varphi}{2} \tag{5.38}$$

according to what we described in section 5.2.

Figure 5.1 at the beginning of this chapter shows this variable interference effect due to the satellite motion. This quantum interference modulation is what we have measured in the experimental realization that we will describe in the following chapter. We have to note that with such implementation we have performed an interferometry experiment with orbiting terminals at satellite distances at single photon level. By modulating and controlling the phase shift introduced by the satellite one can obtain a specified level of interference and thus realize a complete quantum communication.

One of the main advantages of this architecture is the fact that the pulse passes twice in the same interferometer simplifying the problems connected to its stability which must be preserved only for a round trip time, i.e., few tens of milliseconds for Low Earth Orbit satellite or at most for 200 milliseconds for Medium Earth Orbit. This fact simplifies the implementation and makes this satellite quantum communication setup competitive respect to the others (for example, it is not necessary that Alice and Bob share the choice of the horizontal-vertical axes as in polarization encoding). Furthermore, it is not necessary to use satellite with polarization preserving corner cube retroreflectors and so the number of usable orbiting terminals is bigger.

The phase shift introduced by the satellite motion is due to the optical path difference d existing between the propagation of the short $|S\rangle$ and the long $|L\rangle$ pulse, according to

$$\varphi = kd = \frac{2\pi}{\lambda} d \,, \tag{5.39}$$

where k is the wavenumber of the pulse, related to its wavelength λ.

The two pulses emerging from the interferometer have a temporal separation Δt determined by the unbalance l between the two arms

$$\Delta t = \frac{l}{c} , \tag{5.40}$$

where c is the speed of light. As it is shown in Figure 5.11, between the instant $t = 0$ at which the short pulse S is reflected by the satellite and the instant $t = \tau$ at which the long one L is reflected, the satellite has moved at radial velocity v_s that can be assumed constant for a distance

$$\Delta r = v_s \tau . \tag{5.41}$$

The optical path difference d is so twice the distance Δr

$$d = 2\Delta r . \tag{5.42}$$

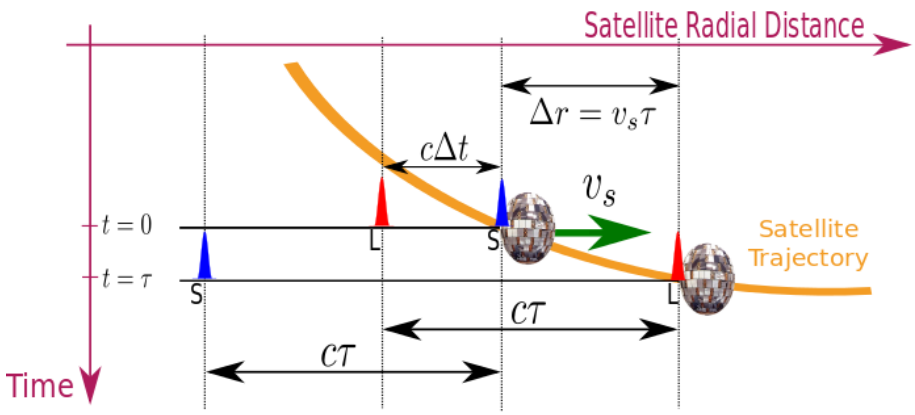


Figure 5.11: The phase shift introduced by the satellite motion.

We have to estimate Δr. From the figure, it is clear that

$$c\tau = c\Delta t + v_s \tau \tag{5.43}$$

and so

$$\tau = \frac{c\Delta t}{c - v_s} = \frac{\Delta t}{1 - \frac{v_s}{c}} \approx \Delta t \left(1 + \frac{v_s}{c}\right) \approx \Delta t . \tag{5.44}$$

Due to the fact that the two pulse propagate at the speed of light, it results that the instant τ can be approximated with the temporal unbalance Δt between the two arms of the interferometer.

Finally, we have

$$\Delta r = v_s \Delta t \tag{5.45}$$

and so the phase shift introduced by the intrinsic motion of the satellite is given by

$$\varphi = \frac{2\pi}{\lambda} d = \frac{2\pi}{\lambda} (2\Delta r) = \frac{4\pi}{\lambda} \nu_s \Delta t \ . \tag{5.46}$$

We will use the last equation in the following chapter to analyze the data collected in the experimental realization at MLRO and to test the feasibility of the time-bin encoding technique along a space quantum channel.

6

SPACE TIME-BIN FEASIBILITY TEST AT MLRO

In this chapter we describe the realization of the space time-bin experiment presented in the last section. As in the case of the experimental quantum communication with polarization encoding, it has been performed at MLRO Observatory in Matera and the quantum channel is a link between a LEO satellite and the optical ground station.

Firstly, we will describe in details the optical and the electronic setup. Then we will measure the coherence time of the laser used and the synchronization between the MLRO system and the setup for Quantum Communication. Finally, we will present the data analysis and the results which have demonstrated the feasibility of the phase encoding along a space quantum channel.

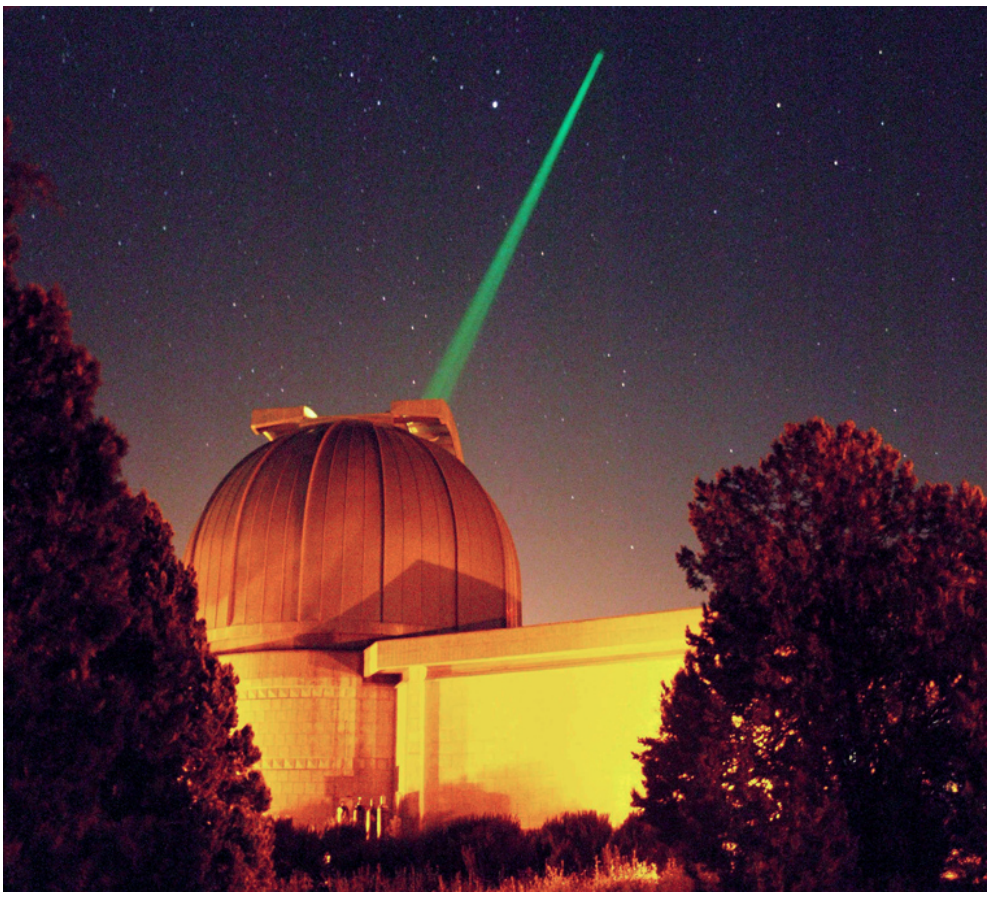


Figure 6.1: The Matera Laser Ranging Observatory (MLRO).

6.1 GENERATION OF THE LASER BEAMS

The experiments involving Quantum Communication realized at MLRO are based on the setup used for Laser Ranging activities. The weak pulse train used for quantum experiments (*qubit pulses*) is obtained from the same master oscillator that produces the Satellite Laser Ranging pulses (*SLR pulses*). In this way the two photon streams are locked together and well synchronized with the atomic clock of MLRO. The setup used for the beams production realized in the optical transmission table (*TX Table*) is represented in Figure 6.2.

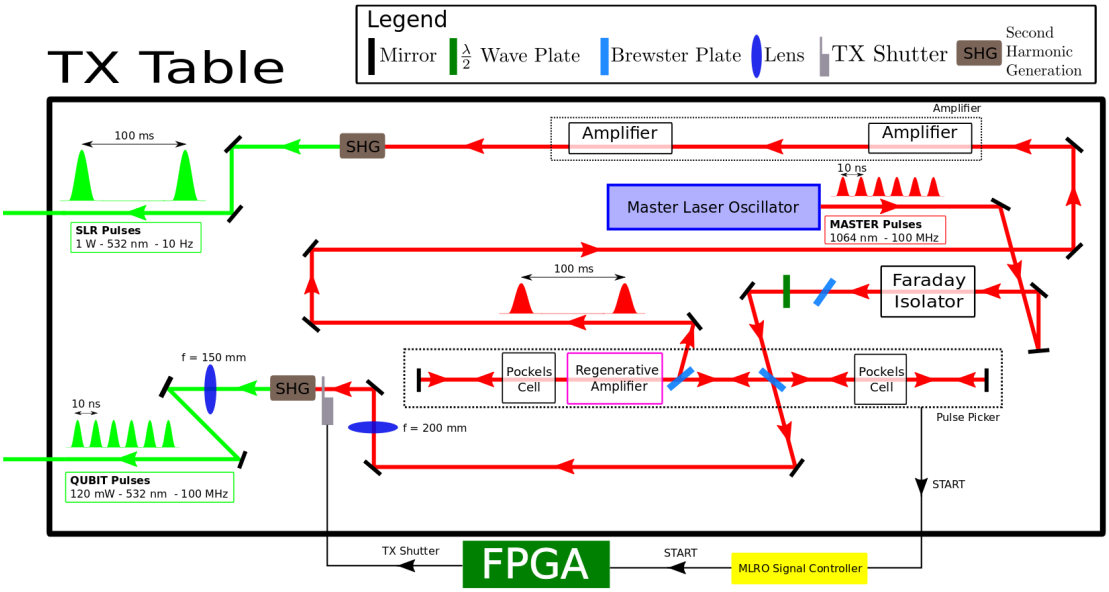


Figure 6.2: The transmission optical table (TX Table) for the production of SLR and qubit laser pulses.

