Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea Magistrale in Ingegneria delle Telecomunicazioni

Tesi di laurea

Signal Handling for Space Quantum Key Distribution

Relatore: Ch.mo Prof. Paolo Villoresi
Correlatore: Dott. Giuseppe Vallone

Laureando: Simone Gaiarin

8 Luglio 2013

Anno Accademico 2012/2013

Abstract

In this work of thesis we will present an experiment, which aims to realize a fully working quantum key distribution system for satellite communications, in order to prove the feasibility of a global quantum cryptography network. In particular we will deal with the implementation issues that arise when such system is realized using the already existing satellite laser ranging facilities. We firstly address the problem of driving electro-optic modulators with a high switching frequency while assuring a stable output voltage, in order to correctly prepare the quantum state of the qubits to be sent to the satellite. Then we will present the QKD system controller implemented with the FPGA technology, that is used to control the modulator driver in order to map the random key to the laser pulses. Further, the controller will allow scheduling the transmission and the reception phases of the QKD protocol, by controlling two shutters, in order to avoid unwanted optical background noise in the receiver. The controller should also be able to provide a fast control over the shutters to prevent that the high energetic pulses of the laser ranging system will damage the receiver photomultiplier tube.

Contents

CONTENTS

Introduction

In the current information age cryptography is becoming increasingly important. Some everyday activities, like commerce, payments, banking, communications and many others, are now commonly performed using only information technologies. While this shift in the information domain has made life easier, it entails higher security risks that must be properly handled by the information systems employed. The security of these technologies is closely dependent on the reliability of the underlying cryptographic systems. Today, the use of classical cryptographic algorithms based on particular mathematical functions is the primary way to guarantee the security of these systems. However, recently the evolution of quantum technologies has made possible to realize new kinds of cryptographic protocols for key exchange, which might allow reaching the perfect security in the near future. This application is named Quantum Key Distribution (QKD) since it is only used for the distribution of the keys and not for the encryption, which is performed with classical algorithms, as one-time-pad, which can guarantee a proved security.

While the few currently commercially available QKD systems are based on the use of optical fiber, which limits the communications range to few hundred of kilometers, new methods that aim to extend this range are being under high development. Recently, a group of researchers was able to operate a QKD protocol over a 144 Km horizontal free space link [1]. However the earth curvature and the atmospheric turbulence, which distort the optical wavefront, won't allow extending the communication distance significantly.

The subsequent evolution that eventually will allow building a global quantum network is to employ satellites to perform the quantum communication. The proof of the feasibility of a single-photon exchange in space has already been given by a recent experiment in which a geodetic satellite equipped with back-reflector has been used to simulate a single-photon source [2]. In this experiment the existing Satellite Laser Ranging (SLR) network has been exploited to send a weak laser pulse to the satellite, which

then reflects it down to the ground station. Using temporal, spectral and spatial filters it was possible to distinguish the emitted photons from the background noise.

The goal of the experiment on which our team is currently working is to implement a fully working QKD system able to exchange an unconditional secure key between a satellite and a ground station, in order to finally prove the feasibility of the quantum cryptography in space. To do this we take advantage of the existing SLR system of the Matera Laser Ranging Observatory (MLRO), located in Matera, Italy.

The integration of a QKD system with the SLR system makes it necessary to deal with some peculiar problems. In particular, in our setup we have exploited the high repetition frequency free-space laser installed in the MLRO as a source of laser pulses necessary to prepare the qubits for the B92 protocol we want to implement. To correctly modulate the polarization of the pulses we have used a Lithium Niobate polarization modulator. The first problem is related to this modulator, indeed it requires a high voltage driver with high switching frequency to be operated. The second problem instead, arise because of the presence of the high energetic laser pulses – used by the laser ranging system to track the satellite and measure its distance from the ground – that need to be blocked in order to avoid the failure of the photomultiplier tube (PMT) installed in our receiver.

In this work we have tried to solve the two presented problems. In particular we have developed a high voltage driver able to pilot the polarization modulator with a sufficiently high frequency. Moreover the driver should be able to provide a stable output in order to let the modulator impress a correct polarization to the qubits. Then we implemented an electronic controller, by using an FPGA, that is able to drive two shutters, used for shielding the PMT against the high energetic pulses, and for alternating the transmission and reception phase of our protocol. The need of separating in time the two phases was necessary to prevent that the transmitted pulses would raise the optical noise on the receiver. Moreover the controller was used to pilot the modulator driver according to the randomly generated key.

The rest of this work is structured as follow. In Chapter 1 we will review the basic notion on classical and quantum cryptography. In Chapter 2 we will review the previous phase of our experiment and we will introduce the setup of our system. In Chapter 3 an analysis of the electro-optic modulators will be presented. In Chapter 4 we will show the high voltage driver we have developed. Finally in Chapter 5 the realization of the QKD system controller will be described.

Chapter 1

Quantum cryptography

1.1 Introduction to cryptography

Cryptography is a science that studies and realizes the different techniques essential to pursue the goal of concealing the information of an exchanged message between two parties. In a basic cryptographic system the message – called *plaintext* – is transformed in an unreadable form – called *ciphertext* – through a process named *encryption*. The process is characterized by a set of instructions that form the *cryptographic algorithm* or *cipher*. The original message is retrieved from the ciphertext by an inverse process named *decryption*.

The need of exchanging information in a secure way dates back to ancient ages when this necessity was almost always connected with military purposes. Because of this many systems for secret message exchange were invented along the centuries. Beginning from the Caesar cipher – a simple cryptographic scheme in which each letter of a message is replaced by the letter shifted by a fixed number of positions in the alphabet – these systems have evolved reaching their maximum evolution with Enigma that is a machine used by the Germans during the World War II to communicate reserved information about the military plans [3].

Security of the early ciphers were based on the fact that a third party, who wants to intercept the message, doesn't know the cryptographic algorithm utilized to encrypt the message. Given that many of this ciphers were based on alphabetic substitution techniques, it was possible to retrieve the encryption algorithm – and so the plaintext –by performing an accurate study on the ciphertext, a so called cryptanalysis. The simplest cryptanalysis attack is the analysis of the frequency of each letter in the ciphertext. Indeed comparing this frequencies with the well-know frequen-

cies of each letters in a given language it is possible to retrieve the plaintext. Once the encryption algorithm were discovered, it was not possible to use it any more. With the evolution of cryptography, the secrecy begin to be make dependent on a short quantity of information called *key*, making so possible to public reveal the encryption algorithm while keeping only the key secret.

Along all the history many ciphers have been invented and most of them have been broken, proving so that they were not perfectly secure. The first perfectly secure algorithm is the *Vernam cipher* or *one-time-pad*, which was invented around the 1920 by Gilber Vernam. The mechanism of this algorithm is pretty simple though powerful: considering a binary message, the encryption is performed by executing a sum modulo 2 (XOR operation) between each bit of the message and the corresponding bit of a random key, which must be as long as the message. To obtain back the plaintext, the same operation is performed on the ciphertext. Shannon in 1949 have proven that this cipher is unconditional secure – that means it is secure against any kind of attack – under the assumptions that the key is as long as the message and that it is used only once [4].

Although the proof given by Shannon made the one-time-pad eligible to be the unique and perfect cryptographic algorithm to be utilized, in practice it is not widely used because the need of a pre-shared key make it utilization impractical. In fact, as for the message to be exchanged, it is not possible to share the key over a communication channel in a secure way, so that the two parties need to physically meet each other to exchange the key prior the communication – if they want guarantee the unconditional security of the algorithm.

The problem of key distribution was initially addressed by modern classical cryptography by the use of public cryptographic algorithms, that however are not able to guarantee an unconditional secure exchanged key. Recently, new systems that employs the basic principles of quantum mechanics have been invented and they have been proven to ensure a unconditional secure key distribution.

1.2 Modern cryptography

In the last few decades – also thanks to the fast development of the electronic – cryptography has become widely used in many fields other than the military one. At the present time cryptography has become a key enabling feature for many everyday life applications such as electronic commerce, on line banking, etc. Moreover, cryptography is not any more related only

to secret communication, but now it can provide all the following security services

- **Confidentiality** or **Secrecy** It guarantees that the sensitive data can only be accessed by the authorized entities. In particular this property allows sending a message over an insecure channel and guarantees that only the intended recipient can read it. Confidentiality is achieved through encryption.
- **Data Integrity** It refers to the action of providing the consistency of the data and prevent that it can be altered by malicious users.
- **Authentication** It provides a method that allows verifying the sender of a message with certainty.
- **Non-repudiation** It is the assurance that someone cannot deny previous actions.

Modern cryptography can be classified in two main classes of cryptographic techniques: symmetric cryptography (or secret key cryptography) and asymmetric cryptography (or public key cryptography).

The first set encompass all those algorithms which use a shared secret key to perform the encryption of the message through the use of a known algorithm, which is used both to perform the encryption and the decryption. The most relevant cipher of this class is the Data Encryption Standard (DES) – it uses relatively short key (56 bits at most in the original version) and is able to perform a very fast encryption of large quantity of data. Even though it was chose by the US as the official government standard because of its presumed high degree of security, it has been proven to suffer of some weakness [5], so that it was substitute by another public standard that is called Advanced Encryption Standard (AES).

The other large class of cryptographic algorithms is the class of the asymmetric cryptographic algorithms. Such cipher utilizes two different keys, a public one to encrypt the message and a private one to decrypt it. In this way anyone can encrypt a message using the well-know public key whilst only the intended recipient can decrypt it. Thanks to this property a public key cipher does not need to pre-share the key, thus solving the problem of key distribution. Moreover a public key cipher can be used in the opposite way to provide a system of signature and authentication. In particular one may encrypt a message (or a signature of it) with its private key so that the message can only be decrypted with the corresponding public key. If the public key is certified to belong to a specific entity, the

correct decoding of the message proves the authenticity of the sender. The public key cipher are build upon some particular mathematical functions that holds the property of being one-way, that means they are easy to compute in one way but extremely hard to compute in the other way. This property allows easily computing the public key from the private one but it makes very hard to obtain the secret key from the public one. The most well know example of this kind of algorithms is the Rivest-Shamir-Adleman (RSA) protocol. This protocol uses the fact that the product of two large prime numbers can be easily computed but the factorization of this product is hard to perform. The term "hard" here means that the currently best known algorithm to factorize a number posses a computational complexity that is exponential.

Although public key cryptography allows solving the problem of key distribution, they have few drawbacks. The first is that the process of encryption and decryption is very slow, making them unsuitable to encrypt very large quantity of data. The second is that the identity of the owner of the key need to be certified, otherwise anyone can create a new pairs of key and distribute the public key claiming to be someone else.

In practice public key cryptography and secret key cryptography are used together to better exploit the best features of both. In particular the public key cipher is used to encrypt a secret key that is then used in an efficient symmetric algorithm to perform the message encryption. The identity of the owner of the key is guaranteed by a hierarchical chain of certification authorities.

1.3 Security of classical cryptographic algorithms

To determine how secure a system is against cryptanalysis attack, it is first necessary to define what security is. In particular we can distinguish two main type of security [6]

- **Unconditional security** A system is said unconditionally secure if it is secure against any kind of attack supposing that the attackers can have an unbounded computational power

- **Computational security** A system is said computational secure if the best know attack against it is computationally infeasible, i.e., the time needed to perform the attack with the current hardware is too large (in the order of tens or hundreds of years)

As stated above the only unconditional secure cryptographic algorithm is the one-time-pad, while the security of all the other classical cryptographic systems is not proven. Both the symmetric and asymmetric cryptographic classes of algorithm are based on the fact that there are still no efficient algorithms and computational power to break them. In particular the RSA protocol assumes that there not exists a classical algorithm which can be used to factorize a large integer in a polynomial time, even though this has not been demonstrated yet. On the other hand, in 1994 Peter Shor designed an algorithm that runs on a *quantum computer*, and that is able to factorize a number in polynomial time. In the following years this algorithm has been implemented in more and more efficient ways [7]. The greatest number a quantum computer can factorize until now is 21, but the rapid evolution of the quantum technologies can let this number grow unexpectedly fast, thus undermining the pillar of classical cryptography.

These considerations show us how the security of the classical cryptographic algorithms are based on assumptions destined to become obsolete near or later, and show us how the need of a practical system able to guarantee an unconditional security is necessary to achieve the final goal of a perfectly secure cryptographic system.

1.4 Preliminary notions of quantum mechanics

In this section we will briefly introduce the basic notions about quantum mechanics needed to understand the QKD protocols we will present later in this chapter. For a complete reference of the basic quantum mechanics principles and notations refer to [8].

1.4.1 The qubit

In the classical information theory the basic unit of information is represented by a quantity called *bit*, that can assume only the values 0 and 1. The corresponding quantity in the quantum information theory is the *qubit*, that is a two-level quantum system, described by a two-dimensional complex Hilbert space. It is possible to map the values 0 and 1 of a classical bit into two normalized and mutually orthogonal quantum states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.1}$$

which form a *computational basis* of this space. While a bit can only takes two possible values, a qubit can be in a superposition of the two states $|0\rangle$ and $|1\rangle$. The general form of the states a qubit can assume is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.2}$$

where $\alpha, \beta \in \mathbb{C}$, with $|\alpha^2| + |\beta^2| = 1$, that is $\langle\psi|\psi\rangle = 1$.

Since state vectors are defined only up to a global phase of no physical significance, it's possible to choose α (and so β) real and positive so that the generic state of a qubit can be written in terms of spherical coordinates as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\end{bmatrix} \qquad (0 \leq \theta \leq \pi, 0 \leq \phi \leq 2\pi) \tag{1.3}$$

Such state can be visually represented in a three-dimensional Cartesian space as a unit vector whose tip lies on a sphere of unit radius that is called *Bloch sphere*. The Cartesian coordinates of the state are related to the polar coordinates by

$$x = \cos\phi\sin\theta, y = \sin\phi\sin\theta, z = \cos\theta \tag{1.4}$$

So far we have represented the state of a qubit as a linear combination of the vectors of the computational basis $\{|0\rangle, |1\rangle\}$, but in general the state of a qubit in a two-dimensional Hilbert space can be represented as a linear combination of any two orthonormal state vectors. Of particular interest are the so called *conjugate bases*

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{1.5}$$

and

$$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \tag{1.6}$$

The couple of vectors that form each of the conjugate bases correspond to the eigenvectors of the Pauli operators σ_z, σ_x and σ_y respectively, and they form a set of mutually orthogonal vectors over the Bloch sphere (Figure 1.1). The particularity of the conjugate bases will be cleared in the next sections.

1.4.2 Polarization encoded qubit

A qubit can be physically realized using any two-level quantum system. Some common examples of these systems are the spin of a photon, the

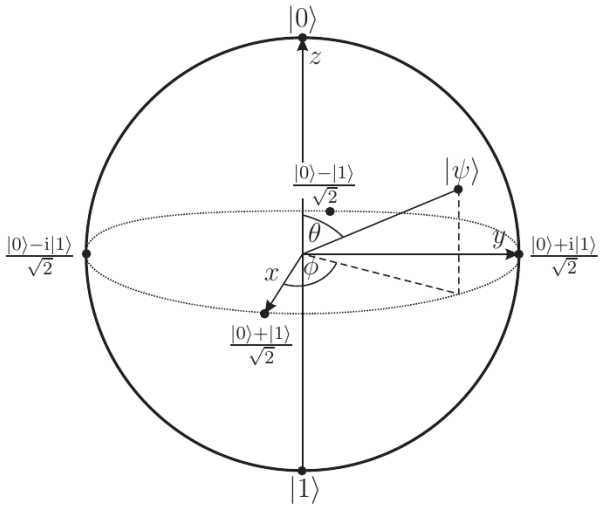


Figure 1.1: The Bloch sphere. Any possible state a qubit can assume is represented by a point lying on the surface of the unit-radius sphere. The three conjugate bases, corresponding to the Pauli operators, form a set of mutually orthogonal vectors [9].

spin of an electron, two electronic levels of an atom, etc. Due to the easiness of managing the polarization of a light wave, usually generated by a laser, many quantum communication systems use polarization to encode the qubit. If we associate the state $|0\rangle$ to the horizontal state of polarization of a photon and the state $|1\rangle$ to the vertical state of polarization as follow

$$|0\rangle \longrightarrow |H\rangle \tag{1.7}$$

$$|1\rangle \longrightarrow |V\rangle \tag{1.8}$$

we still have a computational basis. The corresponding conjugate bases are given by the +45°/-45° diagonal polarization basis (+/-) and by the left/right polarization basis (L/R), which are related to the H/V basis by

$$|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} \tag{1.9}$$

$$|L\rangle = \frac{|H\rangle + i|V\rangle}{\sqrt{2}}, \qquad |R\rangle = \frac{|H\rangle - i|V\rangle}{\sqrt{2}} \tag{1.10}$$

The vectors constituting each three bases correspond to the eigenvectors of the Pauli operators σ_z, σ_x and σ_y respectively.

The different states of polarization of a light wave can be visually represented in the Poincare sphere (Figure 1.2),which is an analogous of the Bloch sphere.

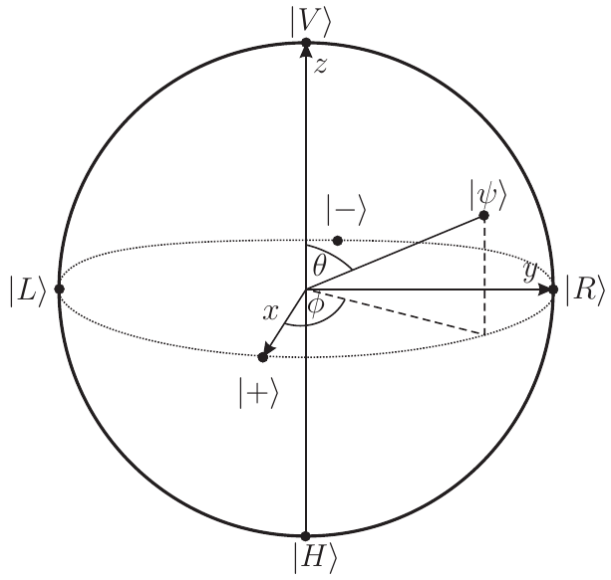


Figure 1.2: The Poincaré sphere. Any possible state of polarization can be represented as a point lying on the surface of the unit-radius sphere. The three conjugate bases (H/V, +/- and L/R) form a set of mutually orthogonal vectors [9].

1.4.3 Qubit state measurement

As we have seen above, the generic state of a qubit is given by the linear combination of two basis state vectors, weighted by the two coefficients α and β. From this, we understand that a qubit can assume an infinite number of different states. At this point one may think that it would be possible to store an infinite quantity of information in a single qubit, i.e., we can store the infinite number of classical bit needed to represent the coefficients α and β in a single qubit. Actually it is possible to prepare a qubit in an arbitrary state – for example we can impress an arbitrary polarization to a photon – but when we want to measure the state of the prepared qubit, the quantum mechanics laws impose a limit on the precision of this measure. To understand this, we recall the third postulate of quantum mechanics [8].

Definition 1.4.1 (Postulate IIIa)**.** *We associate with any observable $\mathcal{A}$ a self-adjoint operator A on the Hilbert space $\mathcal{H}_S$. The only possible outcome of a measurement of the observable $\mathcal{A}$ is one of the eigenvalues of the operator A. If we write the eigenvalue equation for the operator A*

$$A|i\rangle = a_i|i\rangle \tag{1.11}$$

where $|i\rangle$is an orthonormal basis of the eigenvectors of the operator A, and we expand the state vector $|\psi\rangle$ over this basis

$$|\psi\rangle = \sum_i c_i|i\rangle \tag{1.12}$$

then the probability that a measurement of the observable $\mathcal{A}$ results in an outcome a_i is given by

$$p(i) = p(a = a_i) = |\langle i|\psi\rangle|^2 = |c_i|^2 \tag{1.13}$$

The postulate states that when we try to measure an observable – that is a generic dynamic variable such as position, linear momentum, angular momentum etc. – the result of the measure can only be one of the eigenvalues of the operator associated to the observable. This means that with a single measure we can't recover the original state of the qubit, but it would be necessary to perform an infinite number of measure over the same qubit to retrieve its original state [8]. At this point one may think that it would be possible to perform a large number of measures on the same qubit to obtain a good estimation of its original state. Unfortunately this is not possible, in fact the second part of the third postulate of quantum mechanics tell us that when a measurement is performed on the qubit, its original state will be modified preventing so to recover it.

Definition 1.4.2 (Postulate IIIb)**.** *If a system is described by the state vector $|\psi\rangle$ and we measure an observable $\mathcal{A}$, obtaining the outcome a_i, then immediately after the measurement the state of the system is given by*

$$\frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}} \tag{1.14}$$

where P_i is the projection operator over the subspace corresponding to a_i.

To better understand the postulate let us introduce the concept of *projective measurement*.

Definition 1.4.3 (Projective measurement)**.** *A projective measurement is described by a self-adjoint operator M with spectral decomposition given by*

$$M = \sum_i \lambda_i P_i = \sum_i \lambda_i |i\rangle\langle i| \tag{1.15}$$

where P_i is the projector over subspace spanned by the eigenvectors corresponding to the eigenvalue λ_i. When the state $|\psi\rangle$ is measured with the operator M, the probability of getting λ_i as a result is

$$p(i) = \langle\psi|P_i|\psi\rangle \tag{1.16}$$

The second part of the third postulate implies that when we perform a measure on a qubit we project its state over the subspace spanned by one of the two eigenvectors of the measurement operator. At this point another measurement with the same operator on the same qubit will give the same result with unit probability, preventing so to retrieve the original state of the qubit.

Let consider the case of a polarization encoded qubit. Assuming the qubit is prepared in one of the two states $|H\rangle$, $|V\rangle$. We can try to measure the state of the qubit using two different operators

$$M_+ = |H\rangle\langle H| + |V\rangle\langle V| \tag{1.17}$$
$$M_\times = |+\rangle\langle +| + |-\rangle\langle -| \tag{1.18}$$

where the first measures the polarization in the H/V basis and the second in the +/- basis. When the M_+ operator is chosen, the result of a measurement give exactly the original state of the qubit. For example if the qubit is prepared in the state $|H\rangle$ the probabilities of getting H and V are

$$p_+^{|H\rangle}(H) = \langle H|H\rangle\langle H|H\rangle = 1 \tag{1.19}$$
$$p_+^{|H\rangle}(V) = \langle H|V\rangle\langle V|H\rangle = 0 \tag{1.20}$$

due to the fact that internal product $\langle V|H\rangle = 0$ since the state are orthogonal. On the other hand when the operator $M_\times$ is chosen we get a

probability of measuring + when the original state is H given by

$$p_{\times}^{|H\rangle}(+) = \langle H|+\rangle\langle +|H\rangle \tag{1.21}$$

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

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

$$= \frac{1}{2} \tag{1.24}$$

In the same way we obtain $p_{\times}^{|H\rangle}(-) = p_{\times}^{|V\rangle}(+) = p_{\times}^{|V\rangle}(-) = \frac{1}{2}$. This show us that if the qubit is prepared in a basis and we perform the measure in the other basis the result we obtain is completely random, thus the measure is giving no information at all. When two bases satisfy this property they are called *conjugate basis*.

No-cloning theorem

Till now we have shown that the state of a qubit cannot be recovered with a single measure and that the measure itself changes the state of the qubit. The last possible thing we can think to do in order to recover the original state of the qubit is to create many copies of the qubit prior the measure, using a hypothetical *cloning machine*, and then perform different measures using different basis on the various copies of the qubit. In this way it would be possible to recover the coefficient α with the desired accuracy. It can be demonstrated that also this eventuality is forbidden by the laws of the quantum mechanics.

Theorem 1.4.1 (No-cloning theorem)**.** *It is impossible to build a machine that operates unitary transformatons and is able to clone the generic state of a qubit*

1.5 Quantum cryptographic system

Similarly to a classical cryptographic system, the goal of a quantum cryptographic system is to allow two parties – the transmitter is usually called Alice (A) and the receiver Bob (B) – exchanging a message secretly over an untrusted channel, thus preventing any eavesdropper – usually called Eve (E) – to read or alter the message exchanged. To achieve this, beside the classical channel, used to transmit the ciphertext, a quantum channel

is employed to exchange the so called *raw key*, from which the unconditionally secure key will be obtained (Figure 1.3).

The leading idea in QKD is to exploit the intrinsic unpredictability of a quantum measure to detect the presence of an intruder. In fact if an eavesdropper tries to intercept the key, it needs to perform a measure over the exchanged qubits that will disturb (randomizes) the quantum state of them. If the exchanged qubits are prepared in some peculiar states, a proper analysis on the error rate of the key can allow detecting the presence of an intruder in a reliable manner.

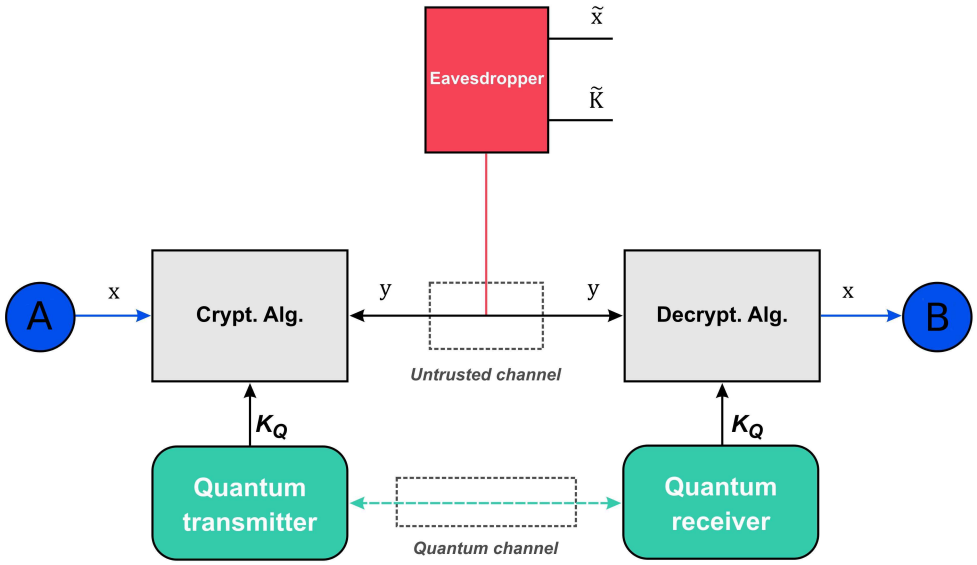


Figure 1.3: Basic scheme of a quantum cryptographic system. Two parties Alice (A) and Bob (B) use a quantum channel to share a raw key K_Q. The raw key is than processed to extract an unconditional secure key, which is then used to encrypt the message x into the ciphertext y. The encrypted message y is sent by A to B over the untrusted channel. An eavesdropper E perform some measurments on both the channel trying to extract the information $\tilde{x}$ and $\tilde{K}$ on the message and on the key respectively [10].

Ideally, if the system is able to generate a secret key with a sufficiently high bit rate, the message encoding can be performed using the one-time-pad protocol, leading so to a perfectly secure communication. On the other hand, if the key is not as long as the message, it can be used to operate a classical algorithm as AES. Although this second choice does not guarantee an unconditional security, it can provide a much higher degree of security

with respect a classical system, due to the fact that it will be possible to change the secret key used in the classical algorithm very frequently – indeed the key is continuously generated by the quantum protocol.

Two remarks have to be done. Firstly, we see that the quantum protocol is not used to encrypt the message but it is only employed to generate the secret key, so that the name quantum key distribution well describes the operation of the system. The second thing we must note is that the two parties need to authenticate each other before been able to exchange a key, otherwise a men-in-the-middle attack can be performed by the eavesdropper. In other words if an authentication phase is not done, the eavesdropper can pretend to be one of the two parties and engage a communication with the other one. From this point of view the quantum protocol can be regarded as a key expander protocol, since it is able to generate an infinite long key beginning form a short pre-shared key.

1.6 The BB84 protocol

The first protocol for QKD was proposed by Bennet and Bressard in 1984 [11]. This protocol uses four different quantum states from two conjugate bases – in the case of polarization encoded qubits the two bases can be chosen as the H/V polarization basis (+) and the 45° diagonal +/- polarization basis (×) ($\{|H\rangle, |V\rangle\}$ and $\{|+\rangle, |-\rangle\}$) – for encoding the values 0 and 1 of a randomly generated raw key. As we will see, the use of the conjugate basis will make impossible to Eve to perform measurements on the quantum channel without being detected. We now describe in details how this protocol works. An example of the operation of this protocol is shown in Table 1.1.

Alice random bits	0	1	0	0	0	0	1	0
Alice random bases	×	+	×	×	×	+	+	×
Transmitted polarization	$\|+\rangle$	$\|H\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|V\rangle$	$\|V\rangle$	$\|-\rangle$
Bob random bases	+	+	+	×	+	×	+	×
Raw Key	1	1	0	0	0	1	1	0
Sifted Key		1		0			1	0

Table 1.1: BB84 operation example.

1. Alice generate a random sequence of bits that forms the raw key.

2. For every bit to be sent, Alice chooses at random one of the two possible bases and encode the qubit according to Table 1.2. The particular choice of the basis is stored for the post-processing phase.

Bit\Basis	+	×
0	$\|H\rangle$	$\|+\rangle$
1	$\|V\rangle$	$\|-\rangle$

Table 1.2: BB84 bit encoding lookup table

3. Bob on the other side, chooses at random one of the basis and measures the state of polarization of the incoming photon with the chosen basis, obtaining so one of the two possible values 0 and 1.

4. Bob communicate to Alice through the classical channel which bits it has detected, in fact due to the channel losses some photons can have been lost.

5. In this phase, called *key sifting*, Alice and Bob publicly communicate the choice made on the bases. When this choice coincides, the values of the bit measured by Bob coincides with the one sent by Alice, whilst if the two bases do not coincide the value that Bob got is correct only half of the times and so the bit must be discarded. In fact, since the bases are conjugate, when the wrong basis is chosen to perform the measurement the result is completely random. At the end of this process Alice and Bob share the so called *sifted key* – the sifted key possessed by Alice and Bob are supposed to be equal, but this is true only if the quantum channel does not introduce errors and the eavesdropper has not tried to intercept the key.

6. At this point Alice and Bob need to check whether there was an eavesdropper present. This can be established from the error rate on the raw key, which is called Quantum Bit Error Rate (QBER). Alice and Bob reveal the same small portion of the raw key on the public channel and they calculate the percent of bits that are not equal. If the resulting QBER is higher than a specific threshold, to assure the unconditional security of the key they must assume the presence of an attacker (even though the high QBER can be caused by errors introduced by the channel or by the optical components), so that they have to discard the key and restart the procedure.

7. If the QBER is low enough they can perform the *information reconciliation*, that is a procedure of error correction with classical methods on the sifted key.

8. Finally they can perform the so called *privacy amplification*, that is a mapping of the current key over a new key, which will be completely uncorrelated from the piece of information possessed by Eve. This operation is usually performed by using hash functions.

We note that Bob will choose the wrong basis 50% of the times, so that only half of the received photons will give a useful bit. We can say that the BB84 has an efficiency of the 50%.

1.6.1 Security

The security of the BB84 protocol has been proved considering many different type of attacks. In particular it has been proven that if the QBER is lower than $\approx 11\%$ the obtained key can be considered absolutely unconditional secure against any possible attack [12]. A less tight threshold of $\approx 15\%$ can guaranteed an unconditional secure key against less general type of attacks, that nowadays are the only that can be realized [13]. We now describe the simplest attack that can be performed by Eve, just to give an idea on how the presence of Eve can be inferred from the QBER.

Intercept-and-resend attack

The simplest attack Eve can do is the so called intercept-and-resend attack (which is nothing more than a man-in-the-middle attack). In this attack Eve is assumed to be able to capture all the photons sent by Alice, and measures the polarization of them. Since Eve does not know the basis chosen by Alice the best she can do is to randomly perform the measure on one of the two bases. If the photon was polarized H for example, and Eve chooses the H/V basis, it will get the correct bit, whereas if she chooses the +/- basis she will get the correct value only half of the times. At this point Eve has to resend the photon to Bob and since she does not know whether the result of the measure is correct or not, the best she can do is to resend to Bob a photon with the same polarization of the one she has measured. If the basis chosen by Eve was correct also the bit received by Bob will be so and the presence of Eve will not be revealed, while if the basis chosen was wrong there is a 50% probability that Bob will obtain the same polarization of the original photon sent by Alice. Finally we can say that the error introduced by Eve on the QBER will be obtained by

multiplying the probability that Eve has chosen the wrong basis by the probability that Bob has obtained the wrong value, leading to a 25% of increase in the QBER.

1.7 The B92 protocol

In the 1992 Bennet introduced a variant of the BB84 protocol, which uses only two non-orthogonal states of polarization. We now briefly describe how this protocol works. An example of the operation of this protocol is shown in Table 1.3.

Alice random bits	0	1	0	0	0	0	1	1
Transmitted polarization	$\|V\rangle$	$\|+\rangle$	$\|V\rangle$	$\|V\rangle$	$\|V\rangle$	$\|V\rangle$	$\|+\rangle$	$\|+\rangle$
Bob random directions	$\|H\rangle$	$\|H\rangle$	$\|-\rangle$	$\|-\rangle$	$\|H\rangle$	$\|-\rangle$	$\|H\rangle$	$\|-\rangle$
Bob click		X		X		X	X	
Raw Key		1		0		0	1	
Sifted Key		1		0		0	1	

Table 1.3: B92 operation example.

1. Alice generate a random sequence of bits that forms the raw key.
2. For every bit to be sent, Alice chooses at random one of the two possible polarizations according to Table 1.4. The particular choice of the polarization is stored for the post-processing phase.

Bit\Party	Alice	Bob
0	$\|V\rangle$	$\|-\rangle$
1	$\|+\rangle$	$\|H\rangle$

Table 1.4: B92 bit encoding lookup table

3. Bob on the other side, chooses at random one of the other two directions of polarization and measures the state of polarization of the incoming photon along the chosen direction. In this protocol if Bob measurement the polarization according with the choice of Alice it has a 50% of probability of revealing the photon. In the other case, when he measures the polarization in the wrong direction it won't reveal nothing with unitary probability.

4. Bob communicate to Alice when it has revealed a photon. All the bit values corresponding to the revealed bits will form the sifted key.

5. The protocol proceeds as in the case of BB84 with the information reconciliation and privacy amplification phases.

In this protocol the efficiency is 25%. In fact Bob will measure in the wrong direction 50% of the times as in the BB84, but here also when he measures in the correct direction there is another 50% of probability of not revealing the photon.

In this protocol when Eve performs an intercept-and-resend attack it can still measure in all the four directions, so since the protocol uses only two states she has a clear advantage. It can be shown that the presence of Eve will increase the QBER of 12.5% (a derivation of this value is shown in [10] sec. 3.3.2).

1.8 Comparison of the BB84 and B92 protocols

The clear advantage of the B92 protocol is an easier implementation. Indeed this protocol can be realized by using only two single photon detectors and there will be the needing to prepare the photons in only two states of polarization. This last aspect (as we will see in Chapter 4) will lead to a great simplification in the implementation of the system.

The disadvantage of the B92 protocol is the lower efficiency, which implies a doubling of the time needed to obtain the same amount of key of an equivalent BB84 system or the need of a double frequency of the transmitted photons.

Chapter 2

Proof of concept of an earth-satellite QKD system

In this chapter we firstly discuss the problems associated with the use of a vertical earth-satellite quantum link. So we will introduce the Satellite Laser Ranging (SLR) infrastructure we have used as an underlying technology to build our system, referring particularly to the installation of the Matera Laser Ranging Observatory (MLRO), located in Matera, Italy. where the experiment was carried out [14]. We then present the results obtained in the first two phases of the experiment where the team led by Paolo Villoresi has proven the feasibility of exchanging a single photon from a satellite to an earth station, while maintaining the state of polarization. Finally we will present the last phase of the experiment, which aim to realize a fully working QKD system able to exchange an unconditional secure key between the satellite and the earth station.

2.1 Problems in the transmission of photons over a vertical link

To properly create a fully working earth-satellite QKD system it is first necessary to model and analyze a real space quantum link. Physically, one has to deal with a free-space dynamic optical link through the atmosphere, in which the transmitter and the receiver are in relative motion between them. The main problems that arise when such link is used for quantum communication purposes are the following:

- Effects due to atmospheric turbulence that causes attenuation ad fluctuations in the signal received.

- Background noise generated by sunlight, moonlight and every source of photons that can be collected by the receiver.
- The relative motions between the transmitter and the receiver, which is the main source of misalignment in the polarization references of the transmitter and receiver.
- Non ideal optics that can cause depolarization, attenuation and distortion in the exchanged photons.

2.2 Satellite laser ranging infrastructure

To study and implement a quantum space link, a transmitter/receiver in space is needed, so that a hosting satellite is required. Unfortunately, there are still no satellites equipped with a transmitter or a receiver since building and operating one is still a challenging task. However, recently some works have been focused on the development of compact transceiver suited to be housed on a satellite [15]. In the meanwhile we can take advantage from the existing SLR network to solve this problem. This, indeed, is the current easiest way to obtain a quantum space link using yet existing facilities, which should – obviously – properly adapted and integrated with the new instrumentations. In satellite laser ranging a global network of earth stations measure the round trip time of ultra short pulses sent to the satellites equipped with retro reflectors. This provides instantaneous range measurements, with millimeters accuracy, which can be used to provide careful measures of satellite orbits and for other geodetic purposes.

2.2.1 Laser ranging earth stations

A laser ranging earth station is usually provided with the following components

- High-speed telescope, able to point and track the laser ranging satellite, which normally orbiting in LEO (Low Earth Orbit) or MEO (Medium Earth Orbit) range
- High energy pulsed laser
- Detector able to receive the weak retro-reflected laser pulses
- Pointing and tracking system
- Data logger system used for collecting the ranging data

The complete specifications of the MLRO SLR system are reported in Table 2.1.

Parameter	Value
Telescope diameter	1.5 m
Laser pulse energy	100 mJ
Laser pulse repetition rate	10 Hz
Laser wavelength	532 nm
Beam divergence angle	45 μrad
Transmission optical efficiency	0.75
Receiving optical efficiency	0.39
Elevation	536.9 m
Telescope effective area	1.7662 m^2
One-way atmospheric transmission T_a	0.14 - 0.89
One-way transmissivity of cirrus clouds T_c	0.31 - 1
Beam pointing error θ	14.6 - 32.4 μrad
Transmitter gain G_t	$1.4 \cdot 10^9$ - $3.2 \cdot 10^9$

Table 2.1: Specifications of the Matera laser ranging observatory satellite laser ranging system.

2.2.2 Laser ranging satellites

The laser ranging satellites are provided with Corner Cube Reflectors (CCRs), which are able of reflecting the incident beam in a counter-parallel direction, regardless of the angle of incidence. In Figure 2.1 are shown two satellites used for laser ranging purposes, while in Table 2.2 is reported a list of the satellites we consider suitable to be used in our experiment.

2.3 Previous works

2.3.1 Matera-1 Feasibility of single photon satellite communications

The experimental demonstration of the feasibility of single photon exchange between a satellite and a ground receiver has been already demonstrated by Paolo Villoresi, Cesare Barbieri et al. [2] in the first phase of the Matera experiment. In particular in this work they simulated a single photon source on a satellite using the retro-reflection of a weak laser

Satellite	Altitude (Km)	Retroreflectors type
Ajisai	1 490	uncoated
Beacon-C	927	metal-coated
Blits	832	metal-coated
Cryosat-2	720	metal-coated
Etalon 1-2	19 120	metal-coated
Giove A-B	23 916	metal-coated
Glonass 102-109-110	19 100	metal-coated
Glonass 115	19 100	uncoated
Goce	295	uncoated
Grace A-B	485	uncoated
HY2A	961	metal-coated
Jason 1-2	1 366	metal-coated
Lageos 1-2	5 700	uncoated
Lares	1 500	uncoated
Larets	485	uncoated
Starlette	815	uncoated
Stella	815	uncoated
Tandem-X	514	metal-coated
TerraSAR-X	514	metal-coated

Table 2.2: List of the satellites suitable to perform our experiment. For each satellite the altitude and the type of coating of the mounted corner cube reflectors are reported.

pulse from a laser ranging satellite (Figure 2.2). To achieve the single photon condition they set the experimental parameters in order to make the mean number of photons per laser pulse in the downward link much less than unity. To detect the incoming single-photons they used an Avalanche Photo Detector (APD) and to discriminate the useful photons from the background noise they filtered the incoming photons with respect to direction, wavelength and polarization. Moreover a precise time tagger were used to take into account only the photons detected in some predefined time bins, in such a way to filter the background noise also in time.

The statistical analysis of the times of arrival of the single-photons shows that there was a returning rate of 5 count per second (cps), corresponding to a probability of detecting a photon per emitted laser pulse of 3×10^{-4}. The rate of emitted photons from the satellite directed to the FOV of the ground telescope taking into account the detection efficiency

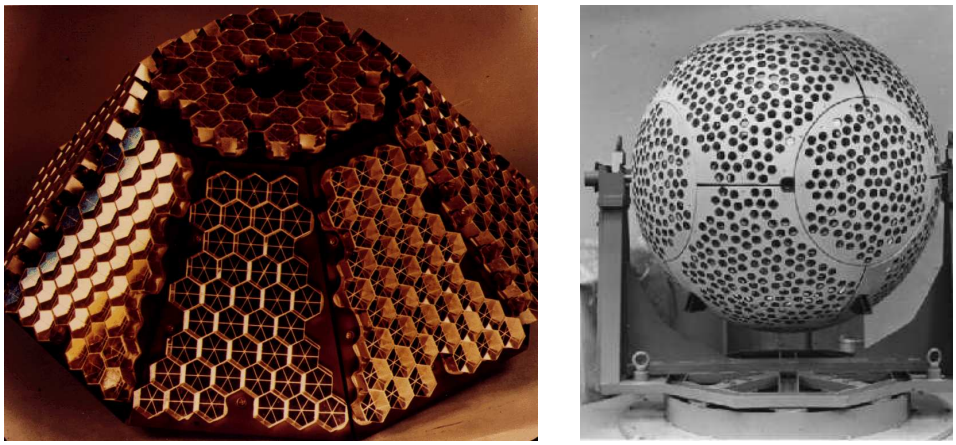


Figure 2.1: Satellites equipped with corner cube reflectors.

and the losses in the detection path can be estimated in 3×10^{-2}, thus confirming that the experiment was taken in a condition of single-photon regime.

This experiment proved that it would be possible to create a quantum communication system in space. Further, in the paper it has also been shown that placing the photon source on the satellite is a better choice with respect other proposed schemes that assume the transmitter to be on the ground. Unfortunately in this experiment it wasn't possible to implement a fully working QKD system because of two main issues. The first is the high loss introduced by the two-way channel and by the detection instrumentation, which was measured in -157 dB for a LEO satellite. The second is that it was not possible to maintain the polarization of the transmitted photons.

2.3.2 Matera-2 Study of the transformation of polarization of a quantum channel in space

In the phase two of the experiment an accurate study on the preservation of the polarization was carried out. Firstly the team of Paolo Villoresi has undertaken an accurate study on how the differently coated CCRs (Figure 2.3) change the state of polarization of the light when this is back-reflected [16]. What they found is that the uncoated CCRs depolarize the reflected light destroying so the information stored in the photon. On the other hand the metal-coated CCRs are able to keep the state of polarization up to rotations in its direction, which can be easily pre-compensated with

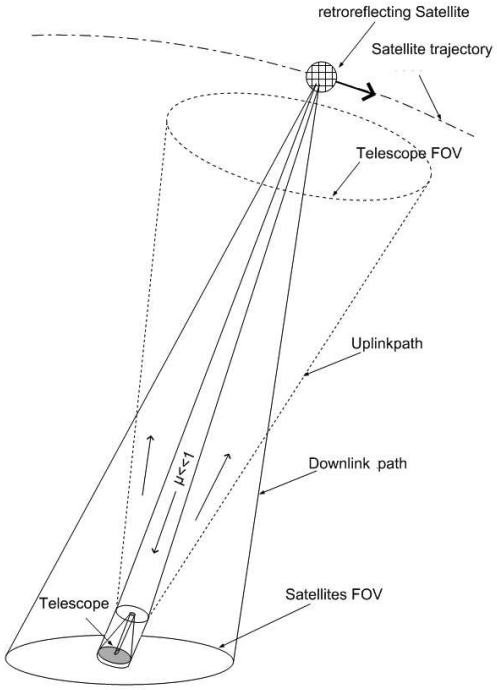


Figure 2.2: The scheme of the satellite single-photon link. A fraction of the beam in the uplink path irradiates the satellite. The corner cubes on the satellite retro-reflect back to the Earth a small portion of the photons in the laser pulse (downlink) and the gathered portion, according to the receiver FOV. This, according to the experimental parameters, is the single-photon channel.

a series of a quarter-waveplate and a half-waveplate. Then they built a four channel Stokes polarimeter [17], which has been integrated in the MLRO system in order to estimate how the quantum channel alters the state of polarization of the transmitted photons. The experiment leads to positive results for some specific satellites. Indeed it was possible to transmit and receive a pulse of light while maintaining its polarization as shown in Figure 2.4.

(a) Aluminium coated CCR (b) Uncoated CCR

Figure 2.3: Example of corner cube reflectors

2.4 Matera-3 A complete QKD implementation

The aim of the third phase of the Matera experiment is the implementation of a fully working QKD system on a satellite-Earth downlink, by merging the results of the previous phases of the experiment on single photon transmission and preservation of light polarization through atmosphere. The system implemented at the MLRO station aims to simulate a single photon source on the satellite by shooting a polarized laser pulse towards a satellite equipped with retro-reflectors and exploiting the reflected pulse as a single-photon source.

To accomplish this goal a sequence of qubits is generated exploiting a laser able to generate pulses with 100 ps Full Width Half Maximum (FWHM) at a repetition rate of 100 MHz. These are polarized according to the B92 protocol and sent between two consecutive 10 Hz laser ranging pulses, referred here as START signal (Figure 2.5). When the telescope tracks a satellite, the MLRO laser pulses are back-reflected to the station, where they are recorded, thus producing a STOP signal. Both START and STOP signals are recorded by a time-tagger as a time reference for the outgoing and returning qubits.

2.4.1 Experiment setup

The complete experimental setup is reported in Figure 2.6. On the sender side (Alice) the 100MHz laser pulses are firstly converted from 1064 nm

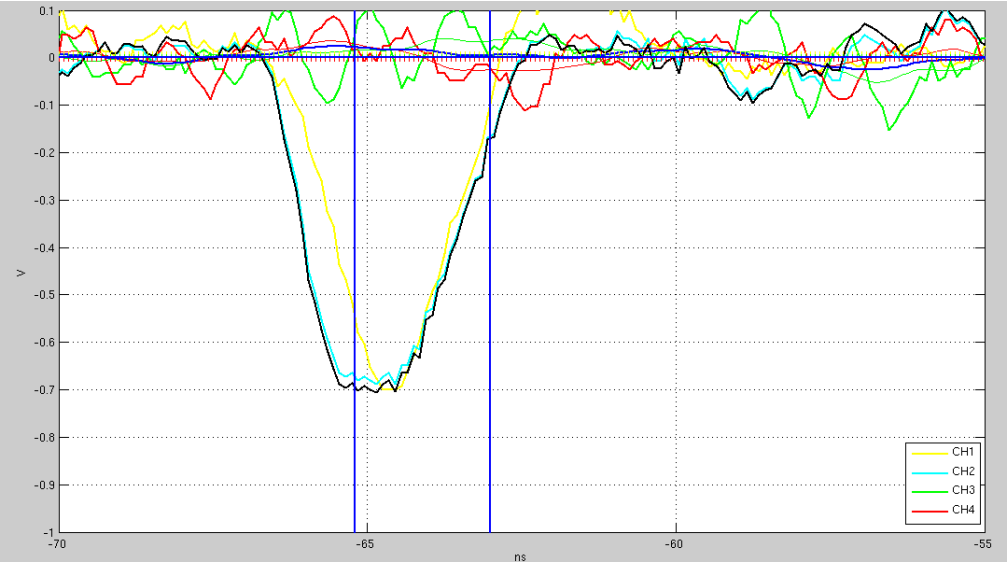


Figure 2.4: Intensity levels measured in the four channels of the polarimeter (H, V, +, R, in the order) for a +45° polarized pulse received from the satellite. The intensity levels of the H and V channels are equal, thus indicating the fact that the measured polarization state is +45°. To be noted that the + and R channels are subjected to a higher loss due to the presence of a second beam splitter. Moreover the APDs used for these channel were not working well during the experiment. This can explain the fact that there was not signal measured in them.

to 532 nm via a second harmonic generator (SHG) crystal, therefore are corrected for any polarization ellipticity by a $\lambda/2$ and a $\lambda/4$ retarder and given as input to a polarization modulator, which generates the two polarization states, vertical and circular left-handed. The signal produced are sent to the caudé optical path via a couple of beam splitters (BSs). On the receiver side (Bob) a primary BS divides the incoming photons between two branches: the one measuring the horizontal polarization uses a polarizing beam splitter (PBS) followed by a single photon photomultiplier tube (PMT) (Hamamatsu H7360-2), while on the other branch the circular right-handed polarization is measured with a $\lambda/4$ retarder followed by a PBS and a PMT. An additional $\lambda/2$ retarder has been added to this branch to correct for any ellipticity that may arise in the photon path.

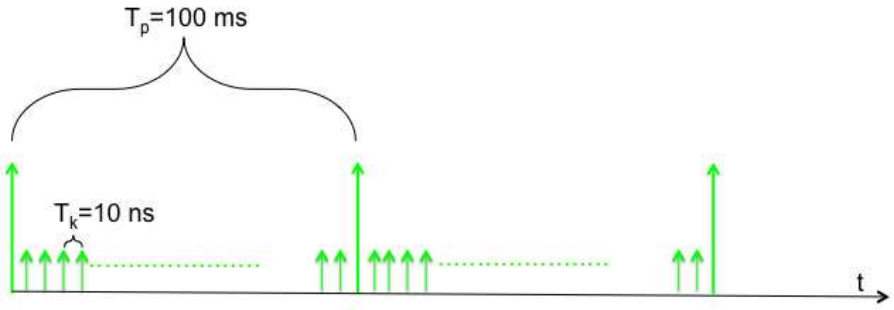


Figure 2.5: Time sequence of the START signals, occurring each 100ms, and qubit signals, which are separated in time by 10 ns.

2.4.2 Implementation issues analysis

Differently from a real QKD system, in this setup both the transmitter and the receiver are in the ground station. Because of this some peculiar implementation problems, that will not be present in a real implementation, arise. The first problem is due to the fact that the transmitter and the receiver share the same optical path and that the whole system must be integrated in the laser ranging architecture. Because of this, two beam splitters are used leading so to a 75% loss both in transmission and in reception. The transmission problem can be partially compensated by increasing the optical power of the laser to a level necessary to assure a single photon source on the satellite, whilst the receiving loss cannot be avoided.

Beside this we noted that the presence of the beam splitter that combines the transmitter optical path with the receiver one causes a strong scattering of the transmitter pulses that will end in the receiver PMT, thus causing a great increase of the background noise. To solve this problem we decided not to transmit continuously as a real QKD system is expected to do, but we opt for a slotted approach, in which in the first portion of time only the transmitter is active while in the second one only the receiver is so. To achieve this, two fast shutters have been used. One shutter has been placed right before the SHG crystal while the second in front of the receiver PMT.

Another problem that arises from the integration with the laser ranging system is that the laser used to measure the distance of the satellite and to track it, is extremely energetic. If such high powerful pulse would be captured by the PMT, it will instantly cause the failure of the component.

For this reason the receiver shutter will also be used to protect the PMT when both the transmitted and the received pulse are expected to come. The specific shutter scheduling protocol will be explained in details in Chapter 5.

The last problem that should be faced when dealing with a vertical quantum link is the high losses regime in which the QKD system has to operate. In fact the laser beam propagating trough the turbulent atmosphere is subjected to many different effects such as beam wandering, intensity fluctuations (scintillation), beam spreading, etc. These effects are mainly generated by small variations ($\approx 10^{-6}$) in the refractive index of the atmosphere. These variations are caused by small changes in the temperature (<1°C) which can give rise to random changes in the wind speed generating whirling. Each whirl can be modeled as a small lens. The cumulative effect of these lenses can redirect the beam, and possibly cause variations in intensity through interference phenomena.

We should note that if the losses are too high and since the average number of photons that leaves the satellite must be unitary (to guarantee the single photon conditions), it will be impossible to receive a sufficient number of photons to generate the key. To address this problem the only action that can be undertaken is increasing the repetition rate of the laser source.

2.4.3 Link Budget

Because of the presence of high losses in the quantum channel, an accurate analysis of the link budget need to be done in order to verify that the QKD system will be able to work properly. Here we present an estimation of practical losses considering a MEO satellite. The key experimental parameters are shown in Table 2.3.

The relevant parameters for the link budget analysis are the following. The pulse energy E is 0.2 nJ (@532 nm); S, the photon number per joule, is $2.67 \cdot 10^{18}$; A_s, the effective area of satellite corner retro-reflector, is 0.30 m^2 for a specific considered satellite; $A_r = 1.7671$ m^2; K_t, the efficiency of transmission system, is 0.2; K_r, the efficiency of optical receiving system, is 0.2, including a 0.8 factor that account for the receiving telescope and a 0.2 factor to account the two beam splitters; T, the one-way atmospheric transmission, is 0.65 (@532 nm); η, the quantum efficiency of receiving detection device, is 0.01; α is 0.05 and represent the attenuation factor (including the influence of satellite retro-reflector efficiency, atmospheric jitter and turbulence); L, the satellite distance in km for a MEO satellite, is2000; θ_t, the laser beam divergence angle, is 50 μrad; θ_s, the diffraction

Parameters	Symbol	Values
Laser repition rate	Δ	100 MHz
Single pulse energy	E	0.2 nJ
Photon number per joule	S	$2.67 \cdot 10^{18}$
Satellite distance	L	20000 km
Geometrical efficency of transmission	$\frac{4\,A_s}{\pi\,\theta_t^2\,L^2}$	$3.82 \cdot 10^{-7}$
Geometrical efficency of receiving	$\frac{4\,A_r}{\pi\,\theta_s^2\,L^2}$	$6.25 \cdot 10^{-6}$
Efficiency of transmission system	K_t	0.2
Receiving system effiicency	K_r	0.2
Quantum detection efficiency	η	0.01
One-way atmospheric transmission	T	0.6
Attenuation factor	α	0.05

Table 2.3: Link budget parameters.

angle of satellite retro-reflector, is 30 μrad.

According to the given parameters we could calculate the one-way channel attenuation from the ground station to the satellite, which result in

$$\eta_{up} = \frac{4\,A_s\,K_t\,T\,\alpha}{\pi\,R^2\,\theta_t^2} \;=\; 2.40 \cdot 10^{-9} \simeq 90\text{dB} \tag{2.1}$$

So the number of photons reflected from the satellite to the earth station is

$$N_0 = E \;\cdot S \;\cdot \eta_{up} \;\simeq\; 1.23 \tag{2.2}$$

From the other side, the attenuation from the satellite to the earth station is

$$\eta_{down} = \frac{4\,A_r\,K_r\,T\,\eta}{\pi\,R^2\,\theta_s^2} \;=\; 7.8 \cdot 10^{-8} \simeq 80\text{dB} \tag{2.3}$$

Therefore, the theoretical number of photons per pulse detected at the receiver is

$$N = N_0 \cdot \eta_{down} \;\simeq\; 4.9 \cdot 10^{-7} \tag{2.4}$$

From the calculations above, and considering the fact that we choose a very distant satellite to carry out the experiment, we have estimated that the satellite can be considered a single-photon source. We should note that due the high losses present, small variations in any of the parameters can lead to great variations in the calculated loss coefficients. From these coefficients and the parameters of the laser we use to transmit the photons, we have estimated to be able to generate a key with a rate of about 10 Hz.

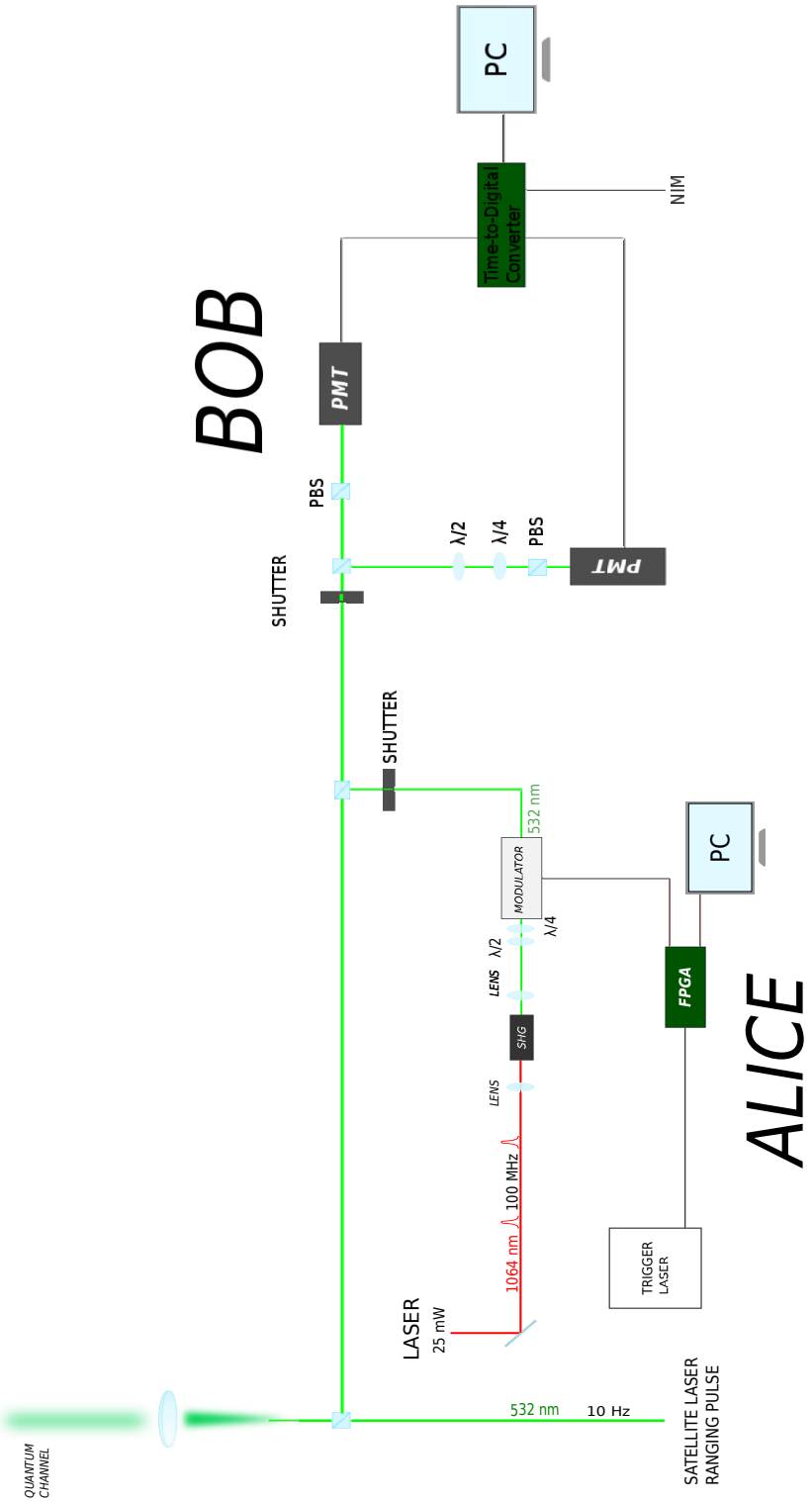


Figure 2.6: Schematic of the optical setup installed at the MLRO. The Alice transmitting module generates the V-L states, while the Bob receiving module measures the received photons on the H-R basis.

Chapter 3

Polarization Modulator

A crucial component of the transmitter of our QKD system is the polarization modulator. This is a wave retarder (or waveplate) that can change the state of polarization of a light wave according to an external applied voltage. In the following sections we will introduce the optics of anisotropic medium and the electro-optic effect following the treatment made in [18], and we will show how an anisotropic crystal, in particular the lithium niobate crystal ($LiNbO_3$), can be used to build an electronically controlled wave retarder.

3.1 Optics of anisotropic crystal

3.1.1 Permittivity tensor

The dielectric properties of a linear anisotropic dielectric medium, as a crystal, are completely described by a quantity called *electric permittivity tensor* $\boldsymbol{\epsilon}$, which is a tensor of second rank

$$\boldsymbol{\epsilon} = \begin{pmatrix} \epsilon_{11} & \epsilon_{12} & \epsilon_{13} \\ \epsilon_{21} & \epsilon_{22} & \epsilon_{23} \\ \epsilon_{31} & \epsilon_{32} & \epsilon_{33} \end{pmatrix} \tag{3.1}$$

This quantity relates the electric field vector $\mathbf{E}$ to the displacement vector $\mathbf{D}$ through the so called *material equation*

$$\mathbf{D} = \boldsymbol{\epsilon}\mathbf{E} \tag{3.2}$$

For most dielectric media, the electric permittivity tensor is symmetric, i.e., $\epsilon_{ij} = \epsilon_{ji}$. In particular this is true when the medium is non-magnetic and no magnetic field is applied to it. When this symmetry is present,

the medium is characterized by only six independent numbers for an arbitrary coordinate system. We recall that, in a given coordinate system, a symmetric second-rank tensor is represented geometrically by a quadratic surface, i.e., an ellipsoid that is said *quadratic representation*. Changing the coordinate system yields a different set of nine numbers, and a surface rotated respect the coordinate system but unchanged in its shape.

3.1.2 Crystal principal axes

It is always possible to choose a coordinate system such that all the off-diagonal coefficients of the permittivity tensor vanish, so that (3.2) simplifies to

$$D_1 = \epsilon_1 E_1,\ D_2 = \epsilon_2 E_2,\ D_3 = \epsilon_3 E_3 \tag{3.3}$$

where $\epsilon_1 = \epsilon_{11}$, $\epsilon_2 = \epsilon_{22}$, $\epsilon_3 = \epsilon_{33}$. In this situation the components of the electric field vector $\mathbf{E}$ and the ones of the displacement vector $\mathbf{D}$ are parallel along these particular directions. This coordinate system defines the *principal axes* of the crystal. The permittivities $\epsilon_1, \epsilon_2, \epsilon_3$ correspond to the so called *principal refractive indexes*

$$n_1 = \sqrt{\frac{\epsilon_1}{\epsilon_0}},\ n_2 = \sqrt{\frac{\epsilon_2}{\epsilon_0}},\ n_3 = \sqrt{\frac{\epsilon_3}{\epsilon_0}} \tag{3.4}$$

Crystals in which the three principal refractive indexes are different are termed *biaxial*, while crystals that present some kind of symmetries that lead to have two principal refractive indexes equal, are called *uniaxial*. In this case, the indexes are usually denoted as $n_1 = n_2 = n_o$ and $n_3 = n_e$, and are known as the *ordinary* and *extraordinary* refractive indexes. The crystal is said to be *positive uniaxial* if $n_e > n_o$, and *negative uniaxial* if $n_e < n_o$. The z axis of a uniaxial crystal is called the *optic axis*.

3.1.3 Index ellipsoid

The index ellipsoid is the quadratic representation of the electric impermeability tensor $\boldsymbol{\eta} = \epsilon_0 \boldsymbol{\epsilon}^{-1}$. When the principal axes coordinate system is used, the index ellipsoid is given by

$$\frac{x_1^2}{n_1^2} + \frac{x_2^2}{n_2^2} + \frac{x_3^2}{n_3^2} = 1 \tag{3.5}$$

with axes of half-length n_1, n_2 and n_3. The optical properties of the crystal (the directions of the principal axes and the values of the principal

refractive indexes) are therefore completely described by the index ellipsoid (Figure 3.1). For a uniaxial crystal, the index ellipsoid reduces to an ellipsoid of revolution.

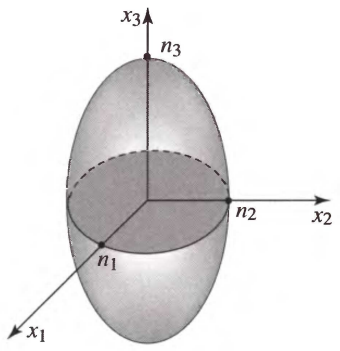


Figure 3.1: The index ellipsoid. The coordinates system axes (x_1, x_2, x_3) are the principal axes while (n_1, n_2, n_3) are the principal refractive indexes of the crystal.

3.1.4 Propagation along a principal axes

Let consider a crystal whose principal axes coincide with a coordinate system $x - y - z$ and a light wave travelling along the z axis. If this wave is linearly polarized along one of the other two principal axes, it will travel inside the crystal without changing its polarization because the electric field has only one component that is aligned with a principal axis so that the displacement vector is $D_i = \epsilon_i E_i$, with $i = 1$ or 2. The Maxwell's equations provides a velocity of light in the crystal equal to c_0/n_i, with $i = 1$ or 2. Thus, the *normal modes* for propagation in the z direction are linearly polarized waves in the x and y directions.

When we consider a light wave travelling in the z direction and linearly polarized along an arbitrary direction in the $x - y$ plane, we can regard it as the sum of the two normal modes. This two waves travel with different phase velocities, c_0/n_1 and c_0/n_2 respectively, in such a way they undergo different phase shifts, $\varphi_x = n_1 k_0 d$ and $\varphi_y = n_2 k_0 d$ respectively, after propagating the same distance d inside the crystal. Their relative phase retardation is thus $\varphi = \varphi_y - \varphi_x = (n_2 - n_1) k_0 d$. The recombination of the two components yields, in the general case, to an elliptically polarized wave.

3.2 Wave retarder

From the properties shown above we understand that an anisotropic crystal can be used to build optical components that can change the state of polarization of an optical wave. This optical component is called *wave retarder* (sometimes called *waveplate*). This device is characterized by its *fast* and *slow axes* and by its retardation

$$\varphi = 2\pi(n_2 - n_1)\frac{d}{\lambda_0} \tag{3.6}$$

Wave retarders are often built from anisotropic crystals in the form of plates, which thickness d determines the relative phase difference φ. In particular, the waveplate retards the component of the incident light wave parallel to the slow axis of the crystal by φ respect the component parallel to the fast axis. In Figure 3.2 it's possible to see how a light wave travelling inside a wave retarder undergoes a progressive retardation of one component with respect the other, thus leading to a change in the state of polarization of the wave. To be noted, as we can see from (3.6), that the phase shift is dependent on the wavelength λ_0 of the incident light wave. This implies that a specific wave retarder can only be used to retard a light wave of a specific wavelength.

Two particular kinds of wave retarders are the *quarter-wave retarder* and the *half-wave retarder*. These two devices are of particular interest because using them in series it is possible to obtain any state of polarization beginning from an arbitrary one.

Quarter wave retarder

A quarter-wave retarder is a plate that introduce a phase shift of $\lambda/4$ between the two normal modes. If the incident wave is linearly polarized and travels along one of the optic axes of the crystal forming an angle of 45° with the other two axes (or the only other for uniaxial crystal) the out coming wave will be circularly polarized. If the angle is not 45° the r will have a generic elliptical polarization. This happens because the two components of the incident wave posses the same magnitude only when the angle is 45° (Figure 3.3). In Figure 3.4 is reported the Poincare sphere corresponding to a quarter-wave retarder.

Half wave retarder

A half-wave retarder is similar to the quarter-wave retarder but it introduces a phase shift of $\lambda/2$ between the two normal modes. This device

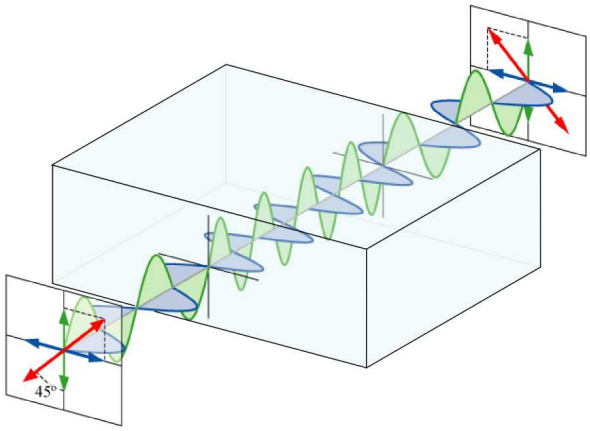


Figure 3.2: The progressive phase shift inside the crystal change the state of polarization of a linearly polarized wave, which angle of polarization is 45° with respect the optic axis, to its orthogonal state of polarization. In this case the crystal act as a half-wave retarder.

is used to change the polarization of a light wave from a specific state of linear polarization to a generic other linear state of polarization. A linearly polarized wave entering the crystal with an angle θ respect the optic axis will exit with an angle of polarization of $-\theta$ respect the axis, so that it undergoes a total rotation of 2θ. In Figure 3.4 is reported the Poincare sphere corresponding to a half-wave retarder.

3.3 Electro-optic effect

Certain transparent materials change their optical properties when subjected to an electric field. This is a result of forces that distort the positions, orientations, or shapes of the molecules constituting the material. The electro-optic effect is a change in the refractive index that results from the application of a steady or low-frequency electric field. An electric field applied to an anisotropic optical material modifies the refractive indexes of this material and thereby the effect that it has on polarized light passing through it. This property can be exploited to implement many types of electronically controllable optic components, including wave retarders. There are two kind of electro-optic effects, namely the *Pockel's effect* and the *Kerr effect*. The first one is a linear effect while the second is a quadratic effect. In the next section we will focus our analysis on the Pockel's effect.

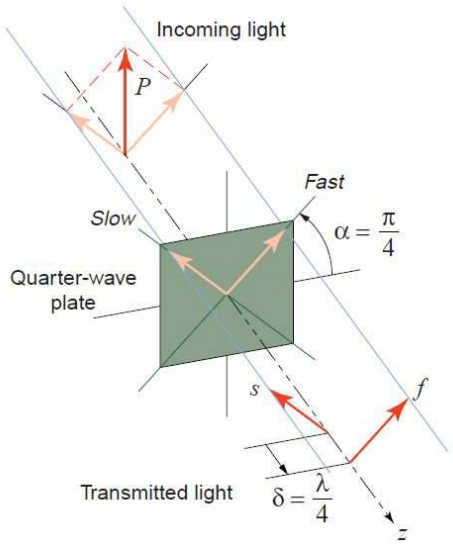


Figure 3.3: The quarter-waveplate retards the the component of the incident light wave parallel to the slow axis of the crystal by $\lambda/4$ respect the component parallel to the fast axis, changing so the polarization from linear to circular.

3.3.1 Pockel's electro-optic effect

When a steady electric field $\mathbf{E}$ with components (E_1, E_2, E_3) is applied to a crystal, the elements of the impermeability tensor $\boldsymbol{\eta}$ are modified and so also the index ellipsoid. To determine the new index ellipsoid it is sufficient to know the new coefficients $\eta_{ij}(E)$, which are functions of the applied electric field. Each of the functions $\eta_{ij}(E)$ may be expanded in a Taylor series about $\mathbf{E} = \mathbf{0}$

$$\eta_{ij}(E) = \eta_{ij} + \sum_k \mathfrak{r}_{ijk} E_k \qquad i, j, k = 1, 2, 3 \tag{3.7}$$

where $\eta_{ij} = \eta_{ij}(\mathbf{0})$, $\mathfrak{r}_{ijk} = \partial\eta_{ij}/\partial E_k$, and the derivatives are evaluated at $\mathbf{E} = \mathbf{0}$. The coefficients $\mathfrak{r}_{ijk}$ are known as *the linear electro-optic (Pockel's) coefficients*. They are $3^3 = 27$ coefficients and they form a tensor of third rank. Because $\boldsymbol{\eta}$ is symmetric ($\eta_{ij} = \eta_{ji}$), $\mathfrak{r}$ is invariant under permutation of the indexes i and j, i.e., $\mathfrak{r}_{ijk} = \mathfrak{r}_{jik}$. Because of this, the nine combinations of the indexes i and j generate six instead of nine independent elements. Consequently, $\mathfrak{r}$ has 6×3 independent elements. It is conventional to rename the pair of indexes (i, j), $i, j = 1, 2, 3$, as a single index

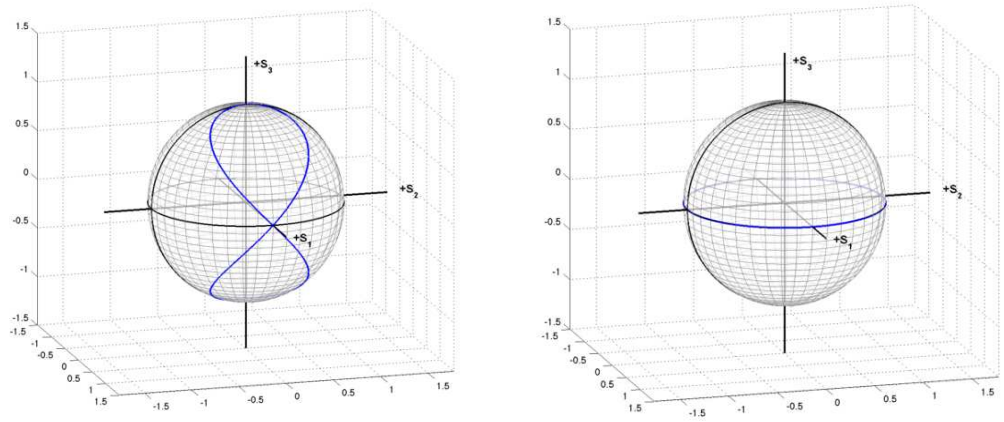


Figure 3.4: Poincare sphere of a quarter-wave retarder (left) and a half-wave retarder (right). The blue line shows all the polarization states reachable from a state of linear polarization using the waveplate.

$I = 1, 2, \ldots, 6$ in accordance with Table 3.1. The symmetry of the crystal adds more constraints to the entries of $\mathfrak{r}$. Some entries must be zero and others must be equal, or equal in magnitude and opposite in sign, or related by some other rule.

j \ i	1	2	3
1	1	6	5
2	6	2	4
3	5	4	3

Table 3.1: Lookup table for the index I that represents the pair of indexes (i,j) of the linear optic coefficient $\mathfrak{r}_{ijk}$

Procedure to get the modified index ellipsoid To determine the optical properties of an anisotropic crystal exhibiting the Pockels effect in the presence of an electric field the following procedure is used

1. Find the principal axes and principal refractive indexes n_1, n_2, and n_3 in the absence of $\mathbf{E}$.

2. Determine the elements of the new impermeability tensor

$$\eta_{ij}(\mathbf{E}) = \eta_{ij}(\mathbf{0}) + \sum_k \mathfrak{r}_{ijk} E_k \tag{3.8}$$

   where $\eta_{ij}(\mathbf{0})$ is a diagonal matrix with elements $1/n_1^2$, $1/n_2^2$, $1/n_3^2$.

3. Write the equation for the modified index ellipsoid

$$\sum_{i,j} \eta_{ij}(\mathbf{E}) x_i x_j = 1 \tag{3.9}$$

4. Determine the principal axes of the modified index ellipsoid by diagonalization, and find the corresponding principal refractive indexes $n_1(\mathbf{E})$, $n_2(\mathbf{E})$, $n_3(\mathbf{E})$.

5. Given the direction of light propagation, find the normal modes and their associated refractive indexes from this index ellipsoid.

3.4 Lithium Niobate Crystal ($LiNbO_3$)

Lithium niobate is a colorless solid insoluble in water. It has a trigonal crystal system, and displays ferroelectricity, Pockels effect, piezoelectric effect, photoelasticity and nonlinear optical polarizability. Lithium niobate has negative uniaxial birefringence which depends slightly on the temperature. It is transparent for wavelengths between 350 and 5200 nm.

The linear optics coefficients matrix $\mathfrak{r}$ takes the following form

$$\mathfrak{r} = \begin{pmatrix} 0 & -\mathfrak{r}_{22} & \mathfrak{r}_{13} \\ 0 & -\mathfrak{r}_{22} & \mathfrak{r}_{13} \\ 0 & 0 & -\mathfrak{r}_{33} \\ 0 & -\mathfrak{r}_{51} & 0 \\ \mathfrak{r}_{51} & 0 & 0 \\ -\mathfrak{r}_{22} & 0 & 0 \end{pmatrix} \tag{3.10}$$

The ordinary and extraordinary refractive index is a function of the wavelength of the incident light. The relation between these two quantities is governed by the *Sellmeier equation*

$$n_o^2 = 2.3920 + \frac{2.5112\lambda^2}{\lambda^2 - (0.217)^2} + \frac{7.1333\lambda^2}{\lambda^2 - (16.502)^2} \tag{3.11}$$

$$n_e^2 = 2.3247 + \frac{2.2564\lambda^2}{\lambda^2 - (0.210)^2} + \frac{14.503\lambda^2}{\lambda^2 - (25.915)^2} \tag{3.12}$$

where λ is in μm. For a light wave whose wavelength is 532 nm, as in our case, the corresponding ordinary and extraordinary indexes are 2.323 and 2.234 respectively.

When we apply an electric field along the optic axis of a $LiNbO_3$ crystal, i.e., $\mathbf{E} = (0, 0, E)$, the modified index ellipsoid is readily shown to be given by

$$\left(\frac{1}{n_o^2} + \mathfrak{r}_{13}E\right)\left(x_1^2 + x_2^2\right) + \left(\frac{1}{n_e^2} + \mathfrak{r}_{33}E\right) + x_3^2 = 1 \tag{3.13}$$

This is an ellipsoid of revolution whose principal axes don't change when the electric field is applied (Figure 3.5). The ordinary and extraordinary indexes, $n_o(E)$ and $n_e(E)$, are related to the electric field $\mathbf{E}$ as

$$\frac{1}{n_o^2(E)} = \frac{1}{n_o^2} + \mathfrak{r}_{13}E \tag{3.14}$$

$$\frac{1}{n_e^2(E)} = \frac{1}{n_e^2} + \mathfrak{r}_{33}E \tag{3.15}$$

Because the terms $\mathfrak{r}_{13}E$ and $\mathfrak{r}_{33}E$ are small the two equations above can be approximated by

$$n_o(E) = n_o - \frac{1}{2}n_o^3\mathfrak{r}_{13}E \tag{3.16}$$

$$n_e(E) = n_e - \frac{1}{2}n_e^3\mathfrak{r}_{33}E \tag{3.17}$$

where we have used the approximation $\sqrt{(1+\Delta)} \approx \frac{1}{2}\Delta$ valid for $|\Delta| \ll 1$.

3.5 $LiNbO_3$ polarization modulator

A crystal that exhibits the Pockel's effect such as a $LiNbO_3$ crystal can be used to build an electrically controlled wave retarder. In fact after a propagation of distance L, the two modes of a light wave undergo a relative phase retardation given by

$$\varphi = 2\pi\left[n_o(E) - n_e(E)\right]\frac{L}{\lambda_0} \tag{3.18}$$

$$= 2\pi\left[(n_o - n_e) - \frac{1}{2}\left(\mathfrak{r}_{13}n_o^3 - \mathfrak{r}_{33}n_e^3\right)E\right]\frac{L}{\lambda_0} \tag{3.19}$$

so that applying the electric field it's possible to modify the difference between the ordinary and extraordinary refractive index in accordance

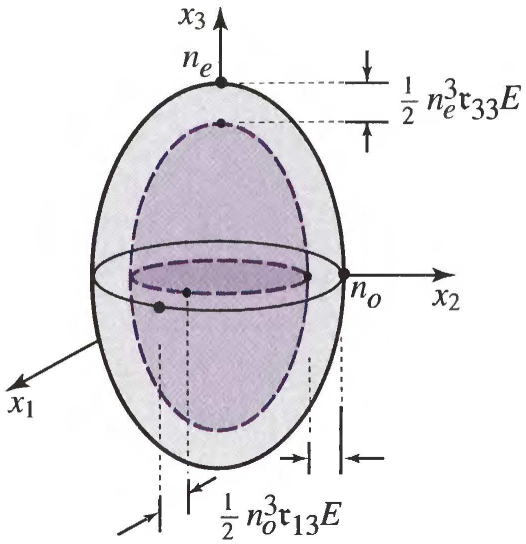


Figure 3.5: Modified index ellipsoid of a $LiNbO_3$ crystal resulting from the application of a steady electric field along the direction of the optic axis. To be noted that the $LiNbO_3$ is negative uniaxial, so that the ellipsoid in figure should be squeezed rather than stretched.

with (3.16) (3.17). If E is obtained by applying a voltage V between two surfaces of the medium separated by a distance d, (3.18) can be written in compact form as

$$\varphi = \varphi_0 - \pi \frac{V}{V_\pi} \tag{3.20}$$

where $\varphi = 2\pi \left[n_o - n_e\right] L/\lambda_0$ is the phase retardation in the absence of the electric field and

$$V_\pi = \frac{d}{L} \frac{\lambda_0}{\mathfrak{r}_{33} n_e^3 - \mathfrak{r}_{13} n_o^3} \tag{3.21}$$

is the so called *half-wave voltage*, which is the voltage necessary to obtain a phase retardation of π.

As we can see from (3.21), there is a linear relation between the optical phase shift and the voltage. One can therefore modulate the phase of an optical wave by varying the voltage V that is applied across a material through which the light passes.

The parameter V_π depends on the crystal intrinsic properties, n and $\mathfrak{r}$, on the wavelength λ_0 and on the aspect ratio d/L of the crystal. The refraction indexes n_o and n_e are also dependent on the wavelength. Moreover, the parameter $\mathfrak{r}$ is dependent on the direction of propagation and on

the direction of the applied field since the crystal is anisotropic.

The aspect ratio is an important parameter, in fact the choice on the direction where to apply the external electric field leads to very different values of V_π. We can distinguish two main types of polarization modulator: longitudinal and transverse modulators.

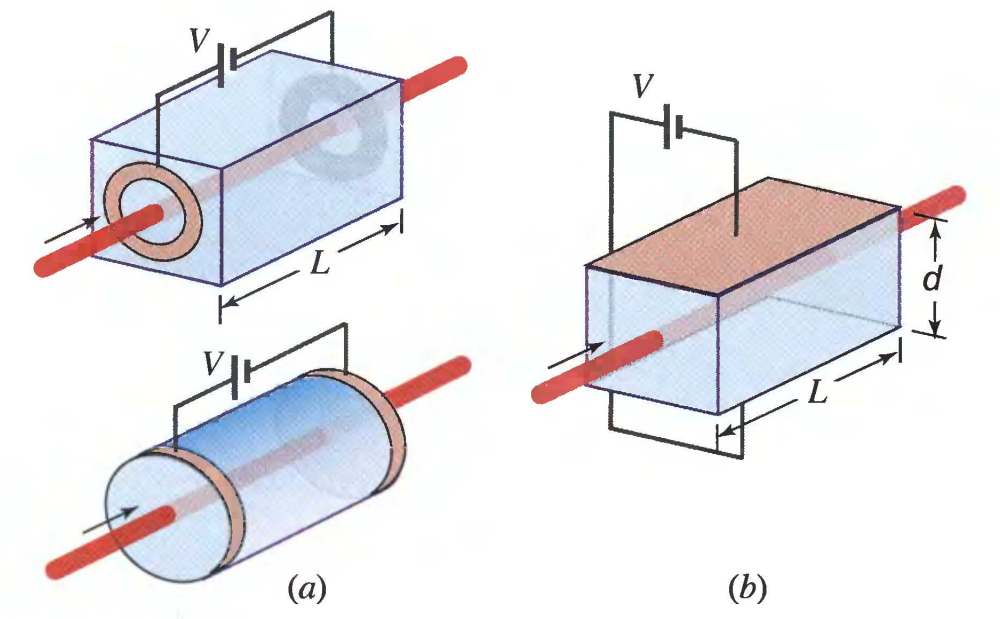


Figure 3.6: Longitudinal modulators with different kind of electrodes (a) and a transverse modulator (b).

3.5.1 Logitudinal Modulator

In longitudinal modulators the external electric field is applied in a direction parallel to the one of the propagation of the light. In this case two ring shaped electrodes are applied at the extremity of the crystal in such a way that when a voltage is applied to them an electric field appeares along the crystal. In this case the ratio between the distance of the two electrodes d and the distance that the light travels in the crystal L is unitary. The V_π voltage is usually in the order of some kV and since the aspect ratio can't be altered it is not possible to lower this value.

3.5.2 Transverse Modulator

In transverse modulator the external electric field is applied in a direction perpendicular to the one of the propagation of the light. The two electrodes are built on the top and on he bottom of the crystal, and the light travels between them. With this configuration it is possible to reduce d and increase L in order to lower V_π up to an order of magnitude.

Considering a $532\ nm$ light wave travelling in a $LiNbO_3$ crystal, we have that the parameters needed to compute V_π are $n_o = 2.323$, $n_e = 2.243$ given by (3.11) (3.12), $\mathfrak{r}_{13} = 9.6pm/V$ and $\mathfrak{r}_{33} = 30.9pm/V$. The corresponding half-wave-voltage is $V_\pi = 2.37\left(\frac{d}{L}\right)\ kV$. An aspect ratio of $1/10$ leads to $V_\pi = 237\ V$, which is significantly lower than the half-wave voltage for a longitudinal modulator.

3.5.3 Integrated modulator

Electro-optic modulators can also be constructed as integrated-optical devices. These devices operate at higher speeds and lower voltages than bulk devices. An optical waveguide is fabricated in an electro-optic substrate of $LiNbO_3$ by indiffusing a material such as titanium to increase the refractive index. The electric field is applied to the waveguide using electrodes. Because the configuration is transverse and the width of the waveguide is much smaller than its length ($d \ll L$), the half-wave voltage can be as small as a few volts. These modulators can operate at speeds that exceed 100 GHz. Light can be conveniently coupled into, and out of, the modulator by the use of optical fibers.

3.5.4 Bandwidth limiting factors

The speed at which an electro-optic modulator operates is limited by the transit time of the light through the material. If the electric field $\mathbf{E}(t)$ varies significantly within the light transit time T, the travelling optical wave will be subjected to different electric fields as it traverses the crystal. The modulated phase at a given time t will then be proportional to the average electric field $E(t)$ at times from $t-T$ to t. As a result, the transit-time-limited modulation bandwidth is $\approx 1/T$.

Another important limiting factor is the fact that the two electrodes form a capacitive load, which should be properly driven from an external electronic driver to achieve fast operating times of the modulator. We will discuss about this in the next chapter.

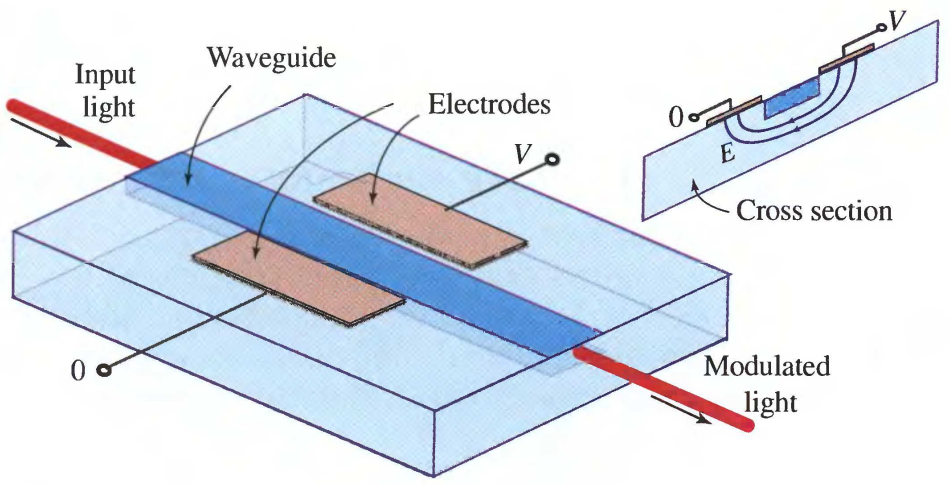


Figure 3.7: Integrated transverse polarization modulator.

3.6 Thorlabs EO-AM-NR-C4 modulator

The thorlabs EO-AM-NR-C4 modulator consists of two lithium niobate crystals packaged in a compact housing with an RF input connector (Figure 3.8). Given that the $LiNbO_3$ presents a static temperature-dependent birefringence, this implies that it induce a polarization change in the light travelling through it also when no electric field is applied. Since the birefringence is temperature-dependent it's not sufficient to apply a bias voltage in order prevent the crystal to modify the polarization, because a small variation of the temperature will reintroduce this change. To reduce this deleterious effect, two $LiNbO_3$ crystals are packaged together with the respective principal axes rotated by 90° with respect each other. Thus the temperature dependent static birefringence in the first crystal is canceled by the temperature dependent static birefringence in the second. In this manner, the temperature sensitivity of the modulator is generally less than 1 $mrad/K$ [19].

The half-wave voltage, which general formula is given in (3.21), for this particular modulator is given by the following simplified formula

$$V_\pi = 0.361\lambda - 23.844 \tag{3.22}$$

where λ is the wavelength in nm.

The $LiNbO_3$ presents photorefractivity: if a high energy optical beam hits the crystal, the spatial distributions of the charge can be altered leading to an inhomogeneous distribution of the charges that generate an elec-

tric field pattern inside the crystal. This internal electric field is able to modulate the local refractive index of the material by virtue of the Pockels electro-optic effect. While this effect is desiderable in some application, e.g. holograms forming, it should be considered a deleterious effect when the crystal is used as wave retarder. The crystal in the Thorlabs modulator is MgO-doped to increase the resistance to photorefractive damage. All the specifications of this modulator are reported in Table 3.2.

Specification	Description
Modulator crystal	MgO-Doped Lithium Niobate ($LiNbO_3$)
Wavelength range	400 to 600 nm
Clear aperture	2 mm diameter
Halfwave voltage V_π	168 V @ 532 nm
Bandwidth	100 MHz
Optic axis orientation	45°
Extinction ratio	> 10 dB
Input capacitance	14 pF (typical)
Maximum optical power density	2 W/mm^2 @ 532 nm
Input connector	SMA female

Table 3.2: Thorlabs EO-AM-NR-C4 polarization modulator specifications

Figure 3.8: Thorlabs EO-AM-NR-C4 $LiNbO_3$ polarization modulator. The 2mm hole in the right-lower part of the housing is the beam entrance. An SMA input connector allows connecting an external high-voltage driver needed to operate the modulator.

Chapter 4

Development of a high voltage driver

As we have seen in the previous chapter to be able to change the state of polarization of a light wave using the $LiNbO_3$ polarization modulator, it is necessary to apply to it a voltage proportional to change in polarization we want to obtain. To apply this voltage a proper electronic driver is required. Due to the high voltage involved and the short switching times requested for this application, it is necessary to care about different implementation aspects to obtain a good optical output signal. Considering the B92 protocol, that is the quantum communication protocol we have used in our systems, we only need to change the polarization between two states belonging to two conjugate bases. A smart choice of these two states would the one of choosing one state corresponding to a linear polarization (V) and the other state corresponding to a circular polarization (L). In this way we minimize the maximum voltage that should be applied to the modulator. In our case, we can extract from the modulator a state V with $0\ V$ applied to it and a state L with $V_{\pi/2} = 84\ V$. As we will see, lowering the maximum voltage is a great advantage in the implementation of the driver.

In the rest of this chapter we will present two simple designs of driver for the polarization modulator, which aim to provide a good shaped high voltage output needed to obtain a good polarization of the transmitted photons.

4.1 Considerations on polarization errors

To correctly polarize the laser pulse in one of the two possible states, when the pulse transits through the modulator the voltage applied to it must be perfectly steady in one of the two allowed levels: 0 or $V_{\pi/2}$. If the voltage is different from 0 or $V_{\pi/2}$, the light pulse will assume a state of polarization that is in general elliptical. Such polarized photons has a non zero probability to be detected at the receiver also when the orthogonal polarization state (respect the one the photon is expected to have) is chosen to perform the measurement. This phenomena leads to an increase of the QBER on the sifted key.

To evaluate how a state of polarization if far from the optimal, we can measure the polarization of this state in a basis that encompass the state of optimal polarization and its orthogonal state, and then we calculate the visibility of the state. The visibility is defined as

$$\mathcal{V} = \frac{I_{MAX} - I_{MIN}}{I_{MAX} + I_{MIN}} \tag{4.1}$$

where I_{MAX} is the optical intensity measured in the direction parallel to the one of the optimal state while I_{MIN} is the optical intensity measured in the orthogonal direction. We note that $0 \leq \mathcal{V} \leq 1$. The lower is the visibility obtained the worse will be the state of polarization respect to the optimal one. As example, if we want to evaluate the quality of the polarization of a laser that is supposed to be left circularly polarized, we should measure its intensity in the L/R basis and calculate the visibility.

It can be shown that for the B92 protocol the QBER increment due to polarization errors is equal to two times the visibility, that is

$$\Delta QBER = 2 \times \mathcal{V} \tag{4.2}$$

Because of this it is important to correctly drive the modulator so it can produce good polarized photons, in order to keep the QBER under the threshold that guarantees an unconditionally secure key.

4.2 Driver requirements

The laser source we have used in our setup produce a pulse train with a repetition rate of 100 MHz, where every pulse has a FWHM of 80 fs. To best exploit the high repetition rate of our laser, every single pulse of light should correspond to a single bit of the random generated raw key and so should be modulated independently on the others. In this situation,

considering the worst case where every bit of the key is different from the previous one (that is a key on the form of $\{10101010101\cdots\}$), the voltage applied to the modulator should be switched from zero to $V_{\pi/2}$ and vice versa every 10 ns, which corresponds to a switching frequency of 50 MHz (Figure 4.1). Achieving this high switching frequency with such high voltage is still a challenge due to the problems shown in the next section.

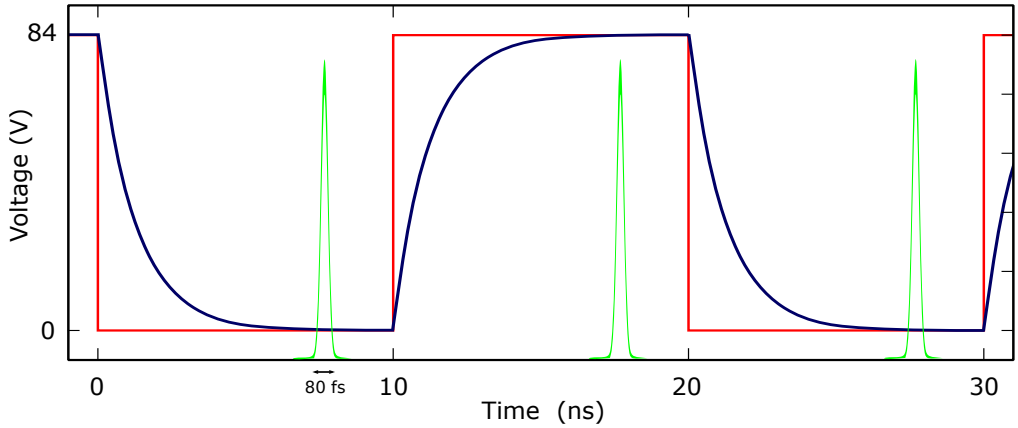


Figure 4.1: The time evolution of the modulation is shown for the ideal case where each pulse (in green) of the train will be modulated independently on the other. The red curve represents the logical signal that pilots the driver; the blue curve represents the effective output voltage of the driver.

A way to modulate the polarization with such high switching frequency would be to use an integrated polarization modulator, which can reach GHz switching frequency and can be modulated with very low voltages. Unfortunately, it was not possible to use this kind of modulator in our setup because of the high losses resulting when coupling the free-space laser with the optical fiber in the input of the modulator. Because of this the solution we have adopted is to group n pulses of the laser together, and perform the modulation on the group of pulses.

The other requirement the driver should guarantee is to reach a steady state before the light pulse transit. Even when the photons are modulated in group this requirement requires that the rising and falling time (switching time) of the driver voltage must be not longer than 10 ns. If the switching time is greater than this value, the first photons of the group will undergo a generic elliptical polarization, leading so to an increase in the QBER. This non-ideal scenario is shown in Figure 4.2.

From Table 3.2 we see that the modulator we want to drive can be regarded as a pure capacitive load with an equivalent capacity of 14 pF.

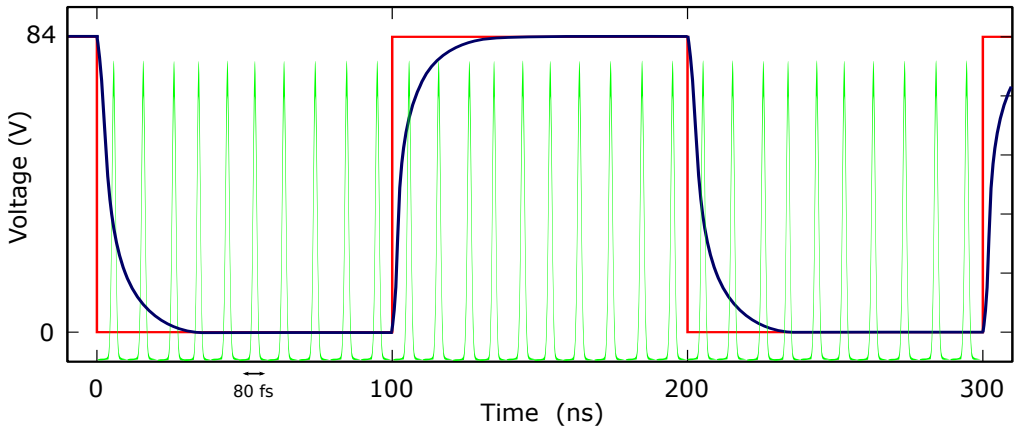


Figure 4.2: The time evolution of the modulation is shown for the non-ideal case where a group of pulses are modulated together. The first pulses of the group will undergo a wrong polarization because the voltage on the modulator has not yet reached the steady state. The red curve represents the logical signal that pilots the driver; the blue curve represents the effective output voltage of the driver.

Hence the driver modulator can be any electronic circuit able to charge and discharge a capacitor satisfying the temporal requirements stated above.

4.3 Theoretical preliminary notions

The typical circuit needed to charge (or discharge) a capacitor can be modeled as an RLC series circuit (Figure 4.3). The system response to a stepped input is characterized by a set of parameters. We will recall the most interesting ones as a function of the circuit parameters

$$\zeta = \frac{R}{2}\sqrt{\frac{C}{L}} \qquad \text{Damping factor} \tag{4.3}$$

$$\omega_m = \frac{1}{\sqrt{LC}} \qquad \text{Undamped resonance} \tag{4.4}$$

(4.5)

The damping ratio determines the type of response we will get, as follow

$$\zeta < 1 \qquad \text{Underdamped} \tag{4.6}$$
$$\zeta = 1 \qquad \text{Critically damped} \tag{4.7}$$
$$\zeta > 1 \qquad \text{Overdamped} \tag{4.8}$$
$$\tag{4.9}$$

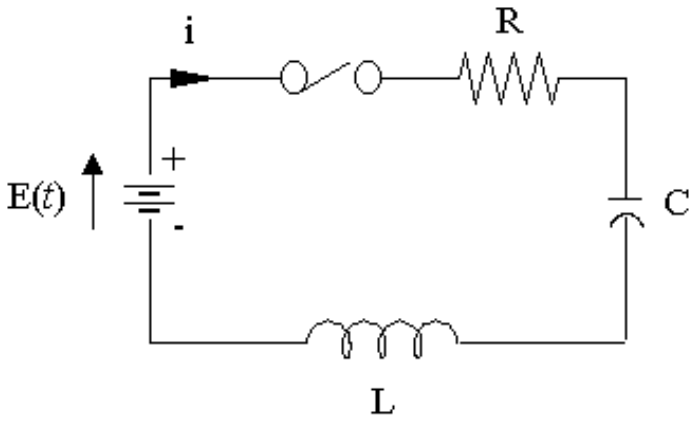


Figure 4.3: RLC circuit model.

In particular, an underdamped response will be characterize by an oscillatory behaviour and fast switching time, an overdamped response instead will be characterize by a non-oscillatory behaviour with slow switching time, and finally a critically damped response will be characterized by an average switching time in absence of oscillations. In Figure 4.4 the three type of response are reported.

The following parameters are of particular interest in the underdamped response

$$\alpha = \frac{R}{2L} \qquad \text{Neper frequency (attenuation)} \tag{4.10}$$
$$\omega = \sqrt{\frac{1}{LC} + \frac{R^2}{4L^2}} \qquad \text{Damped resonance} \tag{4.11}$$
$$t_r \approx \frac{1.8}{w_n} \qquad \text{Rise time} \tag{4.12}$$

The oscillations in the response has a period that is $T = \frac{2\pi}{\omega}$, and exponentially decrease with a time constant $\tau = \frac{1}{\alpha}$. In Figure 4.5 are shown the main parameters that characterize the underdamped response.

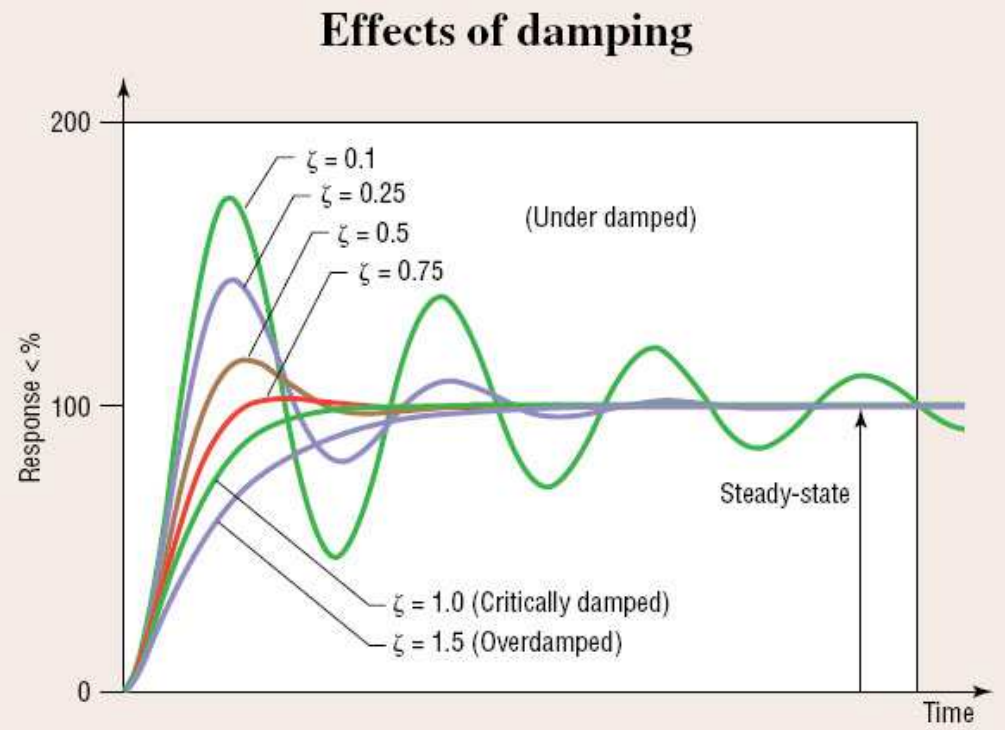


Figure 4.4: Step response of an RLC circuit for different values of the damping factor ζ.

4.4 Half bridge driver

The first circuit we have designed realized a simple half-bridge scheme. In this scheme two n-MOSFETs are connected in series between the power supply voltage V_{DD} and ground, and the output voltage is picked in the node between the two (Figure 4.6). The two MOSFETs are turned on and off alternatively, so that when a MOSFET is on, the other is off and vice versa. By using this configuration, it is important to properly drive the two MOSFETs to prevent the generation of shoot-through currents that can occur if the two MOSFETs are turned on contemporary, thus leading to a short circuit. A MOSFET driver is therefore necessary. Moreover the driver is needed to charge and discharge the gate of the MOSFET very fast, in such a way to achieve very short switching times. The main advantage of the half bridge configuration is that the dissipation of power happens only when a switch occur, so that the output voltage can be kept in a high state or low state for an unlimited time without any power dissipation. Since the output voltage should be modulated as a function of a string of

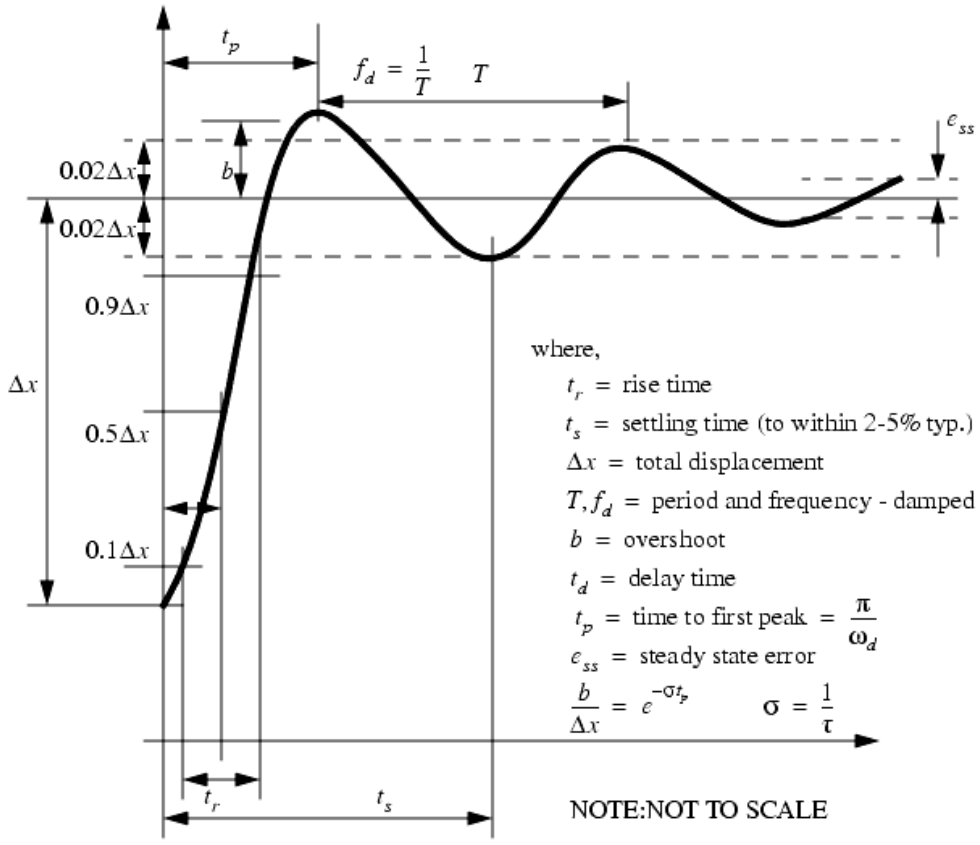


Figure 4.5: Parameters of the underdamped step response.

bit as follow

$$\{0,0,1,0,1,1,1,\cdots\} \rightarrow \{0,0,V_{DD},0,V_{DD},V_{DD},V_{DD},\cdots\} \tag{4.13}$$

even though in the worst case the voltage need to be changed every bit, in an average case, where there are some bit sequence with the same value, the voltage can be maintained steady leading to a lower power dissipation.

Although the scheme is pretty simple, the high voltage and the high-switching frequencies involved require a careful choice of the components to be used, and a correct layout design.

4.4.1 Electronic components and layout

The high-switching frequency the circuit will be subjected make the presence of stray inductance relevant. In the particular case of a half-bridge

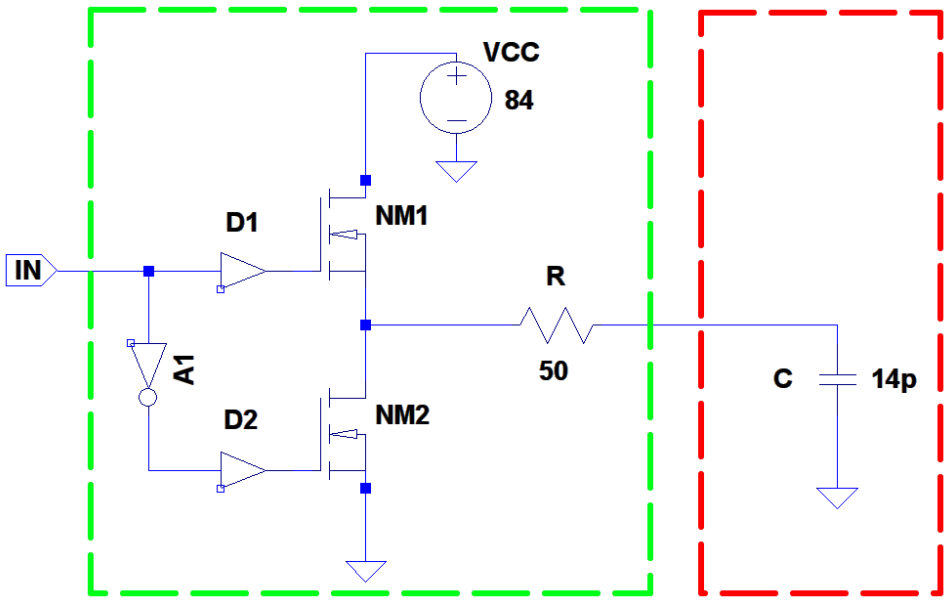


Figure 4.6: Half-bridge driver schematic (green rectangle). An external TTL signal drives a non-inverting high-side driver and an inverting low-side driver. The two drivers turn on and off two n-MOSFETs alternatively making the central node voltage to switch between 0 and V_{DD}. A damper resistance is placed in series with the load to reduce the oscillations in the output voltage. The output voltage is applied to an equivalent capacitive load of 14 pF (red rectangle).

structure, where there are no resistive components other than the small MOSFET internal resistances, the stray inductance can couple with the capacitive load leading to oscillatory behaviour of the output voltage. Stray inductance mainly arises from the presence of wires and from the component package connections. In particular the MOSFET has a gate parasitic inductance (L_G) that when subjected to high frequency act as an open circuit, thus isolating the MOSFET gate from the driver. Moreover, the parasitic source inductance (L_S) can lead to oscillatory state because of the negative voltage drop that happens when a large current derivative is present, which is a consequence of a voltage switch on the MOSFET [20]. To reduce the stray inductance we have implemented the circuit in a Printed Circuit Board (PCB) using only Surface Mounted Device (SMD).

In our layout (Figure 4.7) we have used a single FDS89161LZ chip that is a SO-8 package containing two n-MOSFETs. The MOSFET can sustain a drain-source voltage up to 100 V and can achieve theoretically

switching times lower than 10 ns, thanks to the low on-state resistance. The particular model of MOSFETs has a low input capacitance, needed to reduce the power dissipation on the driver. Having two MOSFETs on the same die assures that the specifics are almost identical. In particular, it is important that their switching and delay times are almost identical to prevent the appearance of shoot-through currents, which can be destructive for the circuit. A MAX15019BASA+ MOSFET driver have been used to drive the two MOSFETs. This integrated circuit is specifically designed to drive two n-MOSFETs in a half bridge configuration. It can be driven with a single TTL input which commands both the internal time-matched drivers. It provides a connection for a boost capacitor, required to ensure an adequate charge to switch the high-side MOSFET. Further, it provides an internal break-before-make logic circuit able to prevent shoot-through currents during the output state changes. The driver is mounted as close as possible to the two MOSFETs to minimize stray inductance. In the output stage, a resistance is connected in series with the load to reduce the undesired oscillations and an optional zener diode can be mounted to clip the overvoltage. To dissipate the heat generated by the driver and the MOSFET packages, an heat sink have been mounted on the top of the board and connected to the component with a silicon thermal interface. To provide the high voltage to the circuit two bench power supply have been connect in series allowing to obtain a voltage up to 95 V. To protect the two power supplies against harmful reverse voltage during the power-on phase, a diodes protection system have been implemented on the board. Finally both the MOSFET and driver power supply have been equipped with filter capacitors to stabilize the voltage.

4.4.2 Power dissipation

The more the switching frequency is raised the more power will be dissipated on the components, and so it needs to be properly dissipated. In a full cycle required to fully charge and discharge a capacitor, the total power dissipation is given by

$$P = C_L V_{DD}^2 f \tag{4.14}$$

where C_L is the capacitance of the load, V_{DD} is the power supply voltage and f is the switching frequency.

In the output stage the power is dissipated over the internal resistance of the MOSFETs. Considering that $C_L = 14$ pF, $V_{DD} = 90$ V and a switching frequency of 1 MHz the resulting power dissipation is 113.4 mW

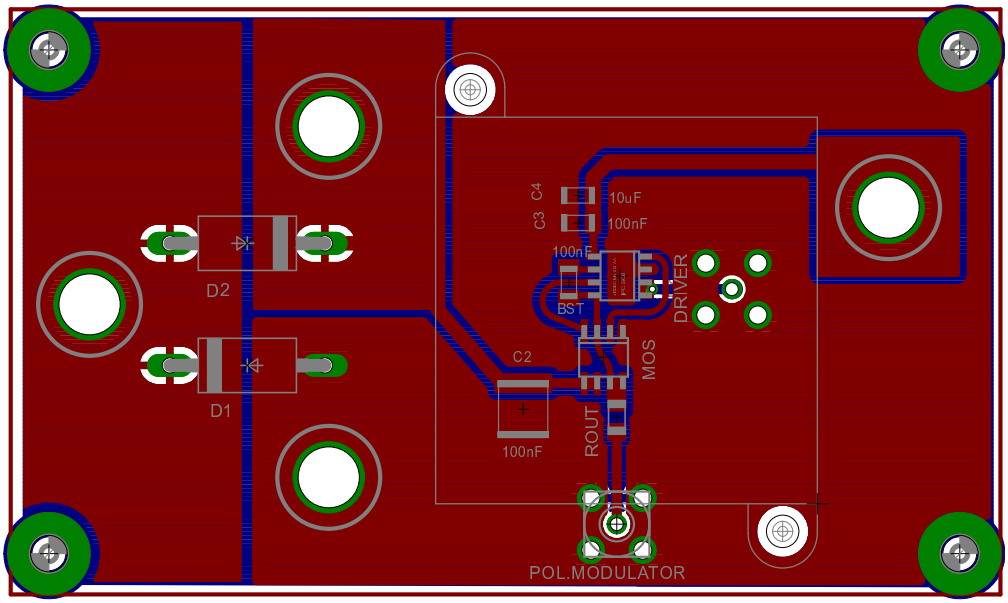


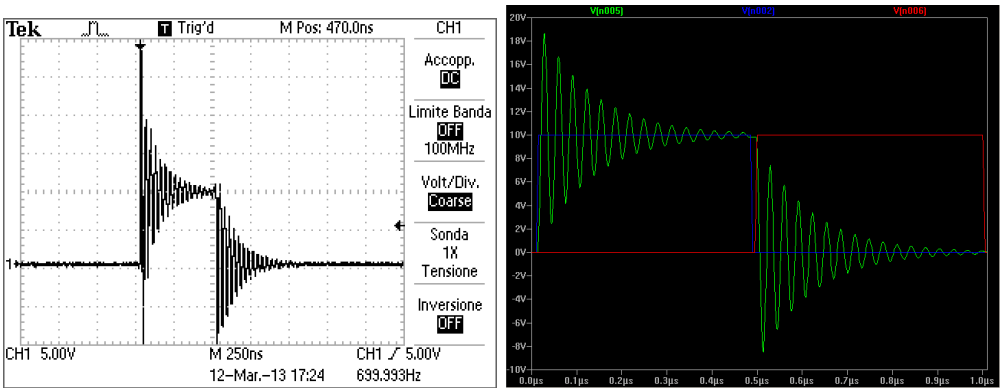
Figure 4.7: Half-bridge driver PCB layout.

which can well sustained by the MOSFET package without the need of a particular heat-sink. The most critical power dissipation source is the MOSFET driver, in fact it needs to move a greater amount of charge to drive the gate of the MOSFETs. The input capacitance of the particular chosen MOSFET is very low to minimize the power dissipation in the driver, and its maximum value is $C_{iss} = 302$ pF. Other than this, the driver dissipates more power also to charge the bootstrap diode.

4.4.3 Results

The electronic signal was first measured with an oscilloscope probe without the modulator attached and without any damping output resistance. The load has been provided by the 10x attenuated probe equivalent capacitance which have been estimated in about 15 pF. The output capacitance of the MOSFETs also contributes to form the total load capacitance. This has been estimated in 130 pF. The waveform measured is shown in Figure 4.8a. From this measure and solving the system of equations (4.10) (4.11) we have derived a total resistive component of 2.24 ohm and a total stray inductance of 187 nH. In Figure 4.8b is reported the result of the SPICE simulation performed with these values. Feeding the value of capacitance and inductance derived to (4.3) we found the value to be as-

signed to the damping resistor to obtain a critically damped response. The value obtained is 75 ohm, but we inserted in the circuit a 50 ohm resistor to achieve better rise time. What we have seen is that the falling edge doesn't show the ringing any more while in the rising edge (Figure 4.9a) still suffer from an anomalous oscillatory behaviour which correspond to the first peaks that can also be seen in Figure 4.8a and that doesn't agree with the theoretical prediction. Finally in Figure 4.9b is shown the modulated optical pulse, obtained by operating the driver at 60 V. We see that it is possible to obtain a very good rise time under 10 ns and a falling time in the order of 25 ns, even though there is a strong oscillation in the first 50 ns of the high state of the pulse. A further increase of the damping resistance will eliminate the oscillation but will lead to a too long falling time.



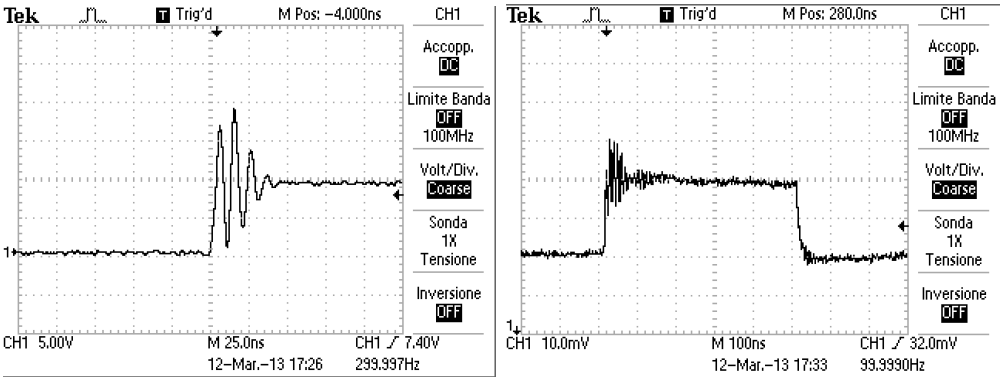
(a) Electrical output (b) SPICE simulation

Figure 4.8: Half bridge driver undamped output. When no damping resistor is placed in series with the output the driver shoes an excessive oscillatory behaviour, which can't be used to drive the modulator.

We have seen that the circuit can operate in a stable way with switching frequency up to 500 KHz. The circuit has been tested with frequency up to 1 MHz but in this range the probability of a driver breakdown is high. The breakdown was probably caused by a non perfect heat sink structure.

We finally note that the oscillatory behavior will lead to the non perfect polarization of about 5 optical pulses, so that the QBER will be slightly increased. Considering an operating frequency of 500 KHz which correspond to a period of 2000 ns we can estimate the increase of the QBER in the worst case as the ratio between the RMS value of the oscillation and the steady value of the signal, multiplied by the fraction of the switching period where the oscillations happen. With our data this QBER increment

has been estimated in 3%, which can be considered enough good for our application.



(a) Electrical output (b) Optical output

Figure 4.9: Half bridge driver damped output. When a 50 ohm resistor is placed in series with the load, the driver is able to switch a high voltage within few tens of ns with a minimal oscillatory behaviour.

4.5 Pull-up resistor driver

To try to reach higher switching frequency we choose to build a through-hole components circuit, which can be easily cooled with the use of properly heat sink. One of the disadvantage of the through hole components is that they carry higher stray inductance. The other problem is that it was not possible to find components with the required specifics that carry two MOSFETs in the same package. Moreover it was not possible to find integrated driver specific for a half bridge configuration. This means that the timing management to correctly drive a half bridge structure in order to prevent shoot-through currents and good rising and falling times, would have to be made manually in the software of the FPGA that control the two drivers. So we prefer to try a new scheme which requires the use of a single driver and a single MOSFET (Figure 4.10). This configuration consists in a series of a pull-up resistor and an n-MOSFET connected between V_{DD} and ground. The output voltage is picked in the node in between the two. The main disadvantage of this configuration is that a constant current flow through the resistor when the MOSFET is kept in an on-state, so that the power dissipation is much higher than a half-bridge configuration.

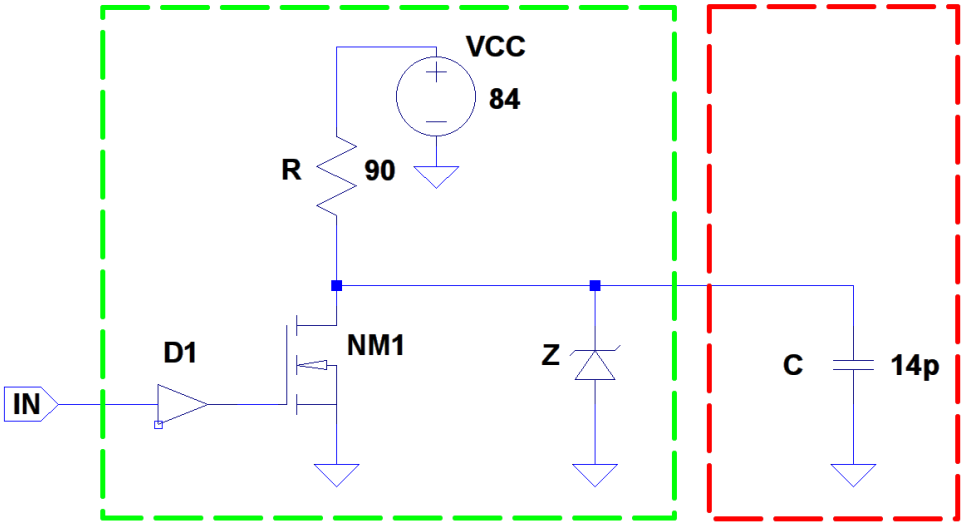
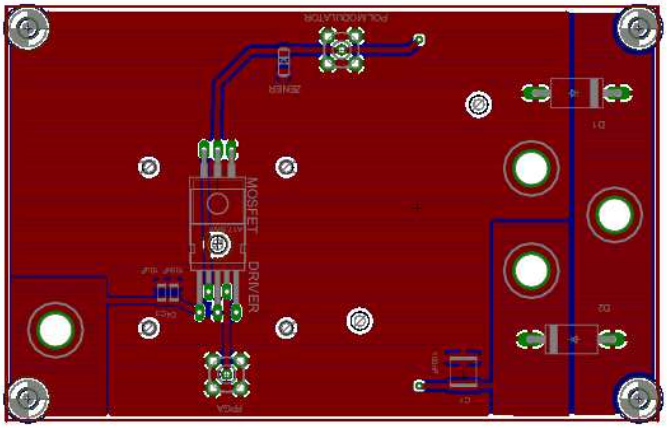


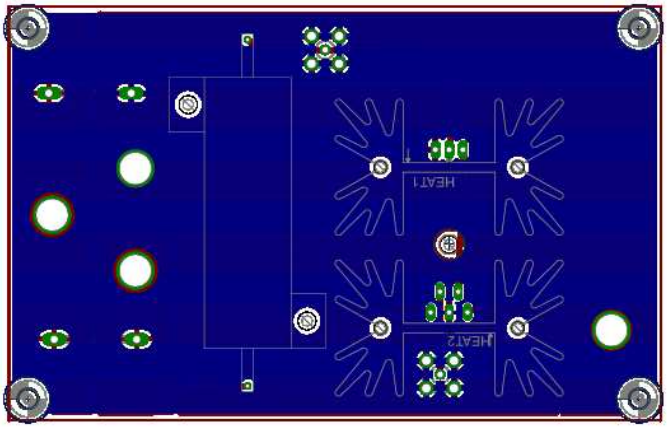
Figure 4.10: Pull-up resistor driver schematic (green rectangle). An external TTL signal drives a non-inverting low-side driver. When the n-MOSFETs is off, the voltage in the output node is kept at V_{DD}. When it is turned on, it brings the potential of the output node to ground, and a constant current begins to flow in the resistor, thus making it dissipate power. A zener diode is placed in parallel to the load to clip any overvoltage. The output voltage is applied to an equivalent capacitive load of 14 pF (red rectangle).

4.5.1 Electronic components and layout

The circuit has been realized using an IRF610 n-MOSFET, which provide a very low input capacitance and switching time under 17 ns. The driver is an IXD614 and it is able to operate the MOSFET at its maximum speed. A 180 ohm power resistor able to sustain up to 35 W was used. In the final configuration two of these resistors have been mounted in parallel to halve the resistance. A zener diode with 91 V breakdown voltage has been placed in parallel with the load in order to cut any overshoot voltage. All the components have been mounted on a dual layer PCB board. Also this circuit has been equipped with a protection circuit to connect two bench power supplies in series. The logical input and the high voltage output are connected to the FPGA and to the modulator driver through two SMA cables plugged in the SMA connectors mounted on the board. The PCB layout of the circuit is shown in Figure 4.11 while a picture of the final PCB board is reported in Figure 4.12.



(a) Top layer



(b) Bottom layer

Figure 4.11: Pull-up resistor driver PCB layout.

4.5.2 Power dissipation

The most critical component in this circuit is the resistor. In fact the average power dissipated on it is

$$\frac{1}{2}\frac{V_{DD}^2}{R} \tag{4.15}$$

due to the fact that the MOSFET will be in an on-state half of the time, since it follows the random modulating sequence of bits (see (4.13)). Oper-

Figure 4.12: Pull-up resistor final PCB board.

ating the circuit at with a voltage of 90 V will lead to a power dissipation over each of the resistance of 22.5 W.

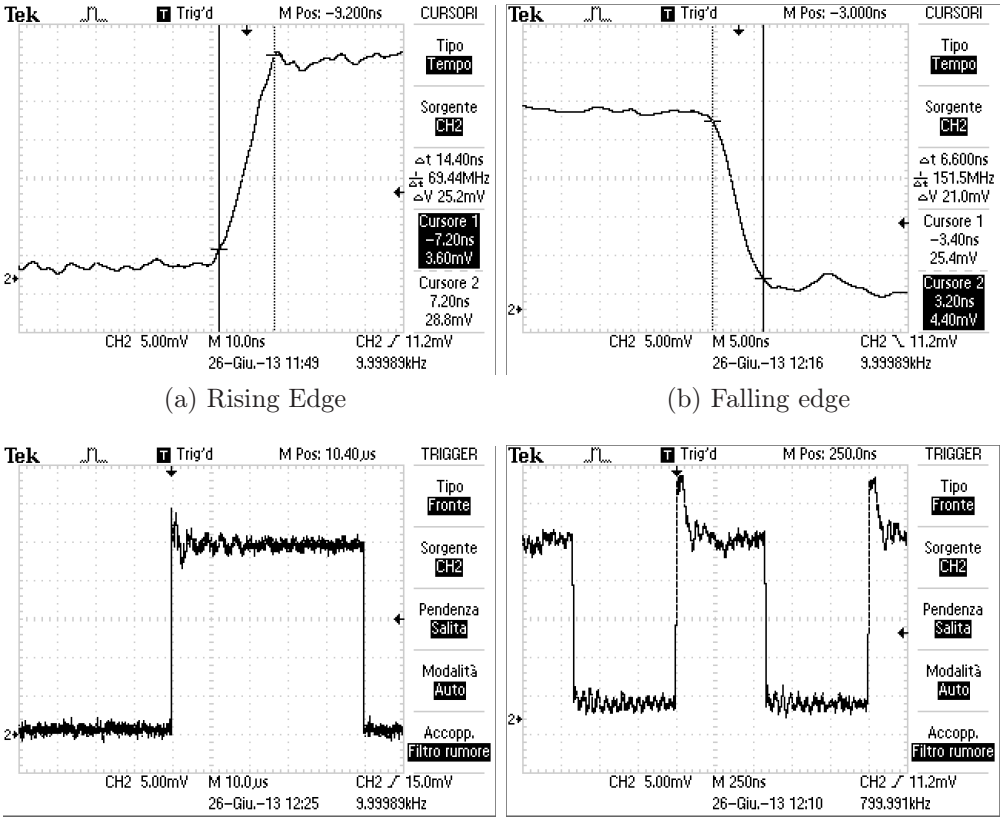
Both the MOSFET and the driver have been provided of heat sinks in order to avoid components failure due to high power dissipation. Finally a fan has been mounted on the top of the board to cool all the heat sinks.

4.5.3 Results

Firstly, the driver have been tested with a 90 ohm resistor, obtained as a parallel of two 180 ohm resistors, and

without the zener diode in the output. What we have seen is a fast switching time accompanied by an oscillatory behaviour like in the case of the half-bridge driver. Instead of increasing the output resistance to reduce the oscillations we mounted the zener diode in parallel with the load and we were able to drastically reduce the oscillations. The modulated optical output of the polarization modulator driven by this circuit with $V_{DD} = 84V$ is shown in Figure 4.13. We were able to achieve switching time in the order of 15 ns both in the rising edge and in the falling edge. Some oscillations there are still present right after the rising edge, but their RMS value is sufficiently low to affect only little the QBER. With this configuration we have reached switching frequency up to 800 KHz without any failure of the components, probability thanks to the better heat sink system. We have noticed that when the switching frequency is increased the voltage

overshoot tends to rise. Even tough, we can see in Figure 4.13d that the overshoot affect only a tenth of the period. In an average case, where the voltage is not switched every bit, the effect of the overshoot on the polarization errors will be even less important.



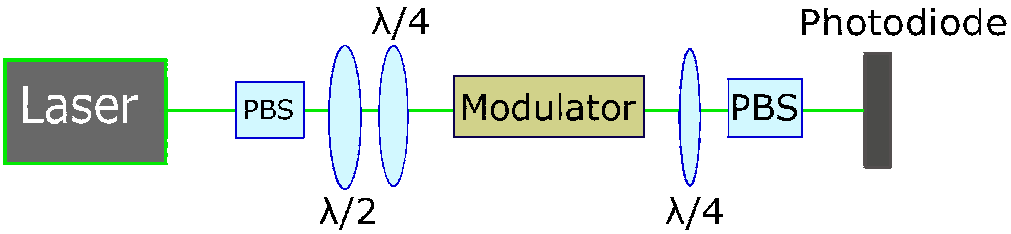
(a) Rising Edge (b) Falling edge

(c) 10 KHz switching frequency (d) 800 KHz switching frequency

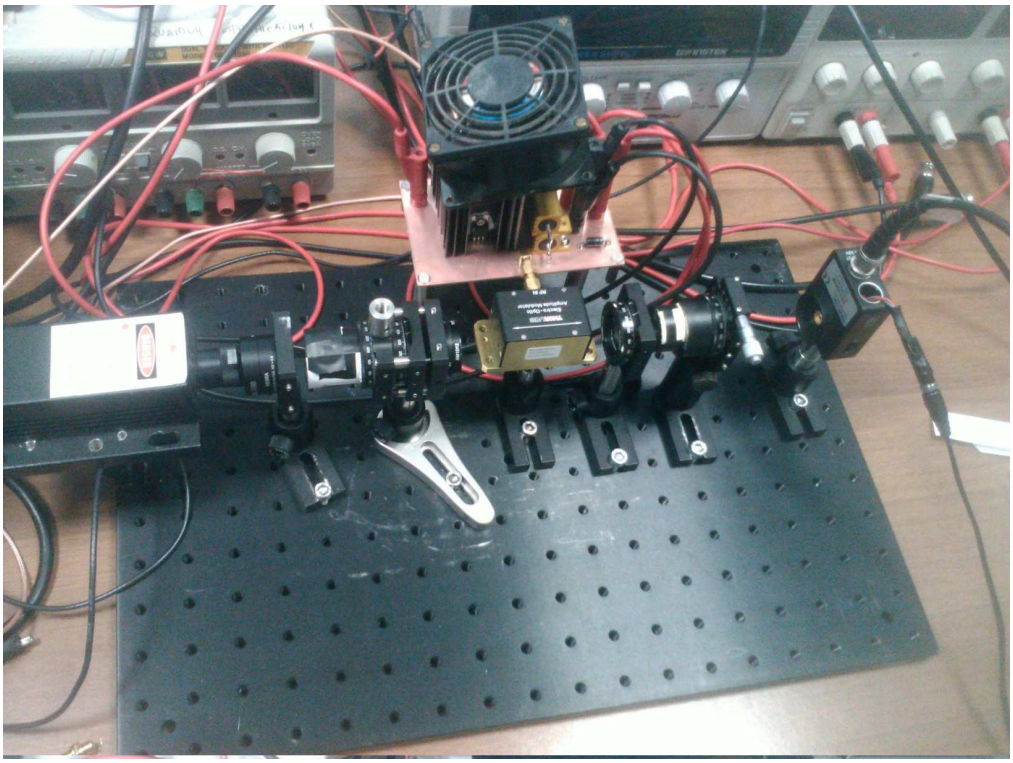
Figure 4.13: Optical output from the polarization modulator at different switching frequency ($V_{DD} = 84V$).

Finally we evaluated the quality of the polarization obtained after the modulation by calculating the visibility of the V and L polarization (Figure 4.15). To achieve this we have used the optical setup shown in Figure 4.14.

The optical power of the components of the output light beam was first measured in the H/V basis obtaining a visibility of the 98.8% for the V polarization, then it was measured in the L/R basis obtaining a visibility of 94% for the L polarization when a voltage of 84 V was used and 98.7% when a voltage of 90 V was used (Figure 4.15). From this last observation



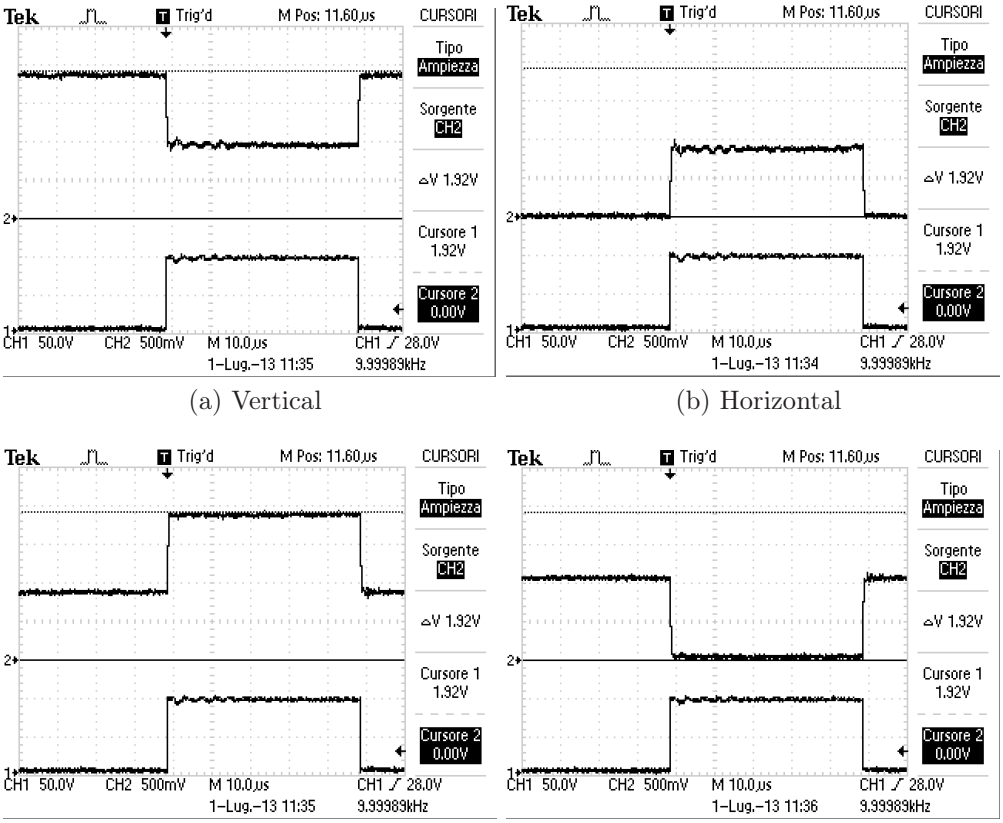
(a) Optical scheme



(b) Real implementation

Figure 4.14: Polarization quality measure optical setup. A 532 nm laser beam has been vertically polarized. The resulting bean has been passed through a series of a half-wave retarder and a quarter-wave retarder in order to pre-compensate any change in the polarization made by the modulator. In this way the beam out coming from the modulator in a rest condition is vertically polarized. A quarter-wave retarder has been placed at the output of the modulator in order to change the measurement basis from H/V to L/R. The final PBS allows performing the measurement in the H/V basis. The optical intensity has been measured with a fast photodiode.

we have concluded that the polarization modulator half wave voltage must be greater than the one specified in the datasheet. Moreover with a voltage of 90 V our driver achieved better result in term of oscillations due to the fact that the zener was working nearer to its breakdown voltage.



(a) Vertical (b) Horizontal

(c) Circular left (d) Circular right

Figure 4.15: A vertical polarized laser beam is modulated and become circularly left polarized. The components of the obtained polarization are measured in the H/V basis and in the L/R basis to estimate the quality of resulting polarization. In the upper part of the graph is shown the optical power, while in the lower part is shown the electric pulse.

Chapter 5

QKD system controller

A quantum cryptographic system requires in general an electronic controller with high timing accuracy and computation capabilities to properly work. In our case the controller is required to drive the polarization modulator driver in order to prepare the qubit to be sent over the quantum channel, and to control the two shutters present in the system. In this section we firstly introduce the shutter scheduling protocol we have used and then we will briefly discuss the current FPGA implementation. Finally we will show the results obtained when the FPGA have been integrated in the real QKD system realized in the MLRO station.

5.1 Shutter characterization

The shutters used in the system are two Thorlabs SH05. The clear aperture has a diameter of 12.7 mm [21]. The shutters is characterized by the following four timing parameters

- **Open/close delay** It is the time that passes from the instant when the logical input is given, to the instant when the shutter begins to open or close respectively.
- **Opening/closing time** It is the time that passes from the instant when the shutter begins to open (close) to the instant when the shutter is fully open (close).
- **Small area opening/closing time** If the laser beam to be blocked is smaller than the full aperture of the shutter the opening and closing time can be regarded as the time needed to fully block or unblock the beam. These times are usually smaller than the opening and closing times.

- **Pulse rate** The maximum frequency the shutter can be operated.

The timing parameter for the SH05 shutter have been evaluated in the laboratory by measuring with a photodiode the optical intensity of a laser beam, made to pass through the shutter. The variation of the intensity due to the shutter action traces a waveform from which the timing parameters can be extrapolated. The results are reported in Table 5.1.

Direction	Delay	Switching time	
		⌀12.7 mm	⌀0.5 mm
Open	9 ms	2 ms	0.4 ms
Close	11 ms	4 ms	0.5 ms

Table 5.1: Thorlabs SH05 shutter timing specification

Another important thing we got from the measures is that the shutter can be operated at frequency higher than 10 Hz, that means it can there be more than one open/close cycle within 10 ms. The limitation we have seen is that if from a closed position of the shutter, a command of the type open-close-open (where the close duration is on the order of 10-15 ms) is given to the shutter, there is the possibility that the shutter does not fully close. In particular, this happens when the first open command is smaller than 20-25 ms. This will be of particular interest for the transmission and reception scheduling we are going to illustrate in the next section.

5.2 Transmission and reception shutter scheduling

As already stated in Section 2.4.2, the QKD system we have implemented will operate the transmitter and the receiver in different moments to avoid unwanted background noise in the receiver. The transmission of the qubits should start right after the laser ranging pulse is sent to the telescope, and should last until that pulse returns to the ground station after being reflected by the satellite. The reception should begin immediately after receiving the laser ranging pulse. In this way the laser ranging pulse, which trigger the START and STOP signal, can be used as a reference to correlate the sent and the received qubits of the QKD system. The alternation of the transmission and reception phases will be achieved with the use of the two shutters. Moreover the shutters are required to block all

the high energy laser pulses generated by the laser ranging system to avoid damages in the PMT. The ideal time diagram of the shutters is shown in Figure 5.1a.

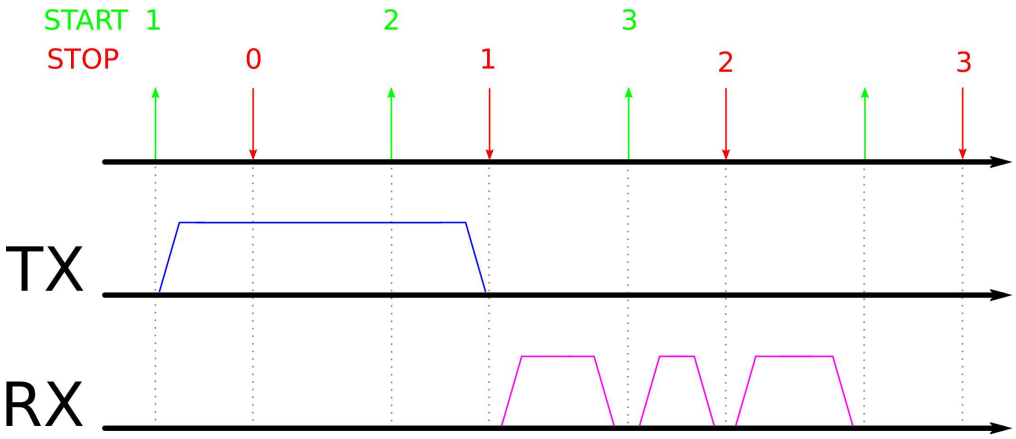
If we consider a situation where a LEO satellite, which orbit is up to 2000 Km, is used to back-reflect the laser pulse, we get that the Round Trip Time (RTT) is on the order of 20-25 ms [22]. Since the useful time for the transmission of the qubits corresponds to the RTT, we see that in this case only the 25 % of a 10 ms cycle would be used to exchange the key, that means the protocol has a 25% *temporal efficiency*. The lower is this value the lower will be the bit rate of the generated key. Beside this, it would be completely impossible to send any qubits because the shutters will not be able to fully open and close in such a short time. Because of this, the experiment can only be performed using MEO satellites, which have a RTT that varies in the range 100-200 ms according with the specific satellite orbit and the position respect the zenith.

If we consider the time between two START signals (10 ms) as the base time slot, we can divide a transmission/reception cycle in three of these time slots. Referring to Figure 5.1, we see that the first slot begins in correspondence of the first laser ranging pulse (START-1). In this slot only the transmitter is active. The third slot begins with START-3 and here only the receiver is active. The first returning laser ranging pulse (STOP-1) will fall in the second time slot. When this pulse is registered the system should switch from transmission to reception. Since the position of STOP-1 is different for different MEO satellites, we can have the following different situations

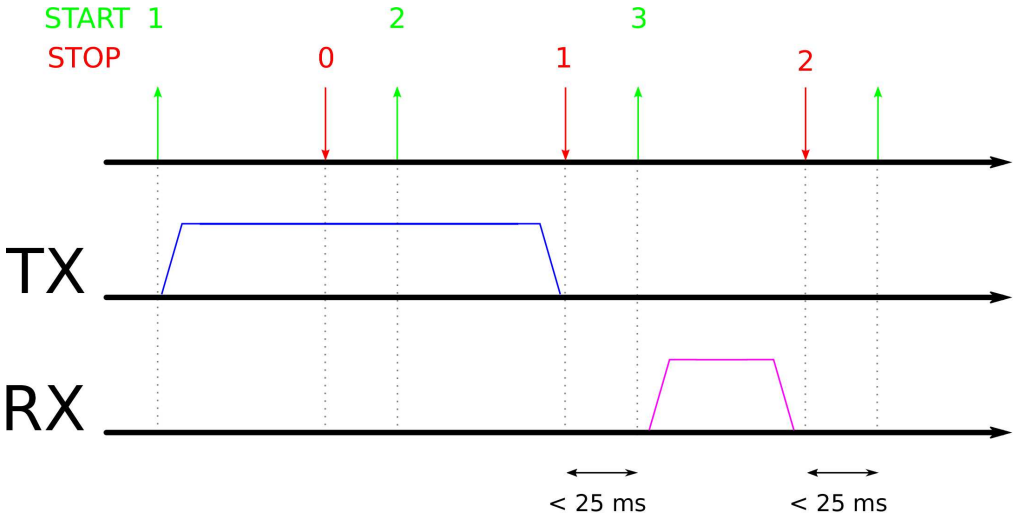
- The RTT is 150 ms (ideal case). This means the generic START and STOP signals are separated by 50 ms and the STOP-1 fall in the middle of the second slot. In this case the transmission and reception time are the same and the QKD system has a temporal efficiency of 50%.

- The RTT is in the range 125-175 ms. In this case the transmission and reception times are asymmetric. The useful time for the QKD protocol to collect qubits corresponds to the minimum of this two times. If the transmission time is higher than the reception time means that some transmitted qubits will be not received, whereas in the opposite case the receiver will be active even when no qubits are expected to come back.

- The RTT is in the ranges 100-125 ms. In this case the START and STOP signals are too close and the shutter will be kept close



(a) Average case



(b) Worst case

Figure 5.1: Shutters open/close time diagram. The transmission and the reception phase are separated in time. The receiver shutter is closed when a START or STOP signal is expected, to protect the receiver PMT. If the distance of two generic START and STOP signals is less than 25 ms the receiver shutter is kept close between them to avoid missing closure. The position of the STOP-1 signals (which varies as a function of the altitude of the considered satellite) determines the temporal efficiency of the protocol.

between START-3 STOP-2 in order to avoid a missing closure due to the limited repetition frequency of the shutter. Because of this a small fraction of the sent qubits will be not received. In this case the transmission time approaches the minimum and the time efficiency can be as low as 30%.

- The RTT is in the ranges 175-200 ms. This is the worst case (Figure 5.1b. Here the reception time approaches the minimum and the shutter cannot be opened for most of the third slot because of the proximity of the START and STOP signals. Here the time efficiency can be as low as 15%.

5.3 QKD system controller implementation

We have implemented the controller using a Field Programmable Gate Array (FPGA) (Figure 5.5). In particular we have used an ML605 board equipped with a Virtex 6 FPGA. The board has a 200 MHz clock that can be up scaled up to 700 MHz with the use of the internal PLL logic circuitry. Such clock frequency together with the timing constraint verification tools made available by the board development environment, make possible to drive both the modulator and the shutters with the required precision. The language used to program the FPGA is VHDL.

The FPGA needs two reference signals to properly synchronize our system to the laser ranging one. The first signal (START) comes from a photodiode, and it indicates the exact instant in which the laser ranging pulse is sent to the telescope. A second signal (STOP) is generated by the laser ranging receiver PMT and indicates the instant in which the pulse is received back. Both the signals follow the Nuclear Instrumentation Module (NIM) standard, that means among other things that the signals voltages are negative. Since such voltage cannot be provided as input to the FPGA, we built a two-channel NIM to TTL converter. The converter can translate the signal from one standard to the other without introducing delays and assuring very steep rising and falling edges.

5.3.1 Shutter controller block

A shutter controller block has been realized in the FPGA in order to drive the two shutters. The block implements a state machine that works as follow

1. Initially the state machine is in an idle state in which both the transmitter and the receiver shutters are kept closed.

2. When the first START (START-1) trigger happens the transmission shutter is opened. The state machine stays in this state until the first STOP (STOP-0) trigger happens. To be noted that while the START signal is practically always triggered, the STOP trigger can be not present. In fact if the telescope tracking is not yet stable, there won't be any reflected pulse from the telescope, so that the photodiode won't be triggered.

3. When STOP-0 is triggered, the state machine moves to the next state in which it activate a counter that will be used to predict the temporal position of the next incoming pulses.

4. The state machine moves to the next state when START-2 is triggered and another counter will be started. This counter will be used to predict the next STARTs position. At this point the FPGA uses the two counters to predict the positions of the next leaving and incoming pulses of light without the need of the START and STOP signal. These predictions are used to close the shutters before the instants where the pulses pass.

5. Before the STOP 1 signal, the transmitter shutter is closed and right after the receiver shutter is opened.

6. Finally the FPGA will close the receiver shutter before every expected laser ranging pulse and will reopen it right after, a part from the case when the next pulse is expected within 25 ms from the current pulse.

The characteristic timing parameters of the shutter have been coded into the software, but it is possible to adjust them by changing the position of an array of dip switches mounted on the board. Furthermore, it is also possible to vary the amount of time which the shutter should stay closed before and after the expected pulse. A shorter time allows to increment the temporal efficiency but increases the risk that the shutter does not close in time to fully block the pulse. By using these switches it was possible to quickly calibrate the shutter controller installed in the real setup.

An array of eight leds has been used to show the state of the state machine in order to allow a faster debug.

5.3.2 Modulator controller block

The current implementation of the modulator controller block is pretty simple. In fact it just produces a square wave signal of a chosen frequency in correspondence to the transmission phase. The square wave produced will drive the polarization modulator to produce the desired qubits. The square wave needs to be correctly aligned in time to the reference START signal in order to allow the time-tagger to discriminate the different polarized photons.

Of course once the experiment will be proved to work, the modulator controller can be extended in order to drive the modulator with a true random key.

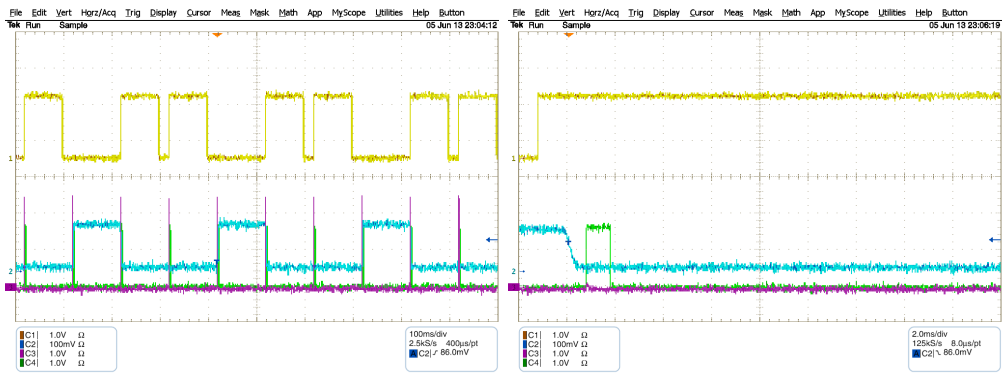
5.4 Results

The FPGA controller have been integrated and tested in the MLRO laboratory. A first test was performed by using as input to the FPGA two logical signals (not the ones from the photodiodes) for the START and the STOP. The first signal is a 10 Hz signal used as reference time by the source laser of the observatory, while the second signal is a prediction of the STOP signal that can be extrapolated from the data collected by the laser ranging system when a satellite tracking is ongoing. In Figure 5.2 is shown the time diagram for the transmission shutter. As we can see the controller is able to predict the position of the start and stop signals and thus is able to close the shutter in time. In Figure 5.3 are shown the time diagrams for the receiver shutter for different RTT. As we can see different relative position between the START and the STOP signals will lead to different temporal efficiencies.

Finally the QKD system controller has been operated in the laser room in a real operative situation. Also in this case it was able to correctly drives the two shutter preventing so any damage to the PMT.

5.5 Future development

We aim to further develop the QKD system controller in order to support more advanced functions. An already work in progress update of the software will allow to fully control the parameters of the controller directly from the PC in real time by exploiting the Ethernet connection present on the board. A PC interface program has already been implemented even though the FPGA UDP block is not yet completed (Figure **??**). Moreover

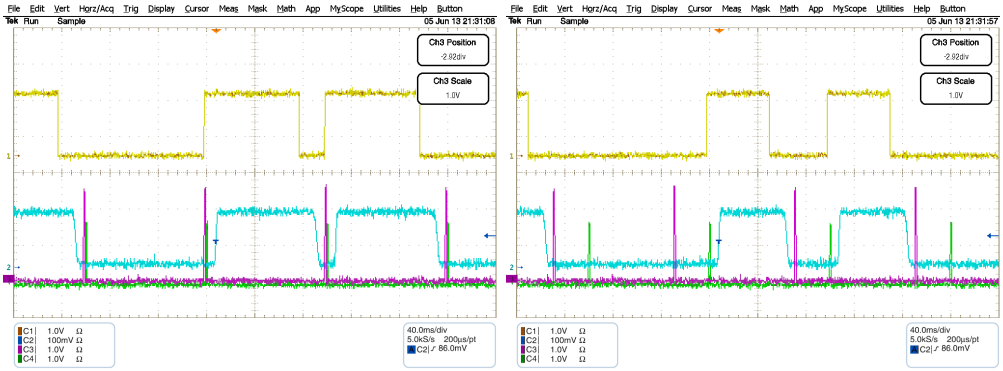


(a) Panoramic view (b) Zommed view

Figure 5.2: Shutter controller test results - Transmission. In figure are shown the START (violet) and STOP (green) signals, the logical command sent to the receiver shutter (yellow) and the real state of the transmission shutter (blue).

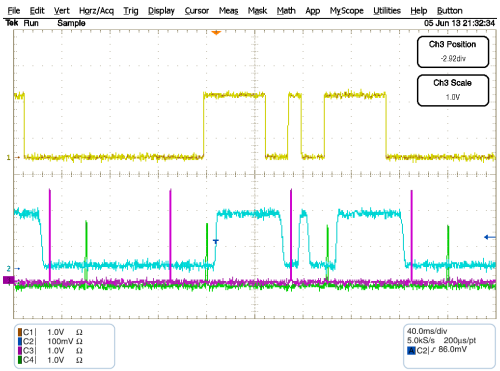
the PC connection with the FPGA can be used to stream a random key directly from the computer in order to operate the QKD system in real time.

To increase the temporal efficiency of the protocol we recently think of a new setup that can be employed. This consists in placing the transmission shutter in front of the MLRO source laser in order to block also the laser ranging pulses when the system is in the reception phase. This will eliminates two out of three START and STOP signals so that it won't be necessary to block them, thus leaving the receiver shutter open for a longer time. Moreover this will reduce the optical background noise generated by the strong light pulses of the laser ranging system. Of course the feasibility of this idea needs to be discussed with the engineers of the MLRO since it will modify the laser ranging system.

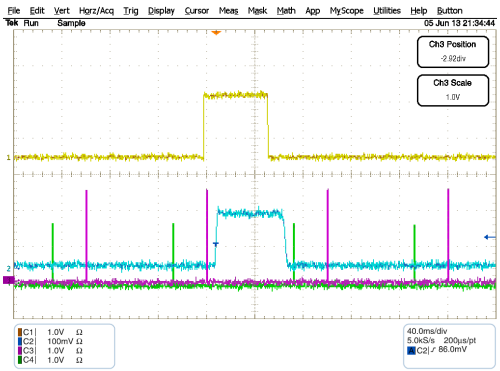


(a) RTT = 102 ms

(b) RTT = 130 ms



(c) RTT = 131 ms



(d) RTT = 172 ms

Figure 5.3: Shutter controller test results - Reception. In figure are shown the START (violet) and STOP (green) signals, the logical command sent to the receiver shutter (yellow) and the real state of the receiver shutter (blue).

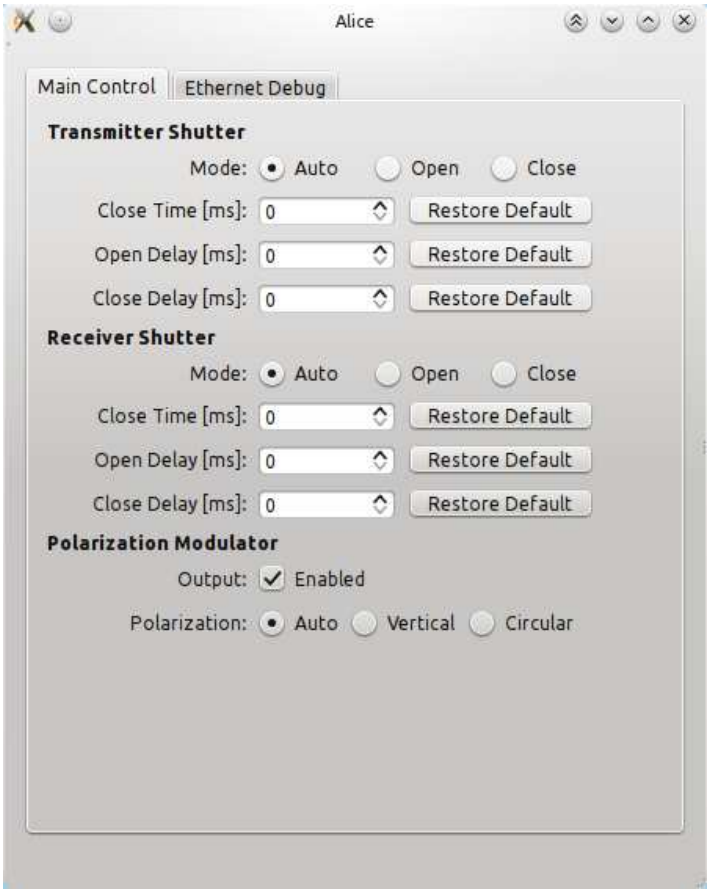


Figure 5.4: QKD system controller PC interface.

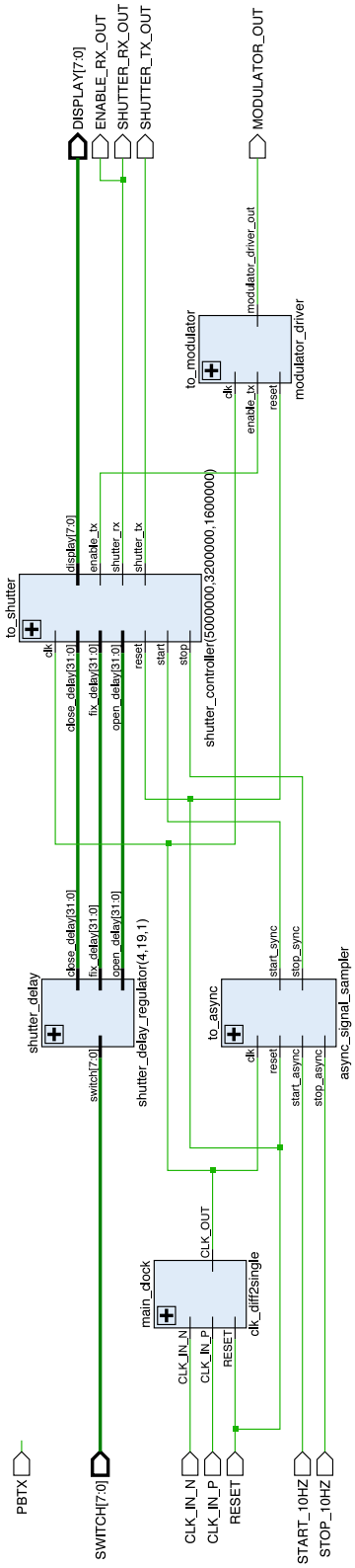


Figure 5.5: Block diagram of the QKD system controller

Conclusion

In this work we have presented the architecture of a QKD system realized upon the existing facilities of the satellite laser ranging station located in Matera, which aims to be the first system to be able to operate a full QKD protocol between a satellite and a ground station.

In particular we address the problem of the implementation of the part of the transmitter that is responsible of the qubits state preparation. The qubits can be prepared in two different state of polarization by using an electro-optic polarization modulator which has been analyzed in detail. We then presented the high voltage driver which has been realized in our laboratory. In particular we were able to operate the modulator with switching frequencies up to 800 KHz while providing a quite stable output that guaranteed an elevated quality of the polarization impressed to the photons.

Then we presented an FPGA implementation of a QKD system controller which has been firstly accurately tested in the laboratory to assure that it could be used to shield the photodiode from the high energy pulses of the laser ranging system. Then it has been tested in a real operating condition, thus proving its efficacy. We also presented a possible improvement in the optical setup, which implies positioning the shutter in front of the MLRO source laser, in order to increase the temporal efficiency of our system.

Thanks to the work presented here all the pieces of the QKD system are now complete, so that the full system could be tested. Unfortunately during the preliminary test of the system in the MLRO station, the telescope receiver has suffered some problems so that we were unable to carry out the full experiment. Soon we will be ready to test the system again, and if the test will gives positive results, we will finally prove the feasibility of satellite QKD, making so the first step towards the creation of a global quantum cryptographic satellite networks.

Bibliography

[1] R. Ursin and F. Tiefenbacher, "Entanglement-based quantum communication over 144 km," *Nature Physics*, 2007.

[2] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New Journal of Physics*, vol. 10, p. 033038, Mar. 2008.

[3] D. Davies, "A brief history of cryptography," *Information Security Technical Report*, vol. 2, pp. 14–17, Jan. 1997.

[4] C. E. Shannon, "Communication theory of secrecy systems," *M.D. computing : computers in medical practice*, vol. 15, no. 1, pp. 57–64, 1948.

[5] T. Helleseth, ed., *Advances in Cryptology — EUROCRYPT '93*, vol. 765 of *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, July 1994.

[6] S. Goldwasser and M. Bellare, "Introduction to Modern Cryptography," 2008.

[7] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," *Nature Photonics*, vol. 6, pp. 773–776, Oct. 2012.

[8] G. Benenti, *Principles of quantum computation and information: Basic tools and special topics*. 2007.

[9] H. Weier, *Experimental Quantum Cryptography*. PhD thesis, Ludwig-Maximilians-Universität München, 2003.

[10] D. Bacco, *Comunicazione quantistica finalizzata alla realizzazione di chiavi in spazio libero*. PhD thesis, July 2011.

[11] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International ...*, 1984.

[12] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, pp. 441–444, July 2000.

[13] C. Fuchs, N. Gisin, R. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," *Physical Review A*, vol. 56, pp. 1163–1172, Aug. 1997.

[14] A. Tomaello, *Quantum communication channels between earth and space and space to earth*. PhD thesis, Jan. 2012.

[15] A. Gardelein, M. Jofre, G. Molina-Terriza, J. Perez, and P. Valerio, "Quantum Transceiver for secure Space Communications," *icfo.eu*, 2009.

[16] N. Baccichet, *Study of the transformation of polarization of a quantum channel in space*. PhD thesis, 2012.

[17] A. Dall'Arche, "Sviluppo di un polarimetro per l'analisi di un canale quantistico fra la terra e lo spazio," Mar. 2010.

[18] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics (Wiley Series in Pure and Applied Optics)*. Wiley-Interscience, 2007.

[19] "Thorlabs Electro-Optic Modulator - Operating Manual." `www.thorlabs.de/Thorcat/15900/EO-AM-NR-C4-Manual.pdf`.

[20] T. Tang and C. Burkhart, "Hybrid MOSFET/Driver for ultra-fast switching," *Dielectrics and Electrical Insulation, IEEE ...*, 2009.

[21] "Thorlabs SH05 Beam Shutter - Operating Manual." `www.thorlabs.com/Thorcat/6900/SH05-Manual.pdf`.

[22] Y. Hu and V. Li, "Satellite-based internet: a tutorial," *Communications Magazine, IEEE*, 2001.

List of Tables

List of Figures