UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede Amministrativa: Università degli Studi di Padova
Dipartimento di Ingegneria dell'Informazione

SCUOLA DI DOTTORATO IN: Ingegneria dell'Informazione
INDIRIZZO: Ingegneria Elettronica e telecomunicazioni
CICLO: XX

Advanced Techniques in Free Space Quantum Communication

Dottorando: Ivan Capraro

Supervisore: Ch.mo Prof. Paolo Villoresi

Direttore della Scuola: Ch.mo Prof. Silvano Pupolin

31 Gennaio 2008

Sommario

Questo lavoro di tesi é incentrato principalmente nelle tecniche avanzate di ottimizzazione per comunicazioni quantistiche, ed in generale applicazioni, a regime di singolo fotone. Il lavoro é inserito in vari progetti che coinvolgono i dipartimenti di Ingegneria ed Astronomia dell'Universitá Degli Studi di Padova.

In particolare il mio contributo é stato lo sviluppo di un sistema di crittografia quantistica, chiamato QuAKE di cui stato realizzato il progetto e si sta terminando l'implementazione. Per lo sviluppo hardware di QuAKE sono state utilizzate alcune tecniche avanzate di filtraggio temporale e spaziale realizzate rispettivamente utilizzando elettronica dedicata e un sistema di ottica adattiva anch'esso realizzato nel nostro dipartimento. E' stato inoltre implementato il software ad alto livello per la crittografia quantistica introducendo ottimizzazioni sia nella struttura logica complessiva che nei singoli algoritmi.

La parte finale di questa tesi é dedicata ad AquEYE, uno strumento astronomico che é stato sviluppato dal nostro gruppo capace di registrare i tempi di arrivo si singoli fotoni da sorgento celesti. In particolare é descritta l'unitá di distribuzione di tempo e frequenza dello strumento, alla quale ho contribuito nell'ultimo periodo del dottorato.

La tesi é suddivisa come segue: dopo una introduzione alla crittografia quantistica (capitolo 1) viene presentato il sistema QuAKE (capitolo 2), vengono descritte l'ottica e l'elettronica del sistema (capitolo 3) e l'apparato di ottica adattiva (capitolo 4), seguono i risultati dei test sul sistema di ottica odattiva all'aperto e integrato nel sistema (capitolo 5) e la descrizione del software ad alto livello con i risultati conseguiti (capitolo 6), la tesi si chiude con la descrizione del sistema di distribuzione tempo e frequenza di AquEYE e dei primi risultati dello strumento (capitolo 7).

Abstract

The main argument of this thesis is the application of advanced techniques for the optimization of single photon communication and in general of single photon applications. The work is inserted in the contest of various projects that involve the departments of Information Engineering and Astronomy of the University of Padua.

In particular my contribution has been the development of a quantum cryptography setup that we called QuAKE. The system has been designed and implemented in our labs and include in the hardware some advanced temporal and spatial filtering techniques. These features has been realized respectively with an ad hoc electronics and with an adaptive optics system, the latter developed entirely in our department. The high level software for quantum cryptography has been also implemented and many optimizations have been realized both in the logical design and in the single algorithms.

The last part of this thesis describes an astronomical instrument, called AquEYE, developed by our group and capable of time tagging single photons coming from celestial sources. In particular a description of the time and frequency distribution unit is given since this has been my contribution to the AquEYE instrument so far.

The thesis is organized as follows: after an introduction to quantum cryptography (chapter 1), the QuAKE system is presented (chapter 2), the electronics and the optical setup are described (chapter 3) as well as the adaptive optics system (chapter 4), it follows a description of the results obtained testing the adaptive optics system outdoor and on the QuAKE system (chapter 5) and the description of the high level software and the related results (chapter 6), last a description on the timing and frequency unit of AquEYE is presented as well as some of the early results of the instrument (chapter 7).

Introduction

This thesis deals with single photon communication, generation and acquisition in a free space channel. In particular the work is focused on the development of engineering techniques for temporal and spatial filtering as well as for the high level software in order to increase the performance of quantum key distribution systems. A study of a temporal filtering system for an astronomical instrument is also presented.

Quantum cryptography, first introduced by Bennet and Brassard in 1984, is a method of exchanging cryptographic keys between two users that exploits the laws of quantum mechanics in order to guarantee its security. Quantum cryptography, normally and more precisely known as Quantum Key Distribution (QKD), is based on the transmission of information encoded in quantum bits (qubits) instead of classical bits. For this reason a dedicated channel is needed in every QKD system for the transmission of the qubits, this channel is called *quantum channel*. Since the first implementations the interest on this technique by the scientific community continuously increased and quantum cryptography is now on its way out of the laboratories and aspires to become the new security standard for global communications. Companies like IBM, Toshiba, NEC, BBN technology but also smaller ones as IdQuantique and MagiQ are presently working on quantum key distribution and many of them have already market products available.

Any QKD setup can be grouped by the protocol it uses and by the quantum channel it exploits in order to exchange the quantum bits. Among the various protocols proposed only some of them have been demonstrated mathematically unconditionally secure: this is the case for example of some which are base on the original idea of Bennet and Brassard i.e. exploiting single photons as information carrier in order to take advantage of the laws of quantum mechanics [40, 76, 81].

Concerning the quantum channel it is interesting to notice that all the commercial QKD system available as well as many scientific experimental setups use optical fiber as quantum channel [83, 42]. A reason for that may be found in the relative simplicity in handling a fiber base quantum channel instead of a free space one, another on the fact that fibers are already widely used whereas optical links are not so diffused.

Although optical fibers offer indeed some advantages, the use of the free space channel would overcome one of the main problem of fiber based implementation: the distance between transmitter and receiver that is limited to about two hundreds Km in the first case [38]. This because a quantum bit cannot be amplified and ri-generated as a classical bit in normal optical communications [50]. Moreover for the same reason it is not clear if the installed fiber infrastructure can be used for QKD.

Using the free space channel instead one could even exploit QKD links between satellites and base stations in order to create world wide quantum communication. Following this idea some recent experiments show respectively the feasibility of a space to earth single photon link (proved by our group at the Univeristy of Padua [4]) and a quantum key exchange over 144 Km [71]. The study and optimization of the free space channel for single photon operations is then strategic for a further development of QKD systems. That is why we decided to build our own system in order to test some new optimization techniques that we have developed.

We started the realization of QuAKE, a QKD prototype, at the end of 2005 although the interest on quantum information in general was already alive in our departments since 2000 with the work of prof. G. Cariolaro, prof. P. Villoresi, and prof. Cesare Barbieri. Beside my contribution to this project which is resumed in this work, a huge amount of work has been done together with Ing. Tommaso Occhipinti mostly on the electronics part and in the high level software.

QuAKE is a low cost prototype, nevertheless it incorporates many improvements with respect to other free space QKD setups. The most important is the use of adaptive optics (AO) in order to compensate for fast atmospheric turbulence induced jitter on the position of received signal [20] . The need for a fast correction of the jitter accumulated during the propagation in QKD has been pointed out many times [75, 35]. Almost all free space QKD experimental setups will benefit from an AO system since in principle the key generation rate of these systems would increase with a better spatial filtering [71, 49, 91]. Spatial filtering means a better optical conjugation between the transmitter and the receiver and a consequent rejection of noisy photons coming from other direction. The AO system which is one of the main argument of this work is fully described here as well as the other details of QuAKE: the control electronics and the high level software.

The electronics is developed using a Xilinx virtex 4 FPGA (Field Programmable Gate Array) in order to guarantee the synchronization between the transmitter and the receiver implementing in this way the so called temporal filtering. Temporal filtering means that the receiver has to know when to expect a photon that was sent by the transmitter. This is another technique that permits noise reduction in single photon communication [22].

Beside that we noticed how many experimental setup were focused on the improvement of the hardware apparatuses for QKD, forgetting that the high level parts of almost any quantum cryptography protocol is also important [10]. We started to develop a Java implementation of the high level software for QKD trying to focus our attention on the integration with the QKD hardware as well as with the final users of the system. We have also worked on the optimization of the algorithms involved in the data processing that goes from the raw material exchanged by the hardware to the cryptographic keys used for encrypting sensible data [21].

In this sense QuAKE, which will be fully operative at the end of 2008, will be a smart, low cost system and we hope it will be able to go out of the lab as many other fiber based QKD prototypes.

The last part of this work describes the time and frequency unit of AquEYE. AquEYE is an astronomical instrument, build for the 182 cm telescope of cima Ekar in Asiago (Italy), that shoul be capable of time tagging each single photon that is arriving to its detectors with a precision of 100 ps. The instrument is a first small prototype of what would be the first quantum astronomy instrument, QuantEYE which has been proposed by our group for the next generation Overwhelming Large telescope (OWL) [19]. The aim of quantum astronomy is to look at the temporal structure of the photons flux in order to characterize its quantum properties but in order to accomplish this task the timing requirements are very strong and also the amount of data that should be collected is very high [18]. In order to have the required precision on time tags and the require accuracy to guarantee long exposure times up to three hours we must feed the instrument with an accurate and stable frequency reference [2, 61]. For this reason designed and characterize a time and frequency unit for AquEYE that exploits a rubidium oscillator for its high stability standards and a GPS receiver in order to guarantee a good accuracy with respect to UTC (Universal Standard Time). The GPS would serve also as synchronizer if multiple telescope operation will be adopted for intensity interferometry measurements.

Contents

Chapter 1

Quantum Key Distribution

This chapter is intended to be a review of the basic concepts of *Quantum Key Distribution* (QKD). Starting from the postulates of quantum mechanics that guarantee the security of such technique we will describe briefly the protocols that one can implement. The chapter ends with some real QKD protocol implementations. Before this introduction i would like to point out that the concept of security is tricky and complex and that anyone who wish to enter this world should well understand the limits and the benefits of any solution and system proposed[1]. This has to be done not only for the system itself but taking into consideration the environment and the social and scientific background. This is to say that Quantum Key Distribution is a very beautiful tool that is trying to find its space in real everyday life, and this seems to be the hardest point in its spreading. That is why in this thesis every concept about security has to be intended in a purely mathematical point of view i.e. regarding only the systems and not the users.

1.1 The Fundaments of Quantum Key Distribution

The security of Quantum Key Distribution is based on the laws of quantum mechanics. In this section we will briefly report the fundamental results that make QKD the most secure technology available in today secure communication. The two important book *"Quantum Computation and Quantum Information"* by M.A. Nielsen, I.L. Chuang [57] and *"The Principles Of Quantum Mechanics"* by Paul Adrien M Dirac [30] has driven the writing of this chapter.

[1] A very good treatment of this concepts can be found in a book by Bruce Schneier [72]

1.1.1 Review of Postulates of QM

The starting point of the quantum mechanical formalism is the Hilbert space over $\mathbb{C}$, with inner product $\langle\cdot|\cdot\rangle$.

Postulate 1 *To any physical isolated system is associated a complex vector space where is define an inner product (Hilbert space) which is called state space of the system. The system is completely described by a state vector, a unitary vector in the Hilbert space.*

This first postulate permits to define the fundamental unit of *quantum information*: the analogous of the classical *bit*.

Definition 1.1 ***(Qubit)*** *A qubit is the simplest quantum mechanics system, a two-dimensional state space.*

Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for a two dimensional state space, then an arbitrary state vector in the state space can be written

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{1.1}$$

where a and b are complex numbers. The values a and b have to satisfy the *normalization condition* for a state vector:

$$\langle\psi|\psi\rangle = 1 \tag{1.2}$$

that implies $|a|^2 + |b|^2 = 1$.

This is the biggest difference between classical and quantum information: as long as the normalization condition is met, the state $|\psi\rangle$ can assume any value between $|0\rangle$ and $|1\rangle$ without being forced to choose one like in the classical case. The state $|\psi\rangle$ is said to be in the **superposition** of the two state $|0\rangle$ and $|1\rangle$.

We recall here the second postulate that describes the temporal evolution of a quantum state $|\psi\rangle$. This is fundamental for *quantum computation* applications.

Postulate 2 *The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi(t)\rangle$ of the system at time t is related to the state $|\psi(t_0)\rangle$ at time t_0 by a unitary operator U which depends only on the times t and t_0*

$$|\psi(t)\rangle = U\,|\psi(t_0)\rangle \tag{1.3}$$

The temporal evolution of a state can be written in the Schrödinger form:

$$i\hbar \frac{d\,|\psi(t)\rangle}{dt} = H\,|\psi(t)\rangle \tag{1.4}$$

where $\hbar$ is the Planck constant and H is the hermitian operator called Hamiltonian of the closed system. This operator describes completely the dynamics of the system.

The third postulate introduces the concept of measurement operators and describes their main properties. As said in the second postulate, a closed quantum system evolves according to a unitary transform, but if an application of quantum information interacts with the system to get some kind of information the system under test is no longer closed. For this reason the system is not necessarily subject to unitary evolution.

Postulate 3 *Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the same space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the system before the measurement is $|\psi\rangle$, the probability that result m occurs is given by:*

$$p(m) = \langle\psi|\, M_m^\dagger M_m\, |\psi\rangle \tag{1.5}$$

and the sate of the system after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|\, M_m^\dagger M_m\, |\psi\rangle}} \tag{1.6}$$

The measurement operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I \tag{1.7}$$

When dealing with systems composed by more than one qubit quantum information can help us with a postulate that describes composite systems:

Postulate 4 *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have a quantum system $\mathcal{H}_i$, $i = 1, .., n$ and system $\mathcal{H}_i$ is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is*

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n \tag{1.8}$$

Now we have the base to define what is known as *entanglement*:

Definition 1.2 ***(Entanglement)*** *A composite system is called entangled if it can't be written as the composition of the states of its component systems.*

To better understand let re-write this definition in simple version for the composite system of two states.

Definition 1.3 *Two quantum states are entangled if it is not possible to find the four parameters a_1, a_2, b_1, b_2 that satisfy the next equation:*

$$|\varphi\rangle = (a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) \tag{1.9}$$

Example of entangled states are Bell's states ([6, 29]) or GHZ states ([62]).

Entanglement have been discussed for many years and represent nowadays the basis for many experimental schemes such as *quantum teleportation* and the communication technique called *superdense coding* [6, 57].

If we want to approach the real application of quantum information, we have to add some other definitions and observations to the big concept of quantum measurement. In fact the definition given us by the third postulate (see Eq. 1.5) is too general, and for this reason is necessary to introduce some particular cases.

1.1.2 Quantum Measurements

We start with the definition of *projective* measurement:

Definition 1.4 ***(Projective measurement)*** *A projective measurement is described by an observable, M, that is an hermitian operator on the state space of the system under test. The observable has a spectral decomposition given by:*

$$M = \sum_m m P_m \tag{1.10}$$

where P_m is the projector on auto-space of the M observable, with eigenvalue m. The possible outcome of the measurement are the eigenvalues m of the observable. From the measurement of the state $|\psi\rangle$. the probability of obtaining the outcome m is given by:

$$p(m) = \langle\psi| P_m |\psi\rangle \tag{1.11}$$

If we have obtained the value m, the state of the physical quantum system after the measurement is:

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}} \tag{1.12}$$

The projective measurements present very interesting properties, for example the mean value of the observable M, also written as $\langle M \rangle$, is:

$$\begin{aligned} E[m] &= \sum_m mp(m) = \sum_m m \langle\psi| P_m |\psi\rangle \\ &= \langle\psi| \left(\sum_m mP_m \right) |\psi\rangle = \langle\psi| M |\psi\rangle \end{aligned} \tag{1.13}$$

and the variance of the observable results:

$$[\Delta(M)]^2 = \langle (M - \langle M \rangle)^2 \rangle = \langle M^2 \rangle - \langle M \rangle^2 \tag{1.14}$$

The variance is intuitively the dispersion of the outcomes around the mean value, then if we act a big number of measurements on a state[2], we can obtain a standard deviation:

$$\Delta(M) = \sqrt{\langle M^2 \rangle - \langle M \rangle^2} \tag{1.15}$$

This formulation permits to introduce one of the most famous result of quantum mechanics, the Heisenberg indetermination principle. Take A and B two hermitian operator and $|\psi\rangle$ a quantum system. Suppose that $\langle\psi| AB |\psi\rangle = x + iy$, with x and y real numbers. Note[3] that:

$$\langle\psi| [A, B] |\psi\rangle = 2iy \tag{1.16}$$

and

$$\langle\psi| \{A, B\} |\psi\rangle = 2x \tag{1.17}$$

The previous equation implies that:

$$| \langle\psi| [A, B] |\psi\rangle |^2 + | \langle\psi| \{A, B\} |\psi\rangle |^2 = 4 | \langle\psi| AB |\psi\rangle |^2 \tag{1.18}$$

From the Cauchy-Schwartz equation we obtain:

$$| \langle\psi| AB |\psi\rangle |^2 \leq \langle\psi| A^2 |\psi\rangle \langle\psi| B^2 |\psi\rangle \tag{1.19}$$

that, combined with (1.18) and dropping a non-negative term, gives:

$$| \langle\psi| [A, B] |\psi\rangle |^2 \leq 4 \langle\psi| A^2 |\psi\rangle \langle\psi| B^2 |\psi\rangle \tag{1.20}$$

[2] The process is to measure the state $|\psi\rangle$, read the outcome, the recreate the state $|\psi\rangle$ in order to measure again the system.

[3] Recall that $[A, B] = AB - BA$ and $\{A, B\} = AB + BA$. If $[A, B] = 0$ we can say that A commute with B. Similarly A anti-commute with B if $\{A, B\} = 0$.

Suppose now that C and D are two observable. Making the substitution $A = C - \langle C \rangle$ e $B = D - \langle D \rangle$ in the last equation we obtain the indetermination principle:

$$\Delta(C)\Delta(D) = \frac{| \langle \psi | [C, D] | \psi \rangle |}{2} \tag{1.21}$$

This elegant formulation of the Heisenberg principle has a correct interpretation. If we prepare a great number of quantum systems into the same state $|\psi\rangle$ and then we measure with C some of them and others with D, then the standard deviation $\Delta(C)$ of the results of C and the standard deviation $\Delta(D)$ will satisfy the disequality 1.21.

Another important case of quantum measurement is represented by the so called POVM[4] formalism. This mathematical tool helps us if we are not interested in the results of the measurements but we are more attracted on the probabilities of the outcomes.

Definition 1.5 *Associates to a measurement operator exist the POVM* ***element*** *E_m defined as:*

$$E_m = M_m^\dagger M_m \tag{1.22}$$

where M_m is a measurement operator put on the quantum system $|\psi\rangle$. The probability of obtaining the result m is:

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \tag{1.23}$$

and, from the third postulate (Eq. 1.5), we can conclude that E_m is a positive operator with the next properties:

$$\sum_m E_m = I \quad \textit{and} \quad p(m) = \langle \psi | E_m | \psi \rangle \tag{1.24}$$

Then the set of the operators E_m is sufficient to determine the probabilities of the different outcomes of the measurements. The set of all the $\{E_m\}$ is called POVM.

To conclude this section we can say that projective measurements has a big property: repeatability. They are repeatable in the sense that if we perform a projective measurement once, and obtain the outcome m, repeating the measurement gives the outcome m again and does not change the state. The repeatability property help us to understand that the concept of quantum measurement is very differentiated. In fact we know that there exist measurements that change or even destroy the state but if we are interested in statistical measurements POVM can indeed guarantee repeatable results.

[4] The acronym POVM stands for “Positive Operator-Value Measure”.

1.1.3 How to Distinguish and Copy Quantum States

An important application of the third postulate and of the different type of measurements that we can perform on a quantum state is the problem of distinguishibility of states. This problem is well understood if we think about a game between two parties: Alice and Bob. Alice chooses a state $|\psi_i\rangle$, $1 \leq i \leq n$ from some fixed set of states known by both parties. She gives the state $|\psi_i\rangle$ to Bob, whose task is to identify the index i of the state Alice has given to him.

In the classical world we are sure that a system is in a state or in another, for example think about the state of a logical bit in a line on a electronic chip, or simply to a coin: we are capable to distinguish if a coin has landed in heads or in tails.

In the world of quantum mechanic this task is not so easy, it depends of the states we are playing with and on out measurement apparatus. For this reason we have the next theorem directly derived from the theory of quantum measurement:

Theorem 1 ***(Distiguishibility of non-orthogonal quantum states)*** *Non-orthogonal quantum states can't be reliably distinguished.*

This important theorem is fundamental for an application deeply discussed in this work: single photon quantum key distribution (QKD) protocols. In order to encode information different quantum states are transmitted and these quantum states are non-orthogonal between eachother (see Par 1.3.2) therefore this theorem applies and moreover it is the key for the security of such protocols. We will go through the security issues in QKD later on in this chapter (see Sec. 1.2.4).

Another very important theorem that is a consequence of the previous consideration is the *no cloning theorem*:

Theorem 2 ***(No cloning)*** *It is not possible to perform a perfect copy of a quantum state*

This theorem is presented for the first time in 1982 from William K. Wootters and Wojciech H. Zureck in the article [93], and the proof was based on quantum electrodynamics. Nevertheless we can give here a simple demonstration based on a proof by contradiction introducing an ideal quantum copy machine.

In fact let $|\psi\rangle$ the unknown state to be copied and $|s\rangle$ another state where it will be copied the state $|\psi\rangle$; then the global state of the system composed by the two qubits is $|\psi\rangle \otimes |s\rangle$. Suppose now that it can be possible to copy the state $|\psi\rangle$, then this operation will be realized with the linear operator $\mathbf{U}$. The operator can act the copy of $|\psi\rangle$:

$$\mathbf{U}\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{1.25}$$

If $\mathbf{U}$ can correctly operate on $|\psi\rangle$, then it can manage also the state $|\phi\rangle$. Then we obtain that:

$$\mathbf{U}\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{1.26}$$
$$\mathbf{U}\left(|\phi\rangle \otimes |s\rangle\right) = |\phi\rangle \otimes |\phi\rangle \tag{1.27}$$

As the operator $\mathbf{U}$ is unitary, we can made the inner product between the equation (1.26) and (1.27), that gives:

$$\langle\psi|\phi\rangle = \left(\langle\psi|\phi\rangle\right)^2 \tag{1.28}$$

This last equation has two solutions: the first is $\langle\psi|\phi\rangle = 0$ an the second is $\langle\psi|\phi\rangle = 1$ i.e the two states are either equal or orthogonal. We can conclude that a copy operator can manage only these two cases an not more general superposed states. We can then observe that this result bring us to the classical case of working on standard bits. In the classical information domain in fact the copy machine is possible and also very useful.

1.2 QKD Introduction

1.2.1 Basic Classical Cryptography

The general and most intuitive scheme for secure communication is called *symmetric key cryptography.* Symmetric because the *cryptographic key* used at the transmitter is the same at the receiver. This scheme is represented in Fig.1.1. A source S takes a secure key K , *a key that must be shared with the receiver*, and encode the message x, called *plain text*, obtaining the cipher text y (the function that performs the encoding, more precisely encryption, of the information is called *cipher*[5]). The transmitter is usually called Alice and the receiver Bob. An intruder, an eavesdropper, normally indicated as Eve, that would like to read the plain text message x, operates some actions (attacks) on the communication channel between Alice an Bob in order to obtain an estimation of the message $\tilde{x}$ and also of the encryption key $\tilde{K}$.

With the scheme described in Fig. 1.1 it is possible to describe all the classical cryptographic schemes even the modern *public key schemes* [68]. This

[5] It is sometimes written cypher.

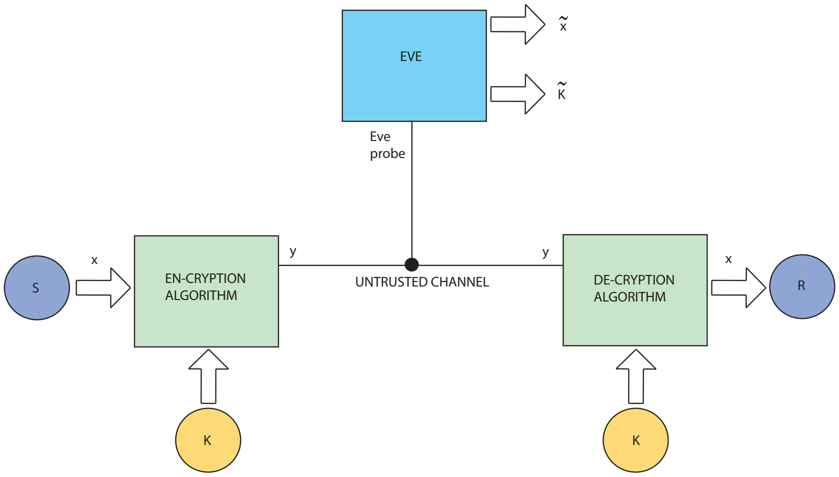


Figure 1.1: A scheme of a generic symmetric cryptographic transmission: the message x is encrypted using the key K. The cipher text y obtained is transmitted and decrypted by means of the same key K shared between the transmitter and the receiver. Eve monitors the channel and can gain information about both key and message. .

is not in the scope of this work (see the book by Schneier [72] for a complete review of cryptographic tecniques).

Speaking about cryptography we have to consider a set of other issues related to the transmission of a confidential message:

- **Confidentiality:**

  Confidentiality ensure that information is accessible only to those authorized to have access to it.

- **Authentication:**

  The act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true.

- **Data Integrity:**

  Data integrity ensures that the information data has not been altered.

- **Non repudiation:**

  Non repudiation is a process that ensures that the information data cannot be disowned.

Any system intended to allow a secure transmission between two parties should accomplish and guarantee these requirements.

1.2.2 Security of Classical Cryptography

During the history of cryptography one thing became more and more evident through the years: *The security of a system is not determined by the secrecy of its algorithm (cipher function), but only by the secrecy and length of the cryptographic key.*

The role of the cipher is the role of a lock that can be opened only with the adequate key. In this sense encryption operation must be *one-way*, as it must be *easy* to compute in one direction (the encryption) while it must be very *difficult* to compute in the other direction. In our analogy it should be easy to open the lock with the right key but very difficult without it. This is the essence of classical cryptography and the words *easy* and *difficult* are here referred to the computational complexity that the problem of decrypting a message needs in order to be accomplished. This point is not always clear and it causes confusion about how hard is to break a system. Security is a strange matter: it concerns psychology, resources, history and everyday apparently useless actions[6]. To break a system one would better look into the bin for passwords than pay thousands of dollars, to break another a supercomputer may be needed, clearly the advantage that one have must be proportionate to the expense. Remember though that "advantage" may not mean money. This is a very interesting topic that goes behind the scope of this work.

Coming to more mathematical and safe place, up to now there is only one algorithm that is mathematically unconditionally secure, and it is a classical algorithm called *One Time Pad* (OTP). One Time Pad is a cryptography cipher and it is derived from Vernam cipher, named after Gilbert Vernam, one of its inventors. The algorithm is very simple: take a message x, take a key k and sum them:

Clear text:	1011010001
Key:	0110100011
XOR	———
Cipher text:	1101110010

Figure 1.2: One Time Pad example

OTP acts the sum modulus A where A is the dimension of the alphabet $\mathcal{A}$ of the plain text x with a perfectly random secret key k. The key k has to

[6] B. Schneier, apart from his book ([72]) has written many essays on the concept of security (www.schneier.com).

satisfy the next properties:

$$k \in \mathcal{A} \tag{1.29}$$

$$k \in \mathcal{U}, \text{perfectly random variable} \tag{1.30}$$

$$\text{length}(k) = \text{length}(x) \tag{1.31}$$

$$k\text{must be used only one time} \tag{1.32}$$

Shannon has introduced the concept of a perfectly secure system [74] and a necessary condition for a system to guarantee perfect security:

Theorem 3 ***(Shannon)***

A necessary and sufficient condition for a perfect secure cryptographic system is :

$$p_{c|m}(\beta|\alpha) = p_c(\beta) \tag{1.33}$$

The ciphertext c must be completely independent from the plaintext m.

This is true for OTP if conditions 1.29 - 1.32 hold.

The problem of security is shifted then to another issue: the *distribution of random keys in a secure way.*

1.2.3 Quantum Key Distribution

What is normally called quantum cryptography can help us to solve the problem just mentioned of the distribution of a random key in a secure manner. Quantum cryptography cannot be used to communicate information in a secure way but it can indeed be used by two users to share a cryptographic key between each other. That is why we normally call quantum cryptography with the name of quantum key distribution. Let's give a definition of quantum key distribution that resume the main feature of the idea:

Definition 1.6 ***(QKD)*** *a quantum key distribution system is a telecommunication system that can create a perfectly secure symmetric key at the transmitter and at the receiver. It needs two communication channels:*

1. *Quantum Channel, for the transmission of the quantum bits.*
2. *Classical Public Channel, for the communication of classical messages between the transmitter and the receiver.*

The cryptographic scheme of Fig. 1.1 can be then slightly modified to add the distribution of the keys in a quantum way, see the result in Fig. 1.3.

We have previously explained that there exists a real totally secure classical encryption algorithm called One Time Pad (OTP or Vernam Code). We can

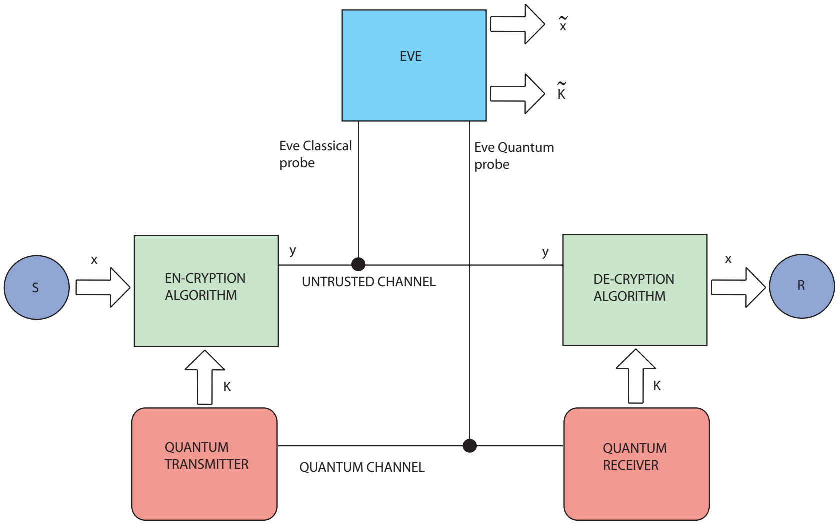


Figure 1.3: A scheme of a symmetric cryptographic system that exploit the benefits of Quantum Key Distribution.

think then to use it together with QKD that creates secure keys in order to communicate in a perfectly confidential way.

Clearly now the eavesdropper has a further chance to attack the system that is the quantum channel but this is also a good news because quantum mechanics guarantee that this channel, under specific assumptions is perfectly secure as we will see shortly.

1.2.4 Security of QKD

The security of Quantum Cryptography rely on the fact that is uses the laws of nature[7].

The innovative idea under the quantum key distribution is very simple and can be written in very general way:

> **Quantum idea**
> *Each measurement on a quantum system perturbs the system itself*

In this particular case each measurement (see Sec. 1.1.2) in some way perturb the state that is traveling in the quantum channel. This is based fundamentally on the no-clonig theorem described in Sec. 1.1.3 and the unconditional security of QKD has been demonstrated in many papers for several

[7] Laws that have never been contradicted so far.

protocol and under different attacks. Some general reference about QKD security are: [54, 40, 66]. It is remarkable that the fact that a measurement of a quantum system alters in some way the system was considered a problem in the applications of quantum information whereas it has been demonstrated very powerful and QKD is indeed the first "real" application that exploit quantum mechanics.

So resuming this paragraph we can say that if we encode the bits of a general message (plaintext) in a series of non orthogonal *qubits* that are transmitted to the receiver, any attempt to read that qubits necessarily alters the quantum systems (the qubits). Alice and Bob are then capable of *hearing* if Eve is present in the communication channel. In this way any attempt to get the key is detected and that particular string that has been attacked won't be used for encryption. It is easy now to understand why this system cannot be used for the transmission of sensible data: only after that the message are received one can check if it has been read by an eavesdropper.

The issue of the security of QKD is a big one and still open. What can be said in this contest is that *Some QKD protocols have been demonstrated theoretically UNCONDITIONALLY SECURE.* Although some problems in practical implementation are still open[8] and it is not clear if people need this level security[9] QKD may become a cryptographic standard in the next years when computational power will be enough to break classical algorithm in a reasonable time. This could be done when quantum computers[10] will be available [57].

1.3 Single Photon Quantum Key Distribution

Since the first implementation of Charles Bennet and Gilles Brassard in 1984 in their famous article ([8]) many protocol and alternative implementations have been proposed. Most of them are based on the original idea and the carrier of information are the photons, more precisely a quantum state of a single photon[11]. Generally speaking we transmit a qubit $|\psi\rangle$ that lives in a two dimensional Hilbert space represented by the basis $\{|0\rangle, |1\rangle\}$. With this

[8] There are many attacks based on non ideality of apparatus. Some innovative kind for example exploit the non precise temporal filtering of the system [53].

[9] There exist insurance companies, people and institutions seem to prefer this kind of security.

[10] In 2007 a prototype has been presented by D-Wave: http://www.dwavesys.com/.

[11] There exists other protocols that exploit instead continuous variable as the *sqeezed state* protocol (see [23]), the *entangled beam protocols* (see [78]) or the *coherent state* protocol (see [39]).

basis that we assume orthonormal the qubit can be represented by:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{1.34}$$

In many setups based on fiber the information is encoded into the phase shift of the photons [37]. When the quantum channel, instead of optical fiber, is in free space the photon polarization is preferred [41, 91, 49]. The polarization in fact is preserved during the propagation through the atmosphere as the atmosphere itself is non birefrangent. In these free space schemes for the transmission of the information between Alice and Bob the photons are prepared in a pre determined polarization state that we may indicate with $|45\rangle$ or $|⤢\rangle$, the angle in the first case and orientation of the arrow in the second case may vary according to the polarization of the state. The number of encoding states is another variable in QKD protocols. There exist protocol with two state (the B92 is an example that we will describe), with four states as the first proposed BB84 and with more states (see [36]) while others protocol rely on EPR pairs (see [65] [67]). Some of the most recent protocols are the Y-00 protocol based on the bit commitment problem and described in [95] and the Kish-Sethuraman protocol which exploits the homonymous classical cipher [11].

We will now approach the first proposed QKD protocol: BB84 and then we will describe the protocol we have decided to implement in our system, the B92.

1.3.1 BB84

BB84 was the first studied and practical implemented QKD physical layer protocol. It was created by Charles Bennet and Gilles Brassard in 1984 in the article [8]. It is surely the most famous and most realized quantum cryptography protocol. This scheme uses the transmission of single polarized photons (as the quantum states). The polarizations of the photons are four, and are grouped together in two different non orthogonal basis, while the states of each base are orthogonal. Generally the non orthogonal basis are[12]:

- base (+) of the horizontal (0°) e vertical polarization (+90°), and we represent the base states with the intuitive notation: $|\leftrightarrow\rangle$ e $|\updownarrow\rangle$.

- base (×) of the diagonal polarizations (+45°) and (+135°). The two different base states are $|⤢\rangle$ e $|⤡\rangle$.

[12] Another possible basis is ($|\circlearrowright\rangle$,$|\circlearrowleft\rangle$).

In this protocol, the association between the information bit (taken from a random number generator) and the basis are described in Tab. 1.1. This association is basically the modulation scheme of the BB84 transmission system. In fact, a random sting is modulated in the polarization of single photon and then sent to the receiver (Bob).

Bit	Qubit (+)	Qubit (×)
0	$\|\leftrightarrow\rangle$	$\|⤢\rangle$
1	$\|\updownarrow\rangle$	$\|⤡\rangle$

Table 1.1: Coding scheme for the BB84 protocol.

The situation is resumed in Fig. 1.4. The bit sent to Bob in the form of single polarized photons are then measured by the receiver, after passing the quantum channel. At the receiver it is then possible to create a string of data that is, in ideal conditions, the same of the sent string.

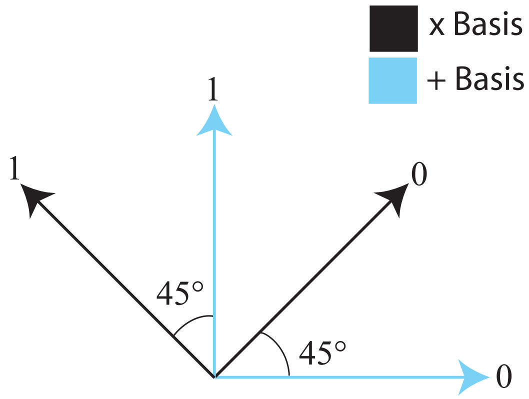


Figure 1.4: A picture of the coding scheme for BB84.

The BB84 protocol steps are:

1. Alice generates the sequence of bits that we call message a to be sent to Bob. Alice generates also the the sequence of basis to use for each single bit of the message. Each generation is a discrete random variable well balanced between the alphabet values, in this case compose by tho value: 0 and 1 ($p(0) = p(1) = \frac{1}{2}$).

2. Alice modulates the bits in qubits, single polarized photons and then send them to Bob through a fiber or free space channels.

3. Bob receives the qubits and decides which base to use in the process of measurement for each single arrived photon. The process of decision is again a uniform random variable. With a demodulation table exactly equal to the 1.1 he extracts the information bit from the photons. The string as it arrive to Bob is called **raw key**.

As the raw key in non ideal condition is different from the transmitted random string (key), it is necessary a process of *cleaning* of the keys. This process is called *sifting* and it consist of the communication between Bob and Alice of the basis used to encode and measure the qubits. Alice compares the information on the Bob's string and communicates to Bob where he used a right choice in the basis. Obviously, as the choice in the measurement basis was completely random, the strings are different in the 50% of the cases, in ideal conditions. We can summarise all the protocol up to this point , including the process of sifting with the next Table (Tab. 1.2).

BB84												
Alice's bits	1	1	0	0	1	0	0	1	0	0	1	1
Alice's basis	+	×	×	×	+	+	×	+	+	×	×	×
Sent polarization	↕	⤡	⤢	⤢	↕	↔	⤢	↕	↔	⤢	⤡	⤡
Bob measuring basis	+	×	+	×	×	×	+	+	×	+	×	+
Bob' measurements	↕	⤡	↔	⤢	⤡	⤢	↕	↕	⤡	↔	⤡	↔
Keep the value?	✓	✓		✓				✓			✓	
Sifted key	1	1		0				1			1	

Table 1.2: This is the step by step algorithm of a BB84 protocol. In this case we uses ideal condition in the transmission and reception (measurement) of the qubits.

After the generation of the sifted key the users Alice and Bob have to accomplish other tasks in order to keep the key secret to an eavesdropper. These task are the same for all single photon QKD protocols and will be described is Sec. 1.3.3 and then studied in depth in Sec. 6.2 and 6.4.

1.3.2 B92

B92 is a *two state* protocol and was presented to the community in 1992 by Charles Bennett in [9].

This protocol is similar to the BB84 in the sense that it exploit non orthogonal basis. In B92 though we use only one polarization state per basis so then the polarizations are non orthogonal. For Alice the value 0 is a single horizontal polarized photon, which is qubit in the state $|\leftrightarrow\rangle$, while the value 1 is the qubit $|\nearrow\!\!\!\!\swarrow\rangle$. The next table describes the so called modulation alphabet that is represented graphically in Fig 1.5:

Bit	Alice
0	$\vert\leftrightarrow\rangle$
1	$\vert\nearrow\!\!\!\!\swarrow\rangle$

Table 1.3: Modulation alphabet for B92 protocol.

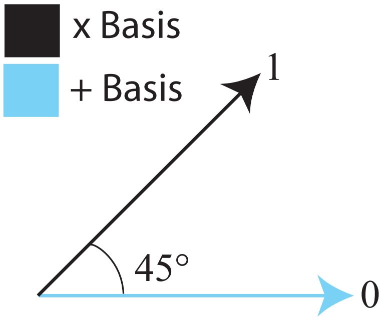


Figure 1.5: A picture of the coding scheme for B92.

Bob uses a particular measurement setup. The receiver is a system capable of random switching between two single photon receivers making in other words a random basis selection. Like in BB84 we would put polarizer in front of our detectors but in this case we orient the polarizers orthogonally with respect to the transmitter each. Keeping the bit logic used at the transmitter and following the path of the encoded bits the decoding rule assume the form resumed in Tab. 1.4

The key point of the protocol is that when the transmitting and receiving basis are the same the detector will never click. In the other case, when the basis are different, there is a chance for the detector to click and a chance to stay still:

$$p(click) = p(noclick) = 1/2 \tag{1.35}$$

Bit	Polarizer
0	⤡
1	↕

Table 1.4: Demodulation rule for the B92 protocol. Notice how the polarizer are orthogonal with respect to the encoding polarizer at the transmitter.

When there was no click nothing can be said but when the detector clicks Bob is sure that the basis used by Alice was different from the one he used for decoding and due to the fact that B92 is a two state protocol he individuate in this way the bit that Alice transmitted. Like in the previous section regarding the BB84 protocol, in this section we describe also the sifting procedure. The following step list and Tab. 1.5 resume the concepts just explained:

B92 protocol								
(1.) Alice bit (a)	0	1	1	0	0	1	1	1
(2.) Alice sends	|↔⟩	|⤢⟩	|⤢⟩	|↔⟩	|↔⟩	|⤢⟩	|⤢⟩	|⤢⟩
(3.) Bob's switching	|↕⟩	|⤡⟩	|⤡⟩	|⤡⟩	|↕⟩	|⤡⟩	|↕⟩	|↕⟩
(4.) Click?	no	no	no	YES	no	no	YES	NO
(5.) Sifting				✓			✓	
(6.) Sifted Key S_K				0			1	

Table 1.5: This is a step by step description of B92 protocol.

1. Alice starts her random number generator and stores the string to send to Bob a_n, $a_n \in 0, 1$.

2. Alice sends the single polarized photons using the modulation alphabet in Tab. 1.3.

3. Bob starts his random generator and at each incoming photon from Alice, chooses one of the two optical lines described in previously in Tab 1.5.

4. Bob measures the incoming photons. As explained if the measurement basis is equal to the transmitting one (columns 1,2,3,5,6) we will have no click. When the basis at the transmitter ad receiver differ there are some cases in which the detector will produce a click (columns 4,7). In this case the bit is decoded properly. In other cases there is no click (column 8) and in this case nothing can be said.

5. Bob send to Alice a message, in a public classic channel, where there are the positions in his string where he got the CLICKs. Alice will discard all her bits except the ones corresponding to the message coming from Bob. Notice that in BB84 Alice and Bob would communicate the basis whereas in this case the basis corresponds to the bit (recall that we have two states an two basis) and cannot be revealed. That is why Alice and Bob uses the positions the obtained a click instead.

6. Finally Alice and Bob will share the same sub-string, in the case described in Tab. 1.5, they will obtain the sifted key:

$$S_K = \text{“01”} \tag{1.36}$$

To conclude this paragraph notice how B92 is half efficient that BB84, respectively 50% and 25%. Nonetheless we decided to implement this protocol due to its simplicity and relatively low costs.

1.3.3 Error Correction and Privacy Amplification

The sifted key that Alice and Bob share at this stage of the protocol is not yet secure and cannot be used for cryptographic purposes. First of all, non idealities in the apparatus or the presence of Eve may have introduced some errors that have to be corrected. The cryptographic keys must be identical. This is done with a procedure of *error correction* that will be largely discussed in the following chapters (See Sec. 6.1). The error correction has another very important role in QKD protocol: it is the eavesdropper detector. By measuring the error rate Alice and Bob are capable to state if the error was due to environmental factors (non idealities, misalignments, atmosphere, ecc..) or to the presence of Eve. In this last case they discard the transmission. The key after the process of error correction is called *reconciled key.*

The fact that Eve could have hidden herself during the transmission maybe introducing a acceptable level of noise and the fact that Eve may gain information also during the error correction phase bring to the next and last step of the protocol: *privacy amplification.* Sometime called advanced distillation it has the aim to reduce the length of the reconciled key by an amount of bits that make the residual information owned by Eve under a certain level of security. The process of privacy amplification will be described in detail in Sec. 6.3. The key after the privacy amplification is called *secure key* and can be used for real cryptography.

1.3.4 Filtering in QKD

In this section we introduce some consideration of *filtering* in single photon Quantum Key Distribution that will be discussed later for the case of our system. When we are dialing with single photons it arises the problem of noise rejection. This is true either for fiber optical based systems or for free space prototypes. We can consider three type of filtering: *temporal filtering, spectral filtering* and *spatial filtering.*

- **Temporal Filtering:**

  The temporal filtering in a QKD system can be associated with the synchronization between the transmitter and the receiver. This synchronization is needed in order to recognize a good photon from a noisy one. The key point is to select the protons that reach the receiver by means to a time base that coincide with the time base used by the transmitter for photon emission. Several methods can be applied in order to accomplish this task and they will be described in Sec. 3.1.2.

- **Spectral Filtering**

  Spectral filtering is a very simple one. As we are interested only in the photons emitted by the transmitter we would like to reject all the wavelengths but Alice's one. This is done usually using spectral filters as described in Sec. 3.3.1.

- **Spatial Filtering**

  Spatial filtering consists on reducing the solid angle visible by the receiver in order to perfectly optically conjugate the single photon sources at the transmitter with the detectors at the receiver. When the quantum channel is the optical fiber this is automatically obtained as the light is driven through the fiber. When instead the quantum channel is free space the field of view of the collector at the receiver have to be carefully chosen. This implies also the issue of atmospheric induced aberrations that can spread the PSF (point spread function) of the beam coming from the source at the receiver so giving an apparent increase of the perceived field of view. This has pointed out in several experiment most of them over a long free space channel path ([71, 49, 35]) or in daylight ([17, 41]). The spatial filtering problem and a proposed solution is given in this thesis and described in depth in chapter 4.

All of those filtering are needed in a modern QKD system in particular for free space QKD. In the following chapters an analysis of those problems is presented related to the implementation of a free space QKD system: QuAKE (Quantum Advance Key Exchanger).

Chapter 2

QuAKE Introduction

In this chapter we describe the main characteristics of QuAKE (Quantum Advanced Key Exchanger) and the general design choices that we made. QuAKE is the free space quantum key distribution system that is being designed and realized in the Department of Information Engineering of Padova (DEI) from the ABF research group (Alice, Bob and Friends Group). The development of the system is inserted in the frame of two projects: the Harrison European Project [1] that will finish at the end of 2008, and the ESA *QIPS* project. The main goal of our part of the Harrison Project is to understand and apply the new generation european global navigation system to application of quantum cryptography and quantum astronomy (see chapter REF). *QIPS* stands for *Quantum Information and Quantum Physics in Space* and has the main scope of investigating the laws of quantum mechanics on very large scale and to put an important seed towards global satellite QKD. The first stage of QIPS has been the evaluation of a ground to ground path of $144Km$ on the canary Islands [71]. A feasibility study and a rough design of the space and ground stations for the next experimental stage have been already designed. The realization of our demonstrator started and the beginning of 2006, the main motivations being the test of the various part of QKD system we were realizing and optimizing and the challenge of realizing our own low cost and compact system. In this chapter we will then describe QuAKE and go through the motivations, the innovative characteristic and the basic design choices. Some of them will be treated in depth in the following chapters. We would like to begin this chapter describing a very useful tool that we developed to facilitate the study and the analysis of a QKD system.

[1] http://www.exodus.gr/harrison/.

2.1 QKD Matlab Simulator

In order to better understand and develop our system we implemented first a high level QKD Matlab simulator. We started with a simple simulation of a quantum channel and completed the simulator with all the protocol phases and at the end with clocks simulators to manage the timing of the protocol. This stage of the research has been very useful and the results will be presented on this thesis and used as a guide for the real design and implementation. In this paragraph a brief description of the key concept of the simulator are presented[2].

The Matlab software is a full simulator of a QKD system. Alice is considered as a faint pulse source (Weak Coherent Pulse) with a mean photon number per pulse that follows a poissonian distribution with mean μ. The repetition frequency as well as the pulse duration and the photon wavelength are adjustable. Every bit is represented by a couple $\{$*number of photons (n), polarization (p)*$\}$, the latter is choses depending on the protocol that is running. Two protocol have been implemented so far: BB84 and B92. In Fig. 2.1 a zoom on 250 bits as they leave the transmitter are represented, in the upper plot the polarization (BB84), in the lower plot the number of photons ($\mu = 0.3$).

The receiver is characterized by simulated beam splitters and polarizing beam splitters that drive the signal into one of the detectors. Each beam splitter is a uniform random variable $x \in \mathcal{U}[0, 1]$ but the choice i.e. the measurement is taken at 1/2 for the non polarizing beam splitter whereas for the polarizing beam splitters is weighted with $cos^2\theta_i$ where θ_i is the angle between the incoming i-th photon's polarization and the axis of the polarizing beam splitter. The configuration of the beam splitters and the number of detectors depend on the selected protocol. The single photon detectors are considered the same for each arm of the receiver.

We have considered so far an ideal transmission, with ideal channel and detectors. Now we start to add sources of noise to our simulator either in the channel itself and in the apparatus. During the propagation of the photons in free space there are attenuation and polarization misalignment as well as on the transmitting and receiving telescope. Moreover every optical component has a non ideal transmission curve that is normally negligible compared to the attenuation of the atmosphere for standard catalog components. In the simulator we treated the atmosphere attenuation with the approximation of *Beers-Lambert* [45]. In this approximation all the factors that concur for

[2] The simulator is fully described in the degree thesis of Paolo Zoccarato and Francesco D'onofrio which had worked with Tommaso Occhipinti and me to its realization [96, 31] .

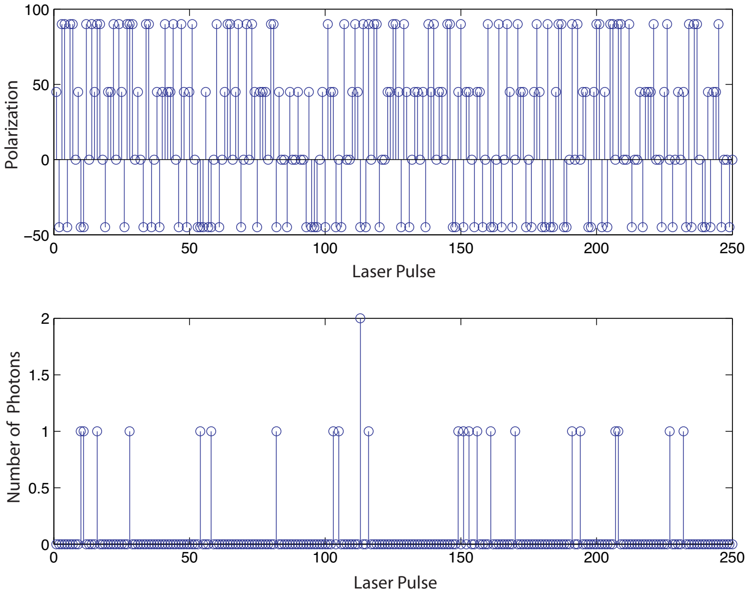


Figure 2.1: Simulation of the sent bits for a faint pulse BB84 with $\mu = 0.3$.

the attenuation such as water adsorption, length of the path, Mie scattering ecc. can be considered by means of only two parameters namely the distance traveled by the light and the *visibility* between the transmitter and the receiver. The visibility V is defined as the distance when the transmitted power decreases by 2% and it's measured in Km. Considering λ the wavelength in nanometers and q a parameter that depends on the visibility following the step function 2.1

$$q = \begin{cases} 1.6 & \text{per } V > 50 \\ 1.3 & \text{per } 6 < V < 50 \\ 1.16V + 0.34 & \text{per } 1 < V < 6 \\ V - 0.5 & \text{per } 0.5 < V < 1 \\ 0 & \text{per } V < 0.5 \end{cases} \tag{2.1}$$

we can write the attenuation per unit length σ

$$\sigma = \frac{3.91}{V} \left(\frac{\lambda}{550} \right)^q \tag{2.2}$$

and then eventually the received power P at a distance D

$$P(D) = P_0 exp(-\sigma D) \tag{2.3}$$

where P_0 is the transmitted power. All other type of attenuation due to optical components are added linearly to this value. Notice that in this approximation the attenuation due to beam wander is not directly taken into account although it can be added knowing its mean value. A version of the simulator with this feature is under construction. Another few words are deserved by the detectors since they performance can affect heavily the performances. Attenuation on the detectors are due to their parameters values and the simulator gives the possibility to change many of them like quantum efficiency, dark counts, dead time ecc.. Notice that the fact of considering the two detectors identical should be avoided since recently an attack to QKD has been proposed that exploit the so called *detector mismatch* [53].

The polarization misalignment is also due either to the atmospheric effects, although atmosphere can be considered at a first glance a non birifrangent medium, and to the system components. Since this effects is the cause of the error rate of the transmitted key and can be considered an AWGN noise added to the transmitted polarization values we use experimental data by Huges in [17] and others in order to model our simulator. For good visibility ($> 6Km$) the error rate in a free space communication with today technology can be fairly kept less than 3%, this corresponds to a AWGN noise with a power of $20dBW$.

In Fig. 2.2 the received bits relative to transmission of Fig. 2.1 after they travelled through the channel and the transmitter and receiver apparatus. Notice how polarizations have changed and pulses have been attenuated.

Clearly polarizations of empty pulses are irrelevant for key generation.

The simulator has been the test bench for the development of Error Correction and Privacy Amplification Algorithm that we will describe in details in chapter 6. Nevertheless at this point we had indeed an instrument for simulating the features of a QKD channel and for comparing the BB84 and B92 protocols. We report here in Fig. 2.3 as an example the efficiency of the two algorithms with respect to the distance between Alice and Bob. If not differently stated all the figures regarding the simulator are averaged on 10 iterations.

As we expect the B92 key length is more or less one half of the BB84 key length due to the intrinsic protocol efficiency (see Sec. 1.3.2). This clearly is valid for the same initial conditions and channel. More detailed simulations can lead to results similar to Fig. 2.4 where the visibility is taken into consideration for different distances between transmitter and receiver or Fig. 2.5 where the visibility is kept constant to a value of 50km and the misalignment is varying. From those figures it is possible to say that the visibility is certainly

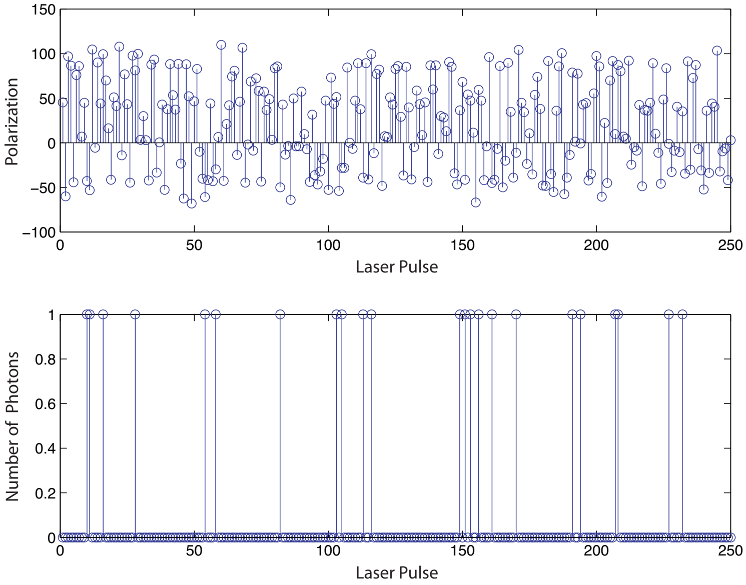


Figure 2.2: Simulation of the received bits for a faint pulse BB84 with $\mu = 0.3$.

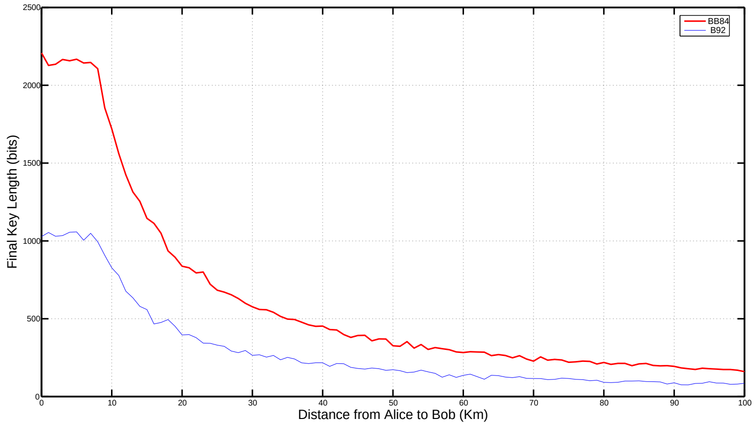


Figure 2.3: Final secure key length for a faint pulse BB84 (bold) and B92 (thin) with respect to the distance between Alice and Bob. Visibility 50Km, misalignment 5dB.

the parameter that most affect the transmission.

Finally we have added to our simulator the presence of Eve, simulating an intercept resend attack strategy with projective measurement and with POVM

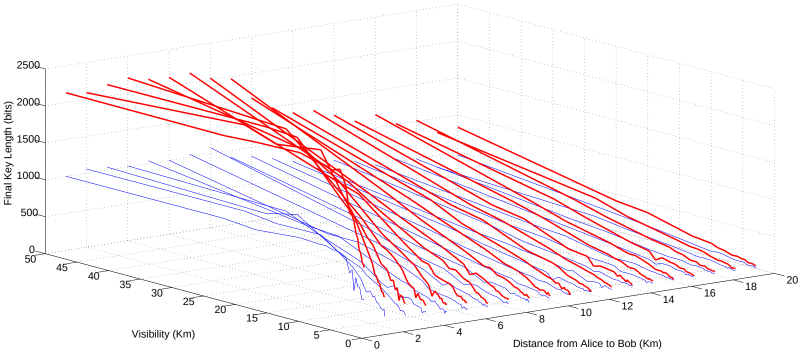


Figure 2.4: Final secure key length for a faint pulse BB84 (bold) and B92 (thin) with respect to the distance between Alice and Bob and the visibility. Constant misalignment of 5 dB.

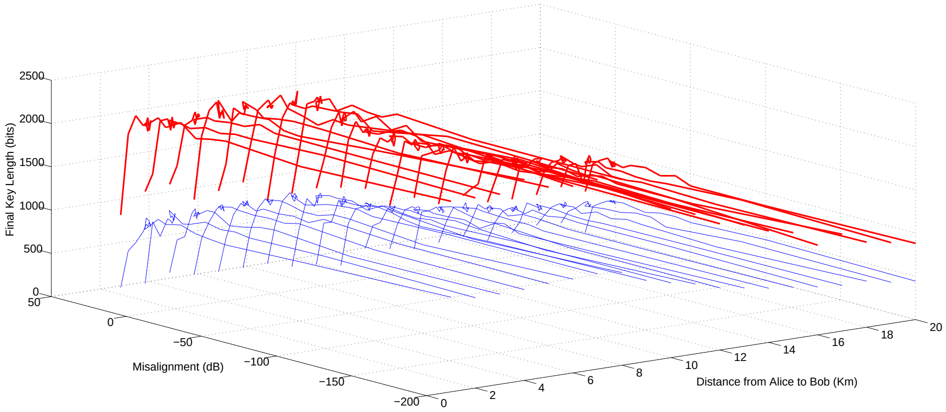


Figure 2.5: Final secure key length for a faint pulse BB84 (bold) and B92 (thin) with respect to the distance between Alice and Bob and the polarization misalignment. Constant visibility of 50 Km.

(see Sec. 1.1.2) in order to test the ability of the system to check whether or not an eavesdropper tried to steal information. In Fig. 2.6 you can see a study on the effect of Eve attacks on the B92 protocol, clearly negative key lengths mean that the protocol could not succeed in generating a key pair.

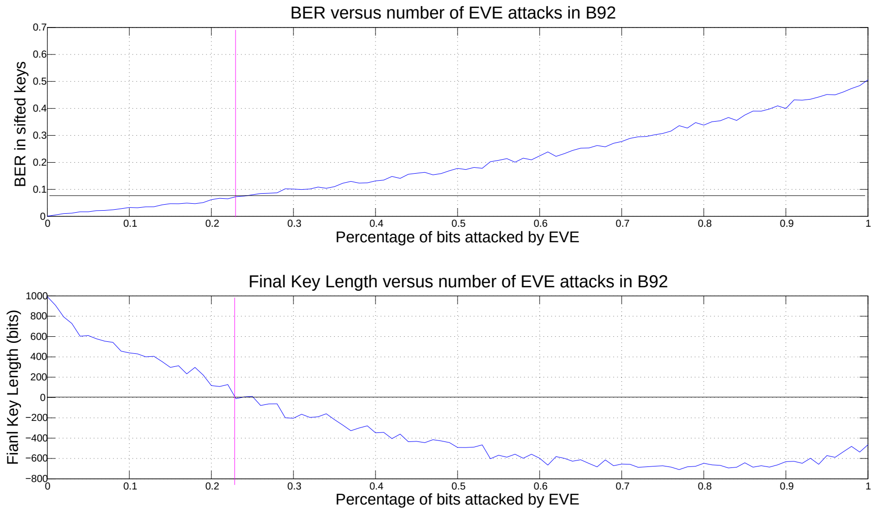


Figure 2.6: A simulation of intercept/resend attack with projective measurement for B92.

The simulator that we developed it is indeed a vary useful tool for the characterization of the performance of many parts of the final system. We developed also a user interface to facilitate the simulation process. A screenshot of the interface is reported in Fig. 2.7

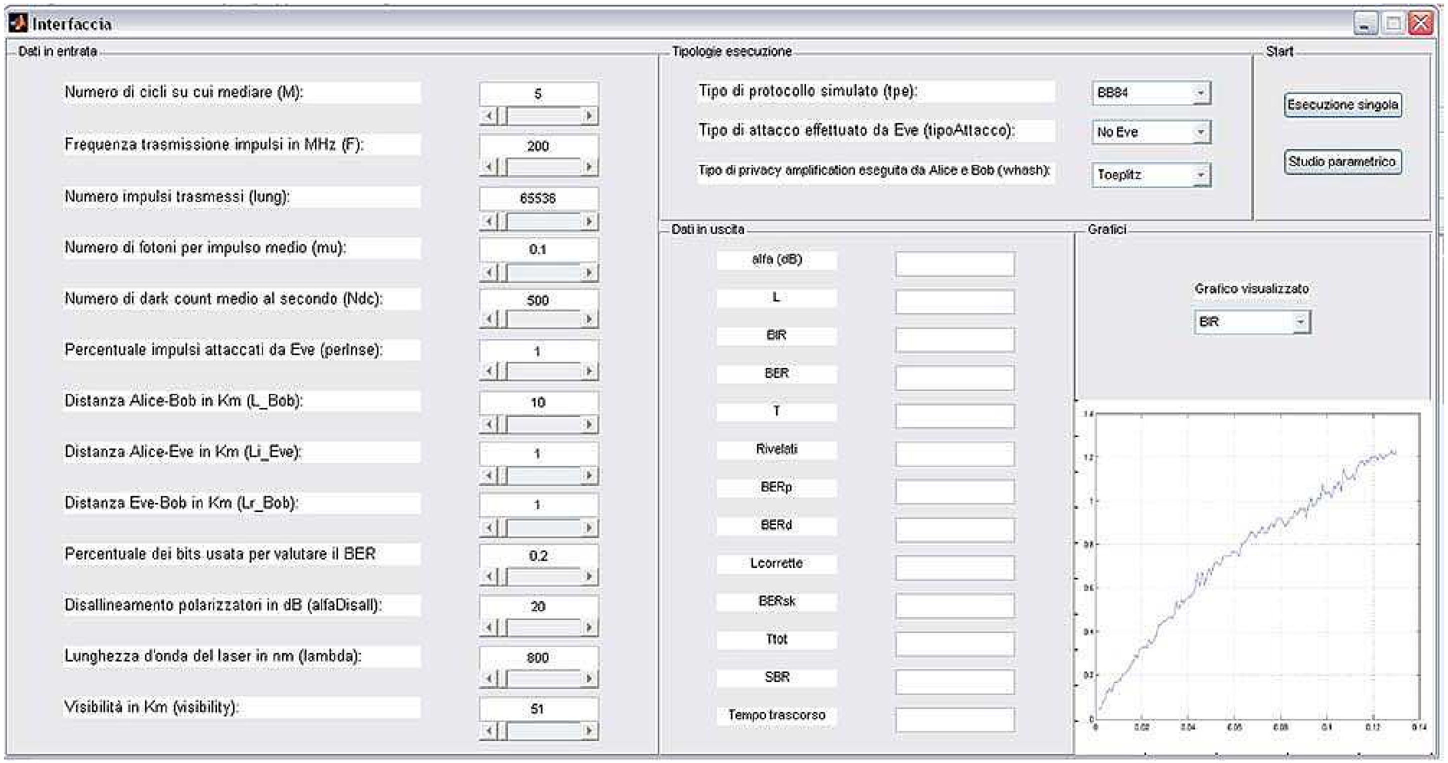
2.2 QuAKE Key Features

We are ready now to analyze the basic features of QuAKE.

In the last years many effort has been done in order to bring QKD systems available to mass commerce. Many companies were focused on fiber optics based QKD and some prototype is now on the market[3] In our department we decided to investigate the features of QKD in order to make some improvements on the system. These new features come from our expertise in optics and in system integration. At the end of 2005 we decided begin the project of QuAKE and at the beginning of 2006 we started its realization. The features of the system were carefully chosen in order to optimize costs and performance improvements.

QuAKE is meant to be a *complete quantum key distribution system*: it

[3] Some companies working on QKD are Toshiba, NEC, MagiQ, IdQuantique. The latter two have already commercial apparatus.



Interfaccia

Dati in entrata

Numero di cicli su cui mediare (M):	5
Frequenza trasmissione impulsi in MHz (F):	200
Numero impulsi trasmessi (lung):	65536
Numero di fotoni per impulso medio (mu):	0.1
Numero di dark count medio al secondo (Ndc):	500
Percentuale impulsi attaccati da Eve (perInse):	1
Distanza Alice-Bob in Km (L_Bob):	10
Distanza Alice-Eve in Km (Li_Eve):	1
Distanza Eve-Bob in Km (Lr_Bob):	1
Percentuale dei bits usata per valutare il BER	0.2
Disallineamento polarizzatori in dB (alfaDisall):	20
Lunghezza d'onda del laser in nm (lambda):	800
Visibilità in Km (visibility):	51

Tipologie esecuzione

Tipo di protocollo simulato (tpe):	BB84
Tipo di attacco effettuato da Eve (tipoAttacco):	No Eve
Tipo di privacy amplification eseguita da Alice e Bob (whash):	Toeplitz

Dati in uscita

alfa (dB)

L

BIR

BER

T

Rivelati

BERp

BERd

Lcorrette

BERsk

Ttot

SBR

Tempo trascorso

Grafico visualizzato: BIR

Figure 2.7: The user interface of the Matlab simulator.

comprises optics, electronics, software and engineering of several components. It is composed of two entities, namely ALICE and BOB linked by a quantum channel and by a public channel. The protocol that we use is B92 protocol described in chapter 1 in order to keep the expense low. The channel for quantum transmission is a free space channel and this choice will be discussed shortly. Let suffice here to say that the system comprise a fully functional Adaptive Optic (AO) system for the correction of atmospheric induced beam wandering. Another public classical channel run in parallel of the quantum one. The reasons are multiple and they will be explained. The channel for public discussion is the internet. The electronics for control and synchronization is developed in FPGA (Field Programmable Gate Array) while the high level software for error correction, privacy amplification and for interfacing the system to the real world has been developed in Java. We can summarize the key feature of QuAKE in the following list:

- **B92 Protocol.**
- **Free Space Quantum Channel.**
- **Auxiliary optical channel.**
- **FPGA control electronics and synchronization.**
- **Java high level software for EC and PA.**
- **Internet public channel.**
- **Integrated AO system for correction of atmospheric induced perturbations.**

As you can see the system is very complicated and comprises several number of logical subsystem that has to be described. But first lets explain some of the choices that have driven the development of QuAKE.

2.2.1 The Free Space Channel

The choice of the free space channel has been done taking in considerations many factors. Firs of all the fact that our expertise in free space optics is higher than with fibers and fibers components. Second and more important the fact that the free space channel is less developed than fiber for quantum key distribution applications. This because many problems of this quantum channel have not been resolved yet, so although the free space channel is more versatile, in the sense that i am going to describe shortly, it is not very diffused in the QKD world. No one of the companies that commerce QKD apparatus has one running in free space! In fiber optical based QKD the main disadvantage is that the fiber itself must be dedicated. This because quantum repeaters do not exist: a quantum repeater would be able to ri-generate the signal (the quantum state) at any fiber infrastructure node without converting it into the electrical domain. The fact that nowadays the ri-generation can be done only switching the optical signal to electrical and then back to optical leads to a destruction of the quantum state of the single photon because it implies a measurement of the photon. That is why many research group are working on *quantum repeaters* [32, 16, 50]. It is clear so than there is a problem of integration of fiber based QKD into the fiber infrastructure: *a new fiber infrastructure as to be done in order to exploit global QKD*. Another issue correlated to the previous is the distance that such a scheme can reach. The fibers in fact are dispersive and they do not preserve in a perfect way polarization. In a normal telecommunication scheme this would not be a problem because a simple ri-generation would avoid it but in QKD this is a serious problem that limit the distance between transmitter and receiver up to ore or two hundreds of Km [38, 42]. These problems are completely resolved if the chosen quantum channel is the free space, clearly other arises but we think that an improvement in the solutions of those problems will bring to the possibility of a global satellite based quantum key distribution networks. Some effort have been done in the recent years by our group with the Matera Experiment [4] and by the european community and ESA with the Qips project in which, as mentioned, we are involved [71] actively. Another important fact is that in parallel to the development of QKD, FSO (Free Space Optics) technology is growing very fast and aim to solve the last mile distribution problem [92]. This would give a commercial push to free space apparatus even for the coverage of zones in which the application of fibers would be difficult. The smooth integration of free space QKD would then be relatively easy. Last but not least there have already been proposal for the integration of Quantum Cryptography into the 802.11 standard [56].

2.2.2 Costs and Time Considerations

QuAKE is a three year project started at the end of 2005. Mainly two persons namely me and Tommaso Occhipinti have worked on it from the initial project since now. We where followed by my supervisor and we followed some undergraduate students that did their thesis on this subject. The chronological development of the various parts of QuAKE has been driven by many factors: mainly experience and money. That is why the first part we developed has been the a simulator, used for studying QKD protocols and performances. Then we implemented and optimized the high level part of the algorithm inside the simulator and meanwhile we started to develop a Java version of the software that we could use in real life applications [21]. As already mentioned QuAKE is equipped with an AO system for correcting the atmosphere induced beam wander implementing the so called spatial filtering (See Sec. 1.3.4). The development of this system has been the next step and represent the main part of this thesis. In the same time the realization of the whole system has been carried on with the alignment of the optical components and the development of the electronics. At this stage a test of the AO system mounted inside the QKD system was possible. A resume QuAKE development is depicted in the Gant graph in Fig. 2.8.

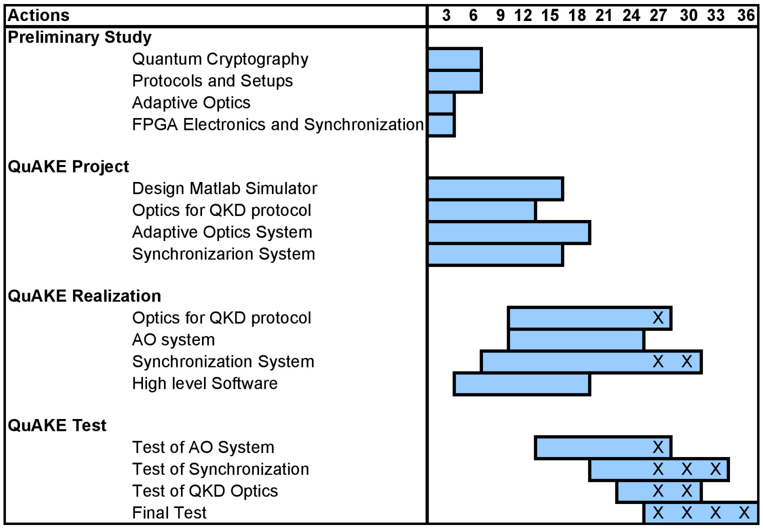


Figure 2.8: Gant diagram of the development of QuAKE. The “X” marked parts have to be completed.

QuAKE is a low cost system. Many mechanical and electronic parts have been developed in our labs. All the AO subsystem was realized in our labs including the deformable mirror, the electronics end the cables. Almost all of the non standard optical mounts were designed ad made manually at our department or at home. We can make a rough estimate of the costs for every subsystem of QuAKE: they are resumed in Tab. 2.2.2

The system then is a very low cost one and its dimension are very contained: the transmitter and the receiver are realized on two home made optical boards with dimensions of 40 by 40 cm. QuAKE is in our opinion a very *smart* system because it is tiny and low budget, easy to transport and easy to put your hands on. Nevertheless it employes innovative techniques such as FPGA electronics and Adaptive Optics that make the system valuable for research project, good

Subsystem	rough cost (Euro)
Quantum subsystem	6000
Synchronization	2000
High level software	500
AO subsystem	5000
Total	< 15000

Table 2.1: Rough estimate of costs for the development of QuAKE.

for didactical purposes and easy to modify and to put on a box for a future eventual business.

2.3 QuAKE Logical Design

2.3.1 QKD Layered Model

A QKD system can be envisage as a network protocol suite with different tasks, different communication channel and different algorithms. To be consistent and for a better explanation we will use a QKD layered model first introduced by Tommaso Occhipinti [60]. As a sort of an ISO-OSI stack it is in fact possible to specify three distinct level in a quantum key distribution system:

1. physical layer
2. data and network layer
3. application layer

It is possible to explain more accurately the Fig. 2.9, looking to the messages that pass through the interface between the physical and the data/network layers and between the data and the application layer. Not considering all the traffic type but only the messages coming from the low level to the upper level we can see that the physical layer gives to the data/network the so called *raw key* (See Sec. 1.3) while the data/network part bring to the application layer the secure key for the subsequent encryption of Alice or Bob plain text x. See Fig.2.10 that describes these concepts.

It is useful for the sake of simplicity in explanation of the key features of the system to look into the detail of each layer and describe the task each layer has to accomplish as well as the subsystems that will be analyzed in this thesis.

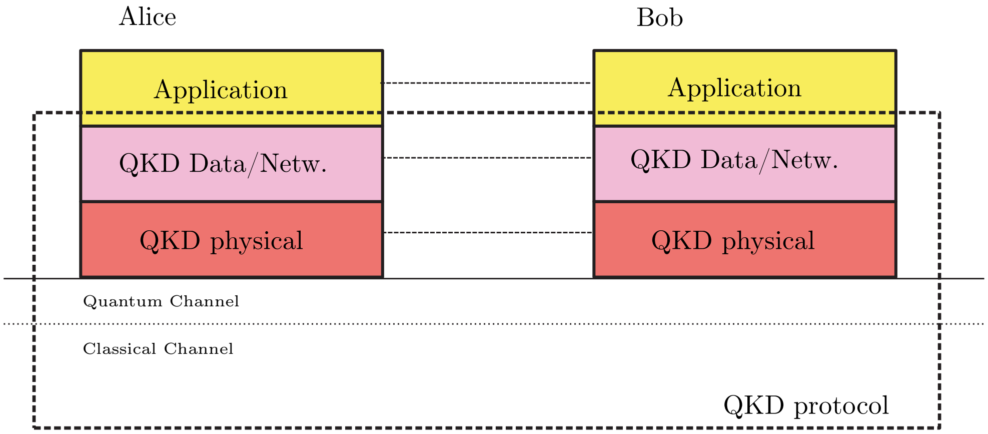


Figure 2.9: The layers in a full QKD system.

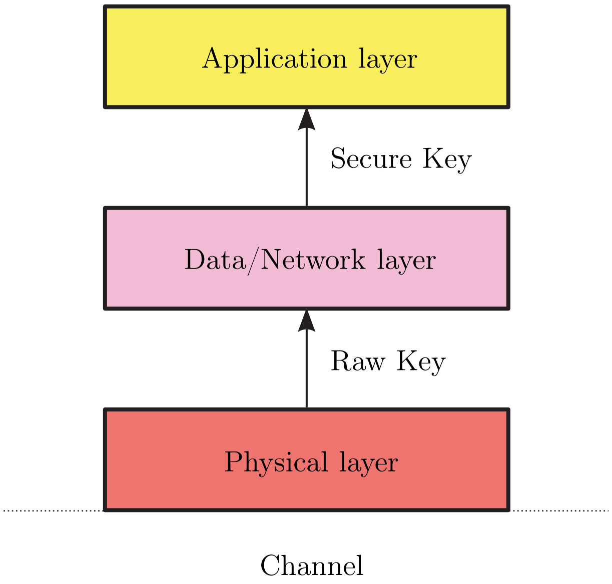


Figure 2.10: The raw key generated by the physical layer is taken by the Data/network layer and processed by means of classical algorithms in order to distill a secure key. This key is then used by the Application layer.

2.3.2 Application Layer

The application layer has a main important task to accomplish that can be summarized as follows:

- It takes the encryption keys from the data layer and it encrypts user data. These data are then secure and ready for a transmission through an untrusted channel.

The realization of this layer is up to the final user and completely separated from the quantum protocol itself which has as main goal the generation of a secure key. Some effort has been done in order to integrate the whole QKD key generation procedure into IPSEC[4] standard [34] so enhancing the concept of VPN (Virtual Private Network) considering the keys generated by QKD. For the purpose of this work it is enough to distinguish between two different ways in which the application layer could use the QKD keys.

1. using them inside conventional encryption algorithms for example the symmetric cyphers AES (Advanced Encryption Standard) or Triple DES[5] (Triple Data Encryption Standard). This method is a very good compromise between the innovation of QKD and the maintainance of the present information technology infrastructures, moreover it requires not so high performances in term of key production rate from the QKD physical layer. Clearly the security is weaker because we encode a message that has a size much greater than the key itself (see Sec. 1.2.2).

2. taking secure QKD keys for One Time Pad encryption. OTP is not very popular now, the main reason being the fact that the size of the key has to be equal to the size of the message and so the problem of key establishment is very hard. QKD at high rate can in principle solve this problem making OTP more attractive even for the internet community.

Usually the first method is used mainly because the key generation rate of a QKD system cannot guarantee enough bits for OTP encryption. Is has to be said that there exists a way in between these two strategies that has been proposed by the Indian division of Alcatel-Lucent and consisting of a cryptosystem capable of generating infinite bit keys starting from a small amount of secure bits exchanged by means of QKD [77]. It is not clear though if this method can keep the security level of Quantum Cryptography. In our prototype the application layer has not been implemented but as we will see a very good and flexible interface between the layers has been realized in order to make the secure keys available for any implementation of the application layer.

[4] IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

[5] AES and 3DES are considered the state of the art encryption algorithms nowadays.

2.3.3 Data and Network Layer

The Data and Network layer is an heteregeneus layer. We can summarize its possible tasks as follows:

- It has to detect for the presence of an Eavesdropper (Eve) during the quantum communication and communicate it to the application layer.
- It has to manipulate the raw material (raw key) coming from the physical layer in order to generate a secure key for the application layer.
- It has to perform authentication between Alice and Bob.
- It manages the creation of keys and the authentication between different users realizing a *quantum cryptography network*.

The last task is accomplished only if a network of quantum key distribution links is present. In fact only few implementation of QKD has more that two parties involved [34]. Usually the networking is very simple or completely absent. The data and network layer is indeed part of the QKD protocol, whether or not a networking sub-layer is present. The raw key coming from the physical layer has to be processed in order to get a secure key (see Sec. 1.3.3). The procedures of sifting, error correction and privacy amplification has to be performed by this layer using a public classical channel. It is important to remember that any information in this layer and above this layer is stored and processed by means of classical bits. In this sense is very similar to classical communication layers even though the tasks it performs are an essential part of the QKD protocol.

In QuAKE the Alice and Bob data layer can be represented as in Fig. 2.11

The raw key is passed from the physical layer to the data layer which by means of a public untrusted channel performs on the key the operations of sifting, error correction and privacy amplification. The secure key is then given to the application layer. We decided to implement the data layer in Java and the software that take care of all the procedures is called QCore and will be described in detail in chapter 6. The key are stored in databases so they can be readily used by the application layer. Concerning networking QCore has been designed taking in consideration future developments that include networking features (see. Sec. 6.5.2).

2.3.4 Physical Layer

The physical layer is by far the most complicated in QKD. At a first glance we can say the main task of the layer is to use the quantum channel to transmit

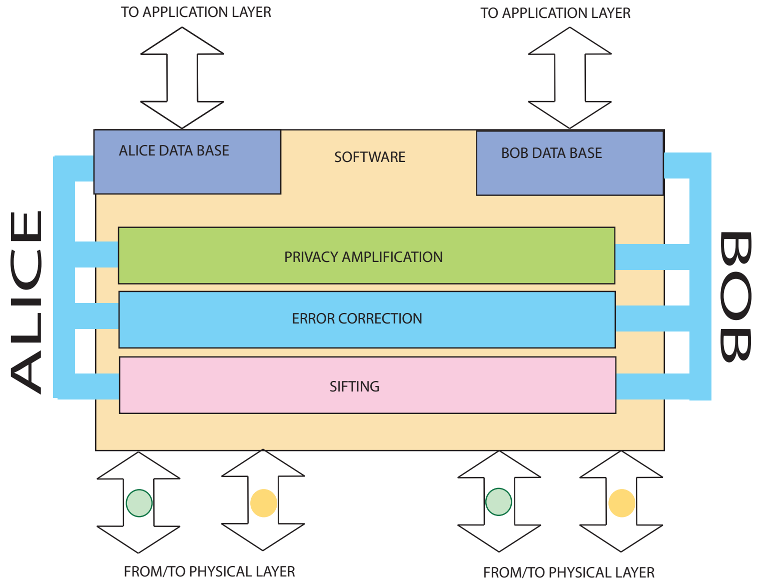


Figure 2.11: Data Layer of QuAKE. It takes the raw keys from Alice and Bob physical layer and performs sifting, error correction and privacy amplification by means of the public channel. It gives the secure key and control signal to the application layer.

qubits from Alice to Bob according to one of the QKD protocols. This can be summarized as follows:

- Alice apparatus has to generate quantum states and encode random information on them.
- Alice has to send these states to Bob using the quantum channel.
- Bob has to measure the states and detect them.
- Alice and Bob has to give respectively the encoded information and the measured information to the data layer.

Notice that in this layer Alice and Bob present evident differences either in the task they have to do and in the apparatus they use. Clearly each of the tasks described is not easy to implement because it requires hardware, electronics, software and efforts. That is why almost all pioneering works in QKD and some of the recent as well just showed efforts to improve the physical layer. The layer can be improved in many ways, either in the quantum communication channel ([51],[71]) or adding interesting features to the transceiver apparatus for instance a public optical classical channel for standard optical communication, synchronization or other purposes.

In QuAKE the physical layer has many features that need to be explained. A schematic of QuAKE physical layer is depicted in Fig. 2.12.

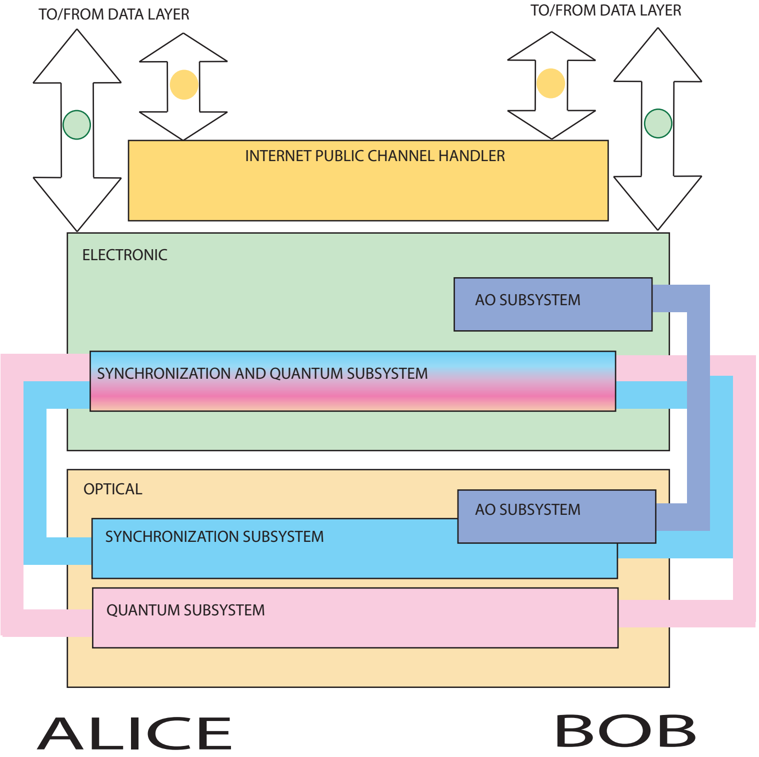


Figure 2.12: Physical layer of QuAKE. The various subsystem are present: electronics, optical and internet management. The Adaptive Optics (AO) subsystem in visible in the Bob side.

The physical layer of QuAKE can be divided into several subsystem, each one can comprise electronic and optics. Three main subsystem can be individuated called respectively *synchronization* , *quantum*, and *adaptive optics subsystem.*

- **Quantum subsystem:**

  this subsystem does exactly the tasks that are required for the establishment of the raw key from Alice to Bob. It comprises an optical apparatus and an electronic controller.

- **Synchronization subsytem:**

  this subsystem has been added in order to facilitate the synchronization between alice and bob. It exploits a classical optical channel that runs in parallel to the quantum one. Like the quantum subsystem it comprises both optics and electronics.

- **Adaptive Optics subsytem:**

  this subsystem has been added in order to correct for the tilt induced by atmospheric turbulence. Is is working only at Bob side.

Each of these subsystem concur to the exchange of the raw key between Alice and Bob. The Quantum and Synchronization subsystems will be described in chapter 3. Since the AO subsystem is one of the main improvement that we introduced we will describe it in details in chapter 4.

Chapter 3

Optical Setup, Electronics and Synchronization

In this chapter part of the physical layer of QuAKE will be analyzed, in particular a description of the quantum subsystem and the synchronization subsystem will be given. After a brief review of the logical schematic of QuAKE physical layer a separated description of Alice and Bob optical setup and electronic will be made.

3.1 Introduction: Design Choices

The main characteristic of this two subsystem is to make possible the transmission of the raw key between Alice and Bob. For this scope the quantum and the synchronization subsystem have to work together. In this chapter a description of the system is given considering the just cited integration between different subsystems. First some of the key features regarding the quantum and synchronization subsystem will be introduced.

3.1.1 Qubit Source

We decided to use the *Weak Coherent Pulse (WCP)* technology in order to generate the quantum state. In particular we used laser diodes from WorldStarTech[1] that we attenuated down to the single photon level starting from pulses of 20ns. This technology has been demonstrated as valid as the entanglement based QKD in terms of security [3, 27]. The distribution of photons

[1] http://www.worldstartech.com/.

inside a laser pulse follows a Poissonian distribution:

$$P(\mu, l) = e^{-\mu} \frac{\mu^l}{l!} \tag{3.1}$$

We can act on the mean parameter μ in order to set the desired value in order to maximize the pulse with one photon and minimize the number of pulses with two or more photons. In many implementation of faint pulse QKD a value of $\mu = 0.1$ is used. This lead to the probabilities of obtaining zero or one photon in a pulse:

$$P[n_f = 0] = e^{-\mu} = 0.905 \tag{3.2}$$

$$P[n_f = 1] = \mu e^{-\mu} = 0.090 \tag{3.3}$$

The probability to have instead more that one photon per pulse is:

$$P[n_f > 1] = 1 - P[n_f = 0] - P[n_f = 1] = 1 - e^{-\mu} - \mu e^{-\mu} = 4.7 \cdot 10^{-3} \tag{3.4}$$

After the first fully functional implementation some research group has pointed out that the mean photon number μ has to be determined taking in consideration the whole QKD protocol with sifting, error correction and privacy amplification. Following the result for a fiber based QKD system obtained by Elliot in [63] we used our Matlab simulator in a free space case with the parameters of our system. The result is reported in Fig. 3.1.

The transmission efficiency (i.e. the ratio between the transmitted pulses and the final secure key rate) is plotted against the mean photon number μ. The different curves represent different BER in the sifted keys i.e. different channel conditions. It is possible to notice that the maximum is obtained for $0.5 < \mu < 0.7$ depending on the BER. This effect of shifting of the best mean photon number from $\mu = 0.1$ to higher is mostly due to the benefit of the privacy amplification process. We have chosen $\mu = 0.6$ for our system.

The qubit is encoded in polarization. For the B92 protocol two non orthogonal quantum state have to be generated. We used vertical and 45 degrees polarization. The alphabet we used is resumed in Tab. 3.1.

Symbol (a)	Alice
0	$\lvert\leftrightarrow\rangle$
1	$\lvert\nearrow\!\!\!\!\swarrow\rangle$

Table 3.1: Modulation alphabet.

The choice between the state to send is done by a random number generator. In QuAKE the random number generator is a software one. In the system

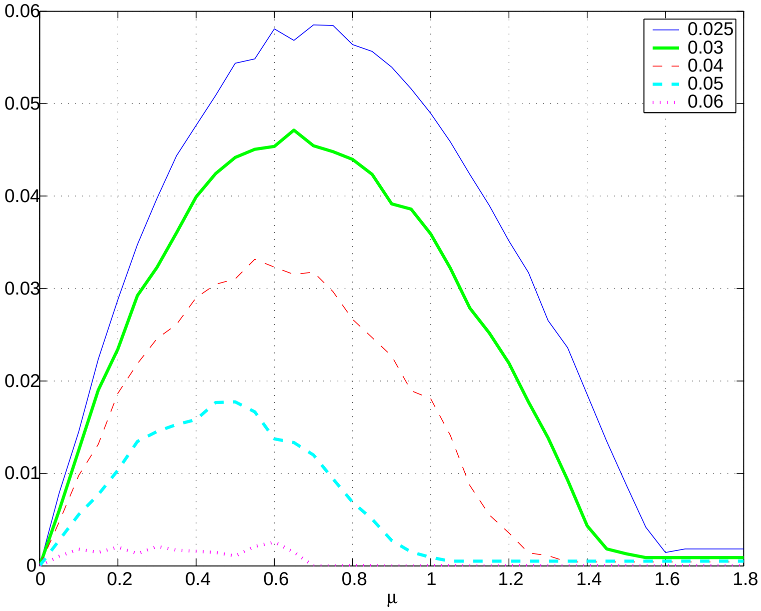


Figure 3.1: Transmission efficiency versus mean photon number per pulse at different BER between sifted keys.

we have two distinct laser, called *signal laser one (Ls_1)* and *signal laser two (Ls_2)* that fire according to the value of the random number generator. The single photon generation is resumed in Tab. 3.2.

Quantum Communication	
Qubit $\|\updownarrow\rangle$	WCP laser with polarizer
Qubit $\|\swarrow\!\!\nearrow\rangle$	WCP laser with polarizer
T_{SLOT}	20 ns
Power of the Ls_1 and Ls_2	3.5 mW
Attenuation for WCP	77 dB^2

Table 3.2: Generation of the qubits at the transmitter.

3.1.2 Synchronization

In a QKD system the synchronization can be done in several ways. The main goal is to obtain a temporal filtering for the transmission. This means that it is essential to know that the measure made by Bob at a certain instant t_1 is the measurement of exactly the qubit sent at the instant t_0 by Alice. This is important for several reasons in particular for noise reduction, rejecting the signals that arrive outside of a specified time windows will preserve from unwanted detection. Moreover it is important to exploit the characteristics of the optical detectors used in the communication system. The single photon detector (SPAD, Single Photon Avalanche Diode) for example, after every detection, have a dead time (from 40 to 100 ns) in which it can not detect any photons, and for this reason any unwanted detection has a double negative effect: it is unwanted as it decreases the final secure key rate and it blinds the SPAD for the duration of the dead time preventing the detection of a good photon. This is why any QKD system, either in free space or optical fiber based, can be run with or without the so called gated mode. In the fist case the detectors run freely detecting everything they can. In the second case we would Òswitch onÓ our detector only when we expect the arrival of one of the sent photon. Time synchronization is important for both methods: to assign a precise time tag or to open the gate of our receiver only at the right time. Nevertheless the first method is very sensible to noise for the reasons mentioned before and it is not considered feasible. That is the reason in QuAKE we used the so called gated mode. Another difference between synchronization methods come from the way we distribute the time signal between Alice and Bob:

- **external synchronization**

  In this case both Alice and Bob have their own timing clock. As soon as the two clocks are relatively synchronized (same starting point) they can be used either for the photon tag in non gated mode or for the gate signal reference in gated mode. The relative synchronization of the two clocks is normally done in advance by means of the use of Pseudo Random Sequences and then adjusted during the communication phase [49]. We are currently working on the *Harrison Project* in order to study and implement this type of synchronization. A first theoretical analysis performed by means of our QKD simulator can be found in [22].

- **self synchronization**

  Alice and Bob can extract the synchronization signal by the transmitted data as many usual telecom- munication schemes do. Since in QKD we deal with single quantum state transmission and detection in order to implement this kind of synchronization an additional bright laser is needed [12]. In some case, namely when the protocol used exploits four or more quantum state generated by separated devices, it is possible to use as synchronization event the simultaneous click of all the detector so avoiding a dedicated APD [24].

The *self synchronization* is the technique we have chosen for Quake at least for an initial stage of the project. We implemented it using a third laser, called *synchro laser (Ls_s)*, in the same optical path in order to transmit information about the timing of the system. We organized the communication in *frame* and *slots*: a slot corresponds to a couple pulse of the transmitting laser whereas a frame is a collection of 512 slots. The number of frames to be transmitted at every communication is adjustable and can be chosen accordingly to the needs and the capabilities of the transmitting electronics (max 15000 frames/transmission). The number of slot and frame are communicated using a pulse width modulation (PWM) of the laser Ls_s changing the duty cycle d_c. The clock reference is instead transmitted using on off modulation (OOK) of the same laser during the transmission. The additional classical channel is resumed in Tab. 3.3.

Classical Communication	
Rate of transmission R	1.25 MHz
Synchronization	OOK
Frame/Slot message	PWM mod. (d_c = 25% to 40%)
N_F Number of frames	variable
N_S Number of slots	512

Table 3.3: Characteristic of the synchronization subsystem at the transmitter.

In order to decide the starting point of the transmission a so called *starting sequence* is also present at every communication. It consists of a certain number of bright synchronization pulses with a duty cycle of 25%. After this sequence the frame encoding starts and run continuously at each frame until all the frame are transmitted. A new communication will require another starting sequence to be transmitted.

3.1.3 Choice of the Transmitting Wavelengths

The choice of the wavelength of the signal (Ls_1 and Ls_2) and synchronization (Ls_s) has been done taking in consideration several factors. First we have a peculiar response of the quantum efficiency of the single photon detector (SPAD) that has values that vary from 50 to 10 % in the range 400−900nm (see App. B.0.1). Outside this range the quantum efficiency goes to unacceptable values. We then have to choose a value in this range. The light has to propagate through atmosphere in a free space channel. We then has to choose between one of the telecom windows for free space communication. A picture of the transmission of the atmosphere is depicted in Fig. 3.2.

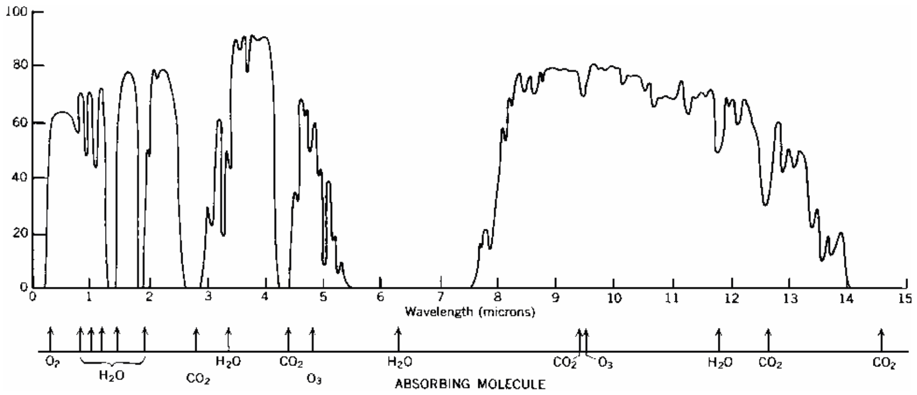


Figure 3.2: Transmission bands of hearth atmosphere. On the y axis the percentage transmittance.

Another factor that we have to take into consideration is that although we want different wavelength for the syncro and the signals lasers we do not want them too different. The reason for that being that we would like to use the synchro laser also fot the Adaptive Optic subsystem (see. Chapter 4) in order to measure the effects of the turbulence on the beam. Those effects are wavelength dependent, that is why the two lambda have to be close to each other. Last but not least the costs of the laser diodes in general increase with frequency. An infrared or red laser is less expensive that an blue or violet on. After all these consideration we have chosen a wavelength of $850nm$ for the signals laser Ls_1 and Ls_2 and a wavelength of $808nm$ for the synchronization laser Ls_s.

3.2 Transmitter: Alice

3.2.1 Optical Setup

All the concept explained in the previous section are included in the optical setup of the transmitter. The full optical setup at alice side is described in Fig. 3.3.

The two subsystems are sketched in separated blocks. In this design also the Adaptive Optics subsystem is included and in the case of the transmitter it coincides with the synchronization subsystem. The 3.5mW, 850nm laser diode are collimated with a built in lens. Then they are polarized in order to enhance the intrinsic low polarization (Ls_1 and Ls_2 extinction ratio respectively of 4.86, 9.25) by means of two polarizing beam splitter cubes. The measurement of polarization with the polarizing cube are reported in Fig. 3.4.

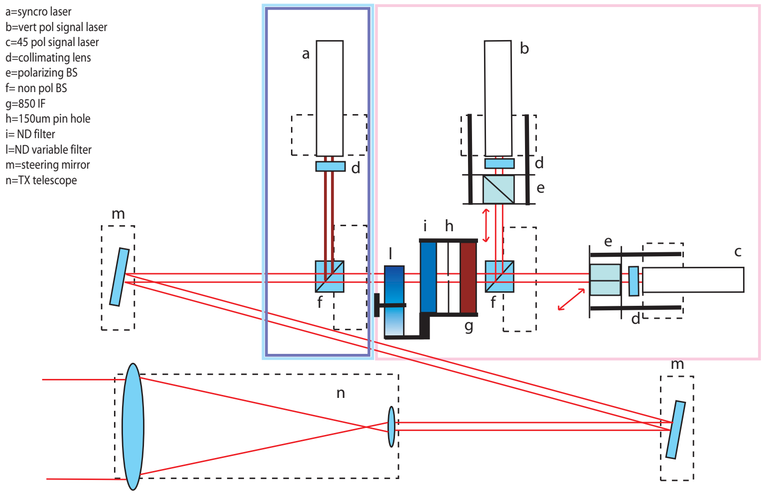


Figure 3.3: Optical setup of QuAKE transmitter.

The two signal lasers are then combined with a non polarizing beam splitter, spectrally filtered using a 10nm bandwidth interferential filter centered at 850nm , partially spatially filtered using a 500μm pin hole and attenuated down to the single photon level with some fixed and variable neutral density filters. Considering that the the signals lasers travels along two balanced beam splitter, the pin hole and the interferential filter the residual attenuation needed can be deduced from Fig. 3.5 and it is 21×10^3 i.e. 43.2 dB for a mean photon number per pulse $\mu = 0.6$ on our 20 ns pulses[3].

The synchronization laser Ls_s (808nm, 10mW) is added to the optical path by a second beam splitter. Two steering mirrors direct the beam that is now the sum of the single photon sources Ls_1 and Ls_3 and the syncro bright laser Ls_s towards a transmitting telescope with a magnification of $M_{Tx} = 12$ that produces a well collimated beam of 4.5cm of diameter.

3.2.2 Control Electronics

The transmitting electronic control unit is implemented with a digital input output board from NI (National Instruments), previously used in another system in the LUXOR, optical laboratory. This board (PCI DIO 32 HS) is an internal PCI board pluggable inside a personal computer.

Is has to be said that the National Instruments board is not the perfect candidate to accomplish this task, it is a digital input/output board and usually

[3] Notice that the characterization of the source has to be done taking into account also the quantum efficiency of the single photon detector.

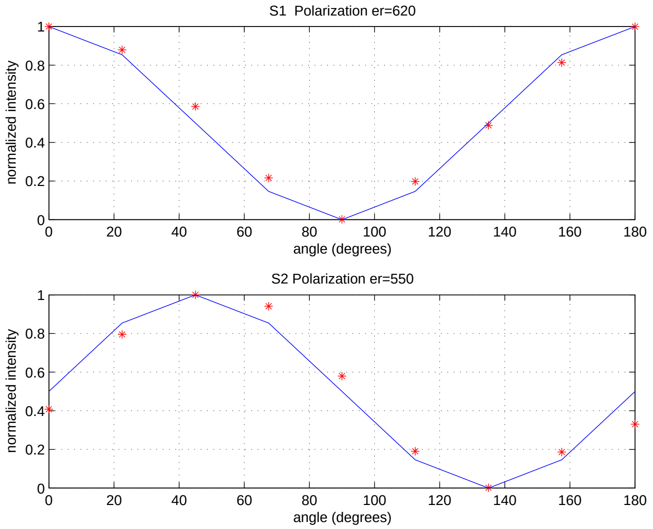


Figure 3.4: Polarization of the signal lasers, notice that the first has a maximum at 0 degrees whereas the second has a maximum at 45 degrees. The extinction ratios are respectively 620 and 550. The continuous line is the theoretical squared sine behavior.

it works with other compatible boards by NI. We removed the standard cable that extends the IO pins in the back of the board and we replaced it with a SCSI external cable. Then we designed an adaption board composed essentially of some trimmer, a buffer, and a stabilized power source that could drive the three lasers and match the impedances. In the next figure (Fig. 3.7) we show the electronic schematic, where it is possible to observe the further 5V external power supply that guarantees the correct driving conditions for the lasers. In Fig. 3.8 a picture of the adaption board.

The electronic at the transmitter can guarantee for the moment signal pulses which duration is 20 ns. This value is considerably high for application for quantum cryptography and we are working on a further improvement: this would be either an analog circuit for shrinking the pulses or a change of technology namely the use of FPGA (Field Programmable Gate Array) like already done at the receiver (see Sec. 3.3.2). A simple software has been developed in $C++$ order to drive the transmission at the receiver. With its interface, represented in Fig. 3.9 it is possible to: a) choose the repetition frequency of the synchronization laser L_{s_s}; b) choose the number of frames to be transmitter ; c) set on or off the signal lasers independently for test purposes ; d) generate a test square wave ; e) choose whether to save a file on the hard disk or not ;

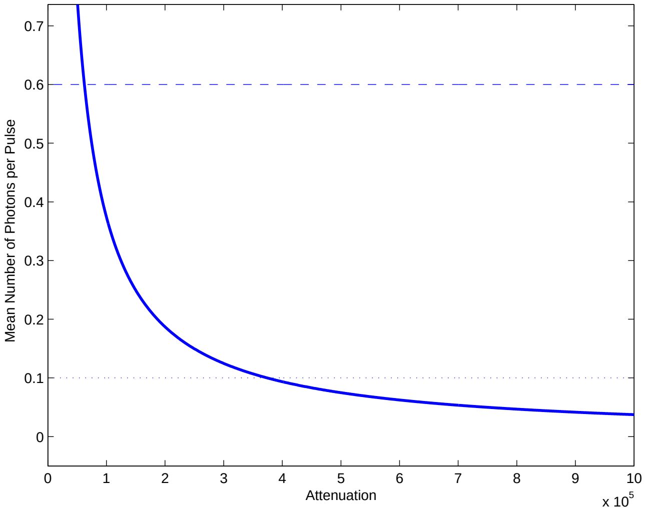


Figure 3.5: Residual Attenuation for a fain pulse source with $\mu = 0.6$.

f) generate a random key.

As discussed early in Sec. 3.1.2 we use a PWM modulation at the beginning of each frame in order to identify it. In Fig. 3.10 is reported an oscilloscope image that shows an example of frame header composed of a code identification of 9 bits in between a *start* and a *stop* bit.

3.3 Receiver: Bob

3.3.1 Optical Setup

The optical setup of the receiver (BOB) is depicted in Fig. 3.11. The beam coming from the transmitter is demagnified (M=0.13) by a 5cm aperture telescope and then directed to the deformable mirror that at this stage can be considered a flat mirror. The beam is focused by a lens and divided by an 850nm interferential filter. Remember that the incoming beam is composed by two different wavelengths: the signals wavelength (850nm) pass through the filter and directs towards the *quantum receiver*, the synchronization wavelength (808nm) is reflected by the filter and goes half into the Adaptive Optics detector (the PSD described in Sec. 4.3) and half into what we have called *Synchronization detector*.

The *quantum receiver* is composed by three beam splitters and two SPADs

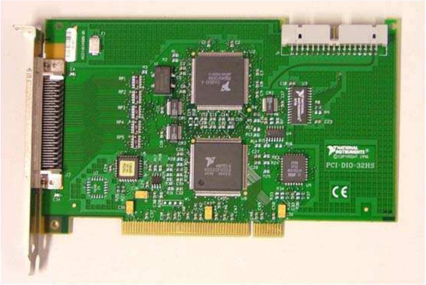


Figure 3.6: PCI DIO 32 HS, digital input output PCI board. This is the driving board for the three lasers.

(Single Photon Avalanche Diode). The first beam splitter has the function of randomly selecting the measurement base according to the B92 protocol (see Sec. 1.3.2). The other two beam splitters are polarizing beam splitters and has the role of filter in polarization the incoming photons. They are rotated orthogonally with respect to the polarization set for the photons at the transmitter, this as well according to B92. The SPADs (see a full description in App. B.0.1) have a detection efficiency at 850nm of 10% and an active area of $50\mu m$. They have a $GATE$ input that is used for synchronization as described in Sec. 3.1.2.

The Adaptive Optics detector can be avoided for the moment. The whole AO system is described in the next chapter. The Synchronization detector is composed by a 10nm bandwidth interferential filter that select the 808nm of the synchronization laser and a avalanche photodiode that has a TTL output and is sensible for PWM modulation as required by our classical communication channel.

3.3.2 Control Electronics

The electronics of Receiver has been developed in a system on chip (SoC). The main tasks the receiver has to accomplish are:

- synchronization
- creation a control function for the SPADs
- time tagging of all the arrival of single photons
- recovering from synchronization problems

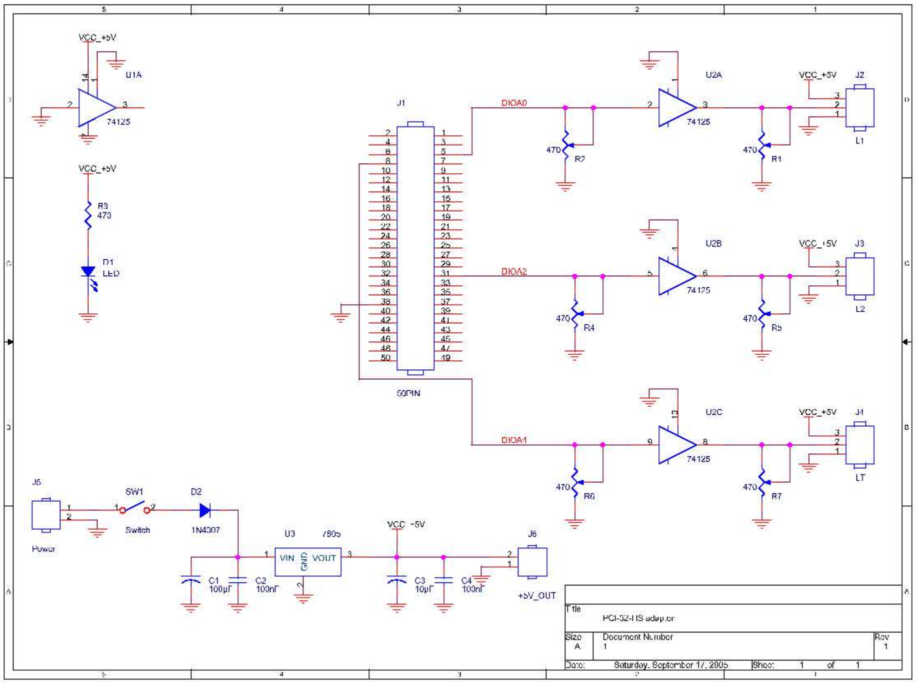


Figure 3.7: Electric schematics of the impedance adaption board. The stabilized power supply of the three lasers is also present.

- storing of all the time tags and statistics into the RAM
- communication with the Bob data/network layer

The board containing all the electronics is a Xilinx Development Boards (ML403, Fig. 3.12) where are present a lot of component and microelectronics chips, but in particular we used these features:

- the FPGA (Virtex 4 Lx, speed grade 11)
- high speed had hoc electronic core (inside the FPGA)
- a PowerPC (300 MHz) micro processor (inside the FPGA)
- 64 MB DDR RAM
- the serial cotroller
- several LEDs for tests

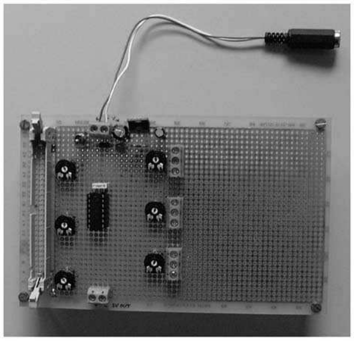
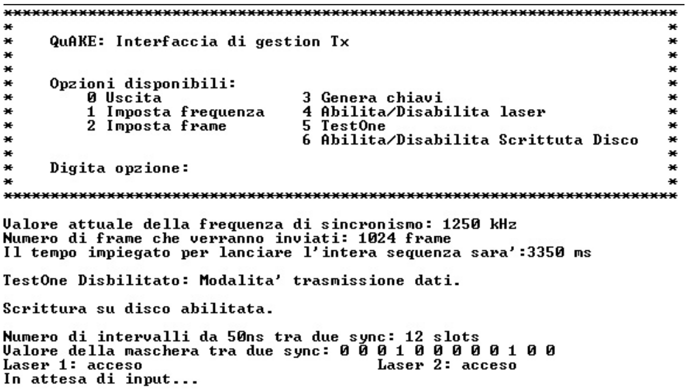


Figure 3.8: A picture of the adaption board



```
************************************************************************
*                                                                      *
*    QuAKE: Interfaccia di gestion Tx                                  *
*                                                                      *
*                                                                      *
*    Opzioni disponibili:                                              *
*        0 Uscita               3 Genera chiavi                        *
*        1 Imposta frequenza    4 Abilita/Disabilita laser             *
*        2 Imposta frame        5 TestOne                              *
*                               6 Abilita/Disabilita Scrittuta Disco   *
*                                                                      *
*    Digita opzione:                                                   *
*                                                                      *
************************************************************************

Valore attuale della frequenza di sincronismo: 1250 kHz
Numero di frame che verranno inviati: 1024 frame
Il tempo impiegato per lanciare l'intera sequenza sara':3350 ms

TestOne Disbilitato: Modalita' trasmissione dati.

Scrittura su disco abilitata.

Numero di intervalli da 50ns tra due sync: 12 slots
Valore della maschera tra due sync: 0 0 0 1 0 0 0 0 0 1 0 0
Laser 1: acceso                         Laser 2: acceso
In attesa di input...
```

Figure 3.9: Simple text interface at the transmitter side.

In the following pages we outline some of the many features of the receiver electronics. The idea of making it in a System on Chip was very useful both for implementing efficiently all the function and for acquiring a good know-how and different skills that we can apply also to different systems and experiments. At the beginning of QuAKE development, we were totally new to the FPGA technology and VHDL programming language, but now we think that using the Virtex4 FPGA we can have shorter time of development in any project where the digital performance are mandatory (an example have been the realization of a coincidence detector that we realized described in [14]).

All the electronic project is divided into the next two parts:

1. **High Speed Electronics (HSE)**

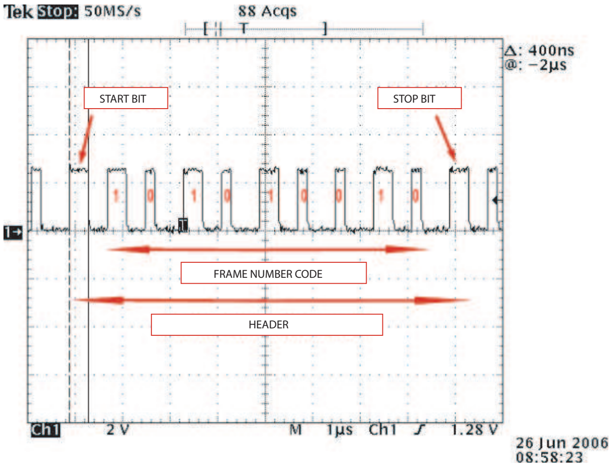


Figure 3.10: Example of the Pulse Width Modulation used to encode frame information.

The HSE is the core of the Bob Receiver and it is described in deep in the next pages. In Fig. 3.13 it is shown all the HSE circuitry which main functions are make the synchronization the systems, read the headers of the data, control the two SPADs and finally create the data for the local storage (DDR RAM).

2. **PowerPC, IO BUS and RAM**

   This part of the FPGA project is essential for the management of the data coming from the high speed frontend. It has been designed with the EDK software by Xilinx. We used this proprietary tool to connect the HSE to the local IO BUS of the PowerPC, in particular to the OPB[4] with the IPIF[5] . Then we tested a C++ programming of the PowerPC in order to transfer the data to the DDR RAM and to send this data, after the stop signal coming from the high speed electronics, to the data network layer (QCore) through a serial RS232 connection. We developed a simple communication language between the PC where runs the data/network layer and the system on chip where is present the PowerPC. The messages between the physical layer and the QCore layer are essentially the data about the timetags (raw key), a simple statistics (number of double counts, see 3.3.4, of none counts, number of synchronization losses and start/end of transmission).

[4] On Chip Peripheral Bus

[5] OPB Intellectual Property Interface

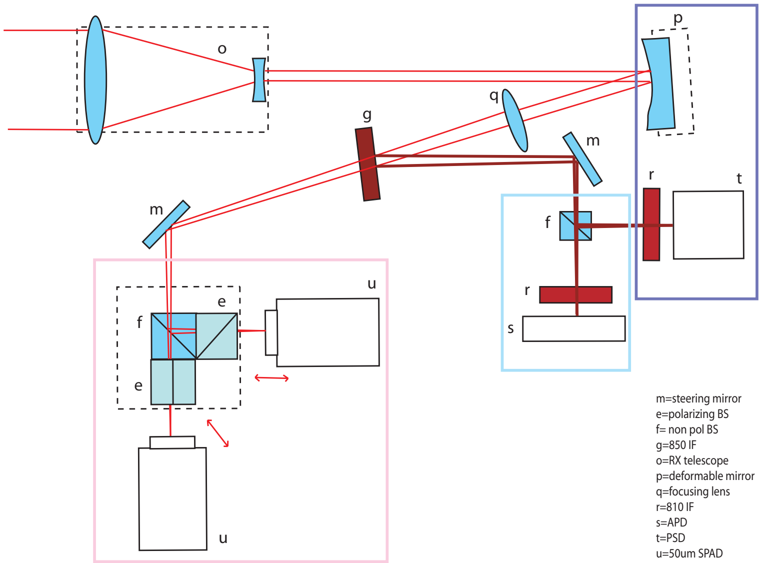


Figure 3.11: Optical setup of QuAKE receiver.

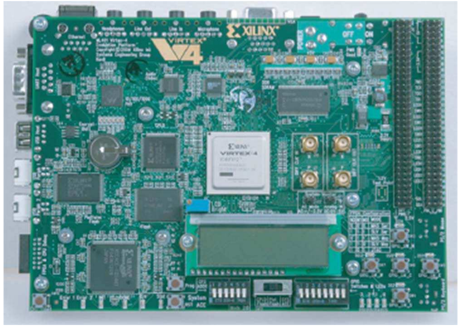


Figure 3.12: This is the SoC board, containing in particular a Virtex 4 FPGA by Xilinx

3.3.3 Implementation of the Synchronization

As explained is Sec. 3.1.2 the synchronization assume a fundamental role when dealing with single photons. We decided then as said, to add to the optical setup a further *synchronization laser* at 810nm that has been used to assure a time reference communication between Alice and Bob at the frequency of 1.25MHz. To do that the electronics at the receiver has to comprise two logical blocks: a sort of digital phase locked loop (DLL) and a start/stop sensitive detector (we call it *synchronizer*). As we will se the synchronizer will benefit from the PWM modulation of the synchronization signal. In Fig.

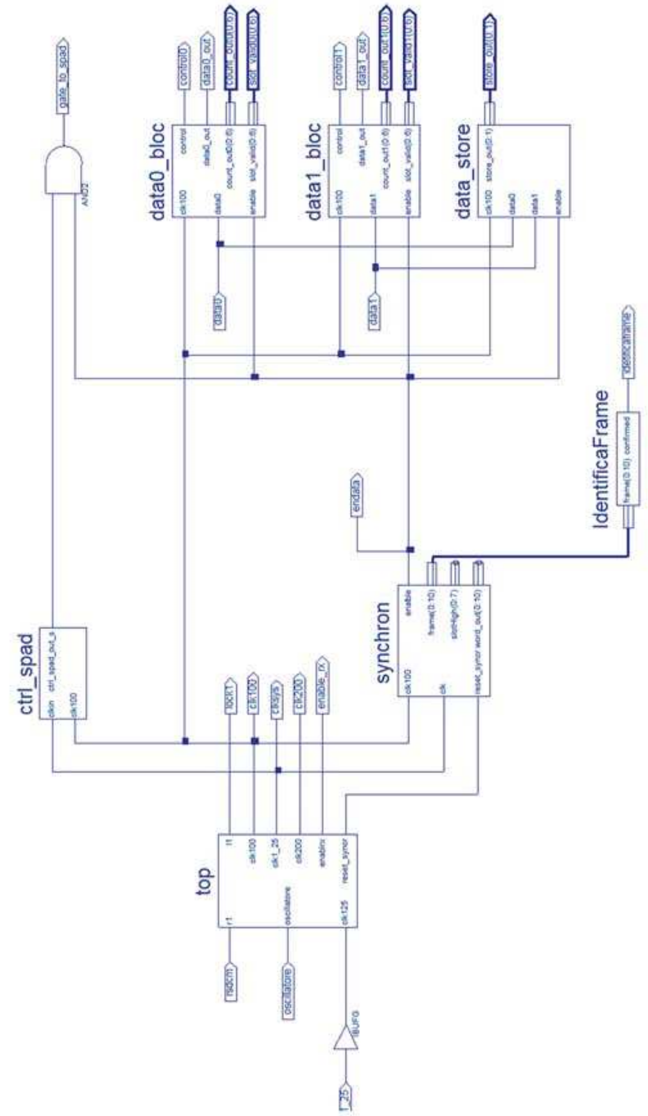


Figure 3.13: The block diagram of the high speed electronic frontend, HSE (Xilinx ISE picture). We have connected this macro-block to the PowerPC input output BUS in order to transfer the time tags from this block to the DDR RAM.

3.13 is shown that we have a block called TOP that, apart from a RESET input, takes the 1.25 MHz signal coming from the APD of the optical receiver setup and a 100 MHz clock coming from a local oscillator inside the ML403 Board. With the help of a DCM Digital Clock Manager (See Fig. 3.14) , we can multiply by 1, 2 and 3 the input 100 MHz clock and then with the block called CAMPIONATORE we can sample the signal coming from the APD. The outputs of the TOP block are the three clocks and the version of the 1.25 MHz clock in phase with the other three.

In this version of the HSE, our phase precision is then given by half of the maximum frequency of the internal sampling clock, 2 ns.

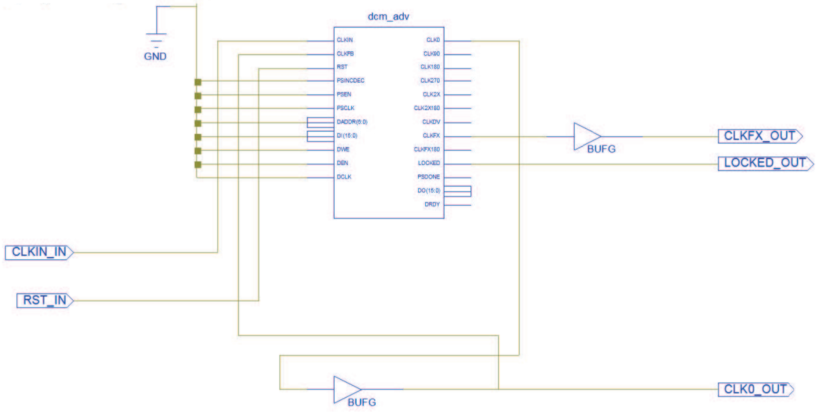


Figure 3.14: The Digital Clock Manager used in the receiver electronics.

In Fig. 3.13 is also present the block called SYNCHRON. This block can extract the pulse duration modulation inside the 1.25 MHz clock and give to the electronics the information on start/stop events and number of frame inside each transmission of a random message by the Transmitter. It takes in input the 1.25 MHz clock (from the output of the TOP block) and sends to the output the frame code and a ENABLE signal for all the next block of the HSE.

3.3.4 Generation of Gating Function

We decided to implement a GATE function for the two SPADs. This because: a) we want to mitigate the background noise. In fact some photons of the background with a lambda compatible to the 850 nm of the interferential filter can trigger the SPADs detectors. In this case we could have an error count and consequently an error time tag; b) during the transmission of the bright pulse (1.25 MHz) some photons can reach the single photon detectors even if the synchro-signal is an 810 nm optical signal and then it should be filtered out. This event can occur as the interferential filter is not ideal. In Fig. 3.15 is represented a scope image triggered on the gate function that show the delay between the rising edge of the gate pulse and the output pulse of a detected event.

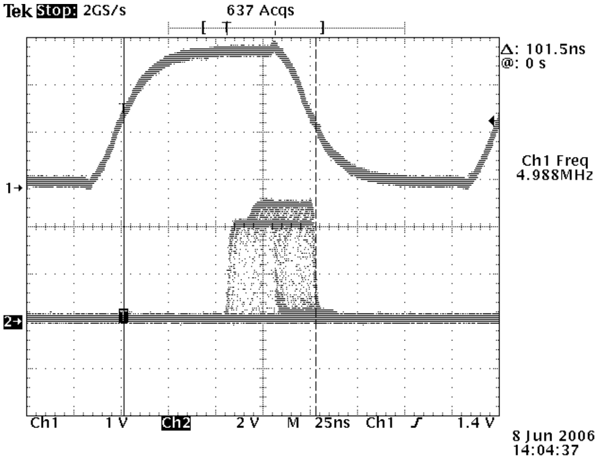


Figure 3.15: A scope picture showing the gate pulse and the event pulse out of a SPAD. Notice the delay (60 ns) between the opening of the gate and the effectiveness of the detections.

In our system we have made a time window function called CTRLSPAD function that reaches the two SPADs in order to gate them. Initially we designed the receiver with the top performances but due to some restrictions given by the Xilinx hardware (both the ML403 hardware and the IP block by Xilinx) we have reduced the number of open windows between two synchronization reference pulses to two. The number of open windows can be easily changed to fit to different boards or configurations. In Fig. 3.16 we present a screen picture of the oscilloscope representing the CTRLSPAD function composed of two gating pulses between two synchronization pulses. From Fig. 3.17 it is possible to see the *enable* function that goes to an high value only when the frame code identification is decoded correctly. Only when this happens the gate pulses are delivered to the detectors. Again, in Fig.3.13 is possible to discover on the top right the block called CTRLSPAD that creates the gate function for the two SPADs.

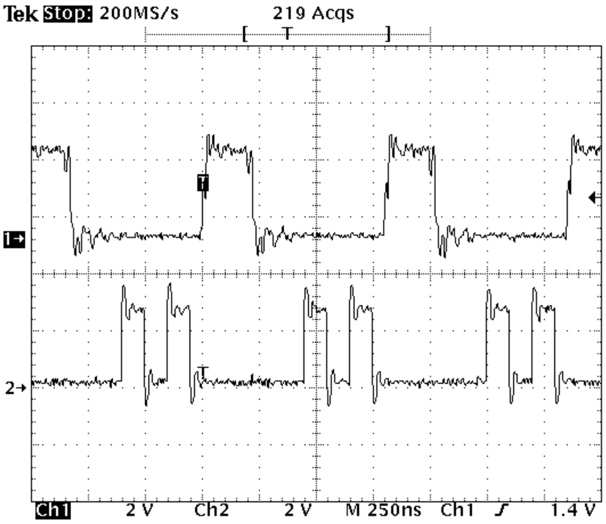


Figure 3.16: The CTRLSPAD function in the case of 2 open windows. The upper signal is the bright pulse for the synchronization, the bottom one is the CTRLSPAD function.

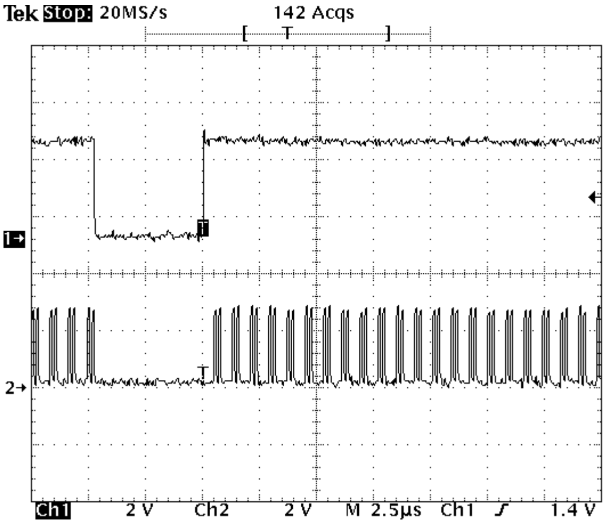


Figure 3.17: The Enable function that prevents the gate function to be delivered while the frame code is being decoded.

Chapter 4

Adaptive Optics System For QKD

In this chapter we analyze the Adaptive Optics subsystem. We start with an introduction on atmospheric turbulence on beam propagation, we then describe the the optical setup and the main components of our system and present some results.

4.1 Atmospheric Turbulence

4.1.1 Introduction

Small variations in temperature ($< 1^oC$) cause changes in the wind velocity (eddies). The small changes in the atmospheric density that occurs give rise to a variation of n, the index of refraction, on the order of 10^{-6}. These variations can accumulate in time and influence drastically the phase of a beam propagating through the atmosphere. The effects on the wavefront could cause beam wander, scintillation and spreading.

These effects have been studied since many years. Although it is not a time invariant, easy to model phenomenon there are various approaches that try to model it. The most used and verified is the Kolmogorov model [48]. He studied the mean-square velocity difference between two points in space separated by **r**. He derived a structure tensor of the form:

$$D_{ij} = \langle [v_i(\mathbf{r_1} + \mathbf{r}) - v_i(\mathbf{r_1})][v_j(\mathbf{r_1} + \mathbf{r}) - v_j(\mathbf{r_1})] \rangle, \tag{4.1}$$

Under the assumptions that:

1. The atmosphere is locally homogeneous or in other words the velocity depends only on **r**,

2. The atmosphere is locally isotropic i.e. velocity depends only on the magnitude of $\mathbf{r}$,

3. The turbulence is incompressible i.e. $\nabla \cdot v = 0$,

the tensor in eq 4.1 becomes:

$$D_v = \langle [v_r(\mathbf{r_1} + \mathbf{r}) - v_r(\mathbf{r_1})]^2 \rangle, \tag{4.2}$$

that is much more easy to handle.

Another simplification can be done introducing the so called *structure function* [46][47]. This is done in order to handle the fact that the generic process $f(t)$ we are analyzing is normally not stationary then if we consider instead the function:

$$F_\tau(t) = f(t + \tau) - f(t) \tag{4.3}$$

for values of τ which are not too large, slow variation in $f(t)$ do not affect $F_\tau(t)$ that could be treated indeed as a stationary process.

The generic structure function can be written in the following form:

$$D_f(t_i, t_j) = \langle [f(t_i) - f(t_j)]^2 \rangle \tag{4.4}$$

When the process is stationary the structure function depends only on the difference $t_1 - t_2$ and then the quantity $D_f(\tau) = \langle [f(t+\tau) - f(t)]^2 \rangle$ is the basic of random process which is said *stationary increment.*

These concepts can be generalized for a random field in three dimensions when the condition of stationarity becomes homogeneity and under these assumptions the velocity field of eq 4.2 can be derived.

In order to go on in an easy way we shall assume that the homogeneous field we are examining is also isotropic in the region G i.e. the distribution functions of $f(\mathbf{r_1}) - f(\mathbf{r_2})$ are invariant with respect to rotation and reflection of the vector $\mathbf{r_1} - \mathbf{r_2}$ with $\mathbf{r_1}$ and $\mathbf{r_2}$ in G. This implies:

$$D_f(\mathbf{r}) = \langle [f(\mathbf{r} + \mathbf{r_1}) - f(\mathbf{r_1})]^2 \rangle = D_f(r). \tag{4.5}$$

We shall see later that this is a strong approximation considering atmospheric turbulence. This approximation anyway it has been uses since nowadays and we should give some results based on this approximation to better appreciate further approaches.

4.1.2 Structure Function and Power Spectrum of Conservative Passive Additives

The microstructure of the refracting index of atmosphere is determined by the structure of temperature, humidity and wind velocity that can be treated to a high degree of accuracy as *conservative passive scalars (CPA)*[1]. The approach of studying the microstructure of the concentration of CPA was first introduced by Obukhov and Yaglom [94][59] and then used to study the index of refraction by Tatarsky[84].

Using the theory of CPA we can individuate two methods of diffusion that take place: the *molecular diffusion* and the *turbulent diffusion* that have opposite effects an that balance each other in stationary conditions.

From these considerations, calculating the distributions of the inhomogeneity of a generic additive ϑ we can derive its structure function ([84]) and the important quantities that characterize it. Since the difference of values in ϑ at two different points $\mathbf{r_1}, \mathbf{r_2}$ depends mainly by inhomogeneity of size $|\mathbf{r_1} - \mathbf{r_2}|$, if this modulo is very small with respect to the outer scale L_0 (i.e. the size of the biggest eddies, l_0 is instead the size of the smallest one), $\vartheta(\mathbf{r})$ can be treated as a locally isotropic random field with a structure function of the form:

$$\begin{aligned} D_\vartheta(|\mathbf{r_1} - \mathbf{r_2}|) &= \langle[\vartheta(\mathbf{r_1}) - \vartheta(\mathbf{r_2})]^2\rangle \\ l_0 << |\mathbf{r_1} &- \mathbf{r_2}| << L_0 \end{aligned} \tag{4.6}$$

The quantities that characterize the turbulence are N (the rate at which the inhomogeneities are leveled out in the smallest eddies[2]) and ϵ (the energy dissipation rate), and it is possible to derive the following:

$$D_\vartheta(r) = a^2 \frac{N}{\epsilon^{1/3}} r^{2/3} \qquad l_0 << r << L_0 \tag{4.7}$$

where a is a numerical constant. This equation was obtained by Obukhov [59] on the basis of qualitative considerations and is called *two third law.* For $r << l_0$ $D_\vartheta(r)$ can be expanded and a first approximation gives a proportionality with r^2 of the form:

$$D_\vartheta(r) = \frac{1}{3}\frac{N}{D} r^2 \qquad r << l_0 \tag{4.8}$$

Where D is the molecular diffusion coefficient. If we consider now l_0 defined

[1] CPA means that if the volume V is characterized by a concentration ϑ of additive, this concentration does not change if the volume is moved in space. Passive, simple means that ϑ does not affect the dynamic regime of the turbulence.

[2] This is equal also to the amount of inhomogeneity transferred per unit time from the largest to the smallest eddies.

as the point of intersection of asymptotic expansion of 4.7 and 4.8 we find:

$$l_0 = \sqrt[4]{\frac{27a^6D^3}{\epsilon}} \tag{4.9}$$

and we can then express the structure function in its final form:

$$D_\vartheta(r) = \begin{cases} C_\vartheta^2 r^{2/3} & r >> l_0 \\ C_\vartheta^2 l_0^{2/3}\left(\frac{r}{l_0}\right)^2 & r << l_0 \end{cases} \tag{4.10}$$

where

$$c_\vartheta = a^2\frac{N}{\epsilon^{1/3}} \tag{4.11}$$

and l_0 is defined by eq. 4.9.

It is important to notice that the *two third law* was introduced to describe the structure function of the velocity in a turbulent flow. In that case the 2/3 exponent was the only that could guarantee the dimension consistency of the function [84].

If now consider the power spectrum of a locally isotropic random field we end up with:

$$\vartheta(\mathbf{r}) = \vartheta(0) + \iiint_{-\infty}^{\infty}(1 - e^{i\mathbf{k}\cdot\mathbf{r}})d\varphi((k)) \tag{4.12}$$

where the random amplitudes $d\varphi(\mathbf{r})$ satisfy the relation

$$\langle d\varphi(\mathbf{k_1})d\varphi^*(\mathbf{k_2})\rangle = \delta(\mathbf{k_1} - \mathbf{k_2})\Phi_\vartheta(\mathbf{k_1})d\mathbf{k_1}d\mathbf{k_2} \tag{4.13}$$

The function $\Phi_\vartheta(\mathbf{k})$ is the spectral density of the structure function $D_\vartheta(\mathbf{r})$ and represents the three dimensional distribution of the inhomogeneity in a unit volume along the wave numbers $\mathbf{k_1}$, $\mathbf{k_2}$ and $\mathbf{k_3}$.

If we consider the form of the structure function described in eq. 4.10 where $p = 2/3$ we obtain

$$\Phi_\vartheta(k) = \frac{\Gamma(\frac{8}{3})sin\frac{\pi}{3}}{4\pi^2}C_\vartheta^2 k^{-11/3} \tag{4.14}$$

or, evaluating the multiplicative factor,

$$\Phi_\vartheta(k) = 0.033C_\vartheta^2 k^{-11/3} \tag{4.15}$$

The final form of the power spectrum obtained by Tatarski has to take into account the whole structure function of eq. 4.10. Where $r << l_0$ the structure function has an r quadratic dependence and then a rapid decrease of $\Phi_\vartheta(k)$ is expected for $k > 1/l_0$. Tatarski simply said that we can consider that the power spectrum to vanish for $k > k_m$ where k_m is related to l_0 through eq. 4.9. The final form of the spectrum is then the following:

$$\Phi_\vartheta(k) = \begin{cases} 0.033C_\vartheta^2 k^{-11/3} & k < k_m \\ 0 & k > k_m \end{cases} \tag{4.16}$$

The relation between k_m and l_0 can be obtained confronting eq 4.10 with the structure function reconstructed from its power spectrum:

$$k_m l_0 = (0.033\pi)^{-3/4} = 5.48 \tag{4.17}$$

4.1.3 Structure Function and Power Spectrum of Index of Refraction

Tatarski states that the structure function of the index of refraction and its power spectrum could simply be derived by the considerations on conservative passive additives treated above. The structure function has then the form:

$$D_n(r) = \begin{cases} C_n^2 r^{2/3} & l_0 << r << L_0 \\ C_n^2 l_0^{2/3} \left(\frac{r}{l_0}\right)^2 & r << l_0 \end{cases} \tag{4.18}$$

and the power spectrum is:

$$\Phi_n(k) = 0.033C_n^2 k^{-11/3} \qquad k_0 < k < k_m \tag{4.19}$$

where $k_0 = 2\pi/L_0$ and $k_m = 2\pi/l_0$.

4.1.4 Some Considerations on the Model

We have seen the Kolmogov-Tatarski model of turbulence for a passive scalar ϑ. We are interested in the effects of turbulence on the index of refraction and what this implies to signal transmission. First of all though, it is important to state the limits and the experimental result that validate in some case, and contradict in some other case, the presented model. The key assumption in Kolmogorov's and Tatarski works are homogeneity and isotropy i.e. turbulence does not depend on location in space and on the direction that we are considering. The Kolmogorov power spectrum is valid in the inertial subrange but fails at the inner and outer scale (l_0, L_0) (notice how Tatarski tried to fix this problem stating a zero values for $k > k_m$). At the inner scale the turbulent flow becomes laminar and kinetic energy is dissipated as heat while at the outer scale where clearly the homogeneity and isotropy are both violated because of the finite size of the eddies involved. Kolmogorov spectrum anyway agree well with vertical propagation [69].

There has been various modification of the original formula 4.16 to fix it for inner and outer scale. Von Karman [89] proposed a spectrum that does not diverges at the inner and other scale but retains the 11/3 power low:

$$\Phi_n(k) = 0.033C_n^2(k^2 + k_0^2)^{-11/6} exp\Big[- \frac{k^2}{k_m^2} \Big] \qquad k_0 < k < k_m \qquad (4.20)$$

Other have proposed different approaches and even several experiment have demonstrated that the kolmogorov moded does not agree with the experimental results (for a brief review see [80]). That is why someone considers a generic power spectrum form, given by:

$$\Phi_n(k, \alpha, z) = a(\alpha)\beta(z)k^{-\alpha} \qquad (4.21)$$

where z is the position along the optical path, α is the power low and $\beta(z)$ is the index structure constant. The function $a(\alpha)$ can be worked out easily if we calculate the power spectrum of a generic structur function of the form $D_n(r, z) = \beta(z)r^\gamma$ [80]:

$$a(\alpha) = 2^{\alpha-6}(\alpha^2 - 5\alpha + 6)\pi^{-3/2} \frac{\Gamma\Big[\frac{\alpha-2}{2}\Big]}{\Gamma\Big[\frac{5-\alpha}{2}\Big]} k^{-\alpha} \qquad 3 < \alpha < 5 \qquad (4.22)$$

It is easy to see that the spectrum described in eq. 4.21 reduces to kolmogorov spectrum if $\alpha = 11/3$.

4.2 Effects of Atmospheric Turbulence in Beam Propagation.

The effects of the atmosphere in beam propagation can be various, depending on the power, size, path length of the beam under investigation. The effects are visible in the wavefront of the beam and on its propagation trajectory and are caused by the small variations of the index of refraction described in the previous sections. Before going into details in the effects on the beam lets introduce an useful tool for handling wavefronts.

4.2.1 Zernike Polynomials Expansion of Wavefronts.

In order to describe a wavefront the Zernike Polynomials are usually used. A generic wavefront $\Phi(\rho, \phi)$, $(\rho, \phi) \in C_1$, can be expanded in a orthogonal base of the vector space $H = \{W(\rho,\phi), (\rho,\phi) \in C_1\}$ of the surfaces C_1, i.e. in the set of the complex Zernike Polynomials of radial order n and azimuthal order l:

$$\{V_n^l(\rho,\phi) \quad , \quad n = 0,1,2,... \quad l \in Z : |l| \leq n, \quad n-|l| \quad pari\}$$

The definition is as follows:

$$V_n^l(\rho,\phi) = R_n^l(\rho)e^{jl\phi} \qquad ,(\rho,\phi) \in C_1$$

where

$$R_n^l(\rho) = \sum_{s=0}^{\frac{n-|l|}{2}} (-1)^s \frac{(n-s)!}{s!(\frac{n+|l|}{2}-s)!(\frac{n-|l|}{2}-s)!}\rho^{n-2s} \qquad ,\rho \in [0,1] \tag{4.23}$$

It is possible to use also another orthogonal base of H: the real Zernike Polynomials described by:

$$\{U_n^m(\rho,\phi) \quad , \quad n = 0,1,2,... \quad m \in Z : |m| \leq n, \quad n-|m| \quad pari\}$$

and defined as:

$$U_n^m(\rho,\phi) = \begin{cases} \frac{1}{2}\left[V_n^m(\rho,\phi) + V_n^{-m}(\rho,\phi)\right] = R_n^m(\rho)cos(m\phi) & per \quad m \geq 0 \\ \frac{1}{2j}\left[V_n^{-m}(\rho,\phi) - V_n^m(\rho,\phi)\right] = R_n^m(\rho)sin(|m|\phi) & per \quad m < 0 \end{cases} ,(\rho,\phi) \in C_1 \tag{4.24}$$

The wavefront $\Phi(\rho,\phi)$ can so be expanded in terms of the Zernike polynomials:

$$\Phi(\rho,\phi) = \sum_n \sum_m c_{n,m} U_n^m(\rho,\phi) \qquad ,(\rho,\phi) \in C_1 \tag{4.25}$$

where $c_{n,m}$ are called Zernike coefficients.

4.2.2 Turbulence Effects on Beam Wavefront

Turbulence cause low spatial frequency beam wandering, high spatial frequency spreadind and intensity variations. The effects depend on the ratio between the size of the atmosphere's eddies and the beam size. A useful quantity in characterizing how turbulence affects an optical system is the Fried Coherence Length r_0 defined as follows for a plane wave:

$$r_0 = \left[0.423k^2 \sec(\beta) \int_0^L C_n^2(z)dz\right]^{-3/5} \tag{4.26}$$

Fried parameter r_0 represent the maximum diameter of a collector allowed before the atmospheric distortion seriously limits the performance of the system.

For our case i.e. an horizontal path with constant C_n^2 the 4.26 becomes:

$$r_0|pl = 1.68(C_n^2 L k^2)^{-3/5} \tag{4.27}$$

We can fairly say that the Fried parameter is the coherence length of the atmosphere since it is the length over which the wavefront distortion is limited. Another important parameter in this picture is the coherence time τ_0 that is the time over which atmospheric variations are frozen. This time is proportional to the time that the wind uses to move thing over an aperture of the size of r_0: $\tau_0 \sim r_0/V$ where V is the wind speed. From this parameter we can derive another very useful quantity called Greenwood frequency that is the inverse of τ_0:

$$\tau_0 = f_G^{-1} = \Big[0.102 k^2 \sec(\beta) \int_0^\infty C_n^2(z)|V(z)|^{5/3} dz\Big]^{-5/3} \tag{4.28}$$

An adaptive optics system should have a bandwidth that is at least four time the greenwood frequency in order to correct the wavefront [88].

With those tools we can now analyze the effects of the atmosphere on a beam:

- **scintillation:** this cause a intensity variability at the receiver. This occurs because of small variation in the optical path that can produce destructive or constructive interference and cause intensity variations. The “amount” of scintillation is clearly related to the strength of the atmosphere turbulence, we can write the log amplitude variance as follows

  $$C_\chi = 0.307 k^{7/6} L^{11/6} C_n^2 \tag{4.29}$$

  This value must be integrated along the path L if C_n^2 is not constant.

- **beam wander or tilt:** this cause the beam to wander as propagating. When the wander is fast is called sometimes jitter. The full formula for wavefront tilt variance σ_{tilt}^2 was derived by Sasiela and it is quite long. For our purposes the variance of the tilt angle α^2 can be enough. This is expressed by:

  $$\alpha^2 = 0.364 \Big(\frac{D}{r_0}\Big)^{5/3} \Big(\frac{\lambda}{D}\Big)^2 \tag{4.30}$$

  This formulation represent the overall tilt variance on the beam whereas a further work by Tyler [87] divided the contribution of the G-tilt obtained by a centroid measurement and the Z-tilt i.e. the direction that is defined by the normal to the plane that minimizes the mean-square wave-front distortion. These two effects contribute almost equally to the overall variance. He derived also the typical frequency of those contributions and found them comparable to each other and smaller than the Grenwood frequency that takes into account all kind of distortions. Typical values for astronomical purposes are 10 to 50 Hz for the tilt and 50 to 300 for high order aberrations.

- **high order phase variations:** these variations assume a fundamental role when the diameter of the receiving collector is much grater than the Fried length r_0. In this case the eddies of the atmosphere appear to act locally on the wavefront causing at every point a different slope. This increase the spatial modes that a wavefront sensor would measure and cause a intensity variability at the receiver [88]. If we write the spectrum of the atmospheric turbulence in the spatial domain (spatial frequency K) in terms of the coherence length r_0 we find:

$$\Phi(K) = \Big(\frac{0.023}{r_0^{5/3}}\Big) K^{-11/3} \tag{4.31}$$

and the overall wavefront variance can be obtained integrating this spectrum:

$$\sigma^2 = \int \Phi(K) d^2K. \tag{4.32}$$

Clearly the tilt variance in equation 4.30 or more generally the wavefront error due to specific aberrations can be deduced from the more general formulation just shown considering the desired Zernike modes.

- **thermal blooming:** this is the ionization that occurs when a very intense beam passes through the atmosphere. This phenomenon causes an intensity reduction in the beam but of course it is not a problem for a single photon transmission [88].

4.2.3 The Need for an AO System in QKD

As already introduced in Sec. 1.3.4 spatial filter is a almost mandatory improvement in free space QKD[3]. This has been treated theoretically in a work by Shapiro ([75]) and noticed in many experimental setups [49, 35, 71].

[3] Notice that in QKD this a problem because we are dealing with single photons, for FSO (Free Space Optics) links this is not a main issue because we can enlarge the spot at the receiver. For QKD this would mean a non acceptable lost of signal.

The issue of how and what to correct is an open one mainly for the reason that it is very hard to measure what turbulence does to the wavefront at very high repetition rates, in this sense experiments are going on all over the world. Many paper have been written considering the problem in particular sites taking into consideration different aspects: [45, 33, 80].

What can be said however is that whatever the turbulence does to the beam while it is propagating the aberration that it introduces can be expanded by means of the Zernike terms introduced in sec. 4.2.1. A work by Noll [58] did this expansion considering a Kolmogorov like turbulence and he deduced the residual error that one would expect if the Zernike modes were one by one corrected corrected. By this paper one can see that the error is distributed into the modes in a very non uniform way. Low orders are more present and as we increase the order going to higher spatial frequency the benefit that we have if we correct them is much lower that for the first modes. In Fig. 4.1 the Zernike polynomial residual error coefficient is depicted. The wavefront error can be obtained multiplying this coefficient by $(D/r_0)^{5/3}$. The order j takes into account the radial and azimuthal order [58]. In this sense $j = 0$ is the piston, $j = 2$ and $j = 3$ are tilts[4] and so on.

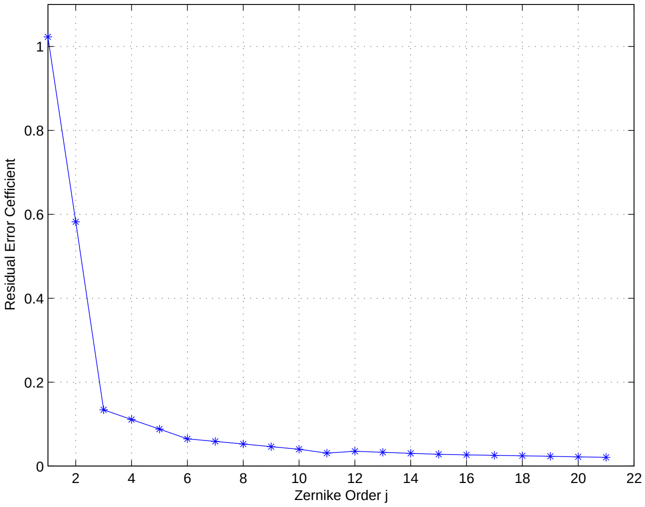


Figure 4.1: Zernike residual error coefficient. To obtain the residual wavefront error multiply these values by $(D/r_0)^{5/3}$.

You can see from Fig. 4.1 that after the correction of piston and tilt the

[4] In particular $j = 2, 3$ corresponds to $Z_2 = 2rcos\theta$ and $Z_3 = 2rsin\theta$.

residual error is very low. One should then start to correct the lower modes and our decision has been to build a system for tilt correction.

4.3 QuAKE AO System Introduction

As just said we decided to build an AO system in order to get rid of the turbulence induced tilt on our QKD system. The full system, at the receiver is the one represented in Fig. 3.3. The beam collected by the receiving telescope is demagnified and directed toward the deformable mirror that is the main component of the system. Then the beam is focused toward the quantum receiver or the position sensing detector (PSD) depending on its wavelength. The PSD is a Duma[5] Lateral Effect PSD with an 9×9 mm sensor with a resolution of 0.1μm, an analog bandwidth of 30 KHz and a minimum input power of 1μW. The system configuration is a closed loop setup.

Another alternative solution that we thought about was to put the deformable mirror at the transmitter. This has an advantage when the propagation distance is very high and consequently the effect of the turbulence is so strong that the beam wander even outside the diameter of the receiving collector. For what we see in our trials this is not the case for our system, moreover the need of sending back the information about the spot position from the receiver to the transmitter has to be studied carefully in such system. The problem of latency is indeed very important in this case. There are anyway occasions in which such a system would be necessary i.e. very high propagation distances [71].

4.4 The Membrane Deformable Mirror

The most important component of the AO subsystem is a membrane deformable mirror. The mirror, completely developed in our laboratory, is composed by a thin nitrocellulose aluminum coated membrane which is deformable by 37 hexagonally shaped electrodes as depicted in Fig. 4.2. The membrane is deformed by electrostatic force created applying an high voltages drop between the electrodes. The membrane is $5\mu m$ thick, its initial flatness is less than 60 nm rms. Pulling all the electrodes at the maximum voltages of 230V, the distance from the central point of the deflected surface to the plano is about $10\mu m$ as depicted in the interferogram. This deformation is a paraboloid that corresponds to a focal length of about 2m. The Fig. 4.3 shows the interferograms, taken by a Zygo interferometer, of the flat surface and of the mirror pulled by the half of maximum voltage (115V).

[5] http://www.duma.co.il/.

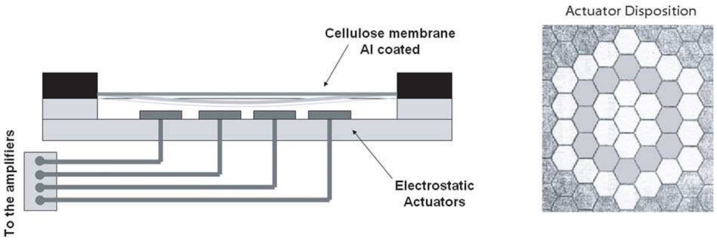


Figure 4.2: Scheme of the membrane deformable mirror.

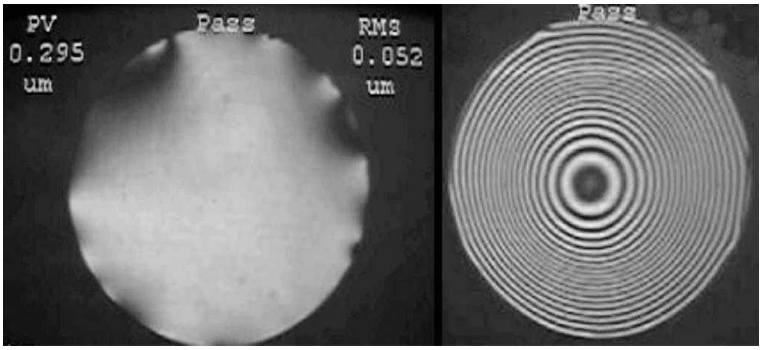


Figure 4.3: Interferogram of the flat surface and of the mirror pulled by half of maximum voltage. Flat Peak to Valley 295 nm, RMS flatness 52 nm.

We want to use the mirror for correcting tilt in a free space propagation path. What we are interested in is then the capability of the mirror of reproducing tilts. In Fig. 4.4 are reported some interferogtams that shows the capability of the mirror of reproducing tilt at various angle. The maximum value of tilt that the mirror can reproduce is about $400\mu rad$ and varies at different angles. These variations can be exploited and compensated (see. Sec. 4.5.5).

Another important thing we are interested in is the bandwidth of the mirror. In particular we focused on the measurement of the tilt bandwidth of the mirror. For the first measure (reported in [13]) we make use of a camera that recorded the images of a tilted spot and by means of asynchronous sampling we could reconstruct the bandwidth. This results are the same that we obtained later exploiting the PSD sensor capability. We imposed a tilt at two opposite angles with increasing frequency and measure the distance between spot centroids. The result is depicted in Fig. 4.5 and shows a 400Hz $1.5dB$ bandwidth.

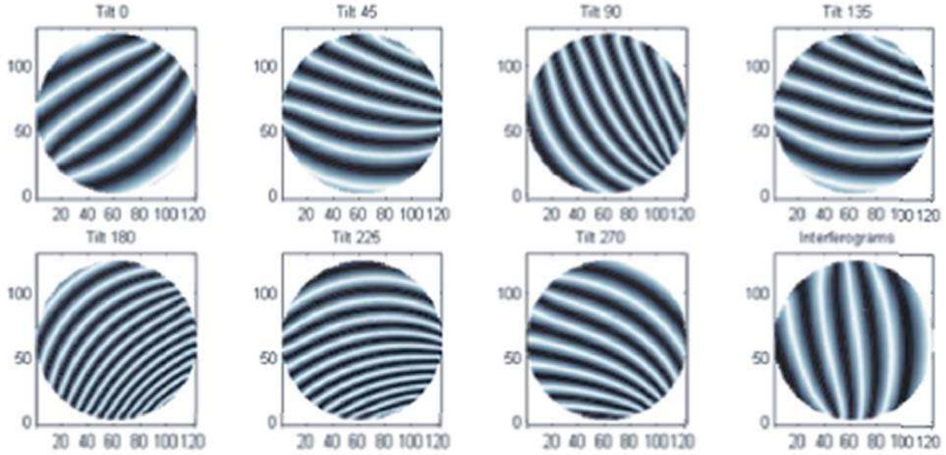


Figure 4.4: Interferograms of tilt at various angles obtained by the deformable mirror.

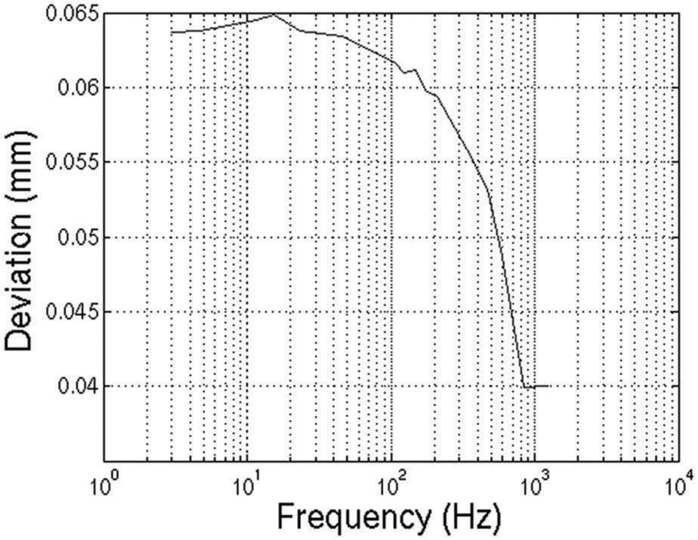


Figure 4.5: A measurement of the mirror tilt bandwidth.

4.5 The Mirror Drive Unit

In collaboration with colleagues in our department a driving system for the mirror has been designed [13, 79]. It exploits PWM modulation in order to decrease power consumption so increasing efficiency with respect to other modules based on linear amplifiers. Another advantage is the decreasing of the slew rate of the system that yields to a faster control.

4.5.1 PWM Modulation

Every i-th output channel of the mirror drive unit is a cascade of a MOS half-bridge followed by a low-pass filter. The control input signal on i-th block is a low voltage PWM signal, generated by the discrete-time modulator:

$$u_1(t) = \begin{cases} 1 \quad , & kT_{PWM} \leq t < (k+\delta)T_{PWM} \\ \\ 0 \quad , & (k+\delta)T_{PWM} \leq t < (k+1)T_{PWM} \end{cases} \tag{4.33}$$

where T_{PWM} is the signal period, δ is the signal duty-cycle. The half-bridge can be modelled as a linear block gain. Thus, the output of the half-bridge is a PWM high voltage signal and it is given by $u_2(t) = V_0 u_1(t)$, where the constant V_0 represents the voltage swing, equal to 250 V, which is introduced by this block.

Filtering this output signal by means an electric lowpass filter, we obtain the mirror driving signal $y(t)$. In the frequency domain, the spectrum of the periodic signal $u_2(t)$ is discrete and is composed by the mean value and by a set of harmonic components with variable amplitudes and with frequencies which are multiple of fundamental $F_{PWM} = 1/T_{PWM} = 26.6$ kHz:

$$U_2(f) = \frac{F_{PWM} V_0}{j2\pi f} \left(1 - e^{j2\pi f \delta T_{PWM}}\right) \tag{4.34}$$

where $f = kF_{PWM}$ and $k, n \in \mathbb{Z}$. The component of (4.34) for $f \to 0$ gives the mean value on the period T_{PWM} of $u_2(t)$. Passing to limit, we find this significative relation:

$$|U_2(f)|_{f \to 0} = \delta V_0. \tag{4.35}$$

Changing the duty-cycle, it is possible to control the mean value of (4.35), that is the mirror driving electrode signal.

4.5.2 Output Filtering

To obtain the mean value and discard the harmonic components of $u_2(t)$, we filter the set of 64 PWM output signals by means a lowpass filters with cut-off frequency f_{cut} which fix the working band of whole system.

In our driving unit, we set the cut-off frequency as $f_{cut} = 450$ Hz and the PWM modulator frequency carrier as $F_{PWM} = 26.6$ kHz. Being $f_{cut} \ll$

F_{PWM}, practically, it is just needed to set a first-order RC lowpass filter for each channel with cut-off frequency at -3 dB $f_{cut} = \frac{1}{2\pi RC}$. Therefore, the frequency spectrum of electrode signals is:

$$Y(f) = \frac{F_{PWM}V_0}{j2\pi f}\frac{\left(1 - e^{j2\pi f\delta T_{PWM}}\right)}{1 + j2\pi fRC} \tag{4.36}$$

where $f = kF_{PWM}$ and $k \in \mathbb{Z}$.

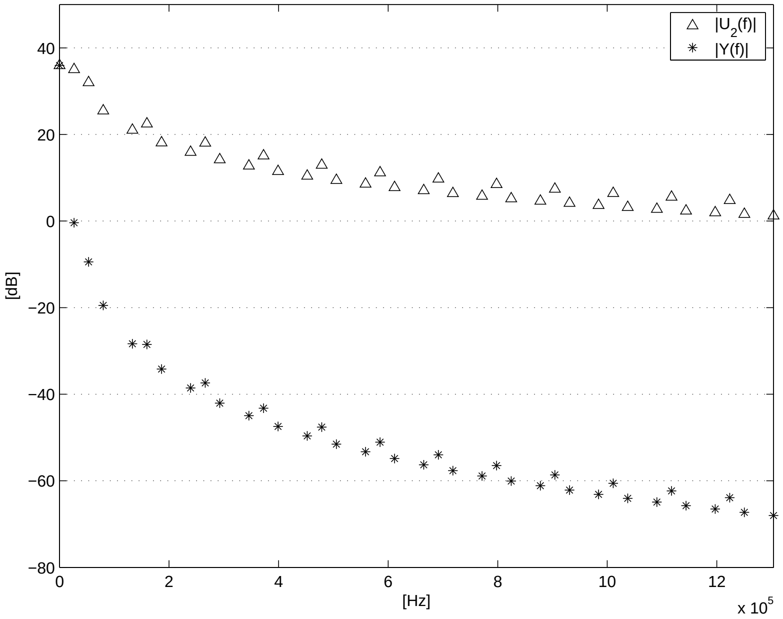


Figure 4.6: Spectrum of PWM signals ($\delta = 0.25$).

It is easy to find that the mean value $< y(t) >= |Y(f)|_{f\to 0} = \delta V_0$. In Fig. 4.6, we compare the spectrum of $U_2(f)$ versus the one of $Y(f)$. It appears that the minimum rejection between the mean value and the harmonic components is more than $36dB$.

4.5.3 Output Distortion

The output mean value is accomplished by a *ripple* residual term as $y(t) = \delta V_0 + r(t)$. To characterize our system, it is fundamental to quantify the magnitude of r(t). For time t in the range $[kT_{PWM}, (k + \delta)T_{PWM})$, we have:

$$r(t) = V_0\left[1 + (1 - \alpha)e^{-\frac{t}{RC}}\right] \tag{4.37}$$

in the range of $[(k+\delta)T_{PWM},(k+1)T_{PWM})$, we find:

$$r(t) = V_0 e^{-\frac{t}{RC}} \left(e^{-\frac{\delta T_{PWM}}{RC}} + \alpha - 1 \right) \tag{4.38}$$

where the parameter α is defined as:

$$\alpha = \frac{e^{\frac{\delta T_{PWM}}{RC}} - 1}{e^{\frac{T_{PWM}}{RC}} - 1} \tag{4.39}$$

Being (4.37) and (4.38) monotonic functions with respect to the time, we can find the peak-peak amplitude of $r(t)$:

$$\Delta r(t) = \max_{\delta}\{r(t)\} - \min_{\delta}\{r(t)\} = V_0(1-\alpha)\left(1 - e^{-\frac{\delta T_{PWM}}{RC}}\right) \tag{4.40}$$

It appears that the ripple amplitude depends on the duty-cycle value and the maximum voltage swing is realized with $\delta = 0.5$.

Finally, to estimate the electric distortion, introduced by PWM modulation in the output signal $y(t)$, we define the ratio between the DC component, and the harmonic components as following:

$$D_y = \frac{\sqrt{\sum_{k=1}^{+\infty} |Y(kF_{PWM})|^2}}{\delta V_0} = \frac{\sqrt{2}}{4\delta F_{PWM} RC}\sqrt{\frac{1}{90} - \sum_{k=1}^{+\infty}\frac{\cos(2\pi\delta k)}{(\pi k)^4}} \leq \sqrt{2}\frac{f_{cut}}{F_{PWM}}. \tag{4.41}$$

Thus, the distortion upper bound is in the ratio of f_{cut} and F_{PWM}. It follows, whatever δ, that the mean distortion does not exceed 2%.

4.5.4 Conditioning Electronics for PSD Signals

The first driving unit had been equipped with only one AD converter (ADS7822 A/D 12-bit converter) because it was thought to be used with genetic algorithm optimization strategy with only one merit function[13]. In this application instead we have two inputs i.e. the x and y coordinates of the centroid position. In order to sample this position in the PSD detector we designed a conditioning electronic board that by means of a analog multiplexer driven by the unit as will be shortly described in Sec. 4.5.5 switch between the x and the y signals coming from the PSD detector and perform a signal conditioning[43]. The circuit full schematic is represented in Fig. 4.7.

The aim of the amplifying stages is to bring the PSD voltage signal range $[v_{inmin}, v_{inmax}] = [-4.5V, +4.5V]$ into the accepted range by the ADC

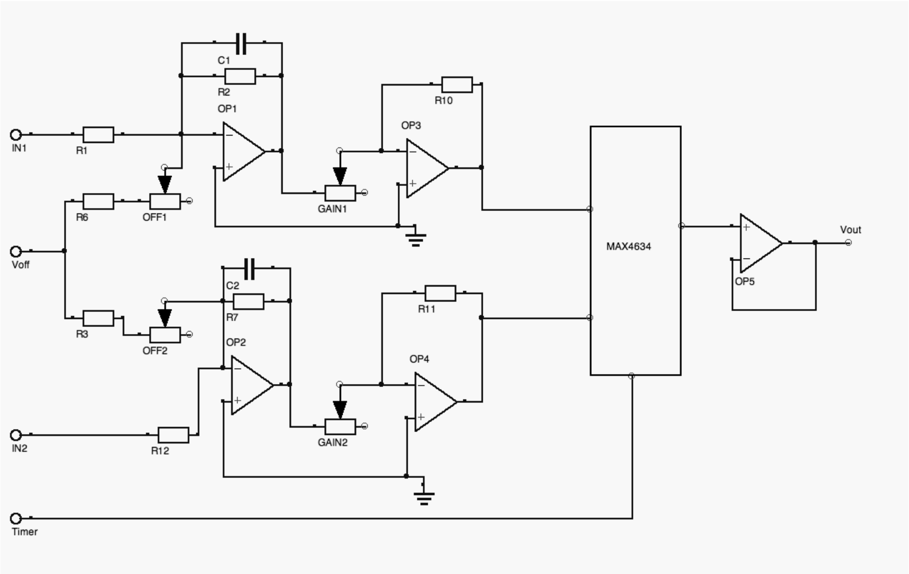


Figure 4.7: The conditioning electronics. Is multiplexes the two $[-4.5, 4.5]$ Volts signals coming from the PSD into one $[0, 5]$ Volts signal accepted by the ADC.

$[v_{omin}, v_{omax}] = [0V, +5V]$. There are so two amplification stages for each channel IN_1 and IN_2 that are the x and y signal from the PSD. The first stage add a continuos component that can be set by two variable resistors (OFF1 and OFF2) and act as a low pass filter with a cut of frequency of $10.6KHz$ in order to reduce noise. The second amplification stage amplifies the signal in order to match the ADC conditions. The amplification can be set by GAIN1 ang GAIN2 variable resistors. The output signal can be written as:

$$v_o = (v_i + A_1 * v_{offs}) * A_2, \tag{4.42}$$

where v_i can be $IN1$ or $IN2$ and A_1 and A_2 are the first and second stage amplifications. The calibration can be obtained using the specified constrains to find the values of A_1 and A_2:

$$A_1 = \frac{v_{imax}v_{omin} - v_{imin}v_{omax}}{v_{omax}v_{offs} - v_{omin}v_{offs}} \tag{4.43}$$

$$A_2 = \frac{v_{omax}}{v_{imax} + v_{offs}A_1}. \tag{4.44}$$

We then calculated the values of the resistors and used a standard and repeatable calibration procedure to set the appropriate offset and amplifications variable resistors. The v_{off} signal comes from the mirror drive unit itself and it is a well stabilized 5 V signal. We then used a signal generator to estimate the performances of the circuit. We created a sinusoidal signal of 300mV peak to valley and sampled with a *National Instruments*[6] sampler in differential mode (Quantization step $\delta V = 0.6mV$) either the input and the output signal. We evaluated the rms noise of the input and output signal when we set an overall amplification of $A_1 * A_2 = 5$. We obtained an output $RMS_{noiseOUT} = 5.6mV$ whereas the input one was $RMS_{noiseIN} = 1.7mV$. This shows that the filter at the first amplification stage remove part of the noise in the input signal.

4.5.5 DSP Signal Control Software

The kernel of whole system is a DSP TMS320 C5502 card which performs many tasks. In this section we analyze the method it acquires acquires the input signals from the conditioning circuit and how it produces the 64 PWM driving signals (only the first 37 signals are used to control the mirror drive unit).

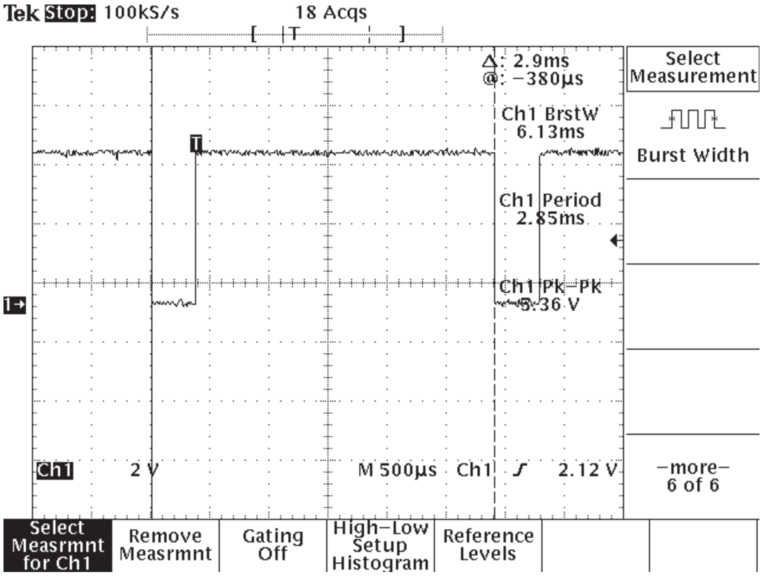
The fist task is done by selecting the channel with a control signal coming from the DSP itself and driven by the software. The measurement routine has been modified in order to make this task transparent in the sense that when you use the routine it gives you directly the x and the y channel. In Fig. 4.8 you can see a scope image of the timing signal. The signal has a default value that of course select a MUX channel. Every time it switchs it means that a measurement of both channels is taken, one in the default channel and one in the other channel. Notice how this signal can be an precise indicator of the overall loop frequency in closed loop operations.

For the mirror diving signal generations, all the PWM signals are created into the DSP memory and driven out from the processor via the DMA channel and the EMIF peripheral pins as shown in Fig. 4.9.

All the 64 PWM signals are stored in a 128 elements memory table (called *signals-table*) where all the elements are 64-bit wide. The *n*-th element represents the *n*-th time slot of the 64 signals. In every column of the table is stored one period of the channels PWM signal, i.e in the *m*-th column is stored a period of the *m*-th channel signal. We choose to split the period of the PWM signal into 128 time slots to have a sufficient granularity of the duty-cycle.

It is important to note that the DMA engine, that feeds the EMIF with the 64 signals values, should work continuously and should never be interrupted by any mechanism in order to guarantee the signal temporal continuity. In order to meet this requirement, we exploit the dual-port capability of the DSP internal RAM. All the auxiliary data and the code reside in a memory block

[6] NI USB-6009 model.



Tek Stop: 100kS/s 18 Acqs

Δ: 2.9ms
@: −380µs

Ch1 BrstW
6.13ms

Ch1 Period
2.85ms

Ch1 Pk−Pk
5.36 V

Ch1 2 V M 500µs Ch1 ∫ 2.12 V

Figure 4.8: The signal that drives the analog multiplexer. Every time it switches a measurement on both channel is taken.

different from the ones used to store the signal table. Therefore, the DMA channel is never interrupted by the CPU memory accesses.

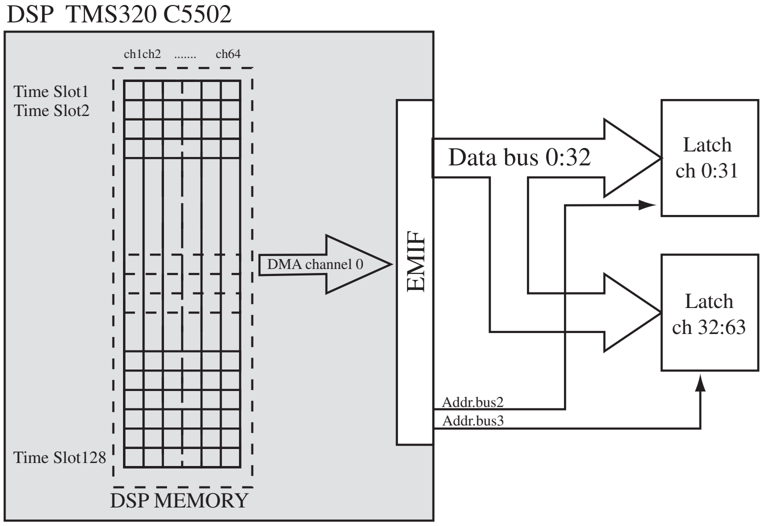


Figure 4.9: The DSP software block diagram for the driving signal generation.

4.5.6 The Closed Loop Control Software

The control software, residing in the DSP, implements an integrator like closed loop control system. This because the effects on the mirror deformation are present directly on the output as well as on the feedback loop.

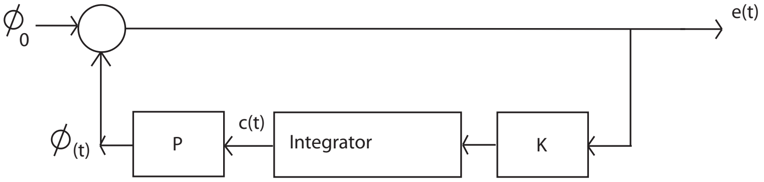


Figure 4.10: The integrator like control loop.

In Fig. 4.10 a representation on the control is depicted, the matrix P represent the constant that relates the PSD measurement i.e. the control signal ($c(t)$) to the mirror position ($\Phi(t)$) and it is also called Poke or Influence Matrix. The gain K is the feedback gain and the integration block performs an integration of the control signal $c(t)$ that in this case is the position on the PSD. In output we have the error $e(t)$ i.e. the difference between the old position and the new one $e(t) = \Phi_0 - \Phi(t)$ that we have to compensate and keep as close as possible to zero. If we are at time t and the system has a control step period of T we can write:

$$\phi(t) = Pc(t) \tag{4.45}$$

$$e(t) = \Phi_0 - \Phi(t) \tag{4.46}$$

$$c(t) = c(t-T) + Ke(t-T) \tag{4.47}$$

Doing the calculation through the system loop gives the solution:

$$\Phi(t) = \Phi_0 + (1 - PK)^{t/T}\Phi(0) \tag{4.48}$$

The control implemented is insensitive to small variation of the process gain P and to small non linearities and distortions.

In order to exploit the limited memory resources of the DSP we used the symmetry of the mirror electrodes pattern. As you can see from Fig. 4.2 the pattern has a $\pi/6$ rotational symmetry. We than loaded into the DSP a normalized table containing the 37 tilt voltages for all of the angle between 0 and $\pi/6$ with a step of one degree. When a position is measured the error $e(t)$ is computed taking in consideration the previously set Φ_0. This could be the position registered with the mirror in flat position or a position $\Phi_0\prime$ that maximize the tilt the mirror can correct in any direction compensating for asymmetries in the tilt correction. In this case an automatic routine calculates $\Phi_0\prime$ and a vector for scaling the surface at each angle. In Fig. 4.11 the calibration procedure is depicted. On the left the center for maximum tilt is calculated, on the right the constants for scaling at each angle are derived.

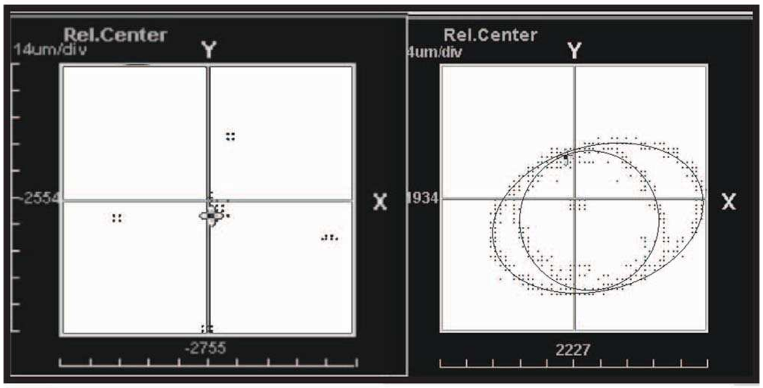


Figure 4.11: Control loop calibration. On the left the relative center is calculated, on the right the scaling vector is derived.

The software allow to set three many important parameter for the system:

- **timeADC:** it is the delay between the switching of the timer signal that control the analog multiplexer described in Sec. 4.5.4 and the acquisition start of the ADC.
- **timeTIMER:** it is the delay between the x and the y acquisition.
- **timeloop:** it is the delay that set the effective system working frequency. The control loop that is the core of the control system has to acquire the position of the centroid given by the PSD, calculate the surface in terms of voltages and give them to the mirror. When this is done the system holds for a time proportional to the value *timeloop*.

4.6 A Simple Optical Model of the AO System

Recalling the receiver optical setup of Fig. 3.3 we can individuate the key components for the AO subsystem. We will have a beam that due to atmospheric induced beam wander will enter the receiving telescope with different angles during time. This will cause the spot on the plane of the detector to move around by a quantity proportional to that variable incident angle. We would like also to have a spot at the receiver plane smaller that the active area of the detector that is $A_{Det} = 50\mu m$. We then try to correct the movements of the spot with the Deformable Mirror described in Sec. 4.4 that has a maximum tilt angle of $\theta_{DM} = 400\mu rad$.

Referring to Fig. 4.12 we see that the key components are the two lenses L_1, L_2 that compose the receiving telescope and that fix the demagnification of the beam an consequently the magnification of the turbulence induced tilt angle at the entrance of the system and the focusing lens L_3 after the DM mirror (The DM is not represented in the scheme) that set the dimension of the spot on its focal plane that corresponds to the detector plane and transpose the DM and atmosphere induced tilts in a displacement of the spot.

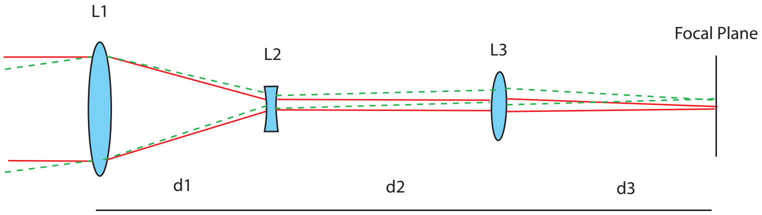


Figure 4.12: Key components of the AO subsystem of QuAKE.

The lens L_1, L_2 and L_3 as well as the distances between them can be modeled by means of the ABCD matrix model in order to study the optical leverage involved. The vector $v\prime$ composed by the heigh of the image $u\prime$ and the angle $\theta\prime$ ($v\prime = (u\prime, \theta\prime)$) on the focal plane of L_3 can be calculated knowing the ABCD matrix of each element in the system starting from the entrance heigh u and angle θ that form the vector v. This is done using the following expression:

$$v\prime = M_{d_3} M_{L_3} M_{d_2} M_{L_2} M_{d_1} M_{L_1} v \tag{4.49}$$

where M_i is the ABCD matrix of the i-th element. We would like our beam to be collimated from lens L_2 to L_3 that is why ignore the component M_{d_2} that represent the distance d_2. Expressing the matrix M_i for each element we can write the equation that describe the system:

$$\begin{pmatrix} r\prime \\ \theta\prime \end{pmatrix} = \begin{pmatrix} 1 & d_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1/f_3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1/f_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & d_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1/f_1 & 1 \end{pmatrix} \begin{pmatrix} r \\ \theta \end{pmatrix} \tag{4.50}$$

With this model we can characterize the system leverage. First of al we start from an expected value of turbulence induced tilt at the entrance of the receiving telescope. This value is very variable both with distance and C_n^2 as you can see from Fig.4.13 for a collector aperture of 50mm at the wavelength we are interested in.

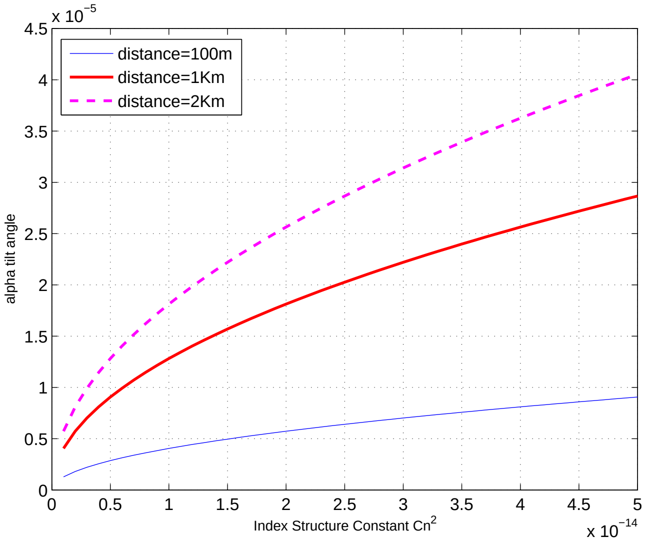


Figure 4.13: Atmosphere induced tilt standard deviation respect to C_n^2 and the horizontal path length for an aperture of 50mm and a wavelength of 850nm.

From one trial of our experiment on 100m path length (see Sec. 5.1) and from the comparison of this data with a standard model such as SLC daytime Model (see [1]) we obtained a mean value for θ equal to: $\theta_{mean} = 13.33\mu rad$ and a maximum value of $\theta_{max} = 36\mu rad$. In order for the system to work properly the maximum value of θ traced through L_1 and L_2 have to be smaller that the maximum tilt that the DM can impose. This is to say $\theta_2 \leq \theta_{DM}$. Another issue is that the demagnification of the receiving telescope has to produce a beam that fits the dimension of the active area of the Deformable mirror. This have an open diameter of $D_{DM} = 18$mm with an active area of 70% of this value $A_{DM} = 12.6$mm. We start dimensioning the system for a 100m path with a collecting lens of $D_{L_1} = 50$mm and focal length $f_{L_1} = 150$mm and for a maximum atmospheric induced tilt of $\theta = 50\mu rad$, a value that is slightly higher that the value we obtain with the SCL daytime model. This is to take into account the high variability of the structure constant C_n^2 in urban environment. f_{L_2}, the focal length of the L_2 can be then calculated and it results:

$$f_{L_2} = \frac{f_{L_1}\theta}{\theta_{DM}} = 18.75mm \tag{4.51}$$

where θ_{DM} is the maximum tilt that the DM can impose. We choose for a first trial a lens that we had in the lab of $f_{L_2} = -20mm$. With this lens we obtain a magnification for the angle $|M| = 7.5$ that corresponds to an angle after the receiving telescope of $\theta_2 \approxeq 385\mu rad$ that fits the first requirements. The second requirement is that $D_2 < A_{DM}$. This holds because if we take $D_1 = D_{L_1}$ we get $D_2 = D_1/|M| = 6.6mm < 12.6mm = A_{DM}$. A consideration has to be made at this point. We are using a DM for correcting tilt only and then we can avoid here an usual AO requirements: if we were correcting higher order aberrations we would need the incident beam to cover almost all the active area of the mirror whereas in this case we don't need to fulfill this requirement.

We can now focus our attention on L_3 and try to find the best choice in order to get advantage from the use of the DM. We can calculate the diffraction limited spot radius at the L_3 focal plane that coincides with the detectors plane with the usual formula:

$$R_{spot} = 1.22\frac{\lambda f_{L_3}}{D_2} \tag{4.52}$$

If we do this for various f_{L_3} and use this value to calculate the overall residual accepted receiver field of view θ_{Dec} in order to keep the spot into the active area of the detector we obtain the graph in Fig. 4.14.

Comparing this value with the maximum tilt introduced by the atmosphere we can see that for every focal length f_{L_3} we would expect a benefit in using the mirror since the angle that the receiver can accept is smaller that the induced tilt. Notice also that the accepted angle goes to zero at the critical focal length that implies a spot size $R_{spot} = A_{det}/2$. We have chosen a lens L_3 with a focal length of 150mm because, as said from previous measurement of the turbulence, in our path we have a mean tilt value of $\theta_{mean} = 13.33\mu rad$. In order to get an appreciable correction by the mirror we have to choose a lens that lead to a smaller field of view. In this case the half field delimited by the detector's aperture is $1.5\mu rad$. This value is very small but has been a good choice for a first testing of the system as we shall see. Moreover we had a choice between 150mm and 100mm but the latter gives an acceptance field of the order of the mean atmosphere induced tilt so precluding a good correction by the DM.

Resuming the optical design of the AO subsystem we have chosen a galileian telescope with lens L_1 with focal length $f_{L_1} = 150$mm and lens L_2 with focal

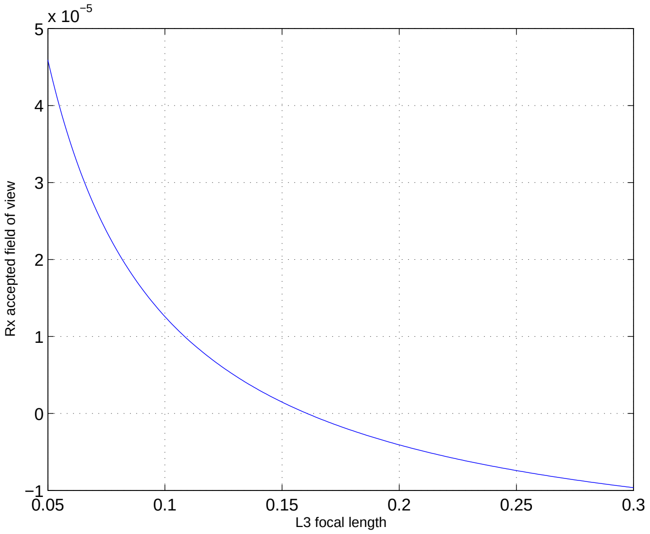


Figure 4.14: The receiver half field of view that maintain all the energy in the active area of the detector for different L_3 focal lengths.

length $f_{L_2} = -20\text{mm}$. We chose the lens L_3 with a focal length f_{L_3} of 150mm.

In the following chapter some experimental analysis of the AO system will be presented either in the laboratory, in outdoor conditions and at single photon regime.

Chapter 5

Experimental Data for the Adaptive Optics System

In this chapter i want to report some results we obtained testing the adaptive optics system two different operating conditions. First in outdoor conditions with a bright laser in order to test the performances and acquire data of real turbulence induced tilt. Following the development of the quantum cryptography optics and electronics the second test of the adaptive optics system was done in the lab, exploiting the single photon detectors (SPADs) mounted on the QKD system and a simplified version of the electronics that is still not fully operating. The first test is also reported in a work on the proceeding of the 6th International Workshop on Adaptive Optics for Industry and Medicine [20].

5.1 Testing of the AO System in Outdoor Environment

As explained the system with the configuration described in Sec. 4.6 have been tested in a 100m optical path. The laser used for testing is a 850nm $3.5mW$ laser diode. The actual wavelength that the final AO subsystem will use is ,as explained, 808 nm. This has no direct implication on the leverage of the optical system nor on the atmosphere induced tilt standard deviation. Remember that the choice of the wavelengths for the QKD system was done exactly with this purpose: the atmospheric induced effects on the beam must be as close as possible for the signal ans synchronization lasers (see Sec. 3.1.3). The spot size at the focal plane of L_3 will be slightly smaller but our single quadrant PSD detector is insensible to spot size being a lateral effect PSD (see Sec. B.0.2). The testing optical setup is represented in Fig. 5.1. A red auxiliary laser has been used to facilitate alignment, a $ND = 10$ filter has been used to attenuate the laser diode before it reached the PSD detector. It is possible to recognize how the components L_1, L_2 and L_3 analyzed in Sec. 4.6 have been inserted in the scheme.

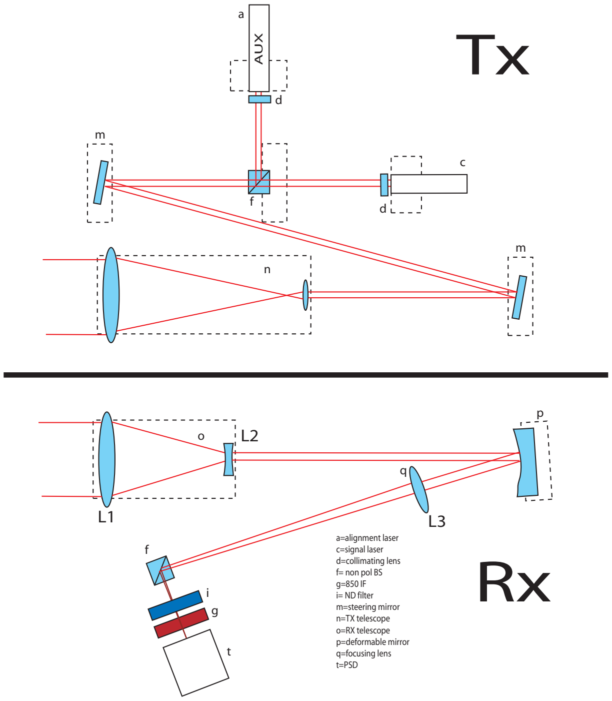


Figure 5.1: The testing optical setup for the AO subsystem.

The x and y position of the centroid that are used to feed the conditioning circuit and then the mirror driving unit (described respectively in Sec. 4.5.4 and 4.5) are also sampled with the National Instruments ADC in order to keep track of the correction. We performed several intermediate step in the lab using a candle as turbulence generator. These steps have been useful to debug and optimize the algorithm as well as to test the bandwidth of the closed loop system.

In Fig. 5.2 a test square wave generated with the mirror and sampled with the PSD is represented. The measurement takes into account all the operations that has to be done in the correction loop. and has been done for three different *timeloop* (see Sec. 4.5.5) that corresponds to a closed loop frequency of respectively 100 Hz (bottom), 200Hz (middle) and 666Hz (top). Clearly the latter frequency is outside the mirror capabilities and we can see that at 200Hz the shape of the wave is getting triangular. For the testing we

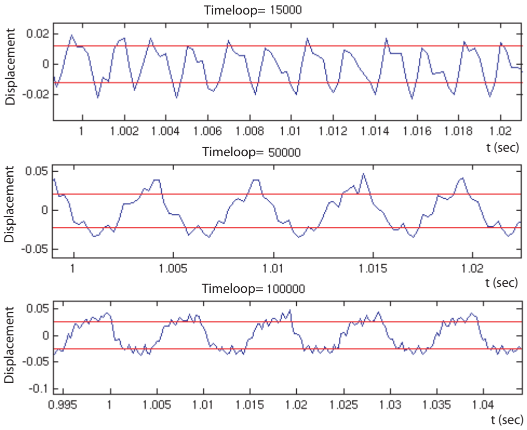


Figure 5.2: A square wave generated by the control loop for three different Timeloops (see Sec. 4.5.5).

used a closed loop frequency of 150Hz. We then went outside in order to test the system in a 100m optical path (Fig. 5.3).

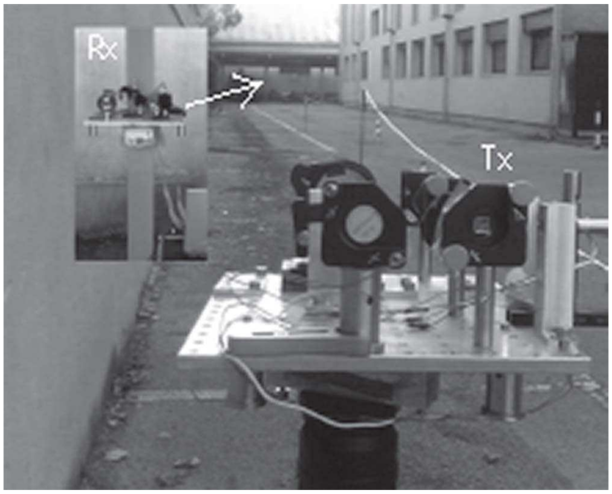


Figure 5.3: The outdoor 100m path.

In Fig. 5.4 you can see 60 seconds of sampling of the turbulence effect on the spot position at the PSD detector that coincide with L_3 focal plane (see Sec. 4.6).

The RMS displacement is found to be $7.2\mu m$, the mean displacement $13.4\mu m$, the Pearson correlation coefficient between the two channels is $r =$

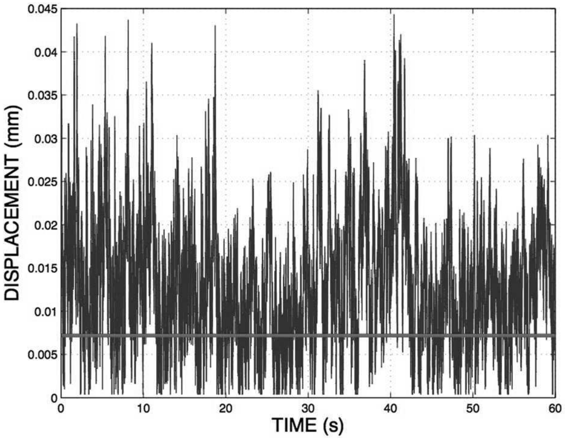


Figure 5.4: Effects of the turbulence on beam centroid displacement from a target zero point over 60 seconds.

0.04. Retracing back the beam through the system described in Sec. 4.6 we calculated the tilt angle at the entrance of the receiver from the spot displacement on the PSD detector: we obtain $\alpha_s^2 = 4.49 \times 10^{-11} rad$ of tilt angle variance. Inverting the formulas for the tilt angle variance and the Fried coherence length for a horizontal path (see Sec. 4.2.2) we obtain:

$$r_0 = \left(\frac{\alpha^2}{\lambda^2}\right)^{-3/5} \frac{D^{-1/5}}{1.83} \tag{5.1}$$

$$C_n^2 = \left(\frac{r_0}{1.68}\right)^{-5/3} \frac{\lambda^2}{4L\pi^2} \tag{5.2}$$

Plugging our results into these formulas we get a Fried coherence length of $r_0 = 7.6\ cm$ and a index of refraction structure constant of $C_n^2 = 3.16 \times 10^{-14}$ $m^{-2/3}$. We can confront these value with a turbulence model or with some experimental data in order to validate the results, of course considering that our experiment has been done at ground level in a urban environment. If, for example, we tune to our conditions the SLC daytime Model [1] we obtain: $C_n^2 = 1.7 \times 10^{-14}\ m^{-2/3}$ and $r_0 = 11\ cm$ that are in agreement with our results.

In addition we obtained the real meteorological data from *ARPAV,Centro Meteo- rologico di Teolo*[1] 12 Km away from Padua for the days of the experiment. In this case we obtained a value of r_0 = 25cm and a tilt variance $\alpha^2 = 6 \times 10^{-12}$. The differences with experimental data can be explained by

[1] ARPAV - Centro Meteorologico di Teolo via Marconi, 55 35037 Teolo (PD), ITALIA http://www.arpa.veneto.it/home2/htm/home.asp

considering the distance of the meteo station to the city where the experiment has been conduced and hence the different conditions from countryside and city center. Data and calculation are reported in Appendix A.

We have then switched on the correction system with the same atmosphere conditions and the behavior of the spot centroid displacement in the PSD plane is now depicted in 5.5. The displacement have a RMS value 1.4μm and a mean value of $2.6 \mu m$ demonstrating an average improvement of 5 times in the radius.

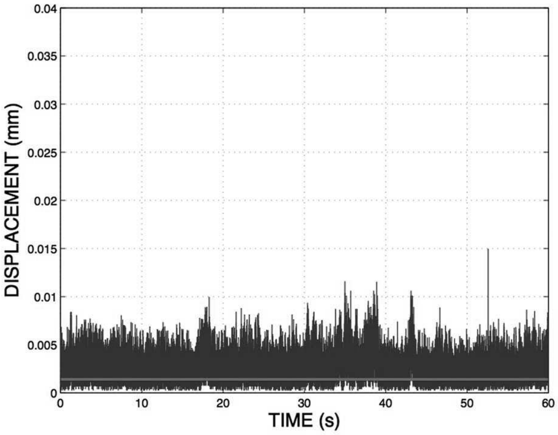


Figure 5.5: Correction of the turbulence in the condition of Fig 5.4.

A better picture of the situation can be deduced from Fig. 5.6, which corresponds to the trace of the centroid positions on the PSD detector screen after 60 second of integration, for the corrected and not corrected beam respectively.

The corrected spot is comparable with the noise of the system measured during calibration in the lab. that is a limit for the displacement of the corrected beam. This corresponds of a rms displacement of 1.35μm on the PSD detector. A frequency analysis has been carried out and the power spectral density using the Welch method has been calculated and is depicted in Fig. 5.7.

From the spectral analysis it is possible to see that the disturbance is corrected for a maximum frequency of about 50Hz although the system bandwidth is higher. In Fig. 5.7 there are also two peaks on the power spectrum of the corrected signals. We are investigating the nature of those peaks: the second, at 150Hz seems to be present also in the graph of the bandwidth and could be a resonant frequency of the mirror itself (see Fig. 4.5), the second at 40Hz could be caused by some software parameter.

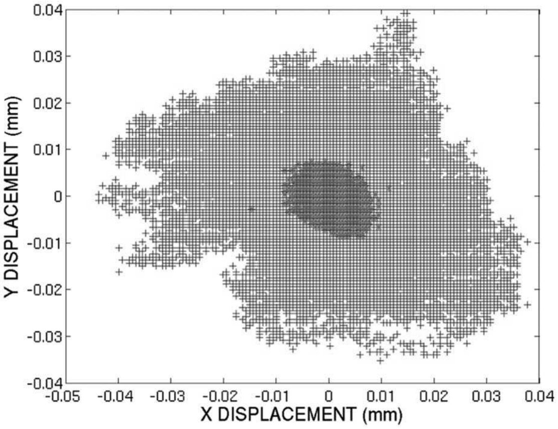


Figure 5.6: Corrected and uncorrected centroid displacement on the PSD detector.

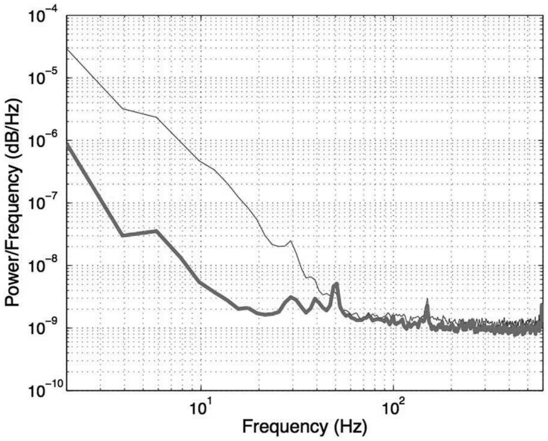


Figure 5.7: Corrected and uncorrected centroid displacement on the PSD detector.

5.1.1 Some Comments

With the experimental data of the turbulence induced tilt obtained (and described in Sec. 5.1) we can make some conclusions on the system performances.

In Fig. 5.8 and Fig. 5.9 we can see respectively the mean displacement and the maximum displacement of the centroid in the PSD plane due to atmospheric effects with respect to the focal length of the lens L_3 (see Sec. 4.6). In each figure the line at the top represents the maximum displacement allowed by the mirror, the bold line represent as said the displacement induced by the

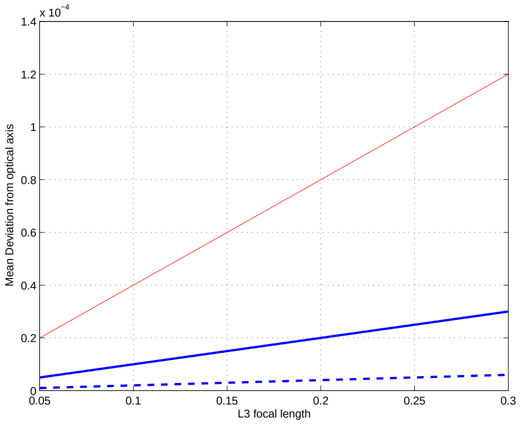


Figure 5.8: Mean displacement due to atmospheric induced tilt on the PSD plane (bold line). Mean displacement with the correction (dotted line). Maximum allowed correction due to the limitation of the deformable mirror (thin line).

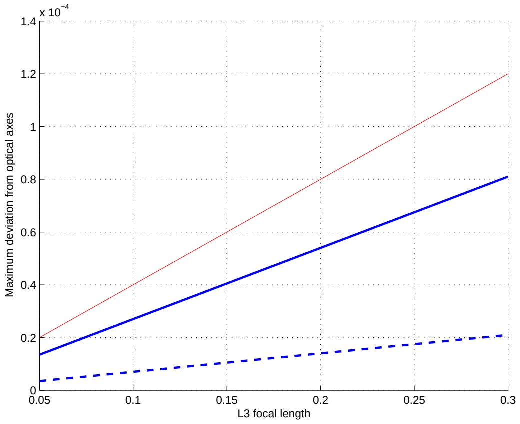


Figure 5.9: Maximum displacement due to atmospheric induced tilt on the PSD plane (bold line). Maximum displacement with the correction (dotted line). Maximum allowed correction due to the limitation of the deformable mirror (thin line).

atmosphere (mean value in Fig. 5.8 and maximum value in Fig. 5.9) and finally the dotted line represent the displacement after the correction. We see that the ratio between the maximum displacement caused by the turbulence and the maximum correction allowed by the mirror is about 2/3. This is a good compromise when considering the high variability of C_n^2 and the fact that the correction AO system is not working if the turbulence effects overcome the mirror capabilities.

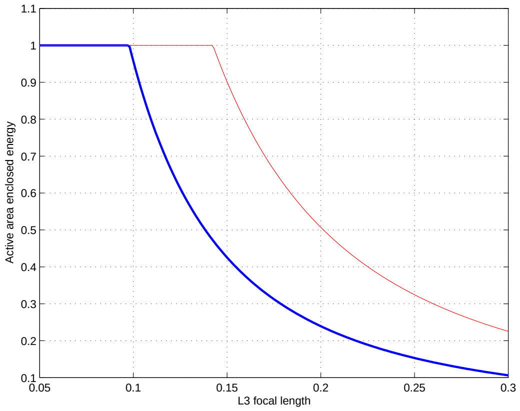


Figure 5.10: Enclosed energy in the detector active area. With the correction and without the correction

We can then calculate the mean enclosed energy on the detector active area as a function of the focal length of L_3 to see how the system can improve the performances. The results is depicted in Fig. 5.10 and has been calculated used the ratio between the radius of the detector active area and the size of the spot due to atmospheric tilt effects. The best performances is obtained with a focal length f_{L_3} of L_3 of 142mm. This would give a reduction in the total field of view of the receiver from $13.3 \times 2 = 26.6\mu rad = 5.5arcsec$ to $2.6 \times 2 = 5.2\mu rad = 1.07arcsec$ and all the energy in the corrected case will fall inside the detector active area. With our testing lens of $f_{L_3} = 150$mm things will be slightly different in the sense that in the corrected case we still would have some losses even considering the averaged case.

We analyzed also the spots at the receiver in order to validate the model in ideal conditions. When we tested the setup outside we had not built the quantum source and the spot we obtained was bigger that the diffraction limited value we expected from the model. The measurements of the spot size are reported in Fig. 5.11.

The *a)* image is a picture of the diffraction limited spot. The image saturates in the central disk, a better picture in order to calculate the spot size is the *central*. The spot at $1/e^2$ is $47.2\mu m$, the expected value for a $f_{L_3} = 150$ mm is $46\mu m$. The upper raw of images show the spot when moved by a value that corresponds to the mean deviation introduced by the atmosphere. The lower row show the spot when moved by the maximum possible tilt introduced

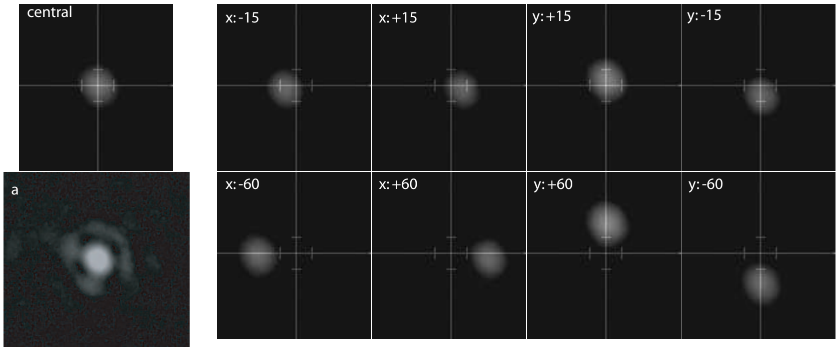


Figure 5.11: Spots of the signal lasers at the receiver. a) diffraction limited spot. Central and others: diffraction limited spot with a displacement indicated in μm.

by the mirror. The cross reference is centered on the centroid of the initial central spot and the $50\mu m$ detector area is marked.

It is possible to see how the measurement are in agreement with the model (see Sec. 4.6).

5.2 Testing of the AO System in the QKD Setup

5.2.1 Testing Setup

The testing setup is very similar to the one described for QuAKE in chapter 3. The main difference is that as the electronic unit is not complete we decided to simplify it in order to be able to obtain some early result on the AO system. We decided to avoid the APD that should read the synchronization signal from the synchronization laser. Instead we decided to use directly the signal coming from the transmitter electronic and used this signal both to drive the synchronization laser that now have the unique role of probing the effect of the atmosphere on the beam during the propagation and to serve as a trigger signal for the receiving electronics. Transmitter and receiver are in the same place and a mirror is used to double the propagation path. The FPGA board is fed directly with the synchronization signal by a connection wire.

The optical design of the transmitter is identical to the one described in chapter 3 whereas the receiver has been slightly modified. The final setup of the receiver is depicted in Fig. 5.12.

As you can see the beam coming from the transmitter is collected by the receiving telescope, it is reflected by the deformable mirror. Then the two different components: the signal beams at 850nm and the synchronization at 808nm are divided by the $850nm$ interferential filter. In this case the beam

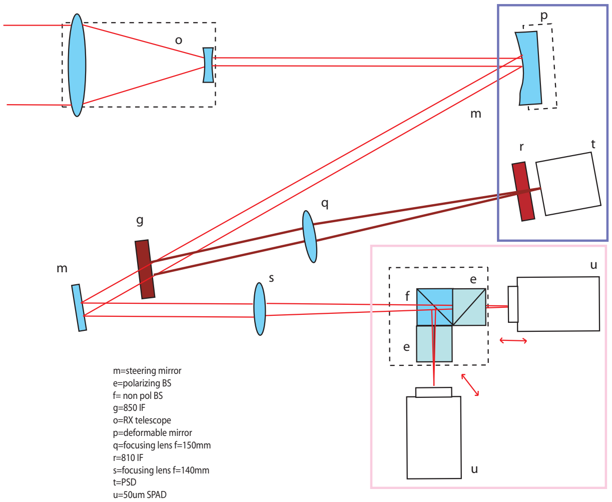


Figure 5.12: Optical setup of the receiver for the AO testing.

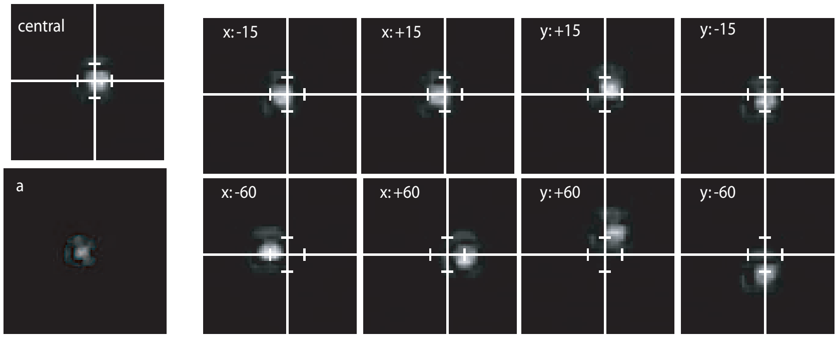


Figure 5.13: Spots of the signal lasers at the receiver. a) diffraction limited spot. Central and others: diffraction limited spot with a displacement indicated in μm.

is still collimated and each part is now focused separately: the 850nm signals beams that pass through the filter are focused with a 140mm focal length piece towards the *quantum receiver* that is the same as before (see Fig. 3.11) whereas the synchronization beam is now focused with a $f = 150$mm lens towards the Position Sensing Detector. This choice reflects the considerations made in Sec. 5.1.1 when we deduced that a $f = 142$mm focusing lens would increase the system performances. We maintained a focal length of 150mm while focusing the synchronization beam on the PSD because a smaller value would increase the noise on the position measurement. We took some picture of the spot displacement in the detector focal plane after the $f = 140$mm lens as already did for the $f = 150$mm lens (see Fig. 5.11). The result is depicted in Fig. 5.13.

The spot at the focal plane that coincides with the SPAD active area plane is measured to be $42\mu m$ wide and its profile is depicted if Fig. 5.14.

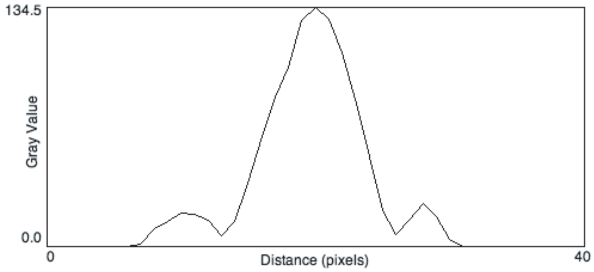


Figure 5.14: Spots profile of the signal lasers at the receiver with a $f = 140$mm lens . The measured spot size is $42\mu m$.

In order to resume and clarify the testing setup a picture of both the transmitter and the receiver are reported respectively in Fig. 5.15 and 5.16. On the transmitter , the two signal lasers after having been attenuated down to single photon level are put together with the synchronization laser and expanded by a transmitting telescope. At the receiver the signal is collected by the telescope and is collimated. It strikes the deformable mirror and after that the 850nm signal and the 808nm synchronization laser are divided by an interferential filter. The synchronization laser is then focused with a $f = 150$mm lens into the PSD while the signal lasers are focused by a $f = 140$mm lens and directed through the polarization discriminator to the SPADs active areas. A detail of the polarization discriminator is depicted in Fig. 5.17.

With this setup some tests were carried on with the goal of testing the adaptive optics capabilities. First an alignment of the SPADs was performed, then, with the help of a heat source and a fan we introduced artificially an unwanted effect. Then we tried to correct it with the help of the AO system. In the following section the results are reported.

5.2.2 Testing Results

In this section the results relative to one SPAD are reported. The other SPAD behave exactly in the same manner since the are no differences neither in the model nor in the optical path to it. With the help of the transmitting electronics we generate trains of single photon pulses. As explained earlier we are sure that the synchronization pulses do not affect the measurement since

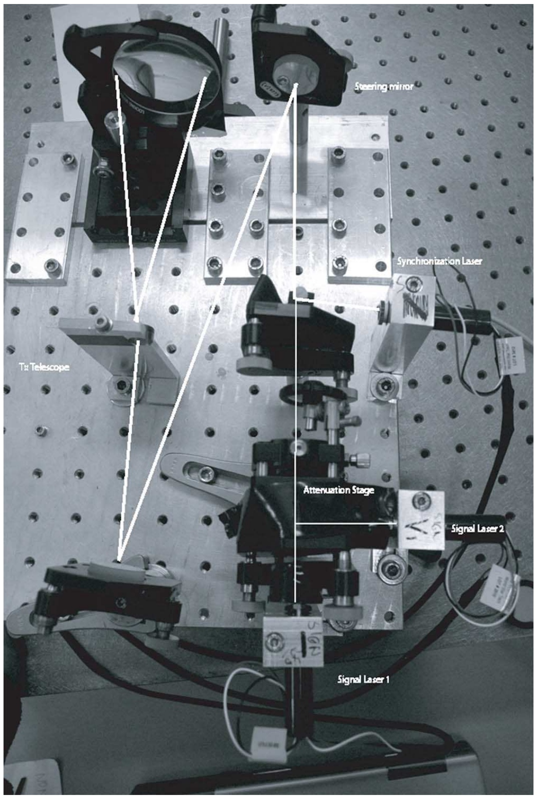


Figure 5.15: The transmitter of Quake, the two signal lasers after having been attenuated are put together with the synchronization laser and expanded by a transmitting telescope.

they are sent when the signal laser are off. This has been tested using the gate functions that the FPGA generate as explained in Sec. 3.3.4. In order to sample the count rate coming from the SPAD we used a remotely controlled universal counter with an integration window of 10ms.

The first step has been to test the alignment intentionally moving the deformable mirror. We applied tilts at the cardinal points of about 1/4 of the maximal strength of the mirror and we acquired the mean rate at different positions. The results are reported in Fig. 5.18 and show that the alignment is fairly good since the counts decrease in every direction. Unbalanced values could be done either to a non perfect alignment (this was checked many times also manually) or to a non uniform tilt in the four directions and this seems to be the case as already observed in Sec. 4.4. Remember although hat this non uniformity is corrected by the closed loop control software.

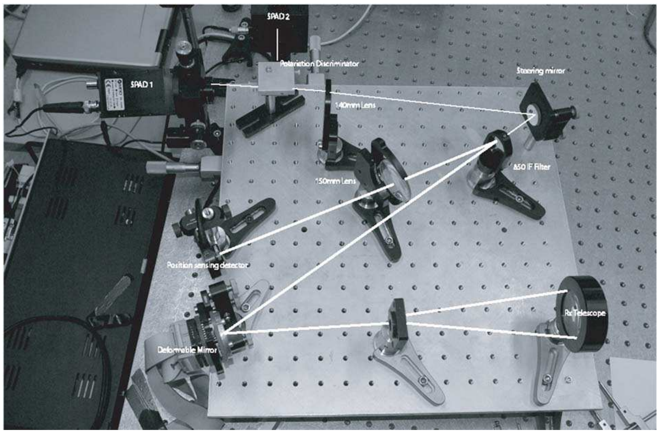


Figure 5.16: The receiver of Quake, the signal is collected by the telescope and is collimated. It strikes the deformable mirror and after that the 850nm signal and the 808nm synchronization laser are divided by an interferential filter. The synchronization laser is then focused with a f = 150mm lens into the PSD (Position Sensing Detector) while the signal lasers are focused by a f = 140mm lens and directed through the polarization discriminator to the SPADs active areas.

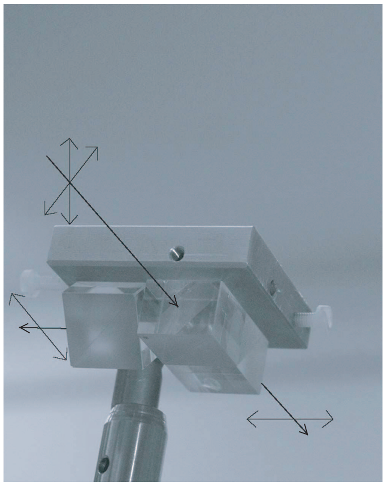


Figure 5.17: The polarization discriminator for the $B92$ protocol. The choice of the basis is done by the first non polarizing beam splitter whereas the other two polarizing beam splitters act as polarization filters according to the $B92$ protocol.

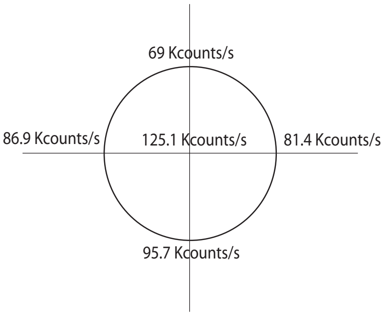


Figure 5.18: Testing of the alignment. Tilts at different cardinal points have been imposed to the mirror and the average count rates of the SPADs have been acquired at different positions.

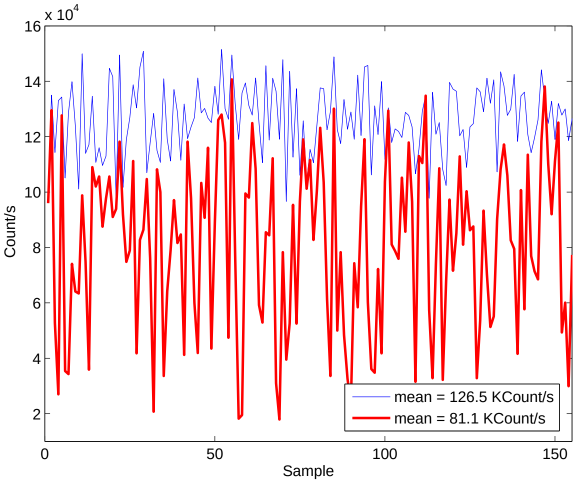


Figure 5.19: Comparison between the count rates of the SPAD with or without the induced turbulence.

At this point several data have been acquired both from the counter and the PSD acquisition software. The first figure, Fig. 5.19, show the count rate of the system where no turbulence was present compared with the count rate degraded by the induced turbulence. Notice that on the x axes there is the sample number and not the time, this because the counter could not sample data continuously because of the communication with the personal computer. The measurement time for each trial has been of the order of 1 minute.

In the figure the two counting rates R_n and R_a are compared and we go from about 126 Kcounts per second to 81 Kcounts per second showing a degradation

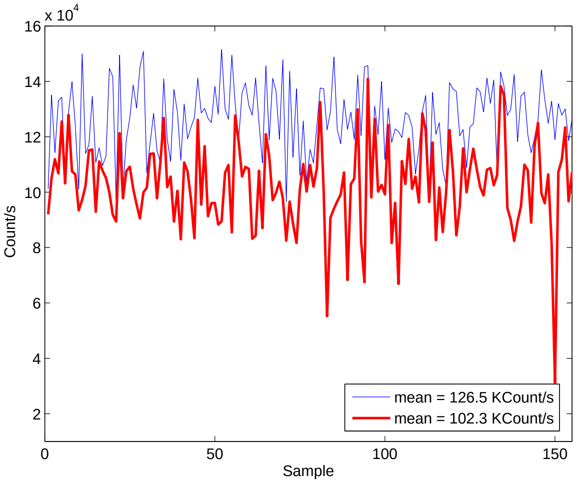


Figure 5.20: Comparison between the count rates of the SPAD without the induced turbulence and with the turbulence corrected with the AO system.

in the system performances. A good way to characterize the behavior of the system is to measure the ratio between the average intensity of the beam with or without the effect of the turbulence. This is normally referred as *Strehl ratio* or normalized intensity and its definition is as follows: the Strehl ratio S is the ratio between the intensity on-axis of an aberrated beam and the intensity on-axis of unaberrated beam. By this definition if tilt is present on the system the axis clearly becomes the normal of the plane of that particular tilt that is why tilt should be removed when evaluating the Strehl ratio. Nevertheless if a system is though and built with the aim of maintaining a beam on a receiver as it is in our case, the time average intensity on the target represent a good way of characterizing the system. After these consideration if we then evaluate the ratio S for our system we get:

$$S = \frac{R_a}{R_n} = 0.64 \tag{5.3}$$

Now we switch on the correction and we report the rate registered by the SPAD. We compare also in this case this curve with the rate we got if turbulence is not present. The results are depicted in Fig. 5.20. In this case the mean rate registered by the SPAD when the correction is activated is about 102 Kcount per second showing a good improvement with respect to the uncorrected case.

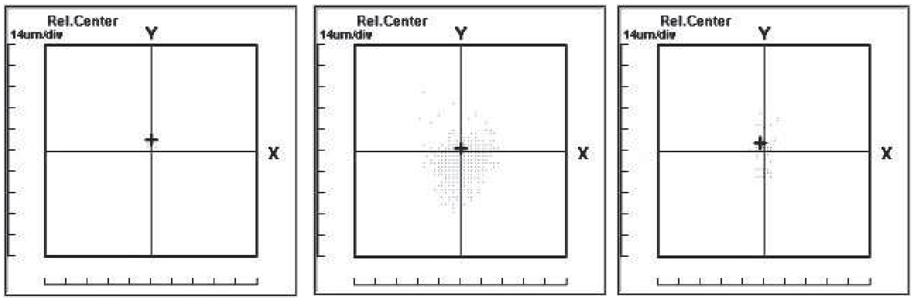


Figure 5.21: A picture of the PSD screen in normal conditions (lent), with the effect of the induced turbulence (center) and when the correction is switched on (right).

Evaluating the parameter S in this case gives:

$$S = \frac{R_a}{R_n} = 0.8. \tag{5.4}$$

We report here in Fig. 5.21 also the PSD screens that show the three conditions, starting from the left: no turbulence, with the turbulence and corrected. Notice that the pictures were taken in different moments with respect to the others and have the aim to show the average behavior of the system. You can see from the corrected case (on the right) that some points are very far from the center. This is caused by the fact that the turbulence induced with the heat and the fan is sometimes too strong for the mirror capabilities. A more interesting view of the behavior of the system is depicted in Fig. 5.22 where the data previously shown in Fig. 5.19 an 5.20 are binned with a bin of 10 Kcount per second. The statics clearly shows the benefit of the correction.

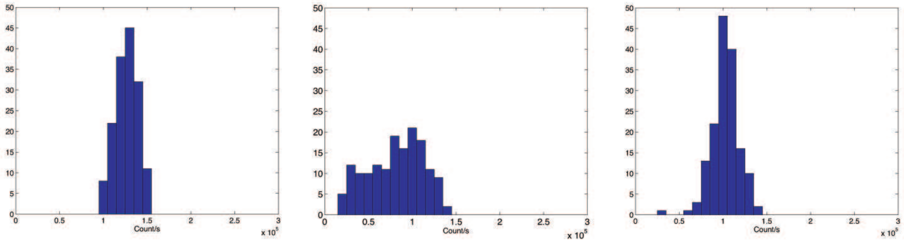


Figure 5.22: Histogram of the count rate in normal conditions (left), with the effect of the induced turbulence (center) and when the correction is switched on (right).

As you can see the AO system of QuAKE shows a good behavior when run at single photon level, there is in fact an improvement on the count rates of the SPADs. The system should be tested in this configuration in an outdoor environment and this is planned as soon as the electronic system for QuAKE will work properly. We will be able then to test the improvement of the real key generation rate. Nevertheless this results show an improvement of 15 % in the count rates and were obtained with an induced turbulence and not in real operating conditions. Considering the results reported in Sec. 5.1 one can expect better performances whit real atmosphere.

Chapter 6

High Level QKD Software

In this chapter we want to describe the basic features of a high level software for QKD. This software is the main part of the data/network layer in the layered model presented in Sec. 2.3. First an introduction to error correction and privacy amplification are presented as well as some preliminary study that we carried on using the matlab simulator described in 2.1. Then the structure of QCore is presented. QCore is our Java implementation of the data/network layer of the QKD system QuAKE. This description is followed by implementation details and results about the software performances that we analyzed by means of a test bench. Finally the web interface of QCore is presented.

6.1 Error Correction: Theory

Many papers where published about the error correcting techniques for QKD. We think that a big work of contestualization and analysis was made by Brassard and Salvail in [15] where they expose to the community the famous CASCADE algorithm.

There has been many effort in order to find a better solution to the error correcting problem in QKD links but because of the nature of the communications as we will see the problem is not trivial. An improvement seemed to be the use of *turbo codes* although this method due to the soft decision techniques involved it can be used only for continuous variable QKD [55, 85].

In this section we report the basic theory of error correction in QKD and the issues involved.

A generic error correction algorithm (ECA) takes the sifted key K_{sift} from the sifting sub-layer of the data layer and correct it. The possible errors in the sifted keys may occur from technical imperfections in the apparatus (Tx and

Rx), from the noise into the quantum channel and finally from the presence of Eve, the eavesdropper as described earlier. For this reason Alice's and Bob's sifted keys may differ in several bits. The aim of the ECA is to correct these differences, in the less amount of time and revealing the less information as possible to an eventual eavesdropper Eve. As a consequence an ECA can detect the presence of Eve by looking at the error rate on the keys. The keys after the process of error correction are called *Reconciled Keys.*

We can start our review from the sifting procedure and consider it as a process that creates a key of length n so then the entropy of the Alice sifted key A is:

$$H(A) = n. \tag{6.1}$$

If we modelize the quantum channel as a $BSC(p)$ channel[1] we can write the entropy of Alice sifted key conditioned with the Bob's sifted key entropy:

$$H(A|B) = nh(p) \tag{6.2}$$

where $h(p)$ takes into account the presence of the channel and can be written as:

$$h(p) = -[p \log p + (1-p)\log(1-p)]. \tag{6.3}$$

With this in mind let us start considering a generic error correction protocol that operates on a $BSC(p)$, call it R^p. The quantity of information exchanged by Alice and Bob during the process of error correction is normally indicated with Q, and is often called *revealed* information. It has a minimum value:

$$Q_{min} = H(A|B) \tag{6.4}$$

and it is revealed during the public discussion over the untrusted channel. The final reconciled keys of Alice and Bob are equal and indicated with W. We say that the R^p protocol has failed if the error free key of Alice is different from Bob's one, this event is graphically signed with: $W =\perp$. If we want to mathematically express that the protocol is applied to the sifted key A and B in order to obtain the key W, revealing into the channel the information Q we can write:

$$R^p(A, B) = [W, Q] \tag{6.5}$$

The amount of *leaked* information is the expected amount of Shannon information than the eavesdropper Eve can get on W given Q and is:

$$I_E(W|Q) \tag{6.6}$$

[1] $BSC(p)$ is a binary symmetric channel with error probability p.

From all the properties of the generic error correction algorithms, we can extract the one that are interesting for the quantum key distribution, keeping particular attention to the fact that a QKD ECA must operate in a high security context where the information revealed on the public channel must be small. For this purpose we can give some useful definition; in particular the robustness, the optimality, the suboptimality and the efficiency of an error correcting algorithm.

Definition 6.1 *an ECA R^p is ϵ-robust if set* $0 \leq \epsilon \leq 1, \exists N_0(\epsilon) : \forall n \geq N_0(\epsilon)$ *so then*

$$\sum_{\alpha,\beta \in \{0,1\}^n} \mathrm{P}[A = \alpha, B = \beta] \mathrm{P}[R^p(\alpha,\beta) = [\perp, \cdot]] \leq \epsilon. \tag{6.7}$$

In other words, an ECA is robust if it will fail the correction of the sifted key with a probability that tends to 0.

It is important to notice that we consider the eventuality that every single error in the sifted keys A and B are caused by Eve [2]. In this case we can say that Eve has an *a priori* information on the keys that has a maximum value of:

$$I_{Eap}(A,B) = H(A) - I(A,B) = nh(p). \tag{6.8}$$

If $H(A|B) = 0$ the a priori information gained by Eve is equal to zero. This is not the only amount of information that Eve can have on W, she can extract more information from the channel because the ECA reveals on it the information Q while operating the correction. Eve is then able to obtain more information on the reconciled correct key W. It is intuitive to see that the leaked information is greater or equal then the a priori information that Eve posses. For this reason an ECA is better than another one if it produces a smaller

$$I_E(W|Q), \text{ with the same } Q \tag{6.9}$$

For the leaked information we have an important theorem derived directly from the noiseless coding theorem from the information theory by Shannon:

Theorem 4 $(\forall p \leq \frac{1}{2}) \,\&\, (\forall R^p)$ *if* $\exists\ 0 \leq \epsilon < 1$ *as* $R^p = [W,Q]$ *is ϵ-robust, then:*

$$\lim_{n \to \infty} \frac{I_E(W|Q)}{nh(p)} \geq 1$$

where n is the length of the keys.

[2] That means that the channel and the apparatus are considered ideal. This case in not so practical but can be a good approximation for massive attacks of Eve although in these cases the protocol would probably abort the key generation. It is although a common approach in cryptanalysis.

This theorem simply state that an algorithm capable of correcting errors on two strings (or keys in this case) can only increase the information that Eve have over the strings to a value greater of equal to the information that Eve already had on the strings. From what just stated it is easy to understand the following definition:

Definition 6.2 *An ECA R^p is defined **optimal** if:*

1. $\forall \epsilon > 0$ *is epsilon-robust;*
2. $\lim_{n\to\infty} \frac{I_E(W|Q)}{nh(p)} = 1$.

in other words the best algorithm (in the sense of optimality) doesn't reveal any more information to Eve that, if this is the case, can rely only on the a priori information $nh(p)$.

The last important definition of this introduction section is the one that describe the condition of **efficiency**: in fact we would like to act an ECA in a small time in order to increase the key production rate. A good indicator of the speed of a ECA is the complexity class of the problem that it can solve. We usually consider the time of execution $\overline{T}^{R^p}$ and try to find a function of the key length n that bounds it from above. Using this scheme we can define an efficient algorithm as follows:

Definition 6.3 *An ECA R^p is called **efficient** if we can find polynomial $t(\cdot)$ where, given its expected running time, $\overline{T}^{R^p}$, we have $\overline{T}^{R^p} \leq t(n)$ for $n \to \infty$.*

and then, consequently:

Definition 6.4 *An ECA R^p is called **ideal** if it is both optimal and efficient*

In many practical cases the feature of optimality is too much restrictive, and we can implement simpler algorithms that may be also faster than the optimal one. The algorithms we are looking for must be obviously robust because they still are required to have correction capability. They have to be fast enough: we would like an expected running time limited by a polynomial $t(n)$ on the key length n. We don't need them optimal but we ask them to be arbitrary near to the definition of optimality in accordance with a margin parameter ζ in agreement with this definition:

Definition 6.5 *An error correcting algorithm R^p_ζ is called **almost ideal** if $\forall \zeta > 0$:*

1. $\forall\epsilon > 0 \quad R^p_\zeta = [W, Q]$ *è ϵ-robust;*

2. $\lim_{n\to\infty} \dfrac{I_E(W|Q)}{nh(p)} \leq 1 + \zeta;$

3. $\exists\, t(\cdot),\ N_0(\epsilon) :\ \forall\, n \geq N_0(\epsilon)$ *we have that:* $\overline{T}^{R^p_\zeta} \leq t(n)$.

Now that we have the necessary background we can start thinking of what is the best choice for the problem we are facing i.e. correcting error in a QKD system. The variety of the ECA that can be divided into three families: *linar codes* , *recursive codes* and *turbo codes*. Linear codes are indeed opitmal but not efficient because in this particular case we do not know both the length of the sifted key, n, and the effective error rate during the transmission. Furthermore we have seen that turbo codes are based on soft decision strategies that cannot be applied to single photon based QKD. It is then natural to look for our candidate among recursive codes.

In a recursive ECA Alice and Bob first break their keys in several blocks, then they execute an error correcting protocol on each block and finally they check each block to verify the effectiveness of the correction[3]. When Alice and Bob find that there is an error in one of the blocks they divide this block in other sub-blocks and re-apply the error correcting protocol to each sub-block. This mechanism goes on until the error is corrected. Usually, to maximize the strength of the algorithm, after having performed a recursive ECA on the keys, the bit of the keys are randomly permutated and then the ECA is applied again on the scrambled keys. This process may be done several times in order to reach a particular grade of reliability of the corrected (reconciled) keys.

6.1.1 CASCADE

CASCADE is today the most common ECA in the practical implementation of a complete quantum key distribution system. It follows a description of the algorithm.

The CASCADE protocol:

1. Alice and Bob measure the error rate p revealing l bit of their n' bits sifted key.

2. They discard the l bits used for step one. The sifted key is now n bit long,$n \leq n'$.

[3] Because of the former steps they are called recursive.

3. They divide A and B in blocks of length $k_1(p)$ and decide a number of iteration $\omega(p)$. These blocks are called *primary blocks* and K_1^v indicates the $v-th$ couple of blocks.
4. Alice sends to Bob all the parity check for these blocks.
5. For every couple of blocks where the parity differs (odd number of error present) they starts a binary search procedure:
   a) Alice sends the parity for the first half of the block
   b) Bob check weather the error is in the first or second half of the block.
   c) They repeat this search for the half block they found in step b.
   d) If the sub block is composed of one bit or two bits with different parity check they discard it. Doing so they eliminate one error in the primary block K_1^v that now has an even number of error present.
6. If the iteration is the last they stop the algorithm, otherwise they operate a permutation of the actual sifted keys in order to redistribute errors uniformly.
7. They divide A and B in blocks K_i^v of lenght k_i where i indicates the current iteraction.
8. They restart in this new iteration from step four.

It is possible to demonstrate that, fixing a particular value of the length k_i, the probability that one of the primary blocks K_1^v will have errors, after the the end of the algorithm, decrease exponentially with the number of iterations ω. In particular the probability that after the step $i \geq 1$ of the iterations there will remain $2j$ errors in the block K_1^v is call $\delta_i(j)$. Moreover we assume that, if we have an error at the step $i \geq 1$, in the relative primary block we will correct another one.

We observe also that the number of errors X in the primary block has a Binomial statistic

$$X \in \mathcal{B}(k_1, p) \tag{6.10}$$

and, for this reason, it's obvious that:

$$\delta_1(j) = \mathrm{P}[X = 2j] + \mathrm{P}[X = 2j + 1] \tag{6.11}$$

If we call E_i the mean value of the errors after the step i, then:

$$E_1 = 2 \sum_{j=1}^{\lfloor \frac{k_1}{2} \rfloor} j\delta_1(j) = k_1 p - \frac{1 - (1 - 2p)^{k_1}}{2}. \tag{6.12}$$

In a similar way, we call γ_i the probability of correcting at least two errors in the block K_v^1 that has some errors in the previous step $i-1$. Because of the fact that the permutations at point 6 of the algorithm are random, at the limit $n \to \infty$ we will obtain:

$$\gamma_i \geq 1 - \left(1 - \big(1 - \frac{k_i}{n}\big)^{\frac{nE_{i-1}}{k_1}}\right)^2 \approx 1 - \left(1 - e^{-\frac{k_i E_{i-1}}{k_1}}\right)^2. \tag{6.13}$$

For this reason, in the case of $i \geq 1$, we have the next relation:

$$\delta_i(j) \leq \left(\sum_{\ell=j+1}^{\lfloor \frac{k_1}{2} \rfloor} \delta_{i-1}(\ell)\right) + \delta_{i-1}(j)(1-\gamma_i). \tag{6.14}$$

Finally let's take

$$k_i = 2k_{i-1} \tag{6.15}$$

with k_i that satisfy the next:

$$\sum_{\ell=j+1}^{\lfloor \frac{k_1}{2} \rfloor} \delta_1(\ell) \leq \frac{1}{4}\delta_1(j), \tag{6.16}$$

Considering the (6.16), we can write a formula for the probability $\delta_i(j)$ in relation with the same probability in the step before:

$$\delta_i(j) \leq \left[\frac{1}{4} + (1 - e^{-2^{i-1}E_{i-1}})^2\right]\delta_{i-1}(j). \tag{6.17}$$

With these formulas we can demonstrate the fundamental fact that the error probability decrease exponentially with the number of iteration in the CASCADE algorithm. In fact if k_1 is chosen in a manner that assure that

$$E_1 \leq \ln 2/2 \tag{6.18}$$

we directly obtain that:

$$\delta_i(j) \leq \frac{\delta_{i-1}(j)}{2} \leq \frac{\delta_1(j)}{2^{i-1}} \tag{6.19}$$

Finding the proper value for k_1 inverting Eq. 6.12 it is easy but the result cannot be written in a closed form. Instead we can rely on the following approximation that holds if $p \ll 1$:

$$E_1 = \frac{k_1 p}{2} \tag{6.20}$$

We now try to estimate the information $I[n]$ that each binary search in a primary block of length n reveals for the correction of one error. Considering that:

$$\begin{aligned} I[1] &= 0, \\ I[2n] &= 1 + I[n], \\ I[2n+1] &= 1 + I[n]\frac{n}{2n+1} + \frac{n+1}{2n+1}I[n+1] \end{aligned} \tag{6.21}$$

we can write the solution:

$$I[n] = k + 2\frac{x}{n} \tag{6.22}$$

where n can be written as $n = 2^k + x$ with $0 \leq x \leq 2^k$. Clearly if n is an exact power of two a binary search would correct one error revealing exactly k parity bits.

The exact revealed information for a primary block of length k_1 in ω iterations is [15] :

$$\begin{aligned} I_w[k_1] \leq \quad 2 \quad &+ \frac{1-(1-2p)^{k_1}}{2}\lceil logk_1 \rceil + \\ + \quad &2\sum_{l=2}^{\omega}\sum_{j=1}^{\lfloor \frac{k_1}{2} \rfloor}\frac{j\delta_1(j)}{2^{l-1}}\lceil logk_1 \rceil \end{aligned} \tag{6.23}$$

and it is possible to verify with some simple numerical example how CASCADE is close to optimality. It Table 6.1 you can see the value of k_1 and the revealed information for four iteration estimated for some value of the error probability p compared with the theoretical best $nh(p)$.

p	k_1	$I_4[k_1]$	$nh(p)$
0,01	73	6,81	5,89
0,05	14	4,64	4,01
0,1	7	3,99	3,28
0,15	5	4,12	3,05

Table 6.1: Some examples of the revealed information in four iteration parameterized by the error rate p with compared to the theoretical limit $nh(p)$.

There are many variations of this algorithm that can be implemented, each resulting more suitable in a specific application as we will discuss later. The theoretical limitation of Cascade is that it fails for error rates greater than 15%. In this case the length of the primary blocks approaches the value of 5 bits and so the revealed information per block is comparable with the length of the block itself. Moreover it is important to notice that the revealed information Q and the leaked information $I_E(W|Q)$ do not coincide for CASCADE[4]. In this case the parity checks that Alice and Bob exchange represent new information with respect to the a priori information I_0 that both Eve and Bob have on Alice's key. If, during the error correction procedure we reveal m parity bits the leaked information is $I_E(W|Q) = I_0 + m$ where in general $I_0 \neq 0$. When we reach the error limit of about 15% even if $I_0 = 0$ we have that $I_E(W|Q) = Q \approx H(A)$ i.e. Eve knows Alice's Key. In general the error rate is far less that 15% and $I_0 \neq 0$ and depends on how Eve attacks the system. A good ECA for QKD would try to estimate I_0 and have $Q \leq Q_{MAX}$ so then:

$$I_E(W|Q) = I_0 + Q_{MAX} \ll H(A). \tag{6.24}$$

6.2 Preliminary Study for Implementation of ECA.

We used the simulator described in Sec. 2.1 to analyze the behavior of CASCADE algorithm in order to optimize some of its features. The results are averaged over a thousand iterations of the algorithm and CASCADE is executed with $\omega = 4$ iteration if not differently stated. First notice that even if the error probability in a block P_{eB} is negligible, for example 0.2%, the error probability P_e for the whole key it is not, take for instance 100 blocks and then $P_e = 18\%$. We can say that the correction capability of CASCADE depends on three main interconnected factors:

1. The length of the keys to be corrected
2. The percentage of bit used to estimate the initial BER between the keys
3. The effective BER between keys

Fig. 6.1 and 6.2 describe the performances of CASCADE implemented as described in Sec. 6.1.1. In the former the estimated probability of failure of CASCADE is shown i.e. the probability that the corrected key are not equal. It can be clearly seen that this happen very often and with probability that tends to one for high initial BER.

In Fig. 6.2 is shown the distribution of the residual error BER_r over a thousand keys processed by the algorithm for different initial BER. On the y axis the number of keys with that particular BER_r. Normally we see that

[4] These two values do coincide for linear codes for example.

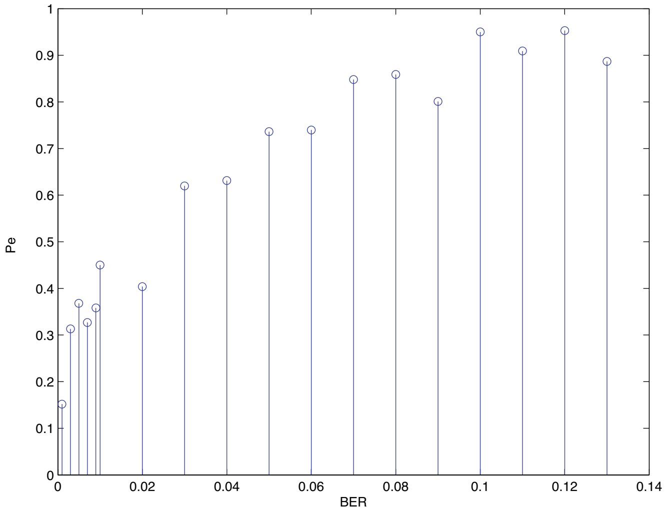


Figure 6.1: Residual error probability P_e versus initial error BER for CASCADE.

$BER_r < BER$ as we expect but as we increase the BER the algorithm is less able to completely correct the key (this correspond to $BER_r/BER = 0$). When the initial BER is low, say under 2% (Fig. 6.2 sx), it can happen that $BER_r > BER$ but this is due to the difficulty of estimating properly the initial BER.

If one thinks about the causes of this behavior it comes out that if the initial error increases, the probability to find an even number of errors per block increases. Moreover the primary block length is decided depending on the estimated error on the keys and for this reason it is essential that the error bits are uniformly distributed on the keys. This because in order to estimate the BER (p) CASCADE randomly samples the key. It is also true that a good sampling for a BER would not be the best one for a higher or lower BER. This problem affects heavily the keys with low initial errors thus leading the algorithm to operate in conditions far from optimality.

A first way in order to increase the performances of CASCADE is to increase the number of iterations ω. This have the advantage that the revealed information does not increase very much with ω going from 40% with one iteration to 50% with 10 iterations but, on the other hand, the method has a big drawback that is that the execution time increases rapidly with ω. A better way to increase the algorithm performances it to overestimate p. Doing so the primary blocks have smaller length reducing the probability of an even numbers of error in a single block. Clearly this trick works good only for small

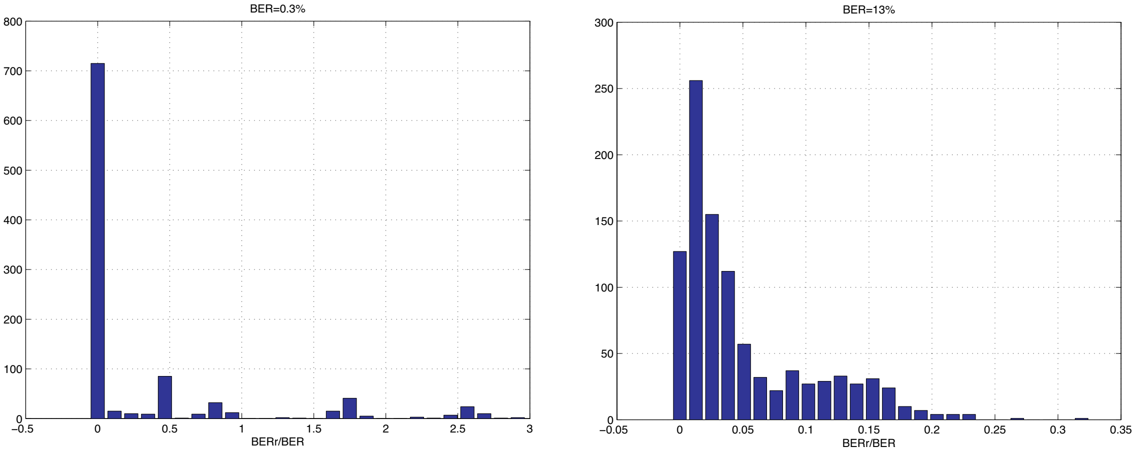


Figure 6.2: Distribution of residual BER_r in 1000 corrected keys with initial $BER = 0.3\%$ (sx) and $BER = 13\%$ (dx). Number of iteration $\omega = 4$.

BER value, say less than 0.01%, when reducing the primary block length has no effects on the revealed information.

For higher BER what we have thought is to run the algorithm straight until the last iteration and for this use block length smaller than the theoretical value. Normally block length double every cycle but is we use $K_w = K_1$ we have a big increase in performances. At this point most of the error have been corrected an so the probability that blocks of length k_1 presents more that one error is negligible. Practically if we had to run $\omega = 4$ iterations of CASCADE we would run CASCADE two times,the first with $\omega = 3$ and the second one with only one iteration using the same estimation of p that we have already used.

In conclusion, overestimating p for small BER and modulating the block length as described we can keep the residual error probability under 2.3% even with initial BER greater that 10% as you can see in Fig. 6.3. Confronting this results with Fig. 6.1 one can appreciate the improvements introduced.

Looking at the revealed information for the modified version of CASCADE it can be seen that it does not increase too much, on the contrary it is pretty close to the original version of the algorithm. This is shown in Fig. 6.4 where a comparison is made plotting the ratios between the leaked information of the modified version of CASCADE and respectively: the theoretical value for standard CASCADE, the Shannon limit, and the leaked information for linear codes.

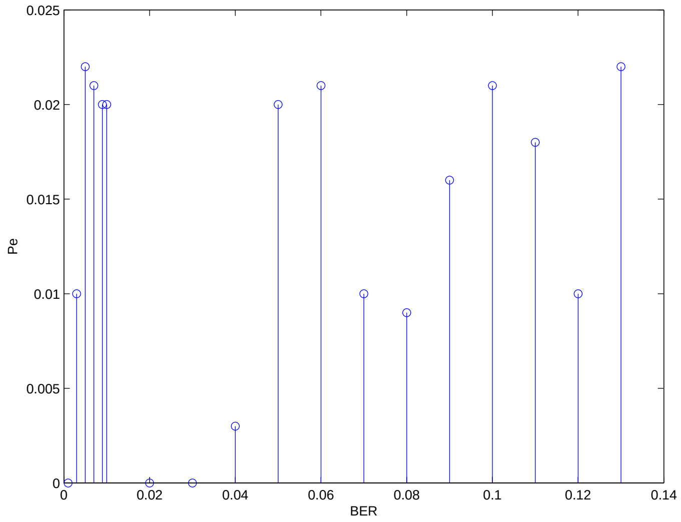


Figure 6.3: Residual error probability P_e versus initial error BER for the modified version of CASCADE.

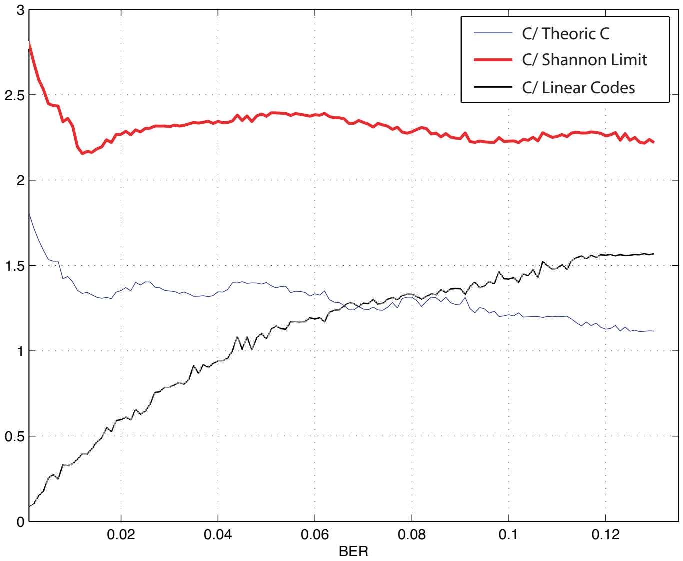


Figure 6.4: Comparison of leaked information. The letter C in the legend stands for Cascade.

It can be seen that CASCADE is better that linear codes regarding the leaked information for BER less that 7%. Moreover the theoretical value for standard CASCADE is pretty close to the value for modified CASCADE since the ratio is fairly close to one.

6.3 Privacy Amplification: Theory

Privacy amplification is the process that permits to obtain a perfectly secure key where the residual information owned by Eve is lower than an arbitrary prefixed quantity. As before, let W be a random variable that represent the error free keys i.e. the keys coming from the process of error correction. Supposing that the ECA succeeded in correcting all the errors, Alice and Bob have the same key. The binary value of Key can be any number between 0 and $2^n - 1$, where n is the length of the key. For this reason the entropy of W is:

$$H(W) = n \tag{6.25}$$

We will indicate the information $I_E(W|Q)$ that Eve has on W with another random variable J with joint distribution p_{WJ} partially controlled by Eve. Alice and Bob will calculate the final secure key K, with the application on W of the function $g(\cdot)$ represented by the random variable G. The function g is a random choice on a group of known functions that Alice and Bob choose at each process of privacy amplification. For this reason we can write the final secure key as:

$$K = g(W) \tag{6.26}$$

During this section we will give some definitions on the so called universal functions, then we will define the hash functions as a particular sub-class of universal functions. During the exposition we will define also the concept of *Rényi Entropy.* With this definition as prerequisites we will describe the privacy amplification process.

Before starting we give the definition of universal function:

Definition 6.6 *Le H a class of functions from F to G. the class H is called **universal**$_2$ and is written H_2, if $\forall\, x, y \in F$, $x \neq y$, the number of functions f in H such as $f(x) = f(y)$ is less or equal to $|H|/|G|$.*

A very important result, that will be demonstrated, is that the length of the final key can be calculated with

$$r = n - t - s \tag{6.27}$$

where t is the information content of J and s is a *security parameter* such that, if $G \in H_2$, the conditional entropy:

$$H(K|G, J = j) \geq 2 - \frac{2^{-s}}{\log 2}; \tag{6.28}$$

hence , Eve information on the key K, if she knows j, is

$$I_E(K;G,J=j) \leq \frac{2^{-s}}{\log 2}. \tag{6.29}$$

The most important results on privacy amplification are present in the papers by Bennet and Brassard in [10, 7], while a good study of the universal and hash functions is in [90]. Here a sketch of those results is given in order to facilitate the understanding of the implementation presented in sec. 6.5.

6.3.1 Universal Hashing Functions and Rényi Entropy

We can re-write the 6.6 with the next two definitions:

Definition 6.7 *a random function G from X to Y is a random variable whose values are in the class function defined by the two sets X and y.*

Definition 6.8 *A random function G from X to Y is called **universal$_2$ function** if $\forall\, x, x' \in X :\ x \neq x'$, we have that:*

$$\mathrm{P}[G(x) = G(x')] \leq \frac{1}{|Y|}.$$

For those functions the *collision probability* is defined as follows:

Definition 6.9 *Let x a random variable on a alphabet A with probability distribution p_x. We define **collision probability $\mathbf{P_c(x)}$ of x**, the probability that x has the same value in two different realizations of itself:*

$$P_c(x) = \sum_{a\in A} p_x^2(a).$$

Definition 6.10 *Let $\mathcal{E}$ a generic event and x a random variable on alphabet A and let the conditional probability be $p_{x|\mathcal{E}}$. We define **conditional collision probability $\mathbf{P_c(x|\mathcal{E})}$ of x given** $\mathcal{E}$, the probability that x assumes the same value in two different realizations:*

$$P_c(x|\mathcal{E}) = \sum_{a\in A} p_{x|\mathcal{E}}^2(a).$$

In order to understand how privacy amplification is implemented we need the concept of *hash functions* and some properties of these tools very important for the world of cryptography: both for classical and quantum.

Definition 6.11 *A family H **of hash functions** is a family of functions that are defined from X to the set Y where $|X| > |Y|$*

Definition 6.12 *An hash family function is called **$\oplus$-linear** if $\forall x,\, x' \in X$ and $\forall\, h \in H$ results*

$$h(x \oplus x') = h(x) \oplus h(x')$$

where $\oplus$ is the bit by bit *xor*, exclusive *or*, between two string x and x' of length m.

Definition 6.13 *An hash family is called **ε-balanced** if $\forall\, h \in H$,*

$$\forall\, x \neq 0,\ x \in\ X,\ \forall c \in Y, \quad \mathrm{P}[h(x) = c] \leq \varepsilon.$$

From the Def. 6.8 e Def. 6.13 we can derive that if an hash function family is both $\oplus$-linear and ε-balanced for $\varepsilon \leq 1/|Y|$, then it is also universal$_2$.

Theorem 5 *Let H an hash functions family from X to Y. If H is $\oplus$-linear and ε-balanced for $\varepsilon \leq 1/|Y|$ it is also a universal$_2$ function family.*

With the collision probability defined by Def. 6.9, we can now define the Rényi entropy.

Definition 6.14 *The Rényi entropy of the second order, or briefly, **the Rényi entropy** of a random variable x on alphabet A is the negative logarithmic of its collision probability:*

$$R(x) = -\log_2 P_c(x) \tag{6.30}$$

A very interesting result makes a connection between the Shannon and the Rényi entropies:

Theorem 6 *For each probability distribution p_x, the Rényi entropy is less then the Shannon entropy and is equal if and only if x is a uniform variable in X.*

$$R(x) \leq H(x) \quad \text{and} \quad R(x|y) \leq H(x|y) \tag{6.31}$$

We can now write the most important result that ensure that the information that Eve can have on the final secure key K is less then an arbitrary constant. This theorem is at the basis of each protocol of privacy amplification.

Theorem 7 *Lets take x a random variable on alphabet X, with probability distribution p_x and Rényi entropy $R(x)$; take also G a universal$_2$ function from $X \rightarrow \{0,1\}^r$, and $Q = G(x)$.*

Then the result is that:

$$H(Q|G) \geq R(Q|G) \geq r - \log_2(1 + 2^{r-R(x)}) \geq r - \frac{2^{r-R(x)}}{\ln 2}.$$

If we introduce also the conditional entropy version of the Theorem 7, we finally derive what is effectively interesting for the world of quantum cryptography. In fact, if we transpose the concept of the previous results into binary strings, like a cryptographic key is, we can state the following:

Theorem 8 *Let W a random string of identically independent n, and $J = e(W)$ the information that Eve can have on the string with an arbitrary eavesdropping function $e : \{0,1\}^n \rightarrow \{0,1\}^t$ ($t < n$), which represents the eavesdropping action and also the error correction function. Then, take $s < n - t$ a positive security parameter that Alice and Bob have chosen with $r = n - t - s$. Finally take the universal function G from $\{0,1\}^n \rightarrow \{0,1\}^r$.*

If $K = G(W)$ then Eve's information on the final secret key K satisfies the next:

$$I_E(K; G, J) \leq \frac{2^{-s}}{\ln 2} \tag{6.32}$$

$I_E(K; G, J)$ can be then chosen to be arbitrarily small according to the parameter s.

6.4 Preliminary Study for Implementation of PA

In the literature a lot of hash universal$_2$ functions are present and each of them is good for security purposes. The key point becomes then the computational power for implementing Eq. 6.26. We would like a practical hashing function to be characterized by these properties

- it has to be in a very large family of hashing functions.
- the number of bit in order to describe a member of this family must not be too large. Remember that this information must be transmitted between Alice and Bob.
- the operation $G(W)$ must be easy to compute for Alice and Bob because a computation has to be made for each shared key.
- the hashing function must be *one-way* i.e. very difficult to invert.

A class of hashing function family is represented by instance by binary matrices. Carter and Wegman have demonstrated that if we take an m by n completely random matrix $\mathbf{A}$ it is possible to create a universal$_2$ function good for privacy amplification. If the string S is n bit long, the operation that calculate the string

$$S' = \mathbf{A}S \tag{6.33}$$

This type of hash function is simple to compute but it is not good for our purposes as it requires $m \times m$ bits to be identified.

We investigated also the use of Bucket hashing introduced by Rogaway [70]. In this technique the string X is partitioned in n words $X = X_1 \dots X_n$. Then the words X_i , $i = 1 \dots n$ are placed in m boxes, a XOR operation is executed on each boxes and thet the results are concatenated.

A scheme of this sort, called $\mathcal{B}$, depends on three parameters: σ, n and m, where $\sigma \geq 1$ is the length of each word ($|X_i| = \sigma$) so then the hashing mapping goes from $\mathcal{A} = \{0,1\}^{\sigma n}$ to $\mathcal{B} = \{0,1\}^{\sigma m}$, $n \geq 1$, $m \geq 3$.

Each hash function $h \in \mathcal{B}$ is then represented by a list $h = h_1 \dots h_n$ of length n where each h_i is a triplet of number $\{h_{i1}, h_{i2}, h_{i3}\}$, $h_{ij} \in \{1, \dots, m\}$, $i = 1 \dots n$, $j = 1, 2, 3$.

A function h of this type can be randomly chosen taking n triplets of elements h_{ij} with the property described and the only condition that if $k \neq l$ then $h_k \neq h_l$.

Another possible implementation that we considered is Toeplitx matrices based hasshing. A Toeplitz function is similar to the matrix $\mathbf{A}$ of Carter and Wegman, but is more efficient in the sense of the communication of its description between Alice and Bob.

Definition 6.15 *A Toeplitz matrix is a matrix* $\mathbf{T}$ *where, for each index* i, j, l, k *results that*

$$T_{i,j} = T_{k,l} \text{ with } k - i = l - j \tag{6.34}$$

Then a feature of a Toeplitz matrix is the particular symmetry of the its elements. An example is:

$$\mathbf{T} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

It is possible to demonstrate that a Toeplitz matrix is described only by its firs row and first column. For this reason all the information that Alice and Bob must share is

$$n + m - 1 \text{ bit} \tag{6.35}$$

We compared the two algorithms described by means of the matlab simulator and the results are summarized in Tab. 6.2 where $l_{corr} = n$ is the length of the corrected key and $l_{pa} = m$ is the length of the final key given by:

$$l_{pa} = l_{corr} - I_E(A) - Q - s = l_{corr} - nh(p) - Q - s. \tag{6.36}$$

Privacy amplification	**execution time**	**bit to be transmitted**	**physical space required**
Toeplitz	$l_{corr} \cdot l_{pa}$ XOR	$l_{corr} + l_{pa}$ byte	$l_{corr} \cdot l_{pa}$ byte
Bucket	$3 \cdot l_{corr}$ XOR	$3 \cdot l_{corr}$ byte	l_{pa} byte

Table 6.2: Comparison of performances of Bucket hashing and Toeplitz matrix ashing.

if CASCADE is used as ECA.

From Tab. 6.2 Bucket seems to be better and in fact it is considering the execution time of the algorithm, the number of bits to be transmitted and the physical space required. Nevertheless if we consider the time for generating either the matrix in Toeplitz case or the bucket table for Bucket hashing and the complexity of these two operations, Toeplitz matrices PA behave slightly better that Bucket. For this reason and because of their relatively simple implementation we decided to use Toeplitz matrices based privacy amplification. In Tab. 6.3 and Tab. 6.4 we report some results of simulation of PA with Toeplitz matrices considering the whole QKD system, with different protocols, different conditions and different eavesdropper strategies. Values are averaged on 10 transmissions with Visibility of 50 Km, misalignment of 5 dB and 500 dark counts per second on the detectors. *Ideal* means that the channel is noiseless, *real* means that attenuation, misalignment etc.. are present but Eve is not. *Projective* and *POVM* mean that there are both noise and Eve acting in between Alice and Bob. As usual negative values have no physical meaning but indicate an aborted communication.

Protocol	**Conditions**	**Attacked pulses**	**Sifted key**	**Reconciled key**	**Secure key**
BB84	ideal	0%	2810	2232	2194
BB84	real	0%	2587	2023	1967
B92	ideal	0%	1406	1113	1093
B92	real	0%	1276	987	950
BB84	projective	30%	2236	1055	463
B92	projective	30%	942	327	-180
B92	POVM	30%	816	460	239
BB84	projective	100%	1355	181	-1043
B92	projective	100%	632	0	-442
B92	POVM	100%	196	2	-186

Table 6.3: Comparison between raw and final secure keys.

Protocoll	**Conditions**	**Attacked pulses**	**Overall efficiency**	**Relative efficiency**
BB84	ideal	0%	0.781	0.983
BB84	real	0%	0.760	0.972
B92	ideal	0%	0.778	0.982
B92	real	0%	0.744	0.962
BB84	projective	30%	0.239	0.439
B92	projective	30%	-0.192	-0.553
B92	POVM	30%	0.293	0.520
BB84	projective	100%	-0.770	-5.762
B92	projective	100%	-0.700	$-\infty$
B92	POVM	100%	-0.950	-93

Table 6.4: Comparison between efficiencies in PA. Overall efficiency is the ratio between final secure key length and sifted key length. Relative efficiency is the ratio between the final secure key with the reconciled corrected key.

6.5 Implementation of ECA and PA: the QCore Software.

We decided to implement the high level protocol for QuAKE in Java. The software has to take the raw key from the physical layer of the system and process it realizing the sifting, the ECA and the PA. Beside this the software should accomplish several other tasks concerning controls signal from different layers. QCore is thought in fact to menage all the operation concerning the realization of the protocol. We can describe all the task by looking at the logical structure of the software.

6.5.1 Structure of QCore

The general architecture of QCore is depicted in Fig. 6.5.

QCore is a client server like application installed on both the transmitter and receiver side of the communications. Notice that there is only one software that works perfectly fine either on the Alice or Bob side, the reason will be clear shortly. The machines on which the software is installed act as appliances that connects the physical layer to the application layer. These machine have several connections capabilities. First of all they have to receive the raw key material from Alice and Bob quantum communication apparatus (QKDS), for this reason they need a trusted connection with the QKDS. It is reasonable to assume that this connection is indeed secure because, very likely, the appliance

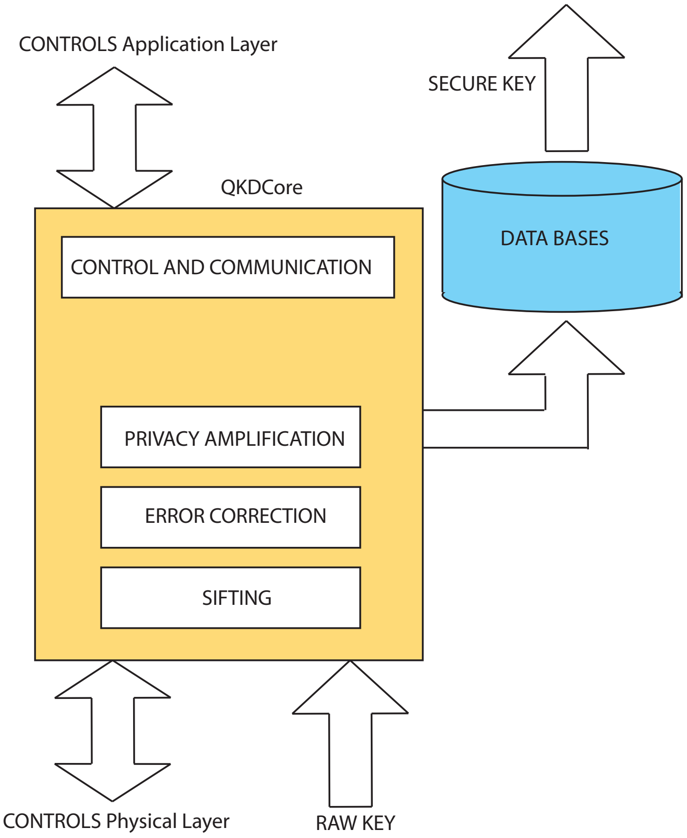


Figure 6.5: General structure of QCore. The raw key coming from the physical layer is processed and the secure key is stored in a database. Controls signals are used to menage all the operations.

and the QKDS would lay in the same secure and trusted environment. Then they need to process the data to get the secure key and for this reason they need a public untrusted channel i.e. the internet. Moreover they need to make the keys available for the application layer. A better view of the situation is depicted in Fig. 6.6.

We wanted to keep the software the most user friendly and versatile. That is why we designed it in order make the architecture and the design independent from the hardware for the quantum communication, independent so from the physical layer. In this picture the roles of Alice and Bob intended as transmitter and receiver are differentiated using the data bases that are present in the structure. Those data bases are not only used for storing keys but also for remembering the identity and the role of the machine where QCore is installed as well as the identity of all parties involved in the protocol of in the network.

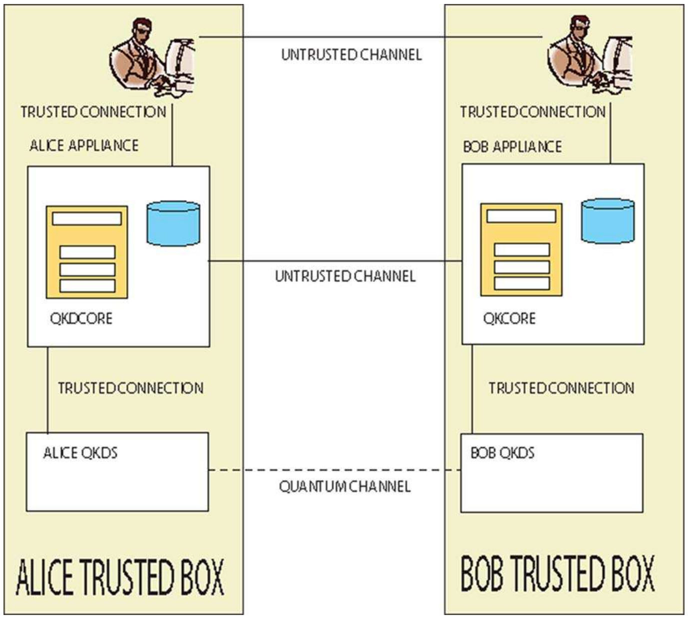


Figure 6.6: Connection for QCore. Alica and Bob have their secure boxes. Communications outside those boxes are unsecure.

Each databases is composed of three tables that we called: *main parameter*, *users* and *keys*. Remember that the database is identical for all of the parties involved in the communication, the only thing that changes is its content as we shall see with an example: the data base of Alice. The *main parameter* table contains information about the name of the machine, the role it has on the protocol i.e. server or client and the port it has to open for the communication through the untrusted channel in the case it is a server. The table and its content are described in Tab. 6.5.

Table 6.5: Structure of table *main parameter* on Alice side

Field	**Value**
whoami	Alice
myport	44400
whatami	Server

In this case Alice is a server and she will accept request connection on port 44400.

The *users* table is a list of all the other parties that are connected to Alice.

It comprises various parameters as Tab. 6.6 explains. In this case Alice has only a user she can communicate with. His name is Bob and in the case Alice wants to communicate with him, they have to use the B92 protocol. The ip address of Bob is clearly indicated as well as the port in which Bob will make his service request. The ipqkds address is the link with the physical layer: it is the address of the machine that manage the quantum communication. The *dirrem* and *dircoc* fields indicates where the files to be transferred are on the qkds and where they have to be stored in the appliance. Last the *dirlog* is the directory where all the log files are stored.

Table 6.6: Structure of table *main parameter* on Alice side

Field	**Value**
id	1
name	Bob
protocol	B92
ipaddress	192.168.1.171
port	44400
ipqkds	192.168.2.182
dirrem	/QKD
dirloc	/home/QCore/files
dirlog	/home/QCore/log
other	

The last database table is called *keys* and its fields are resumed in Tab. 6.7. In this table all the produced keys are stored with and id and the name of the owner. The reason for this choice will be clear in the following section. There is also a timestamp that identify each key, it can be used when there is a request of secure communication in order to verify the authenticity of a key. The keys inside the databases can be formatted in several ways according to the user preferences.

6.5.2 Few Networking Considerations

As you can see from the QCore structure, although the software has been used only for point to point communication there are many networking feature embedded in the code. We are now ready to describe some basic ideas of the QCore networking structure.

Definition 6.16 ***(QNode)*** *QNode is a macro block that includes the system*

Table 6.7: Structure of table *main parameter* on Alice side

Field	**Value**	**Value**
id	1	2
owner	Bob	Bob
timestamp	20070205 10:34:14	20070205 12:22:45
key	0100111....	1100110...

capable of performing the data and network layers of a QKD protocol (QCore system) and a the opto-electronic system for the physical layer (QKDS). We call the transmitting QKDS QTx, while QRx the receiving one.

The QNode can communicate with another QNode through a quantum channel and a public classical channel. Moreover, several QNodes can communicate each other creating a Quantum Key Distribution Network (QKDN).

We can represent a particular QNode with the Fig. 6.7. This node is formed by a central entity for the data and network layer, two physical transmitting layers (QTx) and a physical receiving QKD layer (QRx).

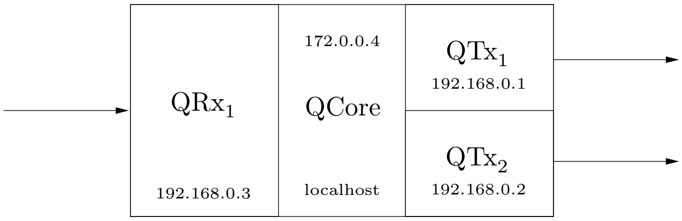


Figure 6.7: This is an example of a Qnode with two transmitter and one receiver. As QuAKE is designed to work in public internet, each QNode has internet protocol address represented in the upper area of the QCore sub-block, while in the bottom of each component there are the local IP address.

We decided to implement the Qnode architecture in an internet like manner. Every classical connection (trusted or untrusted) is implemented with SOCKETS in the TCP/IP protocol and each client and server in the QKD network it is characterized by its IP address inside different IP subnets. Those feature are clearly visible in the database that every QNode includes that are described in Sec. 6.5.1.

From a topological point of view we can see that a network of QKD protocols links can be any of the typical point to point topologies for subnets : star, rings, tree and so on [82]. One has to design the right topology looking to the particular needs of the area where the QKD network will be placed. For example in a metropolitan area network an irregular net will be probably implement, in the case of a single very elevated point of this network, it is possible to implement a centered star QKD network where a bigger transmitter machine will serve different leaves with the relative transmitter.

From a network security point of view it is mandatory for the QNode itself to be secure. For this reason the local connections between the center computation unit and the server and clients of a QNODE will be automatically secure.

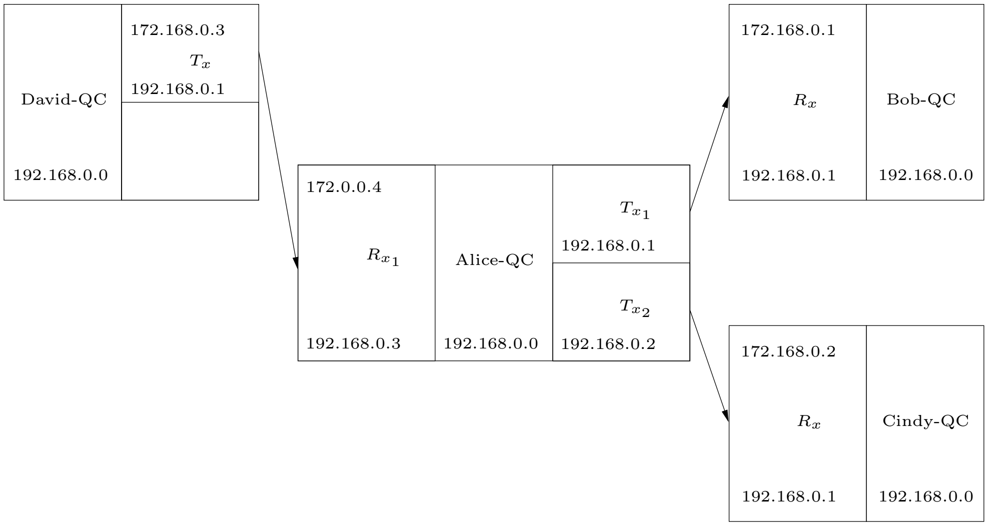


Figure 6.8: This is an example of QKD network. Here David is a sever, Alice is both a server and a client whereas Bob and Cindy are client. The internal structure i.e. QCore is the same for all QNodes.

Whereas QCore has been tested and used only for point to point communication it is evident now that data base structure is perfect if inserted in a networking picture. A single appliance can act as a server and as a client at the same time. Then in its *main parameter* table there will be two entries: one that says *{Alice,* 44400*, server}* and one that says *{Alice, - ,client}*. In this way Alice would open a connection on the port 44400 and wait for some request but she can ask for a connection too. Her *user* table will have entries that are both servers and clients.

You can clearly see how the software has been thought. It does not matter if a QNode is a client or a server, if it has one or ten QKDS, the software QCore is the same for all situation. This seemed to us the best way to build a ready to use versatile software.

6.5.3 ECA and PA Implementation

We implemented the error correction and the privacy amplification taking into account the study described in Sec. 6.2 and 6.4. For ECA the only problem that we faced was the IP connection optimization. At each parity check a bit is transmitted from Alice to Bob or viceversa. It is clear then that is a IP packet is created every time a single bit is transmitted the speed of the algorithm is very degraded because of the overhead that each packet needs. We decided to implement ECA in a parallel fashion using only pointers keep track of the position in the key for the whole binary procedure. In this way all the blocks in which an error is present are processed at the same time and the IP packet contains the parity check for all of them. This speeds up the algorithm because of a better use of the public channel. A sketch of this implementation is depicted in Fig. 6.9.

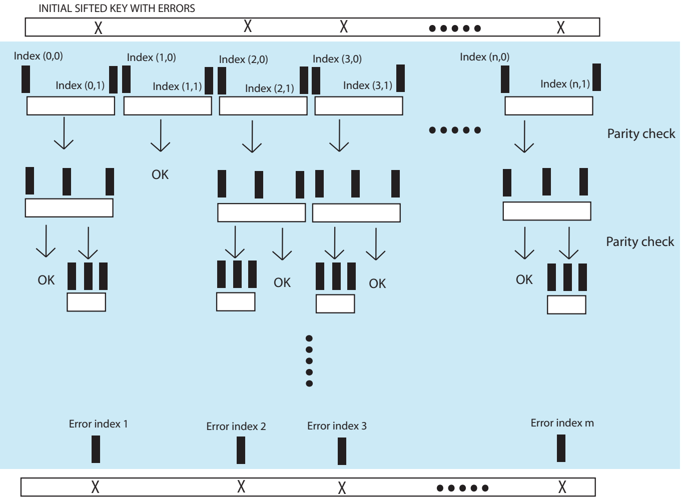


Figure 6.9: Parallel fashion of the QCore implementation of ECA. The algorithm keep track of the position in the blocks using pointers and all blocks are processed at the same time.

The main problem of a practical realization of the privacy amplification is the optimization of the multiplication by a matrix. This is hardly dependent on the length of the key and therefore on the size of the toeplitz matrix. A good way to reduce the time needed to complete this operation is to use the largest matrix as possible so then Alice and Bob can use the public channel in a efficient way to share the matrix and in the same time use subblock multiplication. With an n bits reconciled key and s as security parameter (s includes the bit revealed during Error Correction) the secret key will result of

$n_s = n - s$ bits. We would need a $n \times n_s$ Toeplitz matrix. We need to transmit $n + n_s - 1$ bits in order to share the matrix and more or less $n \times n_s$ operations to do the multiplication as we can see in the following equation:

$$\begin{bmatrix} k_S^1 \\ k_S^2 \\ k_S^3 \\ . \\ . \\ k_S^{n_s} \end{bmatrix} = \begin{bmatrix} t_{1,1} & t_{1,2} & . & . & t_{1,n_s} \\ t_{2,1} & t_{2,2} & . & . & t_{2,n_s} \\ . & & & & \\ . & & & & \\ t_{n,1} & t_{1,2} & . & . & t_{n,n_s} \end{bmatrix} \begin{bmatrix} k^1 \\ k^2 \\ k^3 \\ . \\ . \\ k^n \end{bmatrix} \tag{6.37}$$

where clearly $t_{i,j}$ obey the symmetries of toeplitz matrices $t_{i,j} = t_{i+1,j+1}$ for all i, j. If we use instead subblocks of length $l \times l(1 - s/n)$ with the same overall s parameter we would need the same bits to share the matrix but $l \times l(1 - s/n) \times l/n$ operation. The reduction in time goes as the square of the ratio $m = l/n$. The situation is represented in the following equation:

$$\begin{bmatrix} v_S^1 \\ v_S^2 \\ v_S^3 \\ . \\ . \\ v_S^m \end{bmatrix} = \begin{bmatrix} B_1 & 0 & . & . & 0 \\ 0 & B_2 & 0 & . & 0 \\ . & & & & \\ . & & & & \\ 0 & 0 & . & . & B_m \end{bmatrix} \begin{bmatrix} v^1 \\ v^2 \\ v^3 \\ . \\ . \\ v^m \end{bmatrix} \tag{6.38}$$

where if we call $l(1-s/n) = U$, $i = 0, 1, 2...U - 1$ and $j = 0, 1, 2...l - 1$ then $v_S^{i+1} = [f_S^{i+1}, f_S^{i+1}, ..., f_S^{i+U}]$ and $v^{i+1} = [k^{j+1}, k^{j+2}, ..., k^{j+l}]$. $B_w, w = 1..m$ are Toeplitz matrices of size $l \times l(1 - s/n)$.

Notice that the final key obtained in this way $f^1...f^{n_s}$ is different from the key that we would have distilled with a standard multiplication although the initial key $k^1...k^n$ is the same. It is clear that dividing the key and the matrix in this way the single block does not depend anymore on the whole reconciled key but just on one single block of it. This does not compromise the security and aim of privacy amplification, everything is like we were using smallest initial reconciled keys. Another difference with respect to the standard implementation is that in order then to check the correlation of their secret keys we have to check it for each subblock. That is why we cannot reduce the length of the blocks under a certain level. Nevertheless we can recover part of the secret key because we can eliminate only the blocks where there is no correlation. If we use the whole size matrix this is not possible because even one error after the ECA lead to two completely incorrelated keys. We call this *Recovery Mode* and it can be set ON or OFF depending on the length of the key and on the qber.

6.5.4 Test Bench Setup for QCore

When we realized QCore we did not have all the other subsystems of QuAKE to test the software and so we used a test bench setup simulating the quantum transmission with the matlab simulator described in Sec. 2.1. The setup is composed by one commercial router, in order to create two IP subnets (100 Mbit/s networks). The first trusted subnet is used for the administration of the overall experiment whereas all the traffic generated in the process of sifting, error correction and privacy amplification is handled by the second untrusted subnet. Our JAVA software runs on two dedicated computers, namely Alice and Bob appliances, connected to the two subnets. The appliances are two identical machines equipped with two low power embedded motherboard and produced by VIA Technologies Inc. In each appliance, equipped with a firewall distribution of Linux operative system, two ethernet ports has been used in order to separate the trusted TCP/IP traffic from the untrusted one. As our software has been developed as a JAVA language web application, the appliances has been equipped with a widely used world wide web server, APACHE and an open source JAVA application container, TOMCAT. A picture of the two appliances is depicted in Fig. 6.10.

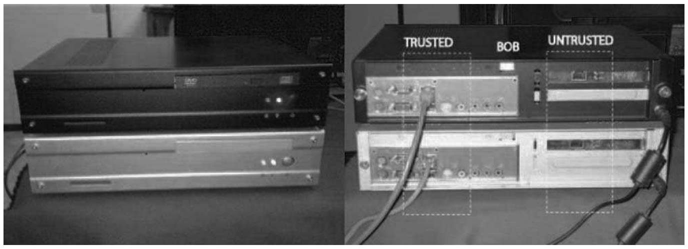
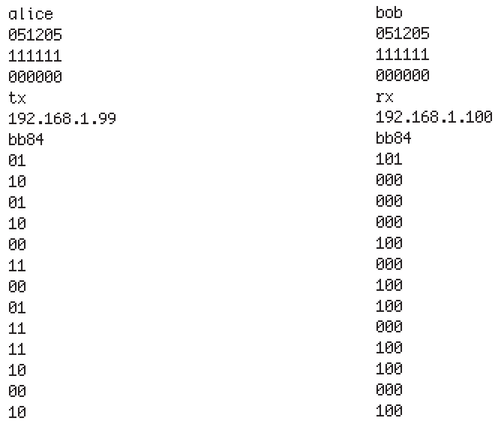


Figure 6.10: The two computers on which QCore is running. The two different subnets are highlighted.

The databases have been realized using MySQL and installed in the same machines. The files to be processed have been created by the MATLAB simulator in order to manipulate various parameter and then loaded into the Alice and Bob machines. In Fig. 6.11 an example of files containing the raw material coming from the physical layer is represented. The protocol in this case is the BB84 protocol, and after a series of control words the data are stored in a column like fashion. At Alice side the bit and the base in which it is encoded are saved whereas at Bob side the first bit represent the base chosen for the measurement, the second and the third the value of the measurement of the detectors. 1 means that a photon was revealed, 0 means no detection took place. There are rows i.e. measurement in which no detector clicked, this can be caused by the intrinsic non ideality of the source, absorption, quantum efficiency.



```
alice                                bob
051205                               051205
111111                               111111
000000                               000000
tx                                   rx
192.168.1.99                         192.168.1.100
bb84                                 bb84
01                                   101
10                                   000
01                                   000
10                                   000
00                                   100
11                                   000
00                                   100
01                                   100
11                                   000
11                                   100
10                                   100
00                                   000
10                                   100
```

Figure 6.11: An example of files containing the raw data of Alice and Bob.

The test has been run simulating a free space communication over $20Km$ and every parameter setup has been averaged over 20 simulated communication runs.

6.5.5 Results

A first investigation of the time needed to complete the various operation has been performed and the result is depicted in Fig. 6.12. The time required to complete the protocol is hardly dependent from the time taken in reading the local files and store them in RAM. The *Protocol time* i.e. the time for sifting, error correction and privacy amplification is much less then the former for every length of the initial set of data. This suggests that a further improvement would be to do the local loading and the processing phase in parallel.

Depending on the various processing times involved, there is indeed a preferred initial file length. In our case you can see from Fig. 6.13 that the average final key size is linear with respect to the number of sent qubits whereas the rate has a maximum at about 45000 (the rate considered is the algorithm key processing rate that well approximates the total QKD key generation rate). This suggests that, once installed in a specific environment and situation, for any QKD system there is a preferred number of qubit to be sent from Alice that maximize the key rate or, putting it in another way, for every environmental situation there is a preferred tuning of the high level software.

Another test has been to provide to the system hardly corrupted initial files with $ber > 5\%$ and see the the differences between various method of

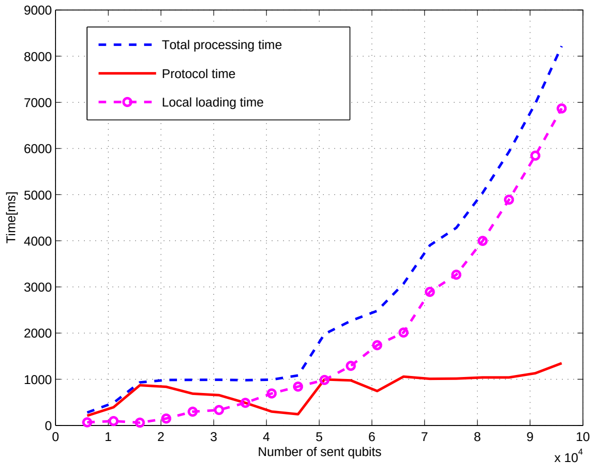


Figure 6.12: Timing of the various processes over the initial length of the set of qubits sent by Alice.

optimization. The results are resumed in Table 6.8. Particularly interesting are the third (without Recovery Mode and simply increasing the number of iterations of cascade) and last two rows (Recovery Mode). In the second case both time of execution and final key size are better than in the first case leading a better key rate.

Table 6.8: Test of Recovery Mode. BE: percentage of bits of the sifted key used for error correction. CC: cascade cycles. SBS: subblocks size (n=full length). t_e: time of execution of the overall algorithm. F_K : final key size.

BE	CC	SBS	t_e [ms]	F_K Size	Key Rate
3%	3	n	6382.6	348 bit	54.5 bit/s
1%	3	n	6682.9	786 bit	117.6 bit/s
1%	4	n	6409.3	1330 bit	207.5 bit/s
1%	3	200	5989.8	1367 bit	228.1 bit/s
1%	3	100	5982.5	1543 bit	257.9 bit/s

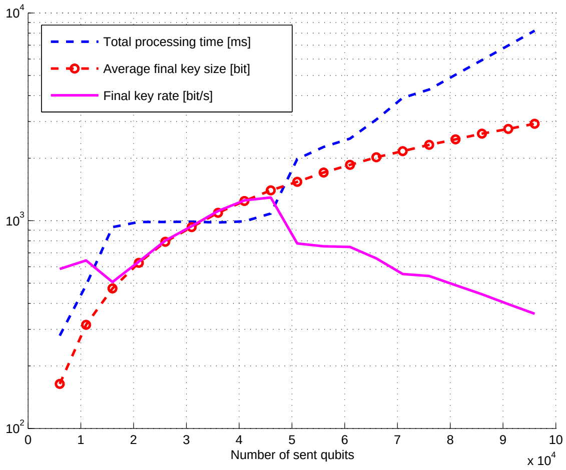


Figure 6.13: Final key rate over initial set length.

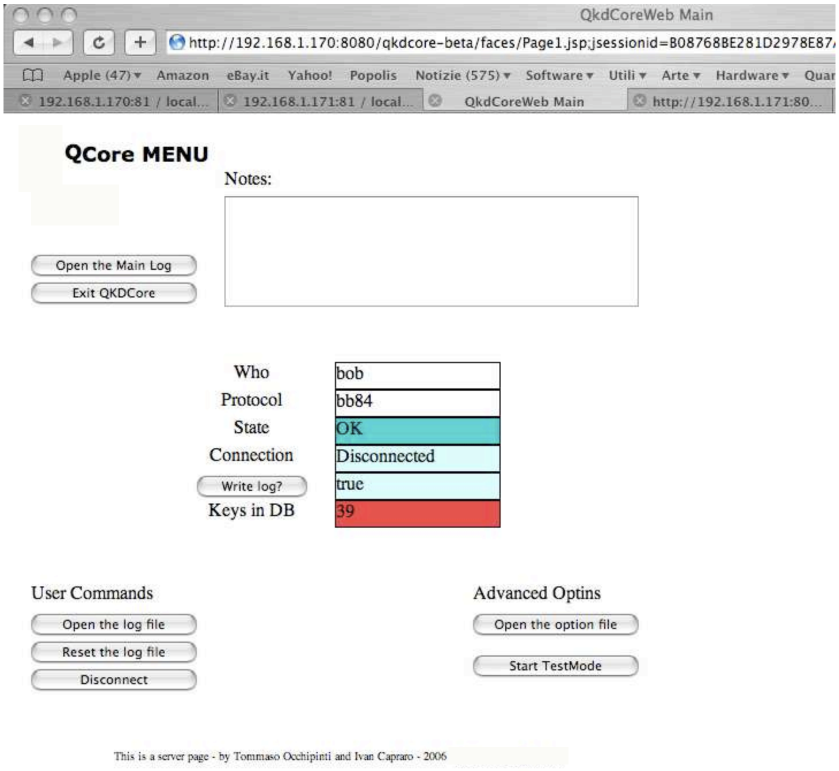
6.5.6 Web Interface of QCore

In order to manage the whole system we wrote a web interface using Java NetBeans that can be reached only from the trusted network. This is the usual way a system administrator accesses a networking unit. The interface support for the moment only a point to point communication. After a first login windows where the administrator is asked for a password, the software itself read from the database what is its role in the communications. If it is a server it runs the control window of Fig. 6.14.

The windows is composed by various parts with different options commands that permits to read a main and a user log file or to change the option for the communication with the user. In the central part an overview of the situation is represented. The *state* field indicates if everything is going well or not. If a problem occurs either a lost of connection or the presence of Eve the *state* flag change. The Bob control window is represented in Fig. 6.15.

This windows is simpler that Alice's one because we used the policy that is the server that manage the protocol. On the client side although it is possible to read the log files and changing the options. It is only a matter of convenience to add in these windows other indicators such as keyrate monitor, graphs of key production and whatsoever.

The options that can be changed are contained for the moment in a file and are: (i) the percentage of bits to be used for error estimation, (ii) threshold of



Notes:

Who	bob
Protocol	bb84
State	OK
Connection	Disconnected
Write log?	true
Keys in DB	39

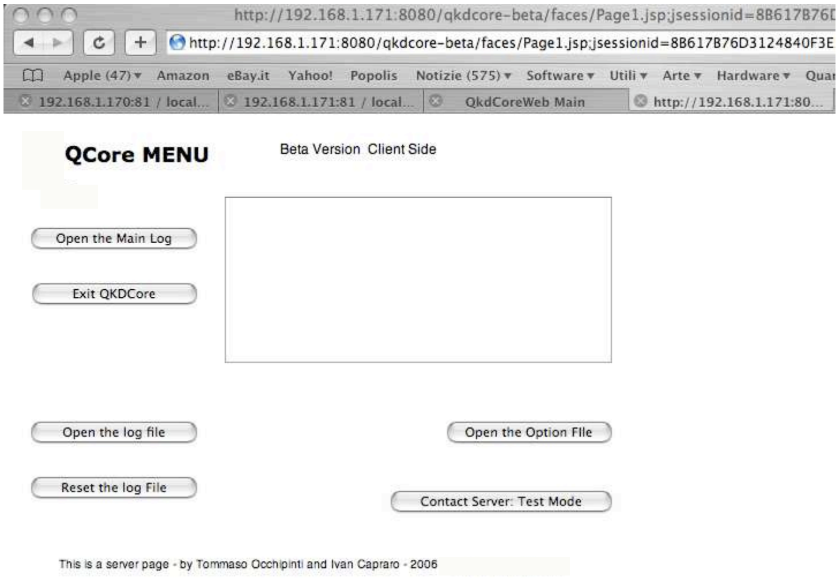
This is a server page - by Tommaso Occhipinti and Ivan Capraro - 2006

Figure 6.14: Alice main control window.

BER after which the modified version of Cascade is used (see Sec. 6.2), (iii) number of cycles of Cascade, (iv) recovery mode status (on or off), (v) length of the subblocks in the Toeplitz matrix for PA (see Sec. 6.4), (vi) number of bits for final correlation check (see Sec. 6.4). The security parameter of privacy amplification is automatically set by the error correction algorithm.

The log structure is very simple: there are two separated log files, the *main log* and the *user log*. The main log is used to track the history of the whole machine. You can find there information about the server, the connections and disconnections , about how many files have been elaborated. The main log cannot been reset nor cancelled by any user. Only who installed the system has access to the main log even though everyone can read its content. An example of main log is visible in Fig.6.16.

The user log, represented in Fig. 6.17, is much more interesting in terms of information content.


http://192.168.1.171:8080/qkdcore-beta/faces/Page1.jsp;jsessionid=8B617B76D
http://192.168.1.171:8080/qkdcore-beta/faces/Page1.jsp;jsessionid=8B617B76D3124840F3E
Apple (47) ▾
Amazon
eBay.it
Yahoo!
Popolis
Notizie (575) ▾
Software ▾
Utili ▾
Arte ▾
Hardware ▾
Quar
192.168.1.170:81 / local...
192.168.1.171:81 / local...
QkdCoreWeb Main
http://192.168.1.171:80...
QCore MENU
Beta Version Client Side
Open the Main Log
Exit QKDCore
Open the log file
Reset the log File
Open the Option File
Contact Server: Test Mode

This is a server page - by Tommaso Occhipinti and Ivan Capraro - 2006

Figure 6.15: Bob main control window.

Starting from the beginning on top we can see information about the loading of the file from the QKDS into the machine on which QCore is installed, information about the sifting operations, the error correction and the privacy amplification phases. After that a resume string is present (and highlighted in Fig. 6.17) with the following informations in it:

- **/home/qkdcore/...**

  this is the identifier of the file that has been elaborated by the system and so the file to which the resume is referred.

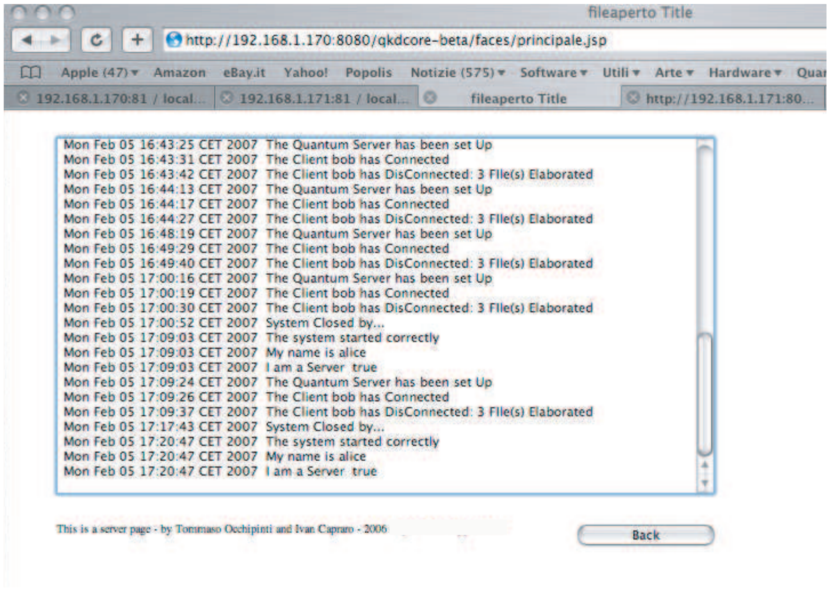
- **time:3590**

  this indicates the time in milliseconds that took the elaboration from loading to storing into database for the specified file.

- **IS=81000**

  this is the initial size of the Alice file. It represent in other words the number of laser pulses that Alice created and stored information for.

- **Do=14**


fileaperto Title
http://192.168.1.170:8080/qkdcore-beta/faces/principale.jsp
Apple (47) Amazon eBay.it Yahoo! Popolis Notizie (575) Software Utili Arte Hardware Quai
192.168.1.170:81 / local...
192.168.1.171:81 / local...
fileaperto Title
http://192.168.1.171:80...
Back

```
Mon Feb 05 16:43:25 CET 2007  The Quantum Server has been set Up
Mon Feb 05 16:43:31 CET 2007  The Client bob has Connected
Mon Feb 05 16:43:42 CET 2007  The Client bob has DisConnected: 3 FIle(s) Elaborated
Mon Feb 05 16:44:13 CET 2007  The Quantum Server has been set Up
Mon Feb 05 16:44:17 CET 2007  The Client bob has Connected
Mon Feb 05 16:44:27 CET 2007  The Client bob has DisConnected: 3 FIle(s) Elaborated
Mon Feb 05 16:48:19 CET 2007  The Quantum Server has been set Up
Mon Feb 05 16:49:29 CET 2007  The Client bob has Connected
Mon Feb 05 16:49:40 CET 2007  The Client bob has DisConnected: 3 FIle(s) Elaborated
Mon Feb 05 17:00:16 CET 2007  The Quantum Server has been set Up
Mon Feb 05 17:00:19 CET 2007  The Client bob has Connected
Mon Feb 05 17:00:30 CET 2007  The Client bob has DisConnected: 3 FIle(s) Elaborated
Mon Feb 05 17:00:52 CET 2007  System Closed by...
Mon Feb 05 17:09:03 CET 2007  The system started correctly
Mon Feb 05 17:09:03 CET 2007  My name is alice
Mon Feb 05 17:09:03 CET 2007  I am a Server  true
Mon Feb 05 17:09:24 CET 2007  The Quantum Server has been set Up
Mon Feb 05 17:09:26 CET 2007  The Client bob has Connected
Mon Feb 05 17:09:37 CET 2007  The Client bob has DisConnected: 3 FIle(s) Elaborated
Mon Feb 05 17:17:43 CET 2007  System Closed by...
Mon Feb 05 17:20:47 CET 2007  The system started correctly
Mon Feb 05 17:20:47 CET 2007  My name is alice
Mon Feb 05 17:20:47 CET 2007  I am a Server  true
```

This is a server page - by Tommaso Occhipinti and Ivan Capraro - 2006

Figure 6.16: An example of the main log at Alice Side.

these are the pulses for which we had a click on both detector meaning that either the pulses contained more than one photon or a noise click occurred in a detector exactly at the same time the other one was detecting the right photon. This may not be due to the detectors only but also to an highly noisy background for example during daylight transmission.

- **Em=80128**

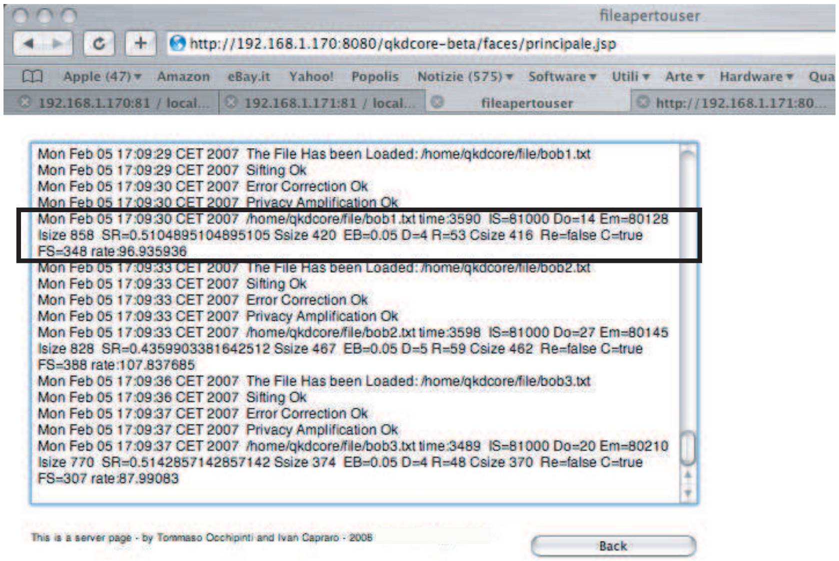
  this is the number of empty slots. Notice that almost all the pulses that Alice sent are empty. The reason is that we are generating single photon attenuating a laser and we would like to minimize the pulses with more that one photon and as the photon distribution i poissonian this lead to a high probability to have an empty pulse (See Sec. 3.1.1).

- **Isize=858**

  this is the initial key length i.e. the length of the raw key that has to be elaborated by the system.

- **SR=0.51...**

  this is the sifting ratio: it should be close to $SR = 0.5$ if the system



fileapertouser
http://192.168.1.170:8080/qkdcore-beta/faces/principale.jsp
Apple (47) Amazon eBay.it Yahoo! Popolis Notizie (575) Software Utili Arte Hardware Qua
192.168.1.170:81 / local... 192.168.1.171:81 / local... fileapertouser http://192.168.1.171:80...

```
Mon Feb 05 17:09:29 CET 2007  The File Has been Loaded: /home/qkdcore/file/bob1.txt
Mon Feb 05 17:09:29 CET 2007  Sifting Ok
Mon Feb 05 17:09:30 CET 2007  Error Correction Ok
Mon Feb 05 17:09:30 CET 2007  Privacy Amplification Ok
Mon Feb 05 17:09:30 CET 2007  /home/qkdcore/file/bob1.txt time:3590  IS=81000 Do=14 Em=80128
Isize 858  SR=0.5104895104895105 Ssize 420  EB=0.05 D=4 R=53 Csize 416  Re=false C=true
FS=348 rate:96.935936
Mon Feb 05 17:09:33 CET 2007  The File Has been Loaded: /home/qkdcore/file/bob2.txt
Mon Feb 05 17:09:33 CET 2007  Sifting Ok
Mon Feb 05 17:09:33 CET 2007  Error Correction Ok
Mon Feb 05 17:09:33 CET 2007  Privacy Amplification Ok
Mon Feb 05 17:09:33 CET 2007  /home/qkdcore/file/bob2.txt time:3598  IS=81000 Do=27 Em=80145
Isize 828  SR=0.4359903381642512 Ssize 467  EB=0.05 D=5 R=59 Csize 462  Re=false C=true
FS=388 rate:107.837685
Mon Feb 05 17:09:36 CET 2007  The File Has been Loaded: /home/qkdcore/file/bob3.txt
Mon Feb 05 17:09:36 CET 2007  Sifting Ok
Mon Feb 05 17:09:37 CET 2007  Error Correction Ok
Mon Feb 05 17:09:37 CET 2007  Privacy Amplification Ok
Mon Feb 05 17:09:37 CET 2007  /home/qkdcore/file/bob3.txt time:3489  IS=81000 Do=20 Em=80210
Isize 770  SR=0.5142857142857142 Ssize 374  EB=0.05 D=4 R=48 Csize 370  Re=false C=true
FS=307 rate:87.99083
```

This is a server page - by Tommaso Occhipinti and Ivan Capraro - 2006

Figure 6.17: An example of the user log at Alice Side.

is working properly. If not some polarization misalignment is present or maybe Eve herself is acting on the polarization so disturbing the protocol.

- **Ssize=420**

  this is the size of the sifted key. It is more or less one half of the raw key.

- **EB=0.05**

  this is the estimation of the BER done by the ECA. Notice in this case an estimation of 5%. This is surely due to the fact that the real error rate is very slow and so the error correction algorithm try to overestimate the BER in order to choose in a better way its parameters (see Sec. 6.2).

- **D=4**

  during the process of error correction a number of bits are deleted. These bits are errors on the sifted key. In this case four errors where found by the algorithm.

- **R=53**

  this is the number of parity check that Alice and Bob transmitted each other in order to individuate the errors. Those bits have to be deleted as well because they are read by Eve during the error correction procedure on the public untrusted channel.

- **Csize=416**

  this is the size of the reconciled (corrected) key. Notice that only the 4 bits deleted by the error correction are missing. The privacy amplification will take care of those bits.

- **Re=false**

  this indicates whether or not the Recovery mode described in Sec. 6.5.3 is switched on or off.

- **C=true**

  this indicates the result of a final correlation test that Alice and Bob do on the keys after the privacy amplification. Remember that if there is at least one residual error on the final keys the probability that they will be uncorrelated is very close to one. Alice and Bob can then use few bits to check this correlation. These bits have clearly to be deleted from the key (see Sec. 6.5.3).

- **FS=348**

  this is the final secure key length.

- **rate=96.9...**

  this is the rate of key creation for the elaborated file in bit per second.

It has to be said that the operation of taking away the double and empty slots from the raw material should be done by the electronics in the physical layer. The obvious reason being that the transfer rate of raw material between the QKDS and QCore will be much higher.

Chapter 7

Temporal Filtering for Quantum Astronomy

In this final chapter i will briefly describe another application i have been involved and for which filtering is very important, in particular time filtering. In the last year i have been working in fact also on the design of the timing system for an astronomic instruments, called AquEYE. After a short and certainly not complete introduction to subject (for a complete description see [28]) i will give some details, simulation results and characterization of the system focusing in particular to the timing unit ATFU (AquEYE Time and Frequency Unit).

7.1 AquEYE, Towards Quantum Astronomy

Two years ago, together with the University of Lund, a proposal for one of the instrument to incorporate into OWL (OverWelmingly Large Telescope) has been submitted to the European Space Agency (ESA). This proposal has been accepted meanwhile OWL size has been reduced from the original 100m primary mirror to the actual 40m. What our group leaded by prof. Cesare Barbieri of the department of Astronomy of the university of Padua, proposed, was an instrument that could go well beyond the milli and micro second scale of actual astronomic devices. The instrument was called QuantEYE.

Numerous discoveries were made with temporal resolutions of milliseconds and slower: optical and X-ray pulsars; planetary occultations; cataclysmic variable stars; pulsating white dwarfs; flickering high-luminosity stars; X-ray binaries; gamma-ray burst afterglows, and so on. A limit for such optical studies has been that conventional CCD-like detectors do not readily permit frame-rates faster than 1-10 ms, while photon counting detectors either had low quantum efficiency or else photon-count rates limited to no more than some hundreds of KHz. Nanosecond time resolution and time tagging capability would enable entirely new studies of phenomena such as: variability close to black holes; surface convection on white dwarfs; non-radial oscillation spectra in neutron stars; fine structure on neutron star surfaces; photon-gas bubbles in accretion flows; possible free-electron lasers in the magnetic fields around magnetars [19]. Besides such applications in high-speed astrophysics, the final aim is to reach timescales sufficiently short to reveal the quantum-optical statistics of photon arrival times. Higher-order coherences of light may in principle convey information about the physics of light emission (e.g., stimulated emission as in a laser) or propagation (e.g., whether photons reach us directly from the source, or have undergone scattering on their way). Such properties of light have been studied for quite some time in the laboratory, but have not yet been applied to astrophysics.

The original design comprised an array of 10 by 10 single photon detector, each coupled to a subpupil of the telescope. The high number of SPADs allow a higher incoming rate to be observed. Calculations proved that a rate of 1GHz can be obtained with this number of detectors. The pulses coming from the SPADs will be then time tagged by a fast electronic TDC (time to digital converter) and then passed through an optical fiber to an elaboration unit. The proposal with the description and of the theoretical bases of the instruments can be found in the original document proposed to ESA and other related works [19, 18, 28].

We now concentrate on a prototype of QuantEYE that we are building at the Asiago Observatory in Italy. We have called this prototype AquEYE (Asiago quantum eye) and it would be a smaller version of QuantEYE. This prototype is working as a testbench and guide for the realization of a bigger and more performing instrument.

7.1.1 Brief Description of the Instrument: Optics

AquEYE has been designed for Asiago-Cima Ekar 182 cm telescope, you can see a picture of the telescope in Fig. 7.1.

The simplest way of realizing this small prototype is to reduce the number of SPADs involved. In the case of AquEYE we decided to divide the telescope pupil in four parts instead of the original 100. This can be easily obtained mounting a simple pyramidal mirror at the back of AFOSC (Asiago Faint Object Spectrograph and Camera), an instruments that was already available at the telescope used in this case as focal reducer. The beams reflected by the pyramid are independently sent along four perpendicular directions, and each of them can be imaged on a SPAD through a train of four commercial doublets (see Fig. 7.2). The target object is selected by means of a pin hole at the focal

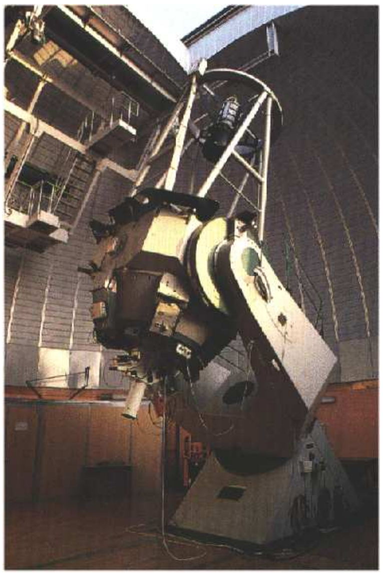


Figure 7.1: The Cima Ekar 182 cm telescope in Asiago, Italy.

plane of the telescope.

Just to give some specifications, the Asiago telescope focal length is only 16.1 m, and a 3 arcsec extended source (the average size of a point-like star, due to the limited seeing) gives a spot size at the telescope focus of about 0.23 mm. In addition, AFOSC introduces an almost 1/2 demagnification factor, bringing the size of the spot at the AFOSC output at about 130 μm. So, the lens train after the pyramid has to further demagnify the spot of only a factor 1/4 to have a final spot size of the order of 40 μm: it is because of this rather relaxed specification that it has been possible to design the system with only commercial lenses.

As in QuantEYE, the system losses are negligible, and essentially limited at the edges of the pyramid, were the radiation beam is splitted. As detectors, we have selected and acquired the 50 μm SPADs produced by the MPD (Micro Photon Devices, Bolzano, Italy) company, the same used for QuAKE (see sec. B.0.1). The optical performance of the designed system, obtained by a ZEMAX simulation, is excellent over the 50 μm size active area, from the blue (420 nm) to the red (720 nm) and it is capable of focusing more than 90% of the incoming flux on the detector active area as shown in Fig. 7.3.

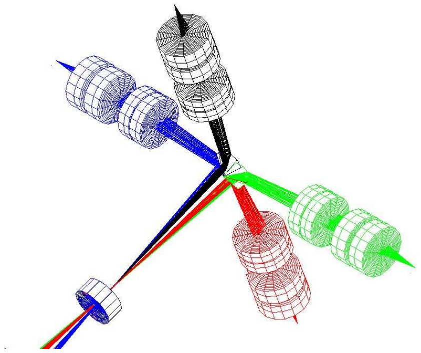


Figure 7.2: Following the last lens of AFOSC shown at the left, a pyramid splits the light to four separate channels to the SPADs.

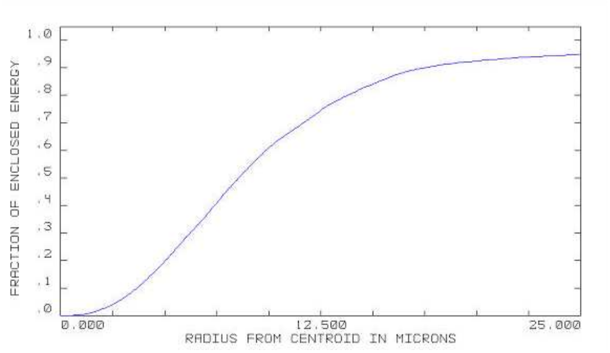


Figure 7.3: Extended source encircled energy plot: percentage of energy falling within a circle of given radius for a uniformly illuminated 3 arcsec extended circular source. The 25 μm limit corresponds to the SPAD sensitive area.

7.1.2 Brief Description of the Instrument: Electronics

The electronics scheme, based on available commercial products, is shown in Fig. 7.4. The core of the electronics system is a CAEN (Costruzioni Apparecchiature Elettroniche Nucleari S.p.A.) TDC board.

This board, that has eight input channel, will take the TTL inputs coming from the four SPADs and will process the signals. Each time tag is buffered inside the board and then put into a standard VME bus. The TDC will be able to tag each event with a time precision of 25 ps per channel in the sense that the local oscillator has a nominal frequency that allow this kind of sampling precision. As the electronics system will be attached to the telescope, the CAEN board will transfer all the data time tags to an external personal

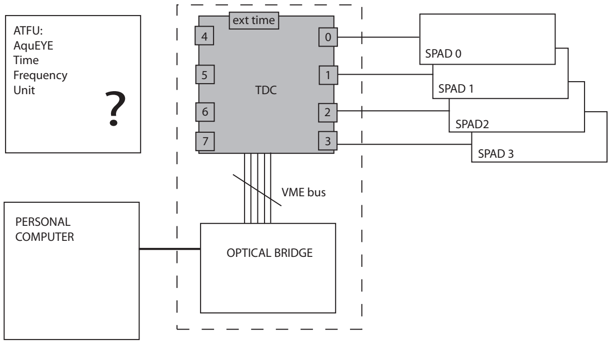


Figure 7.4: The overall electronics scheme of AquEYE, the ATFU: AquEYE Time and Frequency Unit is the object of this study.

computer able to save each tag to a mass storage. The external computer performs the aposteriori data analysis, saving the interesting scientific data.

In the scheme is present also the *ATFU* block that is meant to give a precise time reference to the system. This block that represent the main part of my contribution will be discussed in details in the following sections.

7.2 Timing System For Acqueye

Here a brief explanation of the timing performances needed in quantum astronomy is presented. To follow a description of the timing reference designed for AquEYE, called ATFU. The results of this study can be found on a work that we presented at the Thirty-Ninth Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting [61].

7.2.1 Temporal Requirements for Single and Multiple Telescope Operations

Quantum Astronomy needs to determine the arrival time of photons with a precision of 100 ps or better (the future target may be 1 ps) continuously for the entire duration of the observations, which can last from few seconds up to several hours. We would like AquEYE to provide the time tags of the photons coming from different astronomical sources with an error phase of about 100 ps over exposure times as long as 3 hours. This requirement needs to be transformed in terms of oscillator specifications. Given the simple relation between frequency offset f_0 and phase error δt , $f_0 = \delta t/T$, where T is the measurement time (that we assume being 3 hours), the frequency offset required to satisfy the constrains on phase error is $f_0 = 10^{-10}/10800 =$

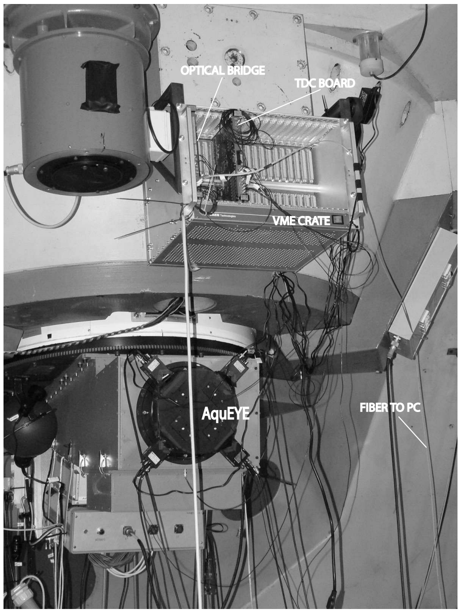


Figure 7.5: AquEYE mounted at the Asiago telescope. On the top the electronics with the TDC board and the optical bridge, on the bottom the instrument with the four SPADs.

9.26×10^{-15} for the $100ps$ requirement and $f_0 = 10^{-12}/10800 = 9,26 \times 10^{-17}$ for the 1ps requirement.

If, as in our case, a real time processing is not mandatory then the requirements about frequency offset are not critical because the frequency offset may be estimated and then removed in processing. Considering the minimum frequency stability required, i.e. the instantaneous deviation of the phase error from the phase offset, we may look at Fig. 7.6. The bold line is the upper limit for the requirements of 100 ps while the dotted one is the one for the requirements of 1 ps.

The second aim of AquEYE is to realize, a modern version of the Hanbury Brown-Twiss intensity interferometry, with a base line from Asiago to the Crni Vrh Astronomical Observatory of Ljubljana, at a distance of about 195 Km. In order to acquire good data for this particular form of Quantum Astronomy it is important to achieve a very good relative synchronization between the two locations of acquisition. The better this synchronization, the easier the task of correlating the data will be.

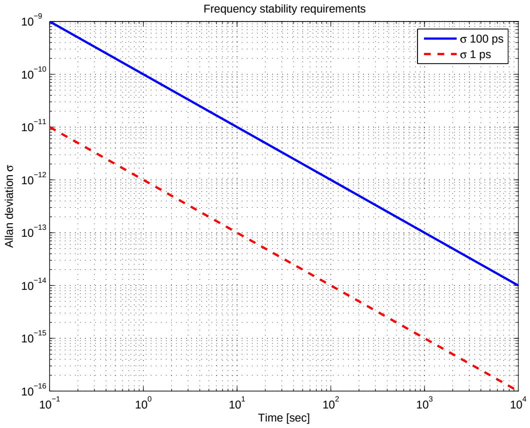


Figure 7.6: Oscillator frequency stability required for Quantum Astronomy. Acceptable values for 100 ps requirements lay below the bold line and for 1 ps lay below dotted line.

7.2.2 Proposed Solutions and Characterization

The frequency reference unit that we decided to adopt in Asiago is composed by a Rubidium oscillator and a GPS receiver. The local oscillator is a FS725 Rubidium frequency standard produced by Stanford Research Systems and the GPS receiver is the Mini-T produced by Trimble. The placing of the AquEYE units (acquisition electronics, time and frequency and control) inside the Asiago - Cima Ekar Observatory is show in Fig. 7.7 on the left, while on the right the possible positions of the GPS antenna now under investigation.

The Time and Frequency unit has been placed in the telescope basement because of worse environmental conditions in the dome, where humidity and temperature can exceed the specified values (the Observatory is at 1340 m altitude).

The Rubidium-based main clock (see Figure 6) has been chosen to provide to the whole AquEYE system a frequency and time reference. This Rubidium oscillator assures stable and reliable performance with an accuracy of $\pm 5 \times 10^{-11}$. Different outputs are provided by the instrument: 10 MHz and 5 MHz sinusoid waves and the PPS (Pulse Per Second) signal; moreover, it can be phase-locked to an external PPS signal (like for example, the reference provided by GPS allowing the synchronization with the Coordinated Universal Time (UTC)).

Considering that the astrophysical experiment will be performed also exploiting interferometric techniques a common synchronization is required be-

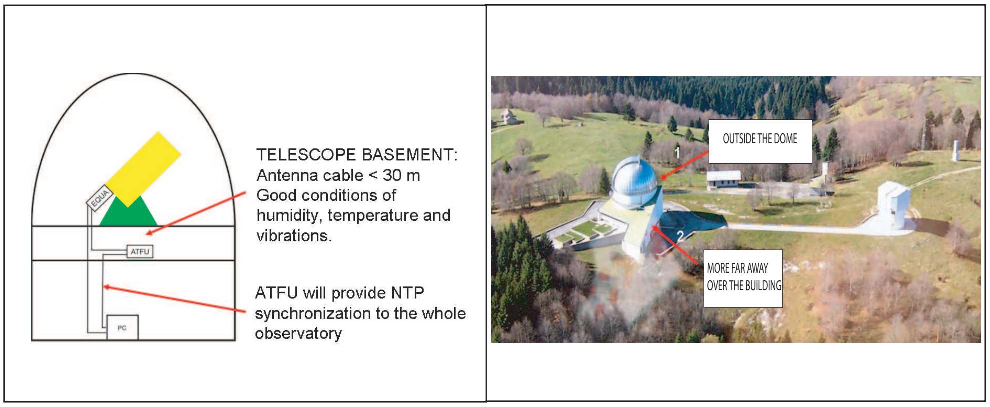


Figure 7.7: Disposition of AquEYE units at the Asiago AO of Cima Ekar (left) and positions of GPS antenna (right).

tween Asiago and a second telescope (Ljubljana). Therefore, together with the Rubidium oscillator, a GPS receiver has also been purchased to discipline the Rubidium to the UTC scale. It is well know that whereas the Rubidium in free-running shows a stable but not very accurate behaviour, with the GPS synchronization, it becomes more accurate but less stable; in this section, we will quantify this concepts through several measurements.

In order to measure the Rubidium performances, in terms of stability and accuracy, we used the "Time and Frequency Laboratory" of the Astronomical Observatory of Cagliari, Italy (see Fig. 7.8). This laboratory, equipped with advanced instrumentation, participates in the calculation of the international time scales by sending its clock data to the BIPM (Bureau International des Poids et Mesures).

It is worth noticing that in order to perform the calibration, the Device Under Test (DUT), in our case the Rubidium, must be compared to a standard that should outperform the DUT by a specified ratio in order for the calibration to be valid. This ratio is called the Test Uncertainty Ratio (TUR); if possible, a TUR of 10:1 is often a right choice. The Cagliari "Time and Frequency Laboratory" is equipped with two commercial caesium clocks (HP-5071A) that provide a practical realization of the second sufficiently accurate for our application. The time and frequency measurements required for the Rubidium characterization have been performed by the Time Interval and Frequency Counter SR620 of the Stanford Research System (hereafter abbreviated to TIC). Briefly, the main performances of the instrument are the single-shot timing resolution (25 ps) and its 1.3 GHz frequency range.

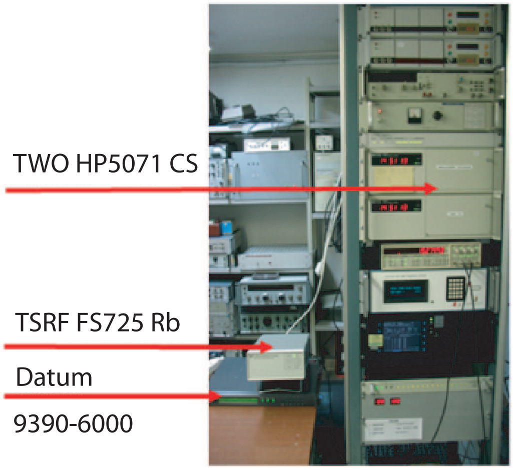


Figure 7.8: Time and Frequency Laboratory of the Astronomical Observatory of Cagliari. The arrows highlight from the top the two Caesium clocks, our Rubidium under test and GPS receiver available in Cagliari.

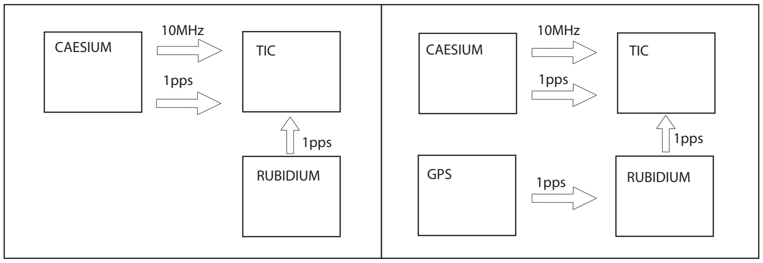


Figure 7.9: Two different measurement setups.

The first two set-up measurements are sketched in Fig. 7.9 ; on the left one can see the characterization of the Rubidium in free running configuration, whereas on the right the atomic clock is disciplined by the GPS. In both experiments, we adopted the Caesium clock for the 10 MHz reference; moreover, the measurements were performed by comparing the time interval between two pps signals: one provided by the Rubidium and the other by the caesium. Data are recorded with a step of 2 seconds. Since the astrophysical experiment should be about 3 hours long, the data acquisition has been performed for the same interval time. Therefore, each file contains about 5000 samples.

The interval delay between the two pps signals are read by the TIC and then, via RS232, sent to a dedicated computer for the data acquisition. After that, off-line, the commercial software Stable 32 has been used for data processing. During the post-processing phase, we are able to convert data from phase to frequency domain, to remove outliers, to plot graphs and to calculate basic and specialized statistics.

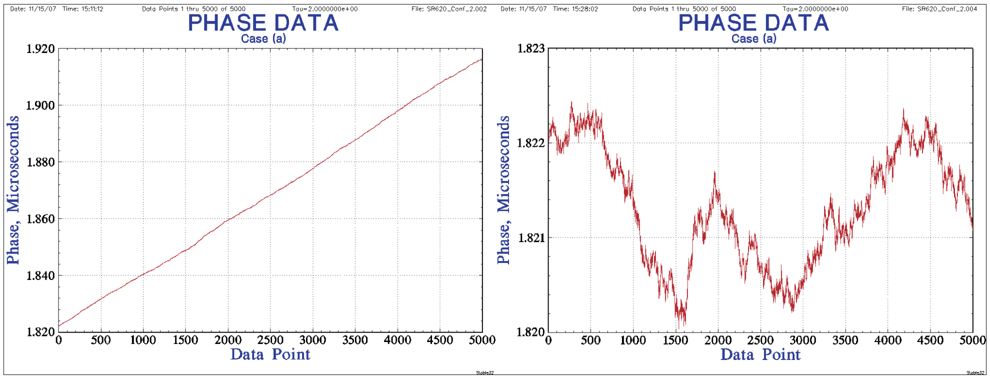


Figure 7.10: Three hours of phase data for the Rubidium in free-running (left) and the residual stochastic error phase after removing offset and drift frequency (right).

Fig. 7.10 shows the analysis of the configuration labelled with the rubidium in free run. For phase data we obtained a linear ramp with a slope of 2×10^{-11}, that also corresponds to the frequency offset. Therefore, the behavior of the rubidium is a bit better than the accuracy declared in the data-sheet. On the other hand, after 3 hours a total phase error of about 100 ns is seen. By removing such drift in the post-processing phase, the curve on the right of Fig. 7.10 obtained. At this stage, the maximum error accumulated during 3 hours is reduced to about 3 ns.

We have evaluated also the Allan deviation, which describes the noise affecting data. In Fig. 7.11 one can see this result, which agrees very well with those expected from the nominal data (see Tab. 7.1). The linear slope of the Allan deviation fits with the white frequency noise which is the most common noise for Rubidium standard in the short-time.

Integration time (sec.)	**From data sheet**	**Measured**
1	$< 2 \times 10^{-11}$	2×10^{-11} at 2 seconds
10	$< 1 \times 10^{-11}$	2×8^{-12}
100	$< 2 \times 10^{-12}$	2×1^{-12}

Table 7.1: Comparison for the Allan deviation between measured and declared values.

As second step, we performed the same analysis for the configuration on the

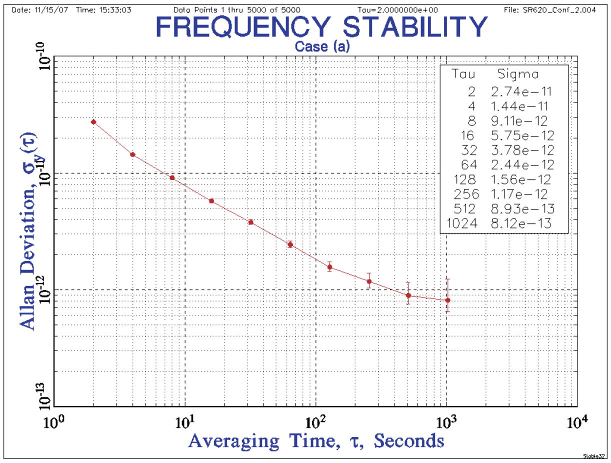


Figure 7.11: Allan deviation fro rubidium in free running.

right of Figure 7.9. This configuration, although reducing the frequency offset, has the drawback of introducing stochastic noise, because the GPS periodically corrects the Rubidium oscillation to keep it aligned as much as possible to the UTC scale.

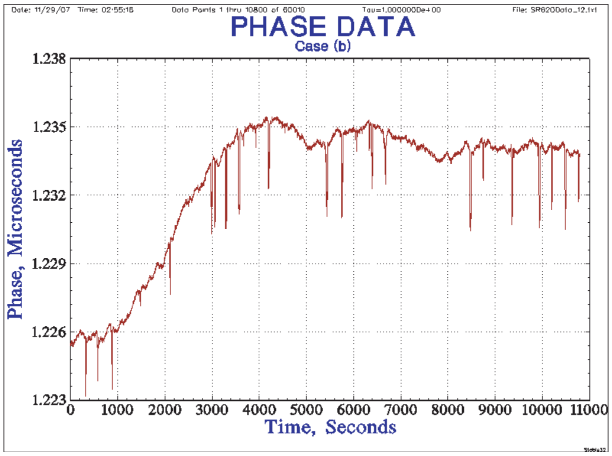


Figure 7.12: Three hours of phase data for the Rubidium disciplined by a GPS pps.

The benefit of this configuration (see Fig. 7.12) is that the maximum phase offset is limited, even for very long period. For example, in this case the total phase error is about 13 ns. On the other hand, the drawback is due to higher noise of GPS with respect to the Rubidium. We are currently investigating the peaks visible in Fig.7.12. They could be the effects of the phase-locking circuitry of our Rubidium and this seems to be a problem of our rubidium model. To overcome this problem another procedure can be adopted. It consists of estimating, with the aid of GPS, the Rubidium offset and drift, and correcting them in post-processing, instead of disciplining the Rubidium with the GPS directly. This configuration is useful also because the final setup of our experiment could not use a TIC instrument. Nevertheless we can take advantages from the precision of our scientific acquisition electronics based on a Time to Digital Converter (TDC, 25 ps resolution). The configuration for this purpose is shown in Fig. 7.13.

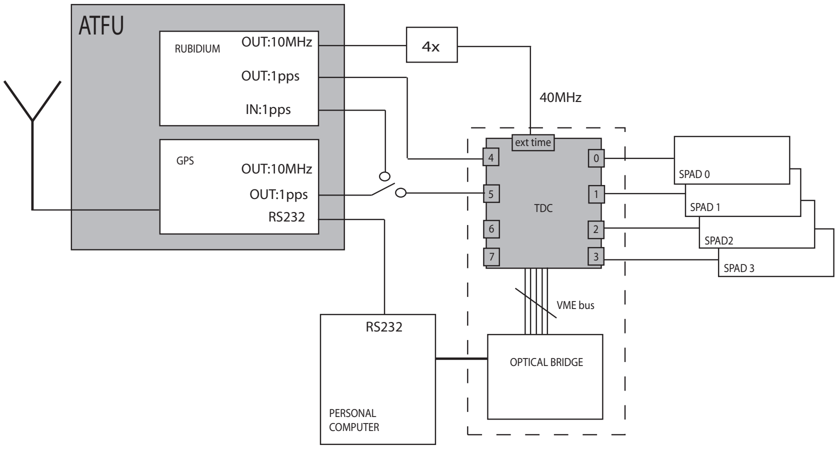


Figure 7.13: Connection of Acquisition Electronics, Time and Frequency unit (ATFU) and Control units.

The practical realization of this procedure may be affected by the fact that the reference frequency of the acquisition electronics is given by the Rubidium oscillator itself. In any case, this problem should affect only the stability of pps measurements, making the pps differences noisier, but the offset estimation should be sufficiently accurate.

In order to verify the feasibility of the above solution, a case test has been realized in the Cagliari laboratory. The 10 MHz from the Rubidium oscillator has been used as reference frequency to the TIC that in this case stands for the TDC, and we have acquired the phase differences between the pps in input from the Rubidium and the GPS. We call this configuration “Operational Configuration” and it is depicted in Fig. 7.14.

The results of TIC measurements are shown in Fig. 7.15. As expected, the data are very noisy, on the other hand the estimated frequency offset is 1.2232×10^{-11}, with a phase error of about 110 ns. This value is of the same

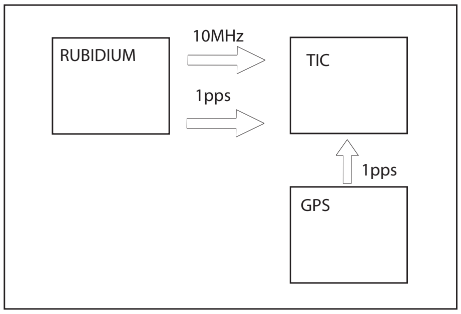


Figure 7.14: Operational configuration test setup.

order of the frequency offset determined with the frequency reference given by the Caesium oscillator, namely 2×10^{-11}.

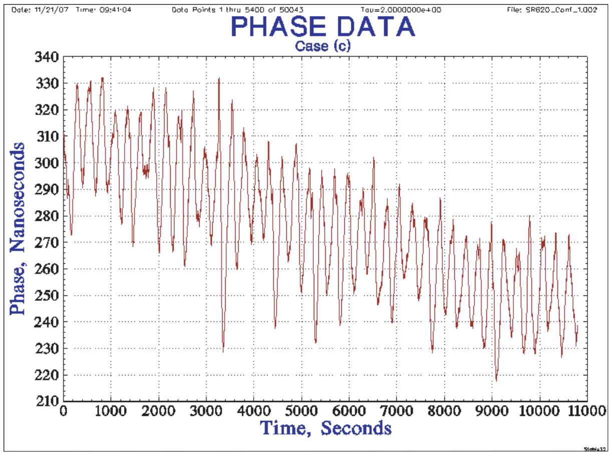


Figure 7.15: Phase data for the operational configuration.

7.2.3 Comments

Although a disciplined rubidium would probably be the preferred stand alone solution exploiting the fact that our system uses a TDC board we can think of different configurations. In particular we can use the rubidium in free running and benefit from its very good frequency stability, an use the GPS in order to correct from the accumulated error exploiting its good stability over long time. This is possible because our TDC board can act as a TIC and measure the difference between the pps coming from the rubidium and the GPS. With this method we expect to have a very good time reference for the future experiments. In the following sections an example of acquired data will be presented showing how a good time reference is mandatory for AquEYE and AquEYE-like systems.

7.3 First Results of AquEYE

As already described AquEYE is capable of resolving photons with a resolution down to 25ps. This resolution comes from the TDC board that uses a 40MHz clock input in order to generate a 40GHz waveform used to assign very precise time tags to the incoming photons. The 40MHz clock can be the quartz internal clock of the electronic board or it can be provided from other sources. As explained earlier the ATFU is the unit that we decided to build in order to give to the system a stable and accurate frequency reference. I want to present here some data that we acquired in Asiago on december 19th 2007. The ATFU unit was not present at that time, it will de tested during the next trials. It is very interesting although to notice how the instrument perform without the time and frequency unit, both to confirm the capabilities of AquEYE and to understand the utility of ATFU.

Among the others observed , the 16-th magnitude pulsar in the Crab Nebula is a very important object for AquEYE. The pulsar have in fact a very well known period that we may use to validate the measurements[1]. The pulsar, which has period is 33 ms that shifts +38 ns per year, has been studied by many astronomers: a short time scale analysis can be found in [44] whereas a long time repeated observation during years is described in [52]. The pulsar have been observed also by the Hubble Space Telescope [64]. A picture of the Crab nebula with the pulsar is depicted in Fig. 7.16.

During the observation of this object the overall mean photon rate we acquired with our instrument was about 4KHz with an $RMS = 140.7$ over 150 seconds. The rate is of course distributed among the four SPADs, in Fig. 7.17 one can see the rate relative to each of the four detectors.

With the type of data that AquEYE can store i.e. time tags of photons arrival times, many kind of different analysis are possible. In this case it is very useful to look at photometric data trying to find variations in the instantaneous intensity of the incoming flux. This is done by binning the photons time tags with a temporal window which has a value that in this case can be chosen arbitrarily since the instrument give us the photon time tags. Then, in order to find periodicities inside the data stream the autocorrelation

[1] Another very useful use of the Crab pulsar is the synchronization between Asiago and the Crni Vrh Astronomical Observatory of Ljubljana described in Sec. 7.2.1. This could be done exploiting the well known oscillation frequency.

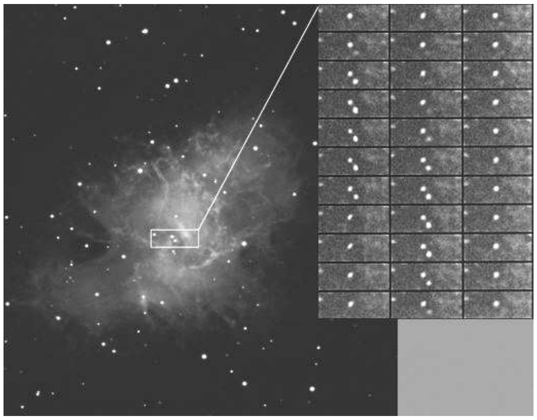


Figure 7.16: A N.A. Sharp/NOAO/AURA/NSF picture of the Crab nebula and its pulsar (*www.noao.edu*).

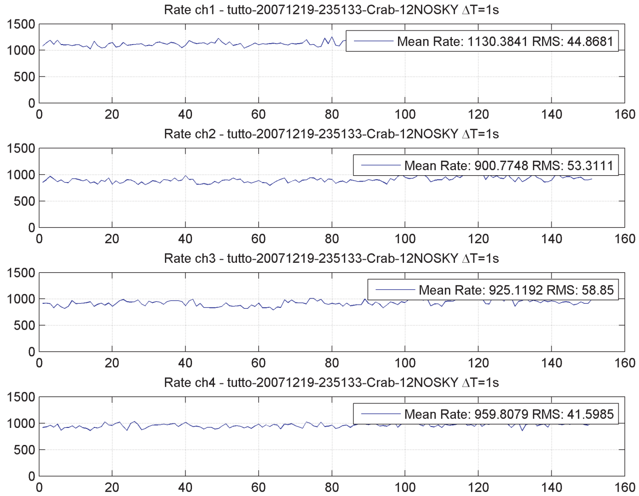


Figure 7.17: Rate of the four SPADs observing the Crab Pulsar.

function is computed. An example of autocorrelation function for the Crab pulsar with a time bin of 180 μs is represented in Fig.7.18.

It is also possible to extract from the data the famous light curve of the Crab pulsar that shows the shape of the oscillation (see Fig. 7.19).

The next and most interesting point in our analysis is to calculate the period of the pulsar from the data that AquEYE acquired without the ATFU unit. The spectral analysis is depicted in Fig. 7.20.

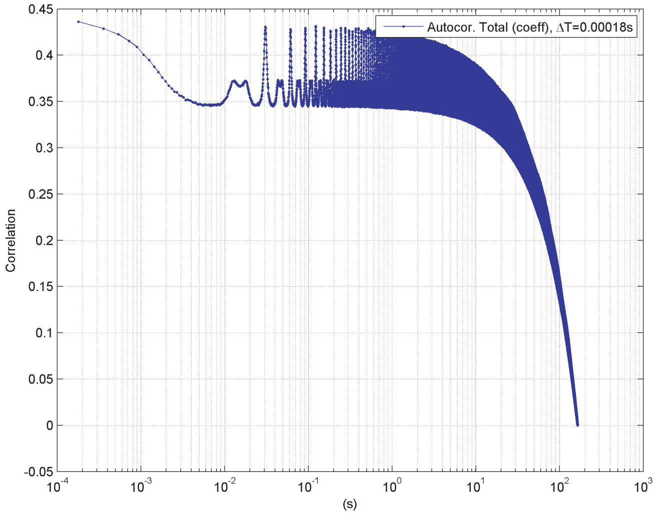


Figure 7.18: Autocorrelation of the Crab pulsar with a time bin of 180 μs.

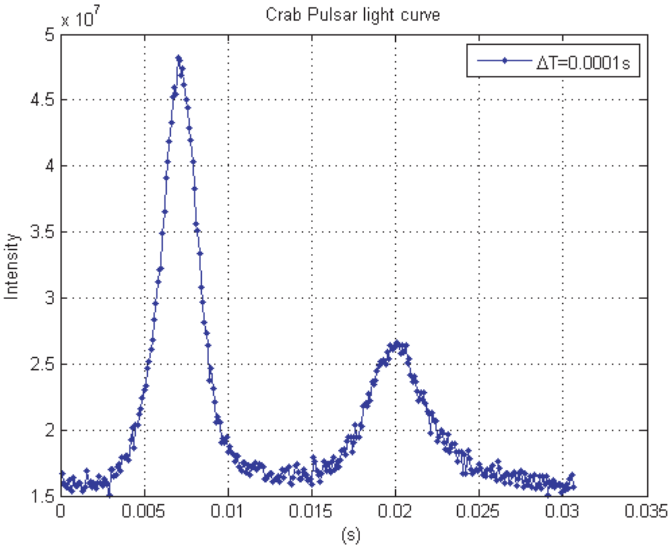


Figure 7.19: Light Curve of the Crab pulsar.

The oscillation period is found to be $T_{meas} = 30.6853$ ms whereas the real value of the pulsar period when the measurement took place was[2] T_{real} =

[2] This value of the pulsar period is obtained compensating for the Ephemeris from

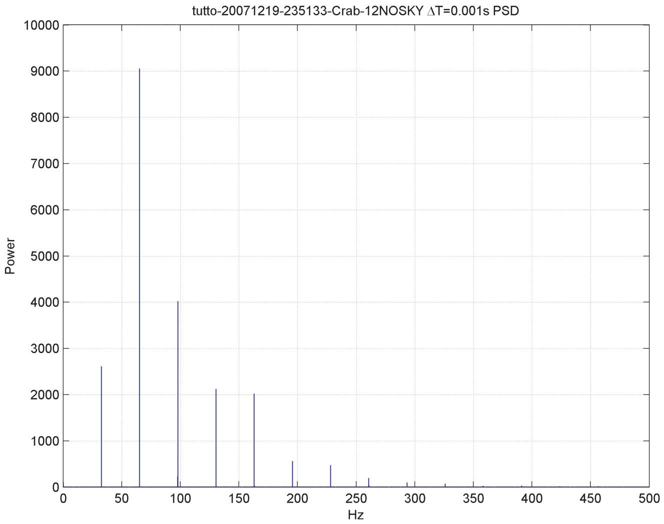


Figure 7.20: Power Spectral Density of the Crab pulsar.

33.61067 ms. This value is different from the expected one and the reason is that the oscillation frequency of the quartz oscillator on the electronic board is slightly different from the nominal 40MHz. Moreover the measurement was done over several minutes but here only 150 seconds are presented. One would expect that a longer measurement would increase the signal to noise ratio but this is not true in this case because of the instabilities of the quartz oscillator itself. That is why if we take pieces of data at different times but with a relatively small duration the light curve is similar to the one depicted in Fig. 7.19 but for longer measurement time the curve blurs out.

Since the ATFU was still under characterization in Cagliari, in order to calibrate our instrument we used a neon lamp which oscillates at 100Hz. Repeating the measurements for the neon lamp at the end of the Crab pulsar acquisition we can in principle re-scale our measurement to get more reliable data. The power spectral density of the neon lamp is illustrated in Fig. 7.21. It is possible to notice how the main oscillation frequency is not nominal $f_{NEON-real}$ = 100Hz but a value slightly grater ($f_{NEON-meas}$=109.4175 Hz), this happens for the same reason as before i.e. the frequency of the quarts on the electronic board is not the expected 40MHz. Nevertheless this gives us a tool in order to correct this error, for example considering the neon frequency exactly 100Hz and re-calibrating the Crab pulsar data. If we do so, the period

www.jb.man.ac.uk/pulsar/crab.html.

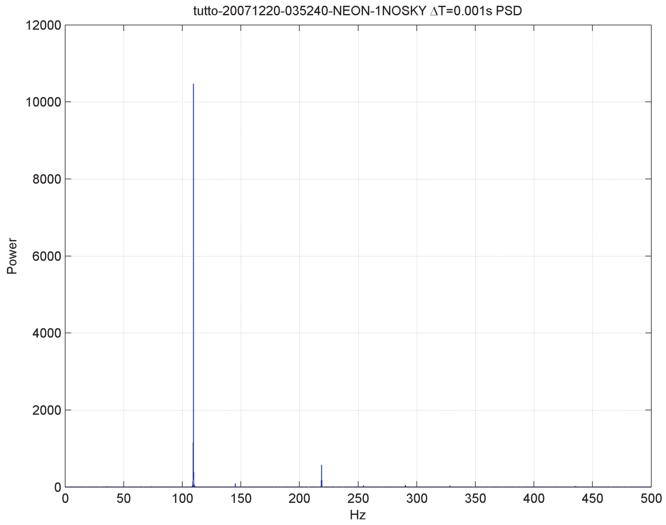


Figure 7.21: Power Spectral Density of a neon Lamp.

of the pulsar is found to be:

$$T_{corr} = \frac{f_{NEON-meas}}{f_{NEON-real}} T_{meas} = 33.5751 \quad ms \tag{7.1}$$

that is very close to the real value real of 33.61 ms.

When the time and frequency unit will be installed on AquEYE this kind of problems will be automatically overcome since the electronic will use instead of its own quartz oscillator a stable and accurate 40MHz reference. This reference, as explained in sec. 7.2.2, is offered by the combination of a rubidium oscillator and a GPS receiver, together with the capabilities of the TDC board.

Conclusions

The aim of this work has been the realization and optimization of a single photon based quantum cryptographic link running in free space channel. First a quantum key distribution (QKD) simulator have been implemented and described. This turned out to be a very useful tool for the initial design phase of QuAKE, the QKD prototype that we are developing in the laboratories of the information engineering department. A full description of the optics and electronics of QuAKE is given as well as the peculiar characteristics of the system that involves some new features in order to optimize the key generation rate. In particular the timing filtering has been implemented by using a leading edge technology such as FPGA (Field Programmable Gate Array) and permits to synchronize the transmitter and the receiver and to share a common time reference. This is done in QuAKE by using a dedicated laser in the same optical channel. The same auxiliary laser is used for sampling the atmosphere by means of a position sensing detector which is part of an adaptive optics (AO) system used in order to optimize the so called spatial filtering. The adaptive optics system allows in fact a better optical conjugation between the transmitter and the receiver so increasing the signal to noise ratio. The system is meant to correct the tilt introduced by the atmosphere during the propagation and is based on a membrane deformable mirror completely developed in our labs. Some tests of the system show that it has good performances both in outdoor environment and at the single photon level when inserted in QuAKE optical setup.

Another point that to our opinion had to be considered is the high level software for quantum key distribution which is normally ignored or not fully optimized. We design and developed a Java version of the high level software introducing modified algorithms and keeping attention to networking and to final users. The software can be used with, and optimized for, any physical QKD implementation and any use of the final keys that are in fact stored in a secure database accessible from any user application.

The last aim of my work has been the application of the techniques of time filtering to an astronomical instrument that is being built for the 182 cm telescope of Asiago (Italy). The instrument is called AquEYE and it should be able to time tag single photons collected by the telescope during some hours of observation time, each photon with a precision of the order of 100 ps. In order to accomplish this task a *time and frequency unit* for the instrument has been designed and characterized. It comprises a Rubidium oscillator and a GPS receiver and it should be able to guarantee the stability and the accuracy that are required for AquEYE.

In conclusion i can say that more precise temporal and spatial filtering systems could be the key points for the development of free space quantum cryptography allowing earth links of several hundreds of kilometers and eventually earth to satellite links. These techniques are fundamental also in other applications that deal with single photon free space propagation and detection as for example the case of AquEYE. This thesis is just my minor contribution to these interesting application areas.

Acknowledgments

For her support and patience i want to thank my love Alessia. She is naturally beautiful!

Many thanks to my father, my mother and my sisters, they always believed in me. They are an endless source of strength!

Thanks to my supervisor prof. Paolo Villoresi. He always supported me and the projects with his constant presence.

Special thanks to prof. Cesare Barbieri for support and suggestions. He also introduced me to the world of astronomy.

I wish also to express my gratitude to my colleague Tommaso Occhipinti, we wanted QuAKE and we are nearly done. It has been a pleasure working with you and it will be the same in the future.

Last, but in the first positions in order of importance i wish to thank all the students and colleagues that have worked in these years to the QuAKE project.

A final special “thank you” to all my friends.

Appendix A

ARPAV Weather Data Analysis

We start with the weather data we collect thanks to *ARPAV - Centro Meteorologico di Teolo*[1]. The meteo station is in Teolo, 12 Km away from Padova but the data collected where useful to have a rough approximation of the values involved. The data collected are resumed in Tab. A.1, for the estimation of the Monin-Obukhov length and the scale temperature the CALMET[2] model have been used.

We used these data to calculate the value of C_n^2 during the experimental session of last february 2th 2007. The trial was done between 17 and 18 so we used those meteo data to find an average C_n^2. First we use the Wyngaard method [1] that is a Boundary Layer Turbulence Model. It uses similarity theory in order to derive the dominant length scale. The Monin Obukhov length describes the heat and momentum transfer between the surface and the atmosphere. The Wyngaard similarity theory can be described by these equations that give the temperature structure constant $C_T^2(h)$ as a function of the altitude above ground.

$$C_T^2(h) = 4.9 T_* h^{-2/3} (1 - 7h/L_*)^{-2/3} \tag{A.1}$$

$$C_T^2(h) = 4.9 T_* h^{-2/3} [1 - 2.4(h/L_*)^{-2/3}] \tag{A.2}$$

where h is the height above ground, L_* is the Monin Obhukov length and T_* is the temperature scaling parameter. Equation A.1 is valid for unstable conditions (daylight) while equation A.2 is valid for stable conditions (nighttime). After that we relate the temperature structure constant with the refraction

[1] ARPAV - Centro Meteorologico di Teolo via Marconi, 55 35037 Teolo (PD), ITALIA http://www.arpa.veneto.it/home2/htm/home.asp

[2] http://www.src.com/calpuff/calpuff1.htm

aa-mm-gg-hh	wind dir	wind v	T(K)	L (MO)	rad	Ts	rel u
2007-02-02-01	149,6	1,2	276,1	12,7	0	2,30E-02	100
2007-02-02-02	173,2	1,8	275,8	12,7	0	5,00E-02	100
2007-02-02-03	123	0,7	275,4	20,3	0	8,60E-03	100
2007-02-02-04	109	1,3	274,4	12,7	0	2,90E-02	100
2007-02-02-05	78	1,1	274,4	12,7	0	1,80E-02	100
2007-02-02-06	16,5	1,8	272,7	12,7	0	5,40E-02	100
2007-02-02-07	17,6	2,3	272,8	12,7	0	8,40E-02	100
2007-02-02-08	25,5	1,8	273,2	12,7	0	5,20E-02	100
2007-02-02-09	46,7	0,9	273,2	12,7	33	1,40E-02	100
2007-02-02-10	56,1	1,2	273,8	12,7	85	2,30E-02	100
2007-02-02-11	6,2	1,3	275,3	-39,4	138	-4,50E-02	100
2007-02-02-12	0,8	2,1	277,7	-92,3	155	-4,70E-02	100
2007-02-02-13	357,6	2,5	278,9	-78,2	220	-7,80E-02	100
2007-02-02-14	13,4	3,2	279,9	-105,7	282	-9,20E-02	100
2007-02-02-15	9,7	2,9	281,3	-89,6	263	-9,10E-02	94,5
2007-02-02-16	10,8	2,2	281,9	-82,2	169	-5,70E-02	89,5
2007-02-02-17	24,3	2	281	12,7	61	6,60E-02	93
2007-02-02-18	0,6	1,5	279,4	12,7	2	3,90E-02	99,25
2007-02-02-19	347,6	1,2	278,3	12,7	0	2,30E-02	100
2007-02-02-20	13,1	0,3	275,6	160,3	0	1,10E-03	100
2007-02-02-21	101	0,2	274,2	270,9	0	6,40E-04	100
2007-02-02-22	6,2	0,4	273,8	53,5	0	3,30E-03	100
2007-02-02-23	349,1	0,2	273,4	375	0	4,60E-04	100
2007-02-03-00	266	0,4	273,4	79,2	0	2,20E-03	100

Table A.1: ARPAV meteo data. Data (aa-mm-gg-hh), wind direction (wind dir) , wind speed (wind v), temperature (T), Monin-Obukhov length (L(MO)), global radiation, scale temperature, relative humidity. All values are expressed in SI units.

index structure constant by means of the relation:

$$C_n^2 = [(n-1)/T]^2 C_T^2 \tag{A.3}$$

where T is the temperature and n is the index of refraction. In literature [1] it is customary to chose $n - 1 = 79 \times 10^{-6} P/T$ The value that we obtain with this calculation is about $C_n^2 = 4 \times 10^{-15} m^{-2/3}$. The values of C_n^2, calculated during 24 hours (Fig. A), show values around this value during the day present a drop to 10^{-18} during the night.

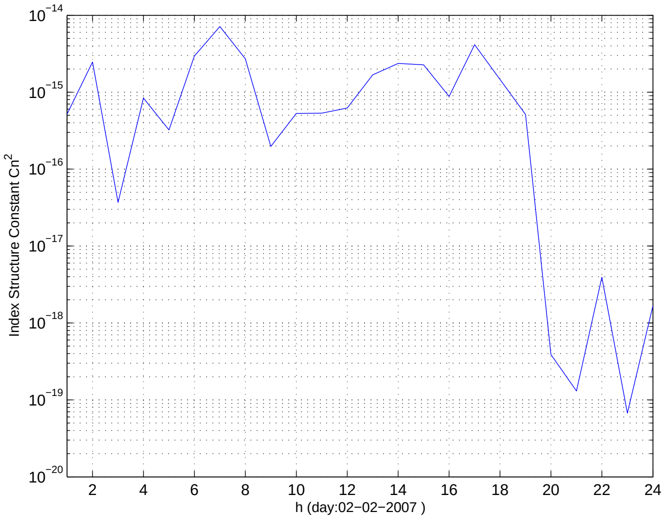


Figure A.1: The value of C_n^2 calculated using the meteo data from ARPAV centro metereologico di Teolo.

Said that we go through a simple calculation to relate C_n^2 to the effects on the propagation of our beam assuming a Kolmogorov like behavior. First we calculate the Fried Coherence Length r_0 using the well known formula 4.26: We obtained a value of $r_0 = 25cm$. If we assume instead the SLC value of C_n^2 we end up with a value of $r_0 = 11cm$. The value of the tilt angle calculated with formula 4.30 is about $\alpha^2 = 6 \times 10^{-12}$. With the SLC model the value would have been 2.4×10^{-11} radiants.

Appendix B

Key Components

In this appendix some of the key components are described. Some of them, not reported here, have been already described in this thesis in particular the deformable mirror for the Adaptive Optics system, built in our department, is described in Sec. 4.4.

B.0.1 Single Photon Detectors

Since an always increasing number of applications require the capability of detecting single photons many techniques have been developed in the last years [5]. It is very common in today quantum optics apparatus the use of SPAD (Single Photon Avalanche Photodiode) as a detector capable of detecting single photons [25, 26]. A SPAD is essentially an APD working in Geiger mode. In this operative mode the active area of the APD (i.e. the pn-junction) has an inverse polarization with a voltage slightly over the breackdown limit (overvoltage). When a single photon comes to this pn-junction an avalanche of electronic current starts and from this current it is possible to produce a digital pulse[1]. In order to be sensible to the next incoming photon, the junction must be recharged as soon as possible this meaning that the avalanche must be stopped and the voltage across the junction restored to the desired value. For this purpose in modern SPAD a so called *quenching* circuit is used for stopping the avalanche and re-charging the junction. The quenching can be obtained in many way, from a single discharging resistor to more complicated approaches like *active quenching circuits* [73]. Depending on material and technology SPADs can be very different from each others. There is a number of companies that produce and sell SPADs mainly using Silicon and indium gallium arsenide (InGaAs). The former are very reliable devices that work well

[1] Typically a TTL (Transistor Transistor Logic) voltage pulse

in the $500 - 900$nm range, the latter were developed for detecting photons at telecom wavelength (1550 nm) but they present still some problems of fabrication and overall efficiency [86]. It follows a list of the main parameters that characterize SPADs, each of these parameters has to be carefully chosen and can be essential depending on the application.

Table B.1: Typical parameters of a MPD (Micro Photon Devices) SPAD. Values as they appear in the data sheet available at www.microphotondevices.com. Measure taken at 25°C, overvoltage $5V$.

Parameter	Value	Units
Active area	50	μm
Dark Counts	$50 - 100$	cps
After-pulsing probability	$0.5 - 1.5$	%
Dead time	75	ns
Rise and fall time	< 2 on 10pF load	ns
Pulse duration	20	ns

The dead time T_d it is the time that the device needs from a detection in order to be ready for the next one. Quenching, manufacturing, impurities on the substrate are key factors for the dead time. Typical values in today devices vary from 50 to 100 ns.

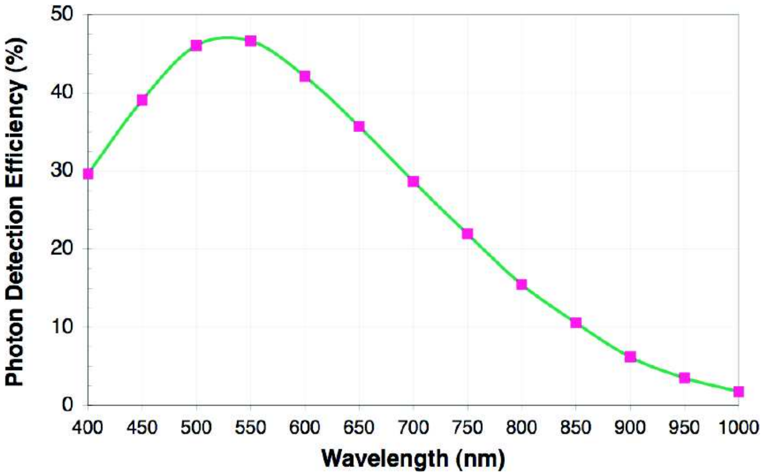


Figure B.1: This is the photon detection efficiency of the commercial SPAD by MPD (Micro Photon Devices) that we have used.

The dark count rate R_{DK} is the rate of counts that one observe is the detector area is kept in the complete darkness. This is mainly do to the operative mode (Geiger mode) that implies an high instable condition for the starting of the avalanche. Spontaneous avalanche can be caused by electrons collisions and the consequent energy transfer among them. A way to reduce dark counts is to cool down the their device by means of Peltier cell. In the last years dark counts rates went from Kcps to cps (cps stands for *counts per second*).

Photon detection efficiency *qe* represents the probability that a photon that strikes the active area is effectively detected. It depends on the wavelength and on the device itself. Typical values go from 10 % in the near infrared to 50% or more in the green.

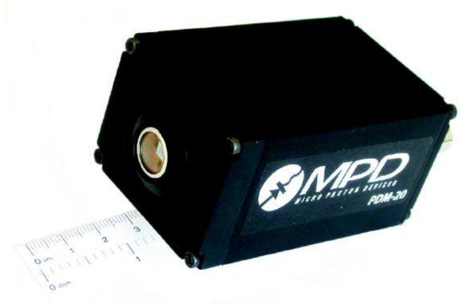


Figure B.2: A picture of the MPD SPAD that we used in our system.

The Timing Resolution indicates the resolution of the time tagging of a photon. The values can vary from device to device depending on the manufacturer and can reach some tens of picoseconds.

The process of fabrication of these devices can introduce a certain level of impurities on both the substrate and junction. Those impurities acts like traps for the electrons during an avalanche and the quenching phase. The electrons remain trapped with a non zero probability of coming out the trap and activate the avalanche that lead to an unwanted count. This problem, called afterpulseing, is very severe for InGaAs devices whereas its effects are pretty much low for Silicon devices.

In our QKD system we used two SPADs from MPD[2] (Micro Photon Devices). In table B.1 you can see a review of our device characteristics as reported on the data sheet. In figure B.0.1 the photon detection efficiency at different wavelengths. In figure B.2 a picture of the device. Consult the website for more information.

[2] www.microphotondevices.com

B.0.2 Position Sensing Detectors

The main components of the Adaptive Optics system installed on QuAKE and described in Sec. 4 are the deformable mirror and the Position Sensing Detector (PSD). The latter is a key component in the system as it has the aim to measure the position of the spot during time. The choice of the component is then very important and many factors have to be evaluated: the precision of the position measurement, the minimum power required and the bandwidth of the detector among the others. PSD normally use a Planar Diffused Photodiode as main component and can be divided into two families: the quadrant PSD and the lateral effect PSD. The former are made by a single substrate in which four different active regions are created. An incident beam will produce then four different currents, those current are all equal is the beam is equally distributed among the four active regions. If this is not the case the beam position can be calculated evaluating the differences between the four currents by the following:

$$X = \frac{(A+D)-(B+C)}{A+B+C+D} \; ; Y = \frac{(A+B)-(C+D)}{A+B+C+D}, \tag{B.1}$$

where X and Y are the centroid positions and A, B, C, D the four photocurrents relative to the different active area.

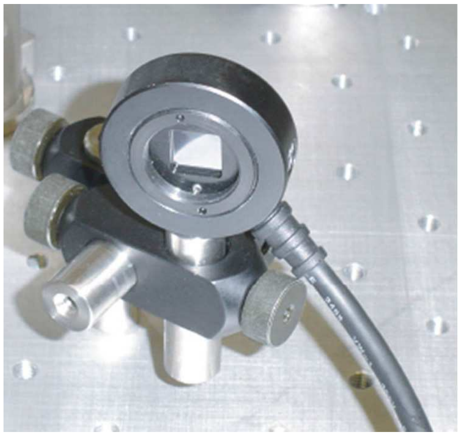


Figure B.3: A picture of the DUMA Position Sensing Detector that we used in our system.

The lateral effect PSD are build with a single active region with four electrodes at the edges. When the light arrive on the detector free photo electrons are created and they flow in the four electrodes finding in their ways different resistances. Form the four currents A, B, C, D it is possible to calculate the spot position using the followings:

$$X = K_x \frac{B-D}{B+D} \; ; \; Y = K_y \frac{A-C}{A+C}, \tag{B.2}$$

Table B.2: Parameters of the DUMA Positioning Sensing Detector as available in the data sheet downloadable from http://www.duma.co.il.

Parameter	Value	Units
Active area	9×9	mm
Beam Size Range	$50 - 8000$	μm
Position Resolution	better that ±1	μm
Position Accuracy[3]	±25	μm
Calibrated Spectral Range	$350 - 1100$	nm
Input Power Range	$1 - 250$	μW
Power Accuracy	±5	%
Data Update Rate	30	KHz in Analog Mode

where K_x and K_y are scaling factors to pass from photocurrent to coordinates. This technique has several advantages with respect to quadrant PSDs: first of all the spot is continuously measured so assuring a very broad analog bandwidth of several KHz, the sensor can measure different spot sizes as soon as the whole spot lay inside the active area. This is not possible with the quadrant detectors that require that all the quadrant are illuminated in order to measure the centroid position. For our system we decided to have a lateral effect PSD from DUMA (http://www.duma.co.il) which specifications are reported in Tab. B.2. The choice was made in order to minimize the accepted input power since wanted to be as free as possible with the our reference in order to be able to use the adaptive optics system with different QKD systems in different operating conditions.

Bibliography

[1] *Atmospheric propagation of Radiation*. SPIE Optical Engineering Press, 1996.

[2] *The Utilization of the Galilieo Timing Signals for Advanced Astronomical Applications*, 2007. accepted.

[3] Antonio Acin and Nicolas Gisin. Quantum correlations and secret bits. *Physical Review Letters*, 94(02051), 2005.

[4] C. Barbieri, G. Cariolaro, T. Occhipinti, C. Pernechele, F. Tamburini, and P. Villoresi. *Qspace Project: Quantum Cryptography in Space*, volume Optical Communication theory and techniques. Springer, 2004.

[5] Wolfgang Becker and Axel Bergmann. Detectors for high-speed photon counting. Technical report, Becker Hickl GmbH, Berlin, becker@becker-hickl.com, 2006.

[6] J.S. Bell. On the einstein podolsky rosen paradox. *Physics 1*, 3(195), 1964.

[7] C. H. Bennet, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Information Theory*, 41, 1995.

[8] C.H. Bennet and G. Brassard, 1984. in "Proc. IEEE Int. Conference on Computers, Sysytems and Signal Processing".

[9] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, settembre 1991.

[10] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

[11] J.A. Bergou and L.B. Kish. An absolutely secure qkd scheme with no detection noise, entanglement and classical communication. *e-print archive*, http://www.arxiv.org/abs/quant-ph/0509097, 2005.

[12] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams. Quantum key distribution with 1.25 gbps clock synchronization. *Optics Express*, 12:2011–2016, 2004.

[13] S. Bonora, I. Capraro, L. Poletto, M. Romanin, C. Trestino, and P. Villoresi. Wave front active control by a digital-signal-processor-driven deformable membrane mirror. *REVIEW OF SCIENTIFIC INSTRUMENTS*, 77(093102-1), 2006.

[14] Edoardo Bortolato. Realizzazione su fpga di un rivelatore di coppie di fotoni entangled. Tesi di Laurea, 2007.

[15] G. Brassard and L. Salvail. Lecture notes in computer science. 1984.

[16] H. J. Briegel, W. Dur, J. I. Cirac, and P. Zoller. Quantum repeaters for communication, 1998.

[17] W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson. Daylight quantum key distribution over 1.6 km. *Physical Review Letters*, 84(24):5652–5655, June 2000.

[18] Barbieri C, Dravins D, Occhipinti T, Tamburini F, Naletto G, Da Deppo V, Fornasier S, D'onofrio M, Fosbury RAE, Nilsson R, and Uthas H. Astronomical applications of quantum optics for extremely large telescopes. *Journal of Modern Optics, special issue of on Single-Photon: Sources, Detectors, Applications and Measurement Methods.*, In press.

[19] Barbieri C, Da Deppo V, D'Onofrio M, Dravins D, Fornasier S, Fosbury RAE, Naletto G, Nilsson R, Occhipinti T, Tamburini F, Uthas H, and Zampieri L. Quanteye, the quantum optics instrument for owl., 2006.

[20] Ivan CAPRARO, STEFANO BONORA, and PAOLO VILLORESI. Fast correction of atmospheric turbulence using a membrane deformable mirror. In *6th International Workshop on Adaptive Optics for Industry and Medicine*, 2007.

[21] Ivan CAPRARO and TOMMASO OCCHIPINTI. Implementation of a real time high level protocol software for quantum key distribution. IEEE International Conference on Signal Processing and Communication, 2007.

[22] Ivan Capraro, Tommaso Occhipinti, Paolo Zoccarato, Cristian Bonato, Fabrizio Tamburini, Cesare Barbieri, and Paolo Villoresi. The utilization

of the galileo timing signals for quantum communications. In *1st Colloquium Scientific and Fundamental Aspects of the Galileo Programme*, 2007.

[23] N.J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys with squeezed states. *arXiv e-print archive*, http://www.arxiv.org/abs/quant-ph/0008058, 2000.

[24] S. Chiangga, P. Zarda, T. Jennewein, and H. Weinfurter. Towards practical quantum cryptography. *Applied Physics B: Lasers and Optics*, 69:389–393, 1999.

[25] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *Journal of Modern Optics*, 51:1267–1288, September 2004.

[26] Sergio Cova. Single-photon photon avalanche diodes: Retrospect and prospect. *Presentation*, 2005.

[27] M. Curty, M. Lewenstein, and Norbert Lutkenhaus. Entanglement as a precondition for secure key distribution. *Physical Review Letters*, 92(21), 2004.

[28] Dravins D, Barbieri C, Da Deppo V, Faria D, Fornasier S, Fosbury RAE, Lindegren L, Naletto G, Nilsson R, Occhipinti T, Tamburini F, Uthas H, and Zampieri L. Quanteye. quantum optics instrumentation for astronomy. In: OWL Instrument Concept Study, ESO document OWL-CSR-ESO-00000-0162. In: OWL Instrument Concept Study, ESO document OWL-CSR-ESO-00000-0162., 2005.

[29] D. Dehlinger and M.W. Mitchell. Entangled photons, nonlocality and bell inequalities in the undergraduate laboratory. Technical Report quant-ph/0205171 v1, Oxford University press, Oxford, Physics Dep.,Reed College 3203 SE Woodstock Blvd. Portland, May 2002.

[30] P.A.M. Dirac. *The Principles Of Quantum Mechanics.* Oxford University Press, 1958.

[31] F. D'Onofrio. Algoritimi di error correction e privacy amplification per la crittografia quantistica. Tesi di Laurea, Padova, 2005.

[32] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller. Quantum repeaters based on entanglement purification. *Phys. Rev. A*, 59(1):169–181, Jan 1999.

[33] Frank D. Eaton, Patrick R. Kelly, Demos T. Kyrazis, and Jennifer C. Ricklin. Impact of realistic turbulence conditions on laser beam propagation. volume 5550, pages 267–274. SPIE, 2004.

[34] C. Elliott, D. PEarson, and G. Troxel. Quantum cryptography in practice. *SIGCOMM 2003*, 2003.

[35] Motti Gabay and Sholomi Arnor. Effect of turbulence on a quantum-key distribution scheme based on transformation from the polarization to the time domain: laboratory experiment. *Optical Engineering*, 44(4), 2005.

[36] G. Gilbert and M. Hamrick. Practical quantum cryptography: A comprehensive analysis (part one). Technical report, Mitre Technical Report and quant-ph/0009027, September 2000.

[37] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. of Modern Physics*, 74:145–195, January 2002.

[38] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. 03.67.dd quantum cryptography, Toshiba Research Europe Ltd.

[39] F. Grosshans and P. Grangier. Continuous variable quantum cryptogra- phy using coherent states. *arXiv e-print archive*, http://www.arxiv.org/abs/quant-ph/0109084, 2001.

[40] H.Inamori, N. Lutkenhaus, and D. Mayers. Uncoditional security of practical quantum key distribution. *arXiv e-print archive*, 2001.

[41] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *Physics Division Los Alamos National Laboratory.*

[42] Richard J. Hughes, George L. Morgan, and C. Glen Peterson. Practical quantum key distribution over a 48-km optical fiber network, 1999.

[43] R.C. Jaeger and T.N. Blalock. *Microelettronica Circuiti Integrati Analogici.* McGraw-Hill, 1998.

[44] S. Karpov, G. Beskin, A. Biryukov, V. Debur, V. Plokhotnichenko, M. Redfern, and A. Shearer. Short time scale pulse stability of the Crab pulsar in the optical band. *Astrophysics and Space Science*, 308:595–599, April 2007.

[45] Isaac I. Kim, Bruce McArthur, and Eric Korevaar. Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. Technical report, Optical Access Incorporated, 10343 Roselle Street San Diego, CA 92121, 2004.

[46] A. Kolmogorov. Dissipation of energy in locally isotropic turbulence. *Doklady Akad. Nauk SSSR*, 32(16), 1941. German translation in "Sammelband zur Statistichen Theorie der Turbulenz", Akademie-Verlag Berlin (1958), p. 77.

[47] A. Kolmogorov. The local structure of turbulence in incompressible viscous fluid for very large reynolds' numbers. *Doklady Akad. Nauk SSSR*, 30:301, 1941. German translation in "Sammelband zur Statistichen Theorie der Turbulenz", Akademie-Verlag Berlin (1958), p. 71.

[48] A. Kolmogorov. *Turbulence, Classic Papers on Statistical Theory.* S.K. FriedLander and L. Topper, 1961. New York.

[49] C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity, and H. Weinfurter. Long distance free space quantum cryptography.

[50] Y. Li, S. Hua, Y. Liu, J. Ye, and Q. Zhou. Quantum repeaters: fundamental and future. In *Quantum Information and Computation V. Edited by Donkor, Eric J.; Pirich, Andrew R.; Brandt, Howard E.. Proceedings of the SPIE, Volume 6573, pp. 65730X (2007).*, volume 6573 of *Presented at the Society of Photo-Optical Instrumentation Engineers (SPIE) Conference*, May 2007.

[51] M. Lucamarini, A. Cere', G. Di Giuseppe, S. Mancini, D. Vitali, and P. Tombesi. Two-way protocol for quantum cryptography with imperfect devices, 2006.

[52] A. G. Lyne, R. S. Pritchard, and F. G. Smith. Crab pulsar timing 1982-87. *Royal Astronomical Society, Monthly Notices*, 233:667–676, August 1988.

[53] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74(2):022313–+, August 2006.

[54] D. Mayers. Unconditional security in quantum cryptography. *Acm Journal*, 48:351–406, 2001.

[55] Kim-Chi Nguyen, Gilles Van Assche, and NicolasJ. Cerf. Side-information coding with turbo codes and its application to quantum key distribution. *arXiv:cs/0406001v1*, jun 2004.

[56] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaouti-Helie. Integration of quantum cryptography in 802.11 networks. In *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, pages 116–123, Washington, DC, USA, 2006. IEEE Computer Society.

[57] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge: University Press, 2000.

[58] R. J. Noll. Zernike polynomials and atmospheric turbulence. *Journal of the Optical Society of America (1917-1983)*, 66:207–211, March 1976.

[59] A. M. Obukhov. Structure of the temperature field in a turbulent flow. *Izv.Akad.Nauk SSSR, Ser.Geograf.Geofiz.*, 13(58), 1949. German translation in "Sammelband zur Statistichen Theorie der Turbulenz", Akademie-Verlag Berlin (1958), p.127.

[60] Tommaso Occhipinti. *Quantum Key Distribution: a Telecommunication Model and a Practical Implementation*. PhD thesis, Scuola di Dottorato in Ingegneria Dell'Informazione, 2006.

[61] Tommaso Occhipinti, Paolo Zoccarato, Ivan Capraro, Pietro Bolli, Filippo Messina, Giampiero Naletto, Paolo Villoresi, and Cesare Barbieri. The importance of time and frequency reference in quantum astronomy and quantum communications. In *Thirty-Ninth Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting*, 2007.

[62] J.-W. Pan and A. Zeilinger. Greenberger-Horne-Zeilinger-state analyzer. *PhysRevA.*, 57:2208–2211, March 1998.

[63] D. Pearson and C. Elliott. On the Optimal Mean Photon Number for Quantum Cryptography. *ArXiv Quantum Physics e-prints*, March 2004.

[64] J. W. Percival, J. D. Biggs, J. F. Dolan, E. L. Robinson, M. J. Taylor, R. C. Bless, J. L. Elliot, M. J. Nelson, T. F. Ramseyer, G. W. van Citters, and E. Zhang. The Crab pulsar in the visible and ultraviolet with 20 microsecond effective time resolution. *Astrophysical Journal*, 407:276–283, April 1993.

[65] A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. R. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. Practical quantum key distribution with polarization-entangled photons. *Optics Express*, 12:3865, 2004.

[66] R. Renner, N. Gisin, and B. Kraus. An information-theoric security proof for qkd protocols. *arXiv e-print archive*, 2005.

[67] K.J. Resch, M. Lindenthal, B. Blauensteiner, H.R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger. Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Optics Express*, 13(1):202–209, 2005.

[68] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications ACM*, 28:120–134, 1978.

[69] F. Roddier. *The effects of atmospheric turbulence in optical astronomy.* Progress in Optics XIX. E. Wolf, New York: North Holland, 1981.

[70] Phillip Rogaway. Bucket hashing and its application to fast message authentication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(2):91–115, 1999.

[71] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144km. *Physical Review Letters*, 98(1):010504–+, January 2007.

[72] Bruce Schneier. *Applied Cryptography.* John Wiley and sons, Inc., 1996.

[73] S.Cova, A.Longoni, and G.Ripamonti. Active-quenching and gating circuits for single-photon avalanche diodes (spads). *IEEE Transactions on Nuclear Science*, 29:599–601, 1982.

[74] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[75] J. H. Shapiro. Near-field turbulence effects on quantum-key distribution. *Phys. Rev. A*, 67(2):022309–+, February 2003.

[76] P.W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000.

[77] Nabeel A. Siddiqui. Quantum-grid infinitesimal bit cryptosystem. IEEE International Conference on Signal Processing and Communications (IC-SPC 2007), 2007.

[78] C. Silberhorn, N. Korolkova, and G. Leuchs. Quantum key distribution with bright entangled beams. *arXiv e-print archive*, http://www.arxiv.org/abs/quant-ph/0109009, 2001.

[79] Bonora Stefano, Capraro Ivan, Poletto Luca, Matteo Romanin, Trestino Cosmo, and Villoresi Paolo. A dsp control system of membranedeformable mirror using tms320 c5502. 2005.

[80] Bruce Edward Stribling. *Laser Beam Propagation in non-Kolmogorov Atmospheric Turbulence*. Afit/geo/eng/94d-04, School of Engineering of the Air Force Institute of Technology, Air University, 1994.

[81] K. Tamaki, M. Koashi, , and N. Imoto. Security of the bennett 1992 quantum-key distribution against individual attack over a realistic channel. *arXiv quant-ph 0212161*, 1, Dec 2002.

[82] A. S. Tanenbaum. *Computer Networks*. Prantice Hall PTR, 1996.

[83] X. Tang, L. Ma, A. Mink, A. Nakassis, B. Hershman, J. Bienfang, R. F. Boisvert, C. Clark, and C. Williams. High speed fiber-based quantum key distribution using polarization encoding. In Optics and Photonics Conference, editors, *Proceedings of SPIE*, volume 5893, 2005.

[84] V. I. Tatarski. *Wave Propagation in a Turbulent Medium*. McGraw-Hill, New York, 1961.

[85] T.C.Ralph. Quantum key distribution with continuous variable in optics. Technical Report quant-ph/0109096 v2, University of Queensland, Dep. of Physics, St Lucia, QLD 4072 Australia, 2001.

[86] Alexei Trifonov, Darius Subacius, Audrius Berzanskis, and Anton Zavriyev. Single photon counting at telecom wavelength and quantum key distribution. *journal of modern optics*, 51(9–10):1399 – 1415, 2004.

[87] G. A. Tyler. Bandwidth considerations for tracking through turbulence. *Journal of the Optical Society of America A*, 11:358–367, January 1994.

[88] Robert K. Tyson. *Principles of Adaptive Optics*. Academic Press, 525 B Street, Suite 1900, San Diego, California, Usa, 1997.

[89] T. von Karman. *Progress in the statistical theory of turbulence*. Classic Paper on Statistical Theory. S.K. FriedLander, L. Topper, 1961.

[90] M.N. Wegman and J.L. Carter. New hash function and their use in authentication and set equality. *Journal of computer and system sciences*, 22, 1981.

[91] Henning Weier, Tobias Schmitt-Manderbach, Nadja Regner, Christian Kurtsiefer, and Harald Weinfurter. Free space quantum key distribution: Towards a real life application. *Fortschr. Phys.*, 54(8):840–845, 2006.

[92] Otakar Wilfert and Zdenek Kolka. Statistical model of free-space optical data link. volume 5550, pages 203–213. SPIE, 2004.

[93] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802 – 803, October 1982.

[94] A.M. Yaglom. On the local structure of the temperature field in a turbulent flow. *Doklady Akad. Nauk SSSR*, 69(743), 1949. German translation in "Sammelband zur Statistichen Theorie der Turbulenz", Akademie-Verlag Berlin (1958), p.127.

[95] H.P. Yuen. Anonymous key quantum cryptography and unconditionally secure quantum bit commitment. *arXiv e-print archive*, http://www.arxiv.org/abs/quant-ph/0009113, 2000.

[96] P. Zoccarato. Decrittazione intrusiva di chiavi quantistiche e contromisure. Tesi di Laurea, Padova, 2005.