A mode-locking master oscillator like that described in section 2.4.2 (in blue in the figure) generates a pulse train characterized by $\lambda = 1064$ nm, repetition rate $\nu_F = 100$ MHz ($T_F = 10$ ns). This beam enters in a Faraday isolator, a device that allows the transmission of light in only one direction, used to avoid unwanted retroreflections. Then, it passes through a Brewster plate and a half-wave plate. Brewster plates are often inserted into laser setup with the purpose of introducing polarization-dependent losses. This can force the laser to emit light with a stable linear polarization, the direction of which corresponds to p polarization at the Brewster plate. Furthermore, the half-wave plate can rotate the polarization direction of a linearly polarized wave. The combination of these two devices aims to control the polarization of the beam and ultimately the optical power of the two beams generated in this optical table.

After the half-wave plate the beam passes through another Brewster plate. The transmitted beam impinges on some mirrors and it is focused by a lens in a SHG crystal (see section 2.5) to produce the qubit pulses ($\lambda = 532$ nm, mean optical power ≈ 120 mW) that have the same repetition rate of the master pulses.

On the contrary, the beam reflected by the Brewster plate enters a pulse-picker made up of two Pockels cells and a regenerative amplifier. A Pockels cell is an electro-optical device based on the Pockels' effect, i.e., the capacity of some crystals under voltage to transform linearly polarized light in circularly polarized. Regenerative amplification is a process used to generate short but strong pulses of laser light. It is based on a pulse trapped in a laser resonator, which stays in there until it extracts all of the energy stored in the amplification medium. The regenerative amplifier selects as seed one pulse of the master oscillator every 10^7 and it is trapped and amplified. In this way, the pulse-picker produces a train of pulses amplified and with repetition rate equal to 10 Hz (and time separation equal to 100 ms). Each pulse is synchronized with the atomic clock, is amplified by two single-pass amplifiers followed by a SHG crystal that produces the SLR pulses ($\lambda = 532$ nm, mean optical power ≈ 1 W) at the repetition rate of 10 Hz.

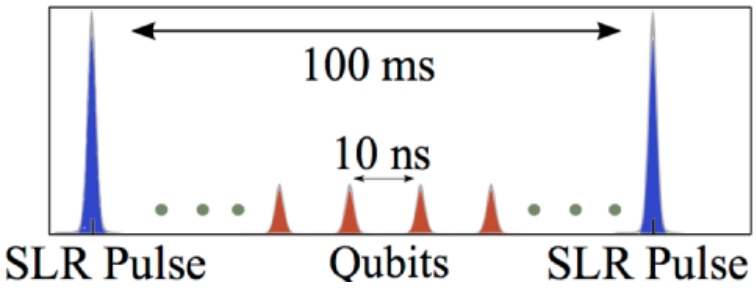


Figure 6.3: The synchronization between the SLR pulses and the qubit pulses.

Summarizing, the TX Table produces the qubit and the SLR pulse train that are well synchronized as shown in Figure 6.3. Between two SLR pulses separated by 100 ms there are 10^7 qubit pulses separated by 10 ns. The instant at which each SLR pulse is generated is known with picoseconds accuracy and controlled by the MLRO system.

The use of the FPGA and of the shutter shown in the figure will be described in the following.

6.2 MEASUREMENT OF THE COHERENCE TIME OF THE QUBIT PULSES

The coherence time of the light source plays a fundamental role in our experiment. For this reason we have experimentally measured the coherence time of the qubit pulses. We realized a Michelson interferometer like that described in section 3.3 and collected the intensity of the light with a *power-meter* for many values of the path difference to obtain the interferogram shown in Figure 6.4.

The fitting of the interferogram envelope gives a temporal coherence function that is Gaussian, with a FWHM equal to 54.9 ± 0.7 ps. From the FWHM we can estimate the coherence time that depends on the pulse lineshape function [42]. The qubit pulses have Gaussian lineashape function and so the

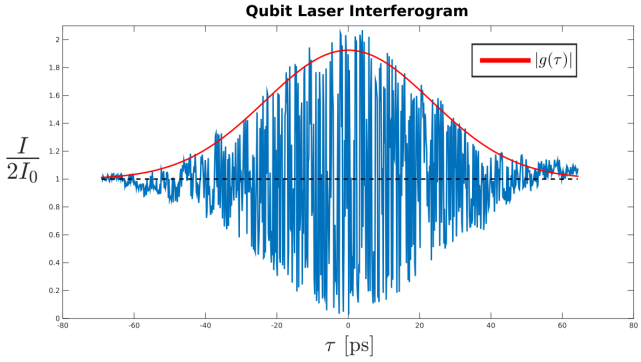


Figure 6.4: Interferogram for measurement of the coherence time of the qubit pulses.

coherence time results $\tau_c = \sqrt{2}FWHM = 78 \pm 1$ ps, and the coherence length is about 3 cm.

The unbalance used in the Mach-Zender interferometer in our experiment is about one meter and so it is well enough to avoid single pass interference. It is clear that a smaller unbalance would be sufficient, but, as we pointed out in section 5.3, the unbalance is fixed by the timing resolution of the single photon detectors and by the timing window (10 ns) imposed by the repetition rate of the qubit laser.

6.3 THE EXPERIMENTAL SETUP

In this section we will describe both the optical and electronic setup, as well as the data acquisition system and the synchronization between MLRO and the "quantum" system.

The unbalanced Mach-Zender interferometer is the fundamental part of the optical receiving table (*RX Table*) that is represented in Figure 6.5.

The two beams emerging from the TX Table of Figure 6.2 enter the RX Table. The SLR beam passes through a collimation system that controls its divergence, two beam splitters and then it is directed to the telescope through the Coudè path (see Figure 6.6). The MLRO telescope is a 1.5 m Nasmyth-Cassegrain telescope (mirrors M_1 to M_3) and it is connected to the RX Table by the Coudè path (mirrors M_4 to M_7). The qubit stream is focused by a 500 mm lens, than it passes through the interferometer, another 500 mm lens an a divergence control module consisting of other two lenses.

The two beams are superimposed at the coupling beam splitter: in this way they propagate together in the Coudè path and are directed to the satellite in the same way. The returning two beams are collected by the telescope, then they arrive at the coupling beam splitter through the Coudè path and they are finally detected by the photomultipliers (PMT) of the two different detection systems.

The MLRO detection system consists of a photomultiplier ad a signal controller. The detection system for qubit laser consist of a focusing lens,

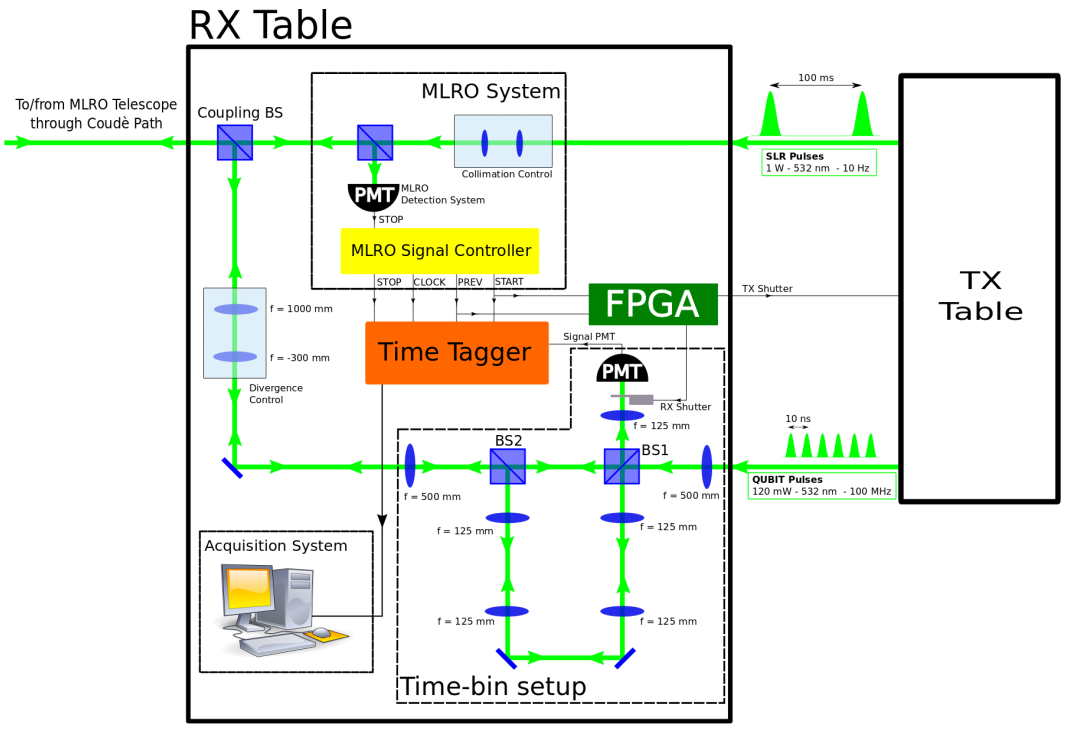


Figure 6.5: The receiving optical table (RX Table) with the optical setup and the detection system.

a mechanical shutter that we will describe in the following and a single photon photomultiplier Hamamatsu H7360-02 (dark counts < 50 cps, detection efficiency $\eta_{det} \sim 10\%$, 22 mm diameter, detection accuracy equal to the timing jitter $\sigma = 0.5$ ns).

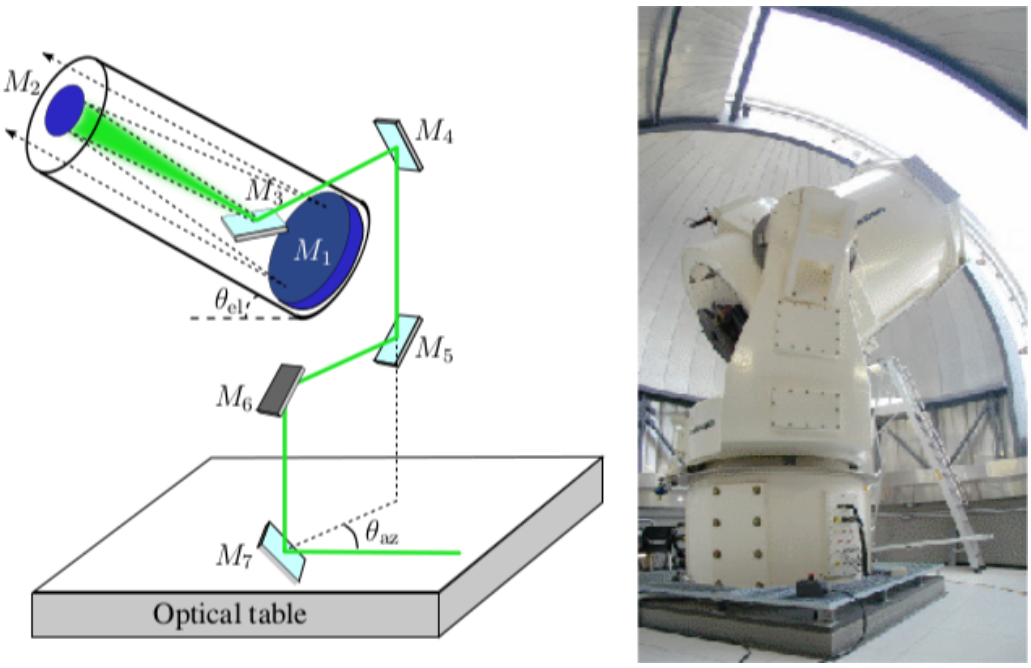


Figure 6.6: The Coudè path and the MLRO telescope.

So far we have described the optical setup and we can now move to the electronic one. Four of the electronic signals controlled by MLRO are important for our purposes. The clock signal (*Clock*) is given by the atomic clock and it is necessary to synchronize and correlate temporally all the other signals. The signal of the trajectory previsions (*Prev*) it is necessary to let the telescope to track the satellites during their passages. The *Start* and *Stop* signals represent the starting time and the arriving time of a SLR pulse respectively and they are characterized by a temporal resolution of few picoseconds. The Start signal is generated by the pulse picker of Figure 6.2 at the moment in which the SLR pulse is extracted, while the Stop signal is produced by a detection event in the MLRO photomultiplier. The time difference between a Start signal and the following Stop signal gives the satellite round trip time, from which we can reconstruct the distance and definitely the satellite trajectory with a sub-centimeter resolution.

The synchronization between the SLR and the qubit pulses is achieved as described above: between two SLR pulses there are 10^7 qubit pulses. In this way, by dividing the interval between two consecutive SLR detections in 10^7 equidistant subintervals, we determine the arriving time of the qubits t_{ref} and we can compare it with the measured one t_{meas}. This technique automatically compensates for the variation of the round trip time duration due to the satellite motion and air refraction.

In both the TX Table and in the RX Table there is a mechanical shutter that we will call *TX Shutter* and *RX Shutter* respectively. Their use is fundamental to curb the problem of *fluorescence*: it is emitted by the beam splitter BS1 irradiated by the outgoing beam. The two shutters implement a separation between the transmission phase and the receiving one as shown in Figure 6.7. In the first half of the 100 ms slot between two SLR pulses, the transmitter

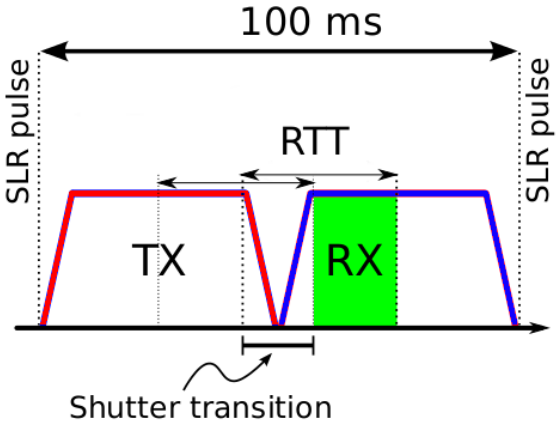


Figure 6.7: Shutter transition.

shutter is opened while the receiver one is closed, to protect the receiver PMT. In the second half of the slot, the shutter controls are reversed and the detector receives the qubits from the satellites. In this way, the effective transmission

time during a slot cannot be larger than the round trip time. The shutter transition must be controlled real time during the satellite passage. To perform this operation a Field Programmable Gate Array device (*FPGA*) is used. A FPGA is a integrated circuit which functionalities can be programmed via software. The FPGA has as input signals Start and Prev and it use them to control the TX Shutter and the RX Shutter respectively.

The electronic setup is completed by a Time Tagger (quTAU: Time-to-Digital Converter for Time-correlated Photon Counting) with 81 ps resolution. It records the four signals of the MLRO system (Start, Stop, Clock and Prev) and the temporal signals due to the single photon detections.

In Figure 6.8 it is shown a typical acquisition screen: the time taggers for each channel are saved by the acquisition system controlled by a PC. The time tagger data are files with two columns: the first one represents the channel recorded and the second the time-tag in a numerical format that can be converted in time by using the Clock signal.

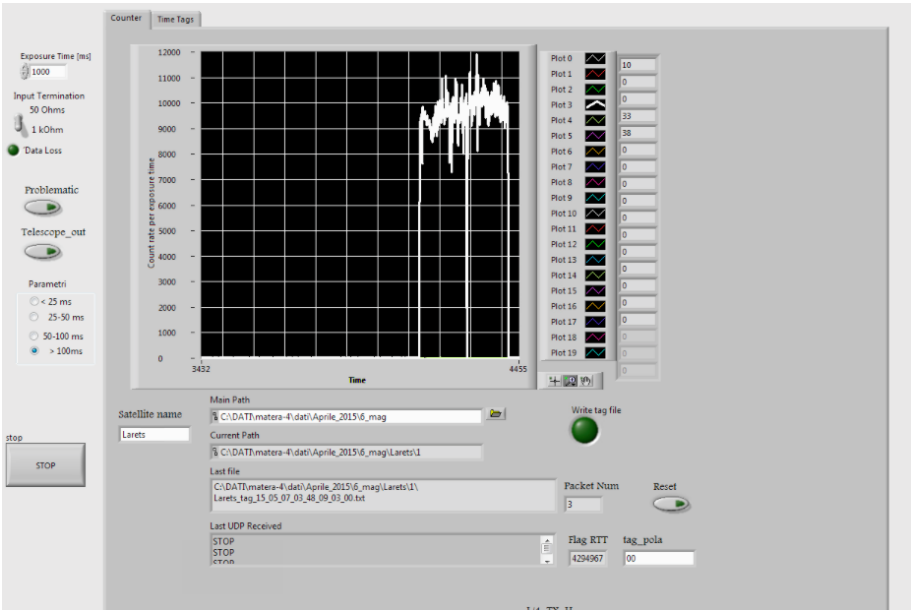


Figure 6.8: A typical screen of the Time-Tagger acquisition system.

6.4 PRELIMINARY OPERATIONS AND DATA ACQUISITION

Due to the insufficient background rejection in the daylight, the data acquisition is realized only during the nigh. Before each acquisition session it is necessary to perform some preliminary operations to control the correct alignment of the system.

We will describe here only the two main operations. The first is the control of the fringe interference pattern obtained at the optical table using a sending-back mirror as in the preliminary test performed at LUXOR Laboratory (see section 5.3). The expected interference effect depends on the exit port of the

beam splitter BS1. The setting up of the interferometer is achieved looking at the spot with the interference fringes, called *interferogram* (but it is not the interferogram used to measure the coherence time of a light source).

Typically, one obtains spot figures like that represented in Figure 6.9. Without explaining the details of interferometry techniques, typically a spot

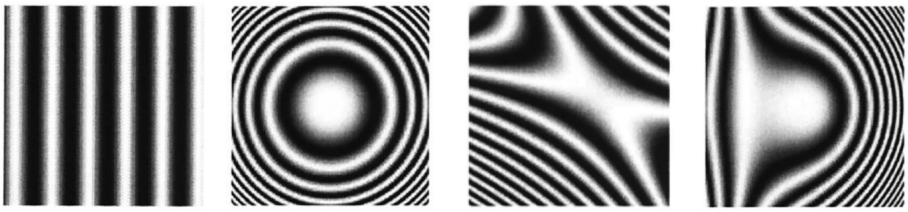


Figure 6.9: Typical fringe patterns obtained in an interferometry experiment.

with parallel fringes indicates that the wave vectors of the two interfering beam are not parallel (Figure 6.9 a), while a spot with concentric fringes arises when the two beams have a different curvature (Figure 6.9 b). There are many other cases and possible interferograms related to the different optical aberrations that can exist in the optical system (for example, astigmatism, spherical aberration, defocus, coma . . .).

The alignment procedure consist in the optimization of the interferogram: it must show a only wide fringe that fills all the spot as you can see in Figure 6.10. Furthermore, this control is performed with the sending-back mirror at two different positions in the optical table to verify that the interference effect holds independently of the distance between the mirror and the interferometer and of the focusing conditions.

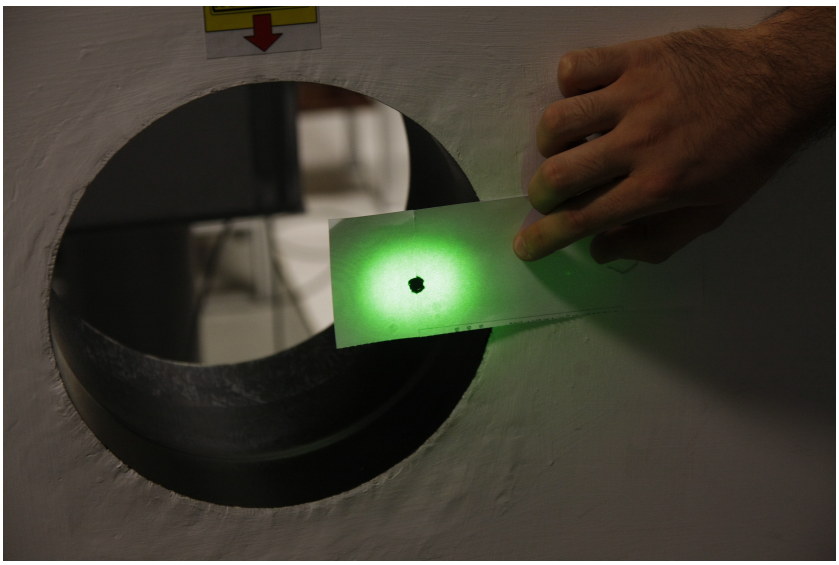


Figure 6.10: Control of aberrations of the interference pattern at MLRO.

The second operation is the control of the double 4f-system observing the light coming from a star. It that can be considered as a plane wave: if the

optical system is correct, the images of the telescope pupil lighted by the star obtained with only one of the two arms of the interferometer open would be equal. Indeed, the light propagation in the two arms would be equivalent for what we have described in 5.3. The two images collected with the star Vega are shown in Figure 6.11: the pupil image on the left refers to the short arm, while the pupil image on the right refers to the long one. As you can see, the two images are well-defined and of the same size and so the double 4f-system is well realized.

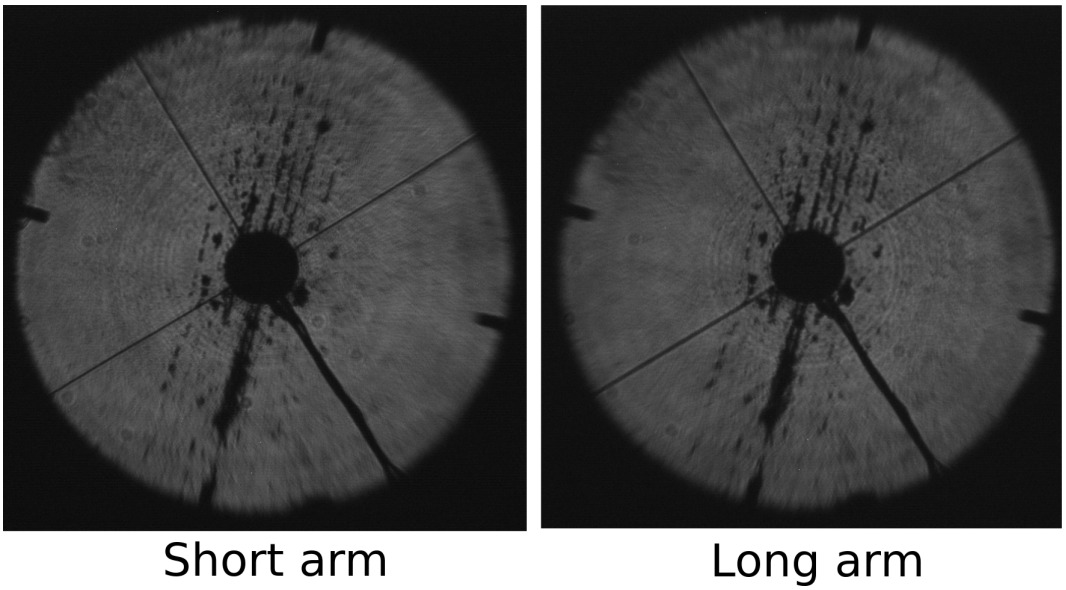


Figure 6.11: Images of the telescope pupil collected pointing to Vega: on the left there is the image of the short arm of the interferometer, on the right the image of the long one.

After the alignment of the system, the data acquisition starts in the following way. After the choice of the interesting satellite (a LEO satellite for this experiment) MLRO technical operators track it and collect their data. At the same time, the qubit laser is sent to the satellite and the single photon returns are recorded. Each satellite passage goes on for ten minutes on average and the quality of the passage depends on the climate conditions and on the overlap between the two beams. For these reasons there can be good and bad acquisition intervals also in the same passage.

Data acquisition is performed during all night and typically ten passages are collected. Each passage is then analyzed off-line as we will describe in the following section.

6.5 DATA ANALYSIS

We will describe in this section the analysis of the data collected in July 2015 at MLRO Observatory in Matera. We will show the analysis steps to perform for pointing out the expected interference effect described in section 5.4. The data analysis, splitted in three parts, is realized with the software MATLAB®.

6.5.1 *Satellite trajectory and qubits return frequencies*

The first three graphs that are realized are presented Figure 6.12. In particular, it is shown the passage of Beacon-C satellite at 23.38 CEST on 10th July 2015.

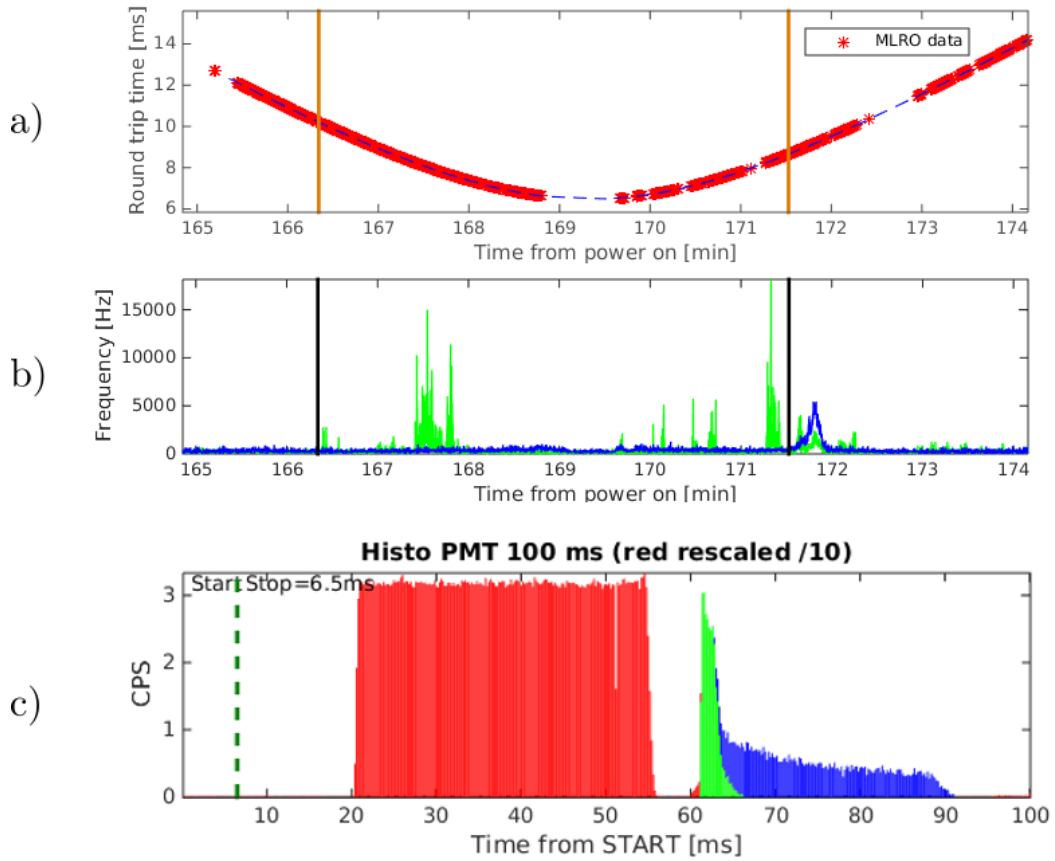


Figure 6.12: A typical screen of the data acquired for a LEO satellite (Beacon-C, 10.07.2015, h. 23.38 CEST). Image *a)* represents the satellite round trip time as a function of the acquisition time; image *b)* gives the return frequencies of the single photon detector; image *c)* shows the experimental shutter transition.

In the *a)* graph it is represented the satellite round trip time (rtt) as a function of the acquisition time (from the switching on of the time tagger). Each red point is a measured rtt given by the time difference between a MLRO Start signal and the consecutive Stop (MLRO data). By fitting the rtt points with a polynomial function we get the satellite trajectory as a function of the time, because its radial distance R is proportional to the rtt according to

$$R = c\frac{rtt}{2}\,, \tag{6.1}$$

where c is the speed of light. Trajectory reconstruction is the preliminary step we must perform to continue the analysis with the following step.

In the *b)* image it is represented the single photon detection frequency as a function of the time. There are two lines: the green one are the good single

photon detections and the blue one represents the background. Indeed, the goodness of a single photon return is determined by the shutter transition: as we have already said in section 6.3 and shown in Figure 6.7, there is only a narrow temporal window in which the detection signals are good due to the mechanical transition of the shutter which experimental behavior is shown in image *c)*. As you can see, in the 100 ms between two Start signals there is a first zone (in red) in which the detector collects only fluorescence photons, then there is the good zone (in green) and then there is a background zone (in blue) in which the detector collects photons that we have not sent. This frequency histogram is realized by averaging all the good Start-Stop data recorded in the temporal window selected by the two vertical brown lines shown in the *a)* graph.

6.5.2 *Experimental phase shift and unbalance estimation*

As we have explained in section 5.4, the satellite introduces a phase shift φ in the interferometer given by (5.46):

$$\varphi = \frac{4\pi}{\lambda} v_s \Delta t \ . \tag{6.2}$$

It depends on the wavelength of the pulse λ, on the satellite radial velocity v_s and on the temporal unbalance Δt of the interferometer.

We have to estimate experimentally this phase shift for analyzing the qubits returns by selecting which satisfy strictly conditions on their phase shift to point out the interference effect.

To achieve this goal, it is useful to describe the interference between the two quantum indistinguishable paths LS and SL of the Two-Ways configuration in the following way. We consider the two paths as two waves of same intensity I_0 that interfere according to the interference equation (3.15):

$$\begin{aligned} I &= I_{LS} + I_{SL} + 2\sqrt{I_{LS} I_{SL}}\, \mathcal{V} \cos(\pi + \phi) \\ &= 2I_0 \left(1 - \mathcal{V} \cos\varphi\right) \end{aligned} \tag{6.3}$$

where we use the fact that the two beam splitters introduce for each reflection a $\pi/2$ phase shift as described in section 3.7 and the definition of visibility $\mathcal{V}$ given in (3.18). If the visibility would be unitary, the intensity of the interfering peak (the central in the expected three peaks figure) should be modulated by the term

$$1 - \cos\varphi = 2\sin^2\frac{\varphi}{2} \propto \sin^2\frac{\varphi}{2} \tag{6.4}$$

as we have said in (5.38). Equation (6.3) is analogue to equation (5.34) that rules the detection probability for this quantum interference effect.

In Figure 6.13 it is shown another passage of Beacon-C satellite (12.07.2015, h. 00.56 CEST). The two graphs on the upper left and the one in the upper

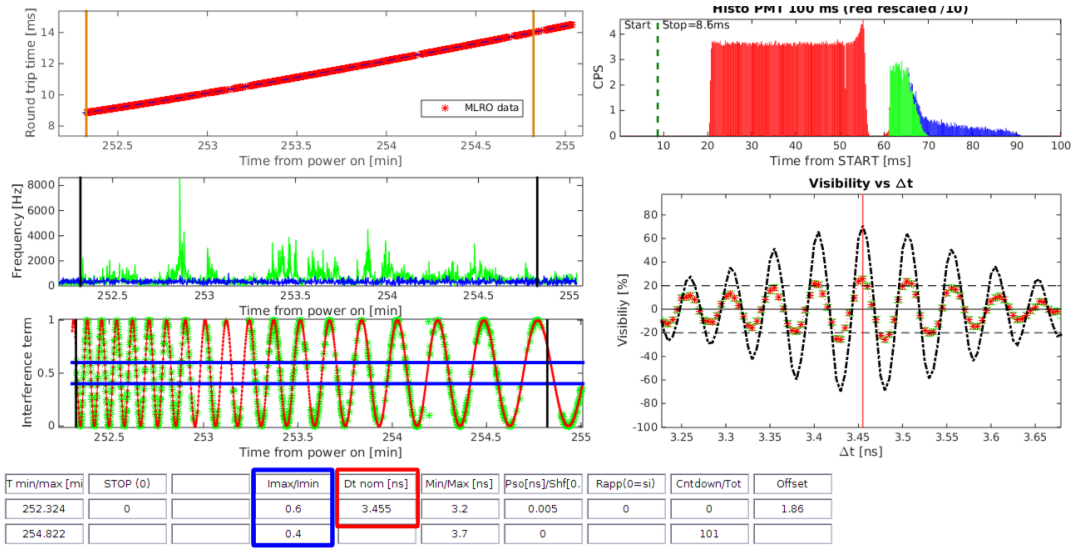


Figure 6.13: A screen of the data analysis used to estimate the correct value for the unbalance Δt (Beacon-C satellite, 12.07.2015, h 00.56 CEST).

right are the images constructed in the first step of the analysis as described above and shown in Figure 6.12.

Due to channel losses the qubit beam is attenuated at single photon level and so for each sent pulse we expect one detection event at most. For each detected photon we can estimate the time difference between the arriving measured time t_{meas} and the expected one t_{ref} as described in 6.3. By representing the histogram of the qubits returns as a function of the time difference $t_{meas} - t_{ref}$ (modulo 10 ns due to the repetition rate) we expect that the distribution presents the three peaks figure. Each peak is centered at one of the three expected time of arrival, corresponding to the short-short path (SS), the interfering short-long (SL) plus long-short (LS) one and the long-long one (LL).

Indeed, taking all the good data of the passage we obtain a histogram like that shown in Figure 6.14. As you can see, the three peaks figure is clear: the histogram has three well defined Gaussian peaks. Their standard deviation is determined by the detector jitter ($\sigma = 0.5$ ns). The two lateral peaks have the same height while the central one is higher. Indeed, the two peaks of the same size represent the photons that take the SS or the LL path and have the same intensity I_0. With the word *intensity*, we will indicate the counts below the Gaussian and we assign to its value a Poisson error. The central peak, on the contrary, gives the number of photons that take the interfering path. The two interfering paths would have the same intensity I_0, but, due to their quantum indistinguishability, they should interfere according to (6.3). However, as you can see, the central peak is equal to the sum of the two lateral peaks (within few percent).

This fact indicates that, taking all the data, we are averaging the interference effect canceling it. Indeed, we have represented in this histogram all the

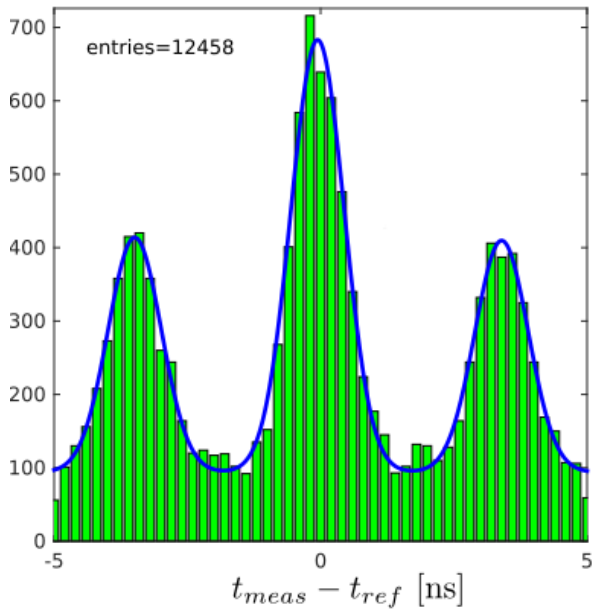


Figure 6.14: Histogram of the qubits return without any data selection.

returns taken along the trajectory, but the phase shift (and so the expected interference) introduced by the satellite varies many times along a single passage and we need to select the qubits depending on their phase to point out the expected effect.

Now, we will see how to estimate experimentally the phase shift introduced by the satellite (6.2). The satellite radial velocity is assumed to be constant for time of the order of 100 ms. We estimate the satellite velocity using the fit of the round trip time rtt (dashed blue line in the first graph of Figure 6.13) that gives the satellite distance R according to (6.1). The ratio of the difference between two consecutive distances $R_\pm$ and the difference between two consecutive Start signal $T_\pm$ gives the experimental velocity of the satellite along the trajectory

$$v_s = \frac{R_+ - R_-}{T_+ - T_-} = \frac{c}{2}\frac{rtt_+ - rtt_-}{T_+ - T_-} = \frac{c}{2}\frac{\Delta rtt}{\Delta T} \ . \tag{6.5}$$

In our analysis, we fix the wavelength of the pulse to $\lambda = 532$ nm, while the unbalance Δt of the interferometer is used as a free parameter and it is determined by maximizing the expected interference effect.

The second step of the data analysis starts with the construction of the curve that described the interference term expected. We choose a value for the unbalance Δt, for example $\Delta t = 3.455$ ns as shown in the red box in Figure 6.13. Given a value for Δt, we calculate the phase shift φ along the all trajectory and the expected interference term is given by $\sin^2(\varphi/2)$, as you can see in the lower left graph in Figure 6.13. The expected interference term is given by the red line, while the green point correspond to the MLRO data points.

Given this curve as a function of the time we can assign to each qubit return its phase shift. Depending on this, we select only the returns characterized by a phase shift that leads to constructive or destructive interference. More precisely, we select the qubits for which the phase φ is in the two bands:

$$0 \leqslant \sin^2 \frac{\varphi}{2} \leqslant 0.4 \quad \Rightarrow \quad \text{destructive interference} , \tag{6.6}$$

or

$$0.6 \leqslant \sin^2 \frac{\varphi}{2} \leqslant 1 \quad \Rightarrow \quad \text{constructive interference} , \tag{6.7}$$

as set in the blue box in Figure 6.13.

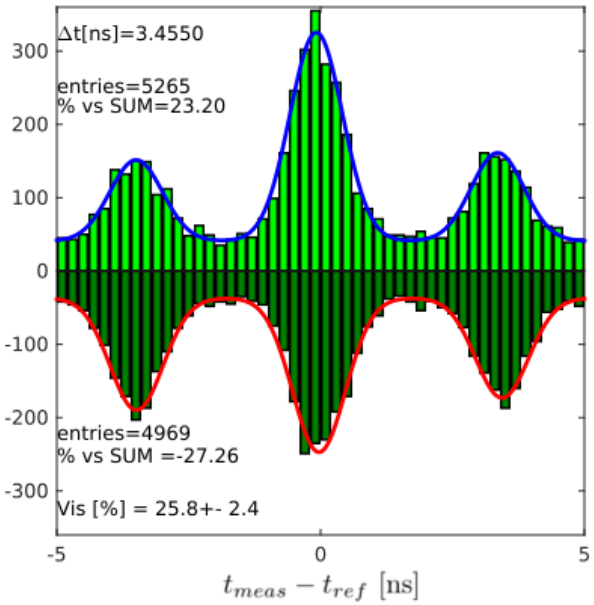


Figure 6.15: The histogram of the constructive and destructive interference used to calculate the visibility for a given value of the unbalance Δt.

After the qubits selection, we realize the two histograms of Figure 6.15: the upper one represents the qubits that should give constructive interference, while the lower one the qubits that should give destructive interference according to the expected interference term.

Now, differently from the histogram of Figure 6.14, the central peak is not the sum of the two lateral peaks. When we expect constructive interference it is more than 20% bigger than the sum, while in the case of destructive interference is more then 20% smaller than the sum

With these two histograms, we can estimate the visibility obtained. Indeed, the intensity of the central peak can be rewritten as a function of the percentage p by which it is different from the sum ($2I_0$) of the two other peaks (that is also the sum of the intensities of two interfering peaks) according to

$$I = 2I_0 \left(1 + \frac{p}{100}\right) . \tag{6.8}$$

From the two histograms we obtain the maximum and the minimum intensity and by using (3.17)

$$\mathcal{V} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{6.9}$$

we calculate the visibility $\mathcal{V}$ in terms of the the constructive interference percentage p_c and of the destructive interference percentage p_d:

$$\mathcal{V}^{exp} = \frac{p_c - p_d}{200 + p_c + p_d} \, . \tag{6.10}$$

In this way we obtain the value $\mathcal{V}^{exp} = 25.8 \pm 2.4$ represented as Vis in Figure 6.15.

So far, we have described the estimation of the visibility for a single value of the unbalance Δt. In fact, we use Δt as a free parameter because its value depends on the alignment conditions determined by the entry direction of the returning beam. We repeat all the procedure to construct the two histograms for many values of Δt separated by 5 ps (around the expected value about 3.40 ns due to the one meter unbalance).

The result of this analysis is the last graph of Figure 6.13. Red points are the experimental values of the visibility given as a function of the parameter Δt used for the data analysis. As you can see, the trend is similar to that of a beat: the visibility oscillates and has a maximum value. We take the Δt value corresponding to this maximum value for the visibility as the correct value (within few picoseconds) of the unbalance Δt. For the passage presented above, the maximum of the visibility is achieved with the value for Δt used above to present the different graphs ($\Delta t_{estimated} = 3.455$ ns).

Superimposed to the experimental red points, you can see the theoretical curve obtained by calculating the expected interference according to the phase shift of the detected qubits. The experimental visibility is clearly smaller than the theoretical one, but the oscillating trend is good.

All this analysis is performed for different passages and, for each passage, on narrower temporal intervals to check the consistency of the estimated Δt value. For example, in Figure 6.16 you can see four different temporal windows for the passage used above. The unbalance value estimated in all the four intervals is the same and we will use this value in the next step of the analysis.

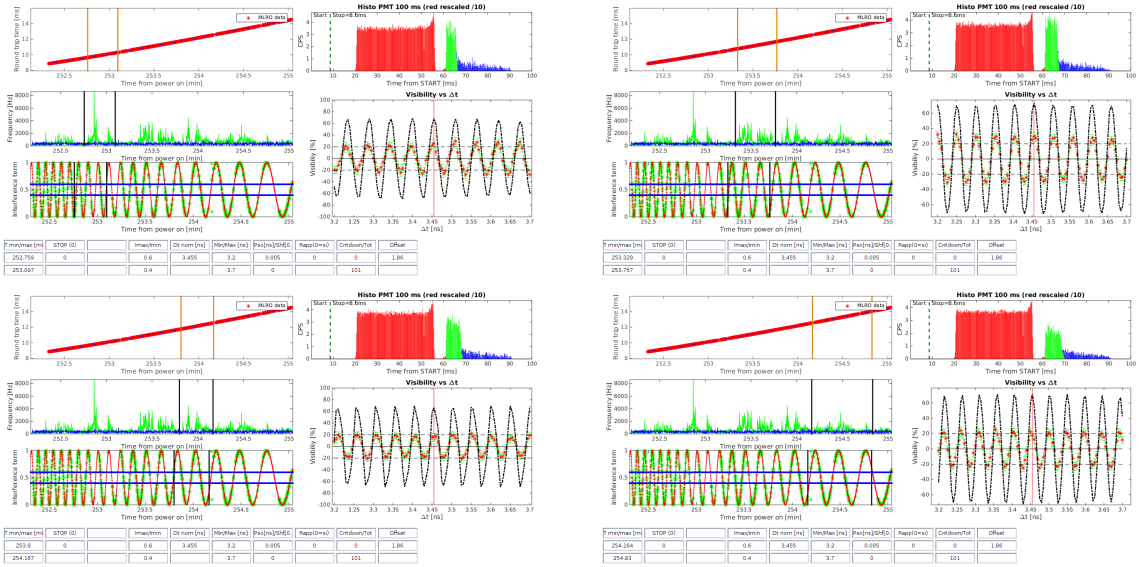


Figure 6.16: Consistency check for the estimated value of the unbalance Δt.

6.5.3 *Experimental verification of the interference effect*

We will show now how the value for the unbalance estimated in the second step of the analysis allows to point out the interference effect expected.

As we showed above, the intensity of the central peak I of the return qubits histogram is a function of the phase shift φ introduced by the satellite. It is given by (6.3) and can be rewritten as a 2π periodic function:

$$\frac{I}{2I_0}(\varphi) = 1 - \mathcal{V}\cos\varphi\ , \tag{6.11}$$

where I_0 are the counts in a lateral peak.

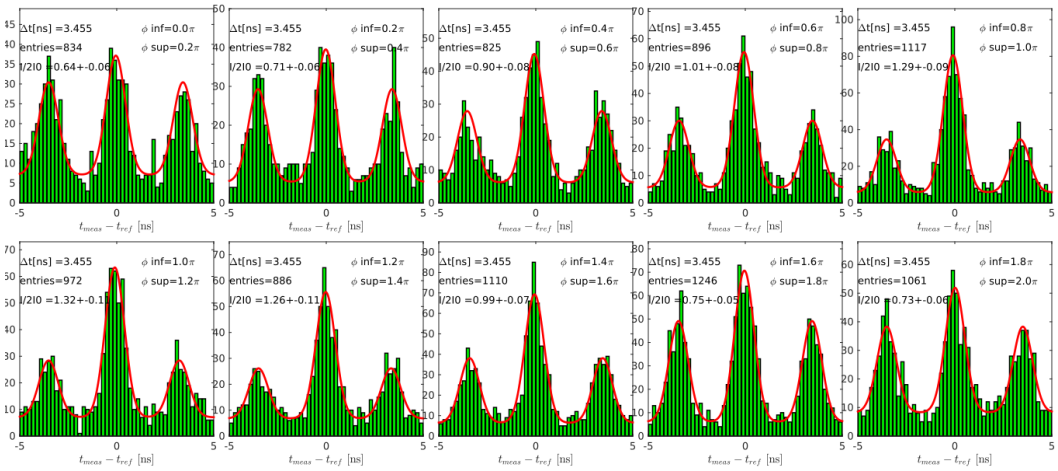


Figure 6.17: The ten histograms of the return qubits selected on the basis of their phase shift φ (modulo 2π).

Now, to point out the expected interference effect we separate the oscillation period in ten intervals with equal width $2\pi/10$. For each interval we realized the return histogram by selecting only the qubits that are characterized by a phase shift (modulo 2π) that falls in the selected range. The ten histograms obtained in this way for the passage of Beacon-C satellite used above are represented in Figure 6.17.

All the ten histograms are characterized by the three peaks figure. From the counts in the central Gaussian peak we can estimate the intensity I, while the other two peaks give the intensity I_0. In this way we can calculate the ratio $I/2I_0$ for each phase interval as shown in the figure.

To verify the expected interference effect we represent the trend of the ratio $I/2I_0$ as a function of the phase shift φ (modulo 2π), as shown on upper right in Figure 6.18. In this graph, the experimental trend in red is fitted by the dashed blue line given by (6.11) to extrapolate the value for the visibility $\mathcal{V}$ (for this passage it is about 34%). The yellow curve represents the theoretical trend obtained with unitary visibility.

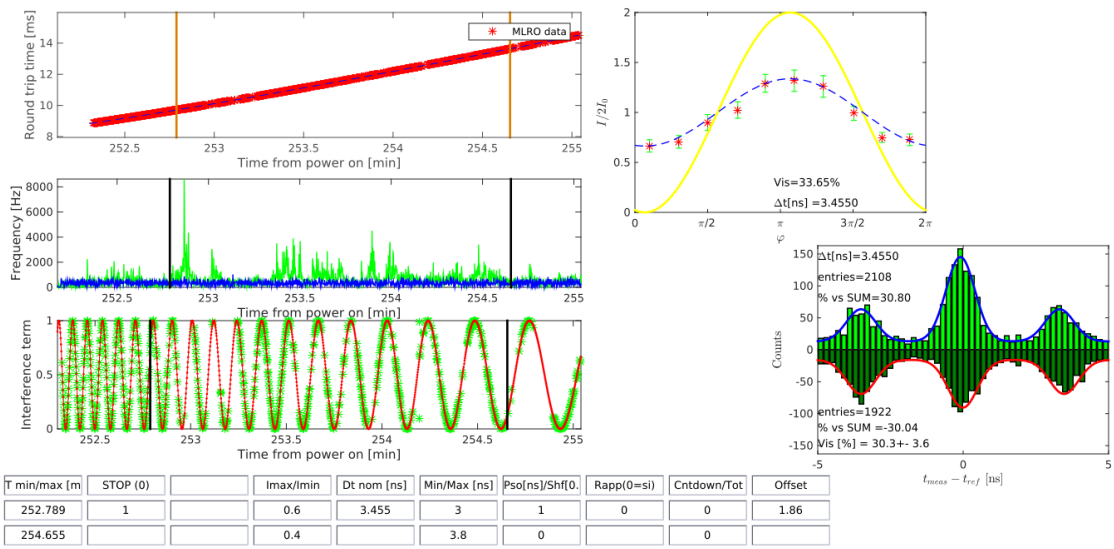


Figure 6.18: Passage of Beacon-C satellite, 12.07.2015 h. 00.56 CEST. It shows the experimental intensity trend as a function of the phase shift introduced by the satellite motion.

To check the goodness of the visibility extrapolated by fitting the curve, the last graph in Figure 6.18 shows the histograms obtained by selecting only the two phase shift intervals that give constructive (around $\varphi = \pi$) and destructive (around $\varphi = 0$ and $\varphi = 2\pi$) interference. From the two histograms we calculate the visibility as described above using the percentage by which the central peak is different from a lateral one according to (6.10).

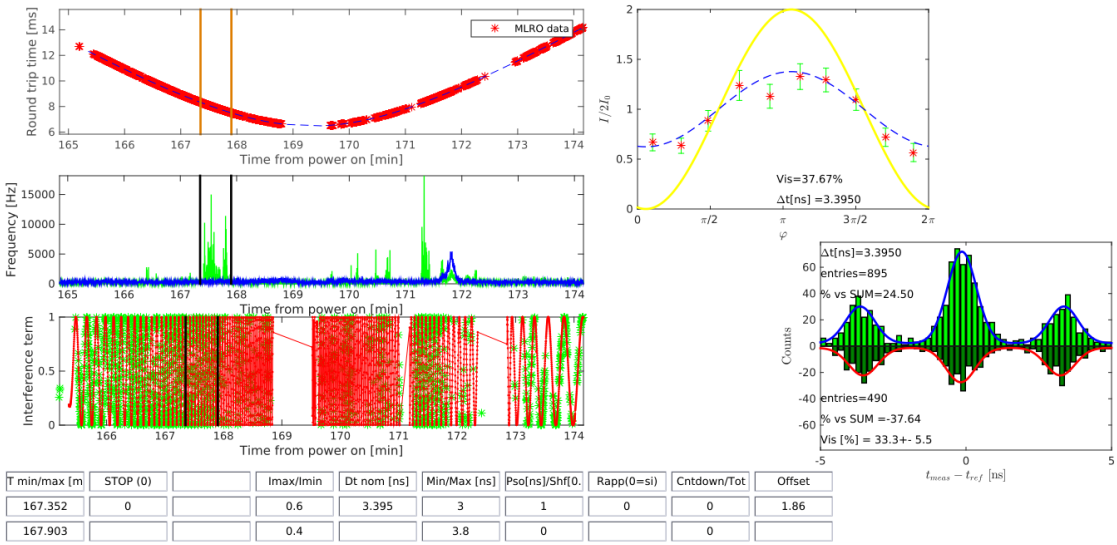
We have described the data analysis in details for a single passage of Beacon-C satellite. In the following section we will present the results also for other passages by showing only figures like 6.18 and we will discuss the obtained results.

6.6 RESULTS AND CONCLUSIONS

In this section we present the results obtained by performing the analysis described above. We will show that the expected interference effect due to phase encoding is clear and so the feasibility of time-bin encoding technique along a space quantum channel is demonstrated. The phase shift between the two time-bin states holds in the propagation and it would be controlled and used to implement a quantum communication.

We present the following five passages, relative to three different satellites:

- Beacon-C, 10.07.2015, h 23.38 CEST - Figure 6.19;
- Beacon-C, 11.07.2015, h 1.33 CEST - Figure 6.20;
- Beacon-C, 12.07.2015, h 00.56 CEST - Figure 6.18;
- Stella, 12.07.2015, h 3.08 CEST - Figure 6.21;
- Ajisai, 12.07.2015, h.3.42 CEST - Figure 6.22.



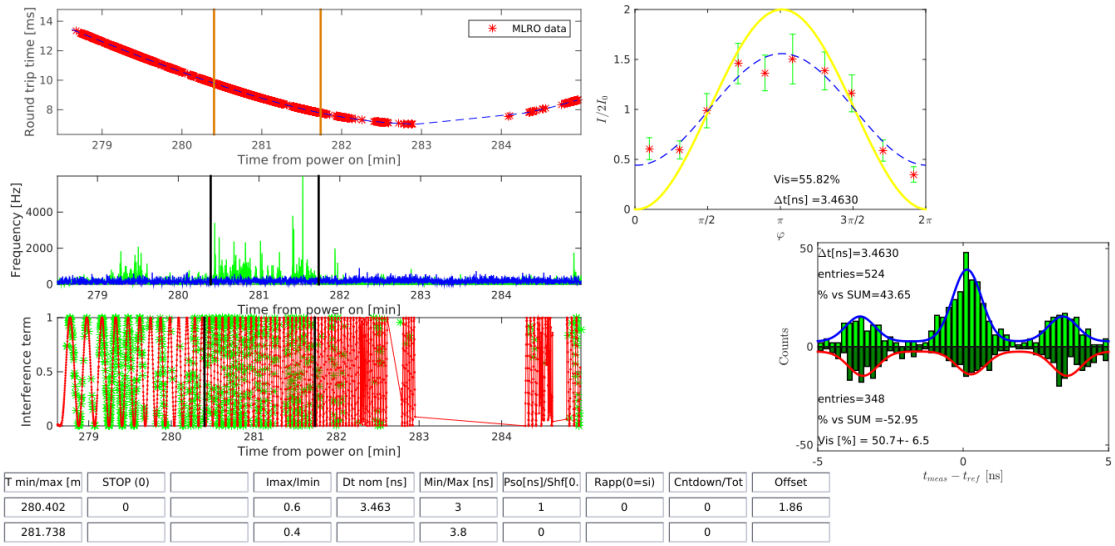
T min/max [m	STOP (0)		Imax/Imin	Dt nom [ns]	Min/Max [ns]	Pso[ns]/Shf[0.	Rapp(0=si)	Cntdown/Tot	Offset
167.352	0		0.6	3.395	3	1	0	0	1.86
167.903			0.4		3.8	0		0	

Figure 6.19: Passage of Beacon-C satellite, 10.07.2015, h. 23.28 CEST.

In all the five figures (one is in the previous section), the fundamental result is the trend of the ratio $I/2I_0$ as a function of the phase shift introduced by the satellite. Each graph of such type is realized by using a value for Δt estimated according to the analysis described above and by selecting a wide temporal window for the passage characterized by a good signal-to-noise ratio for the qubits return frequencies.

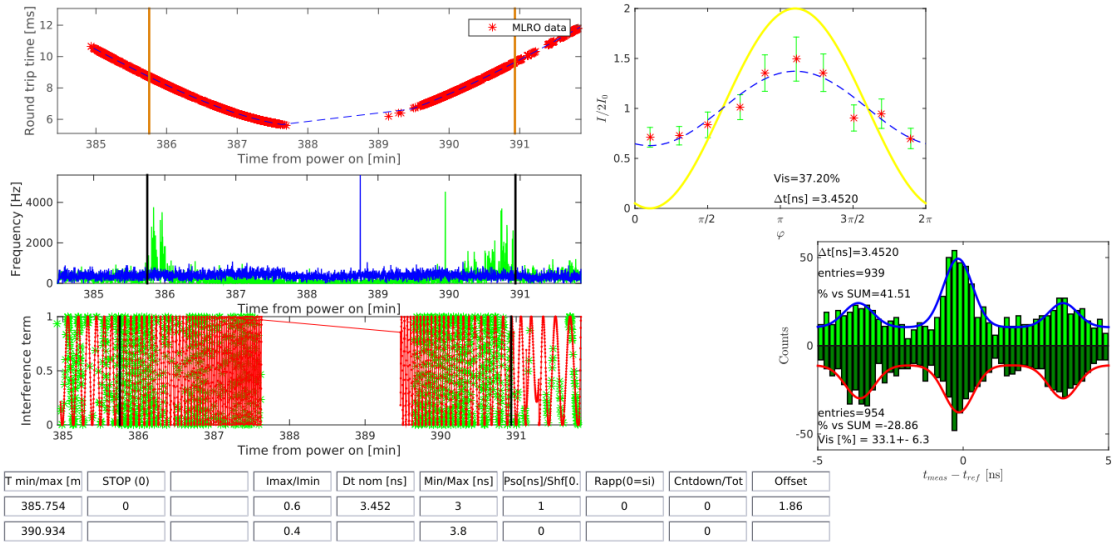
As you can see, all the five images show a good oscillation of the intensity: the experimental points are well fitted by the blue curve and they provide values for the visibility $\mathcal{V}$ always greater than 30%. This estimation is then checked by the two final histograms.

In particular, the passage of Beacon-C shown in Figure 6.20, provided a visibility greater then 50%. It is the most interesting passage because the intensity curve and the histograms are very statistically significant: the temporal window takes almost the passage and it is characterized by a good



T min/max [m	STOP (0)		Imax/Imin	Dt nom [ns]	Min/Max [ns]	Pso[ns]/Shf[0.	Rapp(0=si)	Cntdown/Tot	Offset
280.402	0		0.6	3.463	3	1	0	0	1.86
281.738			0.4		3.8	0		0	

Figure 6.20: Passage of Beacon-C satellite, 12.07.2015, h. 1.33 CEST.



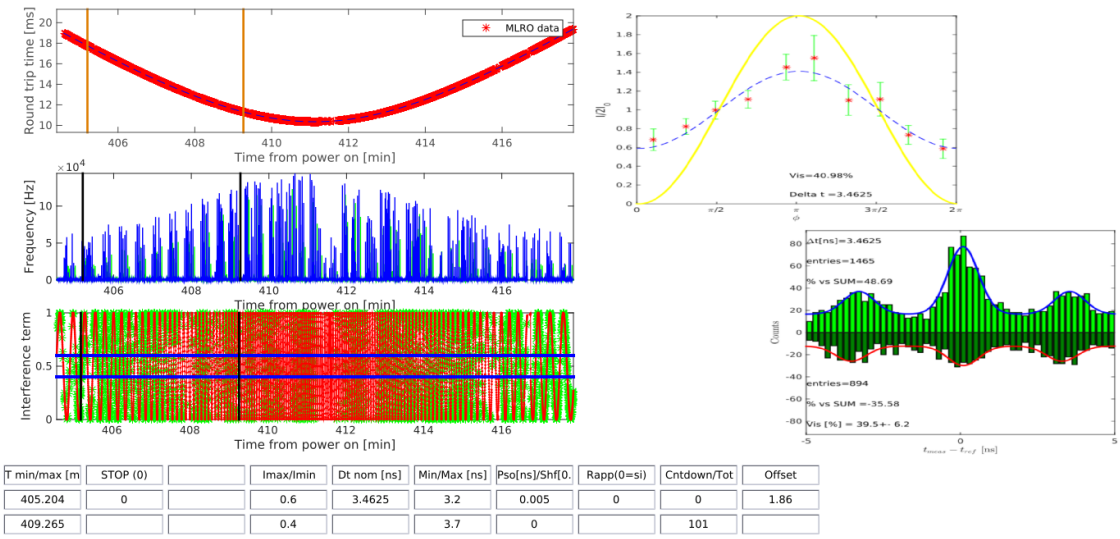
T min/max [m	STOP (0)		Imax/Imin	Dt nom [ns]	Min/Max [ns]	Pso[ns]/Shf[0.	Rapp(0=si)	Cntdown/Tot	Offset
385.754	0		0.6	3.452	3	1	0	0	1.86
390.934			0.4		3.8	0		0	

Figure 6.21: Passage of Stella satellite, 12.07.2015, h. 3.08 CEST.

qubits return frequency. It is to note that in the histogram for the destructive interference the central peak is lower than the two lateral peaks. This is a clear and irrefutable result that the interference effect is well verified.

It is to emphasize also the fact that the interference effect is realized not only with the Beacon-C satellite, but also with other two satellites (Stella and Ajisai), as you can see in Figure 6.21 and 6.22. For Stella and Ajisai the background is higher than for Beacon-C (this is clear by looking at the background return frequencies in blue for Ajisai) and this fact makes the results for them worse than for the best passage of Beacon-C.

We have to note also that the oscillating curve presents a small angular shift (of the order of 0.2 radiants at most) respect to the phase shift calculated with



T min/max [m	STOP (0)		Imax/Imin	Dt nom [ns]	Min/Max [ns]	Pso[ns]/Shf[0.	Rapp(0=si)	Cntdown/Tot	Offset
405.204	0		0.6	3.4625	3.2	0.005	0	0	1.86
409.265			0.4		3.7	0		101	

Figure 6.22: Passage of Ajisai satellite, 12.07.2015, h. 3.42 CEST.

the estimated Δt that is known with an accuracy of few picoseconds. The origin of this fact is still under investigation.

The values for the visibility obtained in this experiment is not sufficient to implement a quantum communication because the QBER obtainable is too high (more than 11%) according to (1.44). We think that the low value of the visibility is due to the weak stability of the optical system that can be improve in future experiments.

We conclude this thesis with the following considerations. The experiment described is the first interferometry experiment performed at single photon level at satellite distances involving moving terminals. It is a *feasibility test*: we want to check the possibility to use phase encoding along a space quantum channel that connects a Leo satellite and a ground station. The Two-Ways configuration has been used so far only with optical fibers for distances up to 100 kilometers. Being able to show that the quantum interference effect is measured with a low visibility, but unequivocally, for distance up to 1000 kilometers it is sure a great physical result. The phase used for the time-bin encoding holds in the propagation and this shows the feasibility of this encoding technique along a space quantum channel. Following studies must firstly improve the visibility and then try to control the phase shift introduced by the satellite for realizing a true space quantum communication with time-bin qubit.

Quantum interference (as that realized in this experiment) is a direct consequence of the coherent superposition of quantum states, while in classical wave-mechanics interference arises from the coherent superposition of classical waves. The characteristic trait of quantum interference is the fact that

it is associated with a nonphysical quantity, i.e., the wave function, while classical waves describe a physical magnitude, e.g., the electromagnetic field. Quantum interference is important at a conceptual and fundamental level to test the limits of quantum superposition. In the last years it is tested in many experimental realizations involving, for example, atom and molecular interferometry or superconducting quantum interference devices [43]. Showing that time-bin quantum superposition holds in free space long distances is part of the debate that wants to investigate wheter Quantum Mechanics is universally valid, an empirical question that will be answered only by future experiments.

BIBLIOGRAPHY

[1] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2011

[2] B. E. A. Saleh, M. C. Teich, *Fundamentals of photonics*, Wiley, 2007

[3] N. Gisin et al., *Quantum Cryptography*, Rev. Mod. Phys. 74, 145 (2002)

[4] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM 21 (2), 120-126 (1978)

[5] P. W. Shor, *Algorithms for quantum computation: Discrete log and factoring*, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, 124-134, IEEE Computer Society Press (1994)

[6] G. S. Vernam, *Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications*, Journal of the IEEE, 109-115 (1926)

[7] C. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, vol.28(4), page 656-715 (1949)

[8] C. H. Bennet, G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York), pp. 175-179 (1984)

[9] C. H. Bennet et al., *Experimental quantum cryptography*, J. Cryptology 5, 3-28 (1992)

[10] V. Scarani, *The security of practical quantum key distribution*, Rev. Mod. Phys. 81, 1301 (2009)

[11] V. Vedral, *Introduction to Quantum Information Science*, Oxford University Press (2006)

[12] Xiao-song Ma et al., *Experimental delayed-choice entanglement swapping*, Nature Physics 8, 479-484 (2012)

[13] *Gaussian beam propagation through a series of thin lenses*, `MATLAB` script, http://www.mathworks.com/matlabcentral/fileexchange/37436-gaussian-beam-propagation-through-a-series-of-thin-lenses

[14] L. Salasnich, *Quantum Physics of Light and Matter*, Springer International Publishing, 2014

[15] M. Fox, *Quantum Optics*, Oxford University Press, 2006

[16] R. J. Glauber, *Quantum theory of optical coherence: selected papers and lectures*, Wiley-VCH, 2007

[17] C. Gerry, P. Knight, *Introductory quantum optics*, Cambridge University Press, 2005

[18] R. Loudon, *The Quantum Theory of Light*, Third Edition, Oxford University Press, 2000

[19] J. Skaar, J. C. G. Escartin, H. Landro, *Quantum mechanical description of linear optics*, American Journal of Physics 72, 1385-1391 (2004)

[20] Chip Elliott, *Building the quantum network*, New J. Phys. 4 46 (2002)

[21] M. Peev et al, *The SECOQC quantum key distribution network in Vienna*, New J. Phys. 11 075001 (2009)

[22] E. Waks et al., *Security of quantum key distribution with entangled photons against individual attacks*, Phys. Rev. A 65, 052310 (2002)

[23] B. Korzh et al., *Provably secure and practical quantum key distribution over 307 km of optical fibre*, Nature Photonics 9, 163-168

[24] A. Fedrizzi et al., *High-fidelity transmission of entanglement over a high-loss free-space channel*, Nature Physics 5, 389-392 (2009)

[25] P. Villoresi et al., *Experimental verification of the feasibility of a quantum channel between space and Earth*, New J. Phys. 10 033038 (2008)

[26] J. Yin et al., *Experimental quasi-single-photon transmission from satellite to earth*, Optics Express Vol. 21, Issue 17, pp. 20032-20040 (2013)

[27] G. Vallone et al., *Experimental Satellite Quantum Communications*, Phys. Rev. Lett. 115, 040502 (2015)

[28] QIPC, *Strategic report on current status, visions and goals for research in Europe*, ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/fet-proactive/press-12en.pdf

[29] https://directory.eoportal.org/web/eoportal/satellite-missions/content/-/article/socrates

[30] http://english.nssc.cas.cn/ns/NU/201410/W020141016603617313704.pdf

[31] https://uwaterloo.ca/institute-for-quantum-computing/qeyssat

[32] D. Bacco et al., *Experimental quantum key distribution with finite-key security analysis for noisy channels*, Nature Communications 4 (2013)

[33] J. Degnan, *Millimeter Accuracy Satellite Laser Ranging: a Review*, Geodynamics Series 25, 133 (1993)

[34] J. Y. Wang et al., *Direct and full-scale experimental verifications towards ground-satellite quantum key distribution*, Nature Photonics 7, 387-393 (2013)

[35] J. Brendel et al., *Pulsed Energy-time Entangled Twin-Photon Source for Quantum Communication*, Phys. Rev. Let. 82, 2594 (1999)

[36] J. D. Franson, *Bell Inequality for Position and Time*, Phys. Rev. Lett. 62, 2205 (1989)

[37] J. G. Rarity, P. R. Tapster, *Fourth-order interference effects at large distances*, Phys. Rev. A 45, 2052 (1992)

[38] C. H. Bennet, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. 68, 3121 (1992)

[39] A. Muller et al., *"Plug and play" systems for quantum cryptography*, Appl. Phys. Lett. 70 793-5 (1997)

[40] D. Stucki et al., *Quantum key distribution over 67 km with a plug&play system*, New Journal of Physics 4 (2002)

[41] http://www.idquantique.com/resource-centre/quantum-key- distribution/

[42] http://www.diss.fu-berlin.de/diss/servlets/MCRFileNodeServlet/FUDISS-derivate-000000005776/09-Chapter05.pdf

[43] M. Arndt, K. Hornberger, *Testing the limits of quantum mechanical superpositions*, Nature Physics 10, 271-277 (2014)

ACKNOWLEDGEMENTS

I want to express my most sincere gratitude to prof. Paolo Villoresi who gave me trust and got me involved in the activities of his research group with enthusiasm and constant support. There are not many of my colleagues that during their thesis work were also able to have fun and for this I will always be grateful to him.

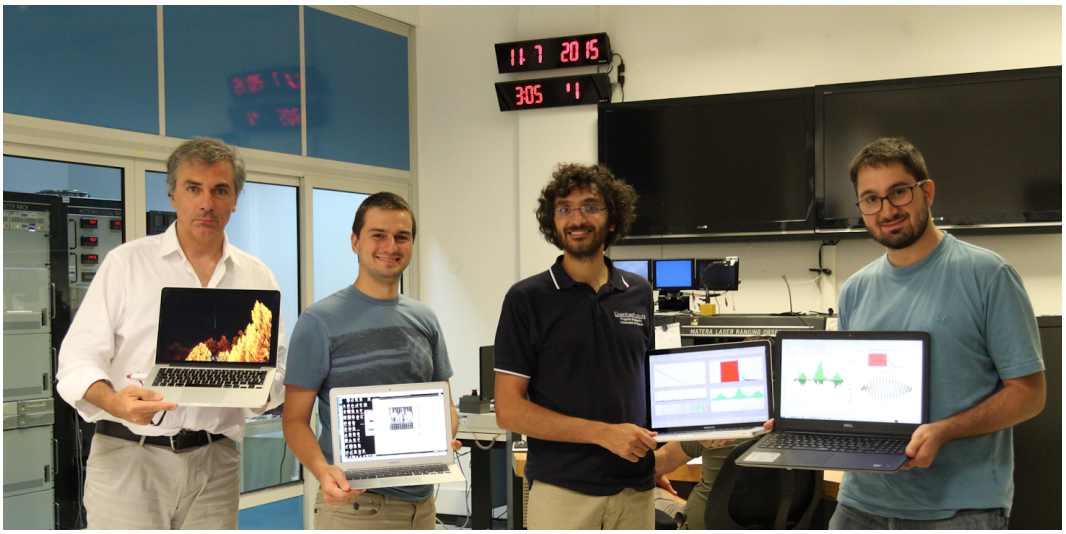
Special thanks to prof. Giuseppe (Pino) Vallone for his clear explanations that make everything looks easy and his ideas which are a constant source of motivations.

I thank all the guys in the Luxor Laboratory, especially Daniele who materially helped me in all circumstances with friendliness and great business ideas.

Special thanks go to my friends Dega, Enrico, Gio, Kza, Livio, Mionz, Yale and Zane (strictly in alphabetical order) for the laughs on weekends and in the most carefree moments and my friends Chiara, Fabio, Giacomo and Tommaso who shared even the difficult moments related to the study.

Thanksgiving Irene deserves a place apart: the beautiful memory of these years of study, but not only, will be always irremediably linked to her.

Finally, I must thank my family: my dad Redi, my mom Stefania and my sister Elisabetta because they always believe in me.



Prof. Paolo Villoresi, Daniele, Pino and I celebrating the positive outcome of the experiment at MLRO.