Free-Space Communication in Quantum Key Distribution

Marco Mariola

March 20, 2015

Submitted in fulfillment of the academic requirements for the PhD degree at the School of Chemistry and Physics, Westville Campus, University of KwaZulu-Natal. As the candidate's supervisor I have approved this thesis for submission.

Name: Francesco Petruccione
Signed:
Date:

ABSTRACT

Quantum cryptography permits the sharing of a secret key hence information between authorized parties such that an unauthorized party is unable to obtain any useful information. A quantum and a classical authenticated channel are used to connect the authorized parties. The security of cryptography is based on the fundamental principles of quantum physics specifically the Heisenberg's uncertainty principle, entanglement and the no-cloning theorem.

Two major quantum channels that are used in quantum cryptography for the transmission of messages are optic fibers and free space. The key is transmitted as a series of single photons and the bits of the key are encoded by the measurement of the quantum state. In recent years, real Quantum Key Distribution (QKD) systems have been built and communication has also been established by using optic fiber networks for the transmission of encoded messages. However, open challenges still remain, for example the distribution of the key over large distances and communication involving moving parties. In the quest to increase the communication distance and have an alignment free reference system, free-space quantum communication has been favoured.

Regardless of free-space communication being seen as a good candidate for quantum communication, it suffers from the problem of alignment when communication involves moving objects, for example between Earth and an orbiting satellite. Although vertical communication between an Earth station and a satellite is possible, horizontal path communication still poses a great challenge. This is mainly due to turbulence in the atmosphere, vapor pressure and pollution.

In this thesis, it is demonstrated how the problem of alignment might be solved. In particular, we will focus on the ways to obtain an autonomous system, which can be used to align the transmitter and the receiver for free-space quantum communication. We assess the possibility of obtaining a tracking system by using open-source electronics. In order to build our tracking system, it was used an algorithm implemented by a microcontroller mounted on a printed component board. The embedded system can be considered to be a coarse tracking for

optical communication and a fine alignment for radio-communications. An angular sensor for the base alignment is plugged into the microcontroller system. To align the polarization bases, the receiver sends a polarized laser beacon to the transmitter and by an angular sensor the transmitter is able to align his bases for the single photon transmission. Then by using a correction algorithm, this system provides an accurate alignment. Moreover, in order to show that our system works, we tested the polarization alignment system in the laboratory. To verify the tracking system, we used both cartography software and a short range experiment.

We finally present the results of the above systems as implemented and tested at the University of KwaZulu-Natal (UKZN).

Preface

The work described in this thesis was carried out in the School of Chemistry and Physics, University of KwaZulu-Natal, Durban, from January 2012 to December 2014, under the supervision of Professor Francesco Petruccione.

These studies represent original work of the author and have not otherwise been submitted in any form for any qualification to any University. Where use has been made of the work of others it is duly acknowledged in the text.

Declaration 1-Plagiarism

I, ____, declare that

i The research reported in this thesis, except where otherwise indicated, is my original research.

ii This thesis has not be submitted for any degree or examination at any other University.

iii This thesis does not contain any other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

iv This thesis does not contain any other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted , then:
a. Their words have been re-written but the general information attributed to them has been referenced;
b. Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed: ____

Declaration 2- publications

This thesis is based on the following publications, which will be referred by their respective designations:

Patent

P1 **M. Mariola**, A. Mirza and F. Petruccione "System and method for determining angles between apparatuses, devices or systems." Provisional patent. Reference number L 2014/03405
My contribution: Primary inventor. I conceived the idea of using a polarized beam splitter to measure the angle between apparatuses. I characterized the PBS in order to find a particular correction function and algorithm.

Peer-Reviewed Journal Papers

M1 **M. Mariola**, A. Mirza and F. Petruccione,"Polarization Alignment system for free-space quantum key distribution", *To be submitted.*
My contribution: I conceived the idea to create a polarization alignment system using two polarisers to lock the alignment the bases of the quantum channel. A better result follows by using a polarising beam splitter with a correction algorithm to obtain a better alignment accuracy.

M2 **M. Mariola**, Y. Ismail and F. Petruccione,"Customized keyboard for a microcontroller", *To be submitted.*
My contribution: I conceived the idea of using an analog input pin of the microcontroller to choose different features provided from the system. I developed an algorithm in order to minimize the memory ram and flash memory of the microcontroller.

M3 **M. Mariola**, Y. Ismail, A. Mirza and F. Petruccione,"Tracking system for optical and radio communication using the GPS" , *To be submitted*

My contribution: I conceived the idea of using the GPS coordinate to align a transmitter and receiver, with a reference points. I developed the algorithm and the software optimized for a microcontroller.

Conference Proceedings

CP1 **M. Mariola**, A. Mirza and F. Petruccione, Quantum cryptography for satellite communication, in Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, edited by I. Basson and A.E. Botha (University of South Africa, Pretoria, 2011), pp. 403 - 408. ISBN: 978-1-86888-688-3. Available online at http://events.saip.org.za
My contribution: I conceived the QKD feasibility in free space for aerospace systems. Was a first approach to study a tracking and synchronization system.

CP2 **M. Mariola**, A. Mirza and F. Petruccione,Influence of the motion of aerospace systems on the polarization angle of qubits for free-space QKD, in Proceedings of SAIP2012: the 57th Annual Conference of the South African Institute of Physics, edited by Johan Janse van Rensburg (2014), pp. 505 - 510. ISBN: 978-1-77592-070-0. Available online at http://events.saip.org.za
My contribution: I study the effects of the polarization bases for a satellite along a generic orbit, and I will shows that is possible align the Ground-station with the satellite by the orbit propagation. I also show that for two aerospace systems, the tracking and alignment can be done using a laser beacon, following some limit condition.

CP3 **M. Mariola**, A. Mirza and F. Petruccione, Open-Source electronics for quantum key distribution, in Proceedings of SAIP2013: the 58th Annual Conference of the South African Institute of Physics, edited by Roelf Botha and Thulani Jili (2014), pp. 470 - 475. ISBN: 978-0-620-62819-8. Available online at http://events.saip.org.za
My contribution: I conceived the idea of using an open-source software and electronics to build a polarization alignment basis system and fine alignment using laser beacon.

CP4 **M. Mariola**, A. Mirza and F. Petruccione, Polarization alignment system for quantum key distribution, SAIP2014 the 59th Annual Conference of the South African Institute of Physics. (Submitted).
My contribution: For obtain a polarization alignment system by using one and two polarisers. I built and designed the experimental setup, the mechanics and electronics.

Talks presented

- **M. Mariola**, A. Mirza and F. Petruccione, “Plug and Play system for optical and radio communication”,*Quantum Information Processing Communication and Control*, Drakensberg, South Africa, 2014.

- **M. Mariola**, A. Mirza and F. Petruccione, “Polarization alignment system for quantum key distribution”, 59th*South African Institute of Physics conference*,University of Johannesburg, 2014.

- **M. Mariola**, A. Mirza and F. Petruccione, “Telecommunication system Moon to Earth in Quantum Key Distribution for Lunar Rover Mission,” Quantum Information Processing and Computing and control Conference, 25-29 November, Pumula Beach Resort, South Africa (2013)” .

- **M. Mariola**, A. Mirza and F. Petruccione, “QKD in free-space”, *Research Day*, UKZN, 2012.

- **M. Mariola**, A. Mirza and F. Petruccione, “Influence of the motion of aerospace systems on the polarization angle of qubits for free space QKD, 57th*annual conference of the South African Institute of Physics*, University of Pretoria, 2012.

- **M. Mariola**, A. Mirza and F. Petruccione, “Quantum cryptography for satellite communication, ”56th *annual conference of the South African Institute of Physics*, University of South Africa, Pretoria, 2011.

Posters Presented

- **M. Mariola**, A. Mirza and F.Petruccione, “Open-Source electronics for quantum key distribution,”59th South African Institute of Physics conference, University of Zululand, South Africa 2013.

- **M. Mariola**, A. Mirza and F. Petruccione,“Telecommunication system Moon to Earth in Quantum Key Distribution for Lunar Rover Mission,” Reseach Day, University of KwaZulu-Natal, Howard College, 2013, South Africa.

- **M. Mariola**, Y. Ismail, M. Senekane, M. Mafu, S. Pillay, A. R. Mirza and F. Petruccione,“Quantum communication in free space”, South African Society for Atmospheric Sciences 2013, 26-27 September 2013, Salt Rocks Hotel, South Africa .

Schools attended

- 6th Winter School on Practical Quantum Cryptography
  Les Diablerets, Geneva, Switzerland
  January 2014

Research Visits

- Visited Professor Paolo Villoresi at Department of Information Engineering
  University of Padova
  Research Interest: Quantum communication
  15 July 2012 - 28 July 2012

Signed: ________________________________

To my father, Alfredo

Acknowledgments

Some years ago, one of my Professors wrote in a book that knowledge is the wing of freedom. The more one knows, the higher one can fly. To obtain wings, it is important to meet people that believe in your ability since they give you courage and an opportunity to fly. For this reason, I would like to thank my Supervisor Francesco Petruccione for giving me the opportunity to work in his Quantum Research Group at UKZN. In this Group, I could express my creativity and I learnt a lot of useful notions, that as an engineer I probably would never learnt had I not been in this Group.

I would also like to thank Professor Paolo Villoresi and his Group, for the knowledge and hints that they gave me during my visit to the University of Padova and during our experiment. Thanks from the professional and human point of view.

Many thanks also goes to the members of the Quantum Research Group at UKZN in particular Dr. Abdul Mirza and Ms. Yaseera Ismail for the reciprocal collaboration and support during the experiments. I am also grateful to Dr. Mhlambululi Mafu for the support during the writing and for correcting the first draft of my thesis. I would also like to thank my friend Dr. Filippo Giraldi for all the fun we had during my studies.

Profound thanks also go to my father Alfredo and my fiancee Melanie for the moral support and encouragement. I would also like to thank my former professors for preparing me for this adventure called PhD.

Without economic support it is impossible to fly. This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

Contents

List of Figures

List of Tables

List of abbreviations

Alice: Transmitter of the secret key

APD: Avalanche Photo Diode

ADC: Analog to Digital Converter

BB84: four state QKD protocol

Bob: Receiver of the secret key

Bus: Infrastructure of the spacecraft

BS: Beam Splitter

C: Capacitor

DGPS: Differential Global Positioning system

E^2PROM: Electrically Erasable Programmable Read-Only Memory

GPS: Global Positioning system

HWP: Half Wave Plate

IDE: Integrate Development Environment

LCD: Liquid Crystal Device

ℕ: Natural number

OP: Optocoupler

PBS: Polarizing Beam Splitter

PLL: Phase-Locked Loop

PM: Phase Modulator

PSD: Position Sensitive Device

QBER: Quantum Bit Error Rate

QKD: Quantum Key Distribution

R: Resistor

RAM: Random-access memory

$\vec{R_{Rf}}$: Position of the reference station

$\vec{R_{RX}}$: Position of the receiver

$\vec{R_{TX}}$: Position of the transmitter

SPAD: Single-Photon Avalanche Diode

TDC: Time to Digital Converter

TTL: Transistor-transistor logic. Used in the text to indicate a digital signal

TX: Transmitter

U: Integrated circuits label

VCO: Voltage-Controlled Oscillator

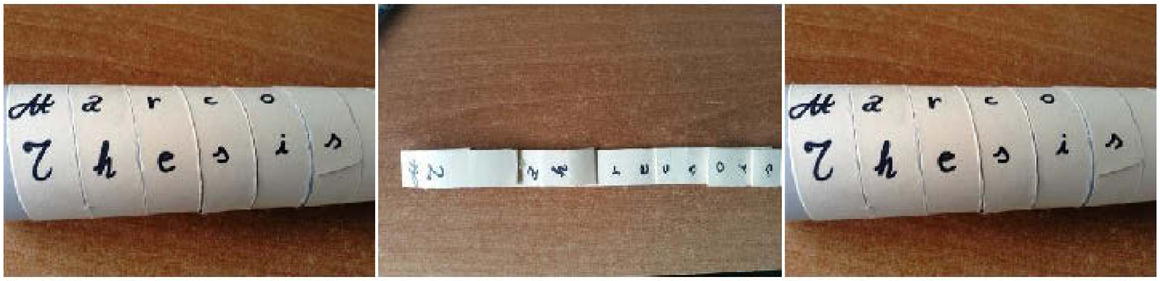
Chapter 1

Introduction

The origin of the word *cryptography* comes from the Greek kryptòs (hidden, secret) and graphè (writing) and it indicates a procedure for hiding a confidential message [1]. Cryptography was used from the 5^{th} century B.C. in order to send secret messages during war. These days, cryptography is used for banking transactions and anywhere else it is necessary to transmit a confidential message. In cryptography, the message is hidden by using an algorithm and a key. The algorithm can be made public but the key must be private, it should only be available to the sender and receiver. If an eavesdropper intercepts the key, the cryptosystem fails. The main problem of cryptography is to share the key between the sender and receiver. For ease of reference, from here on, the sender will be called Alice, the receiver, Bob and the eavesdropper, Eve.

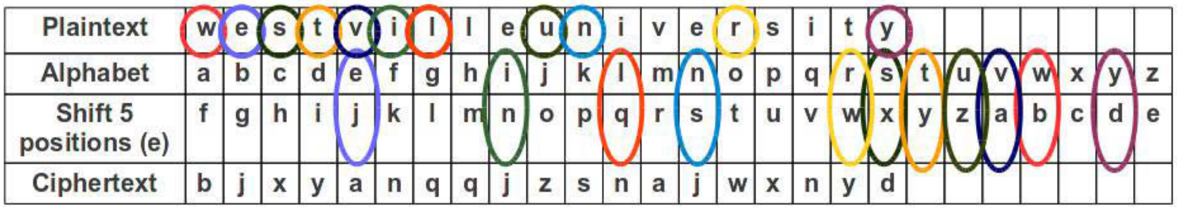
1.1 History

A plaintext can be encrypted and decrypted using a symmetric and asymmetric key. When the key, used to encrypt the plaintext, is the same used for the decryption it is known as symmetric key encryption. When the key, used to encrypt the plaintext is different form the key used to decrypt the ciphertex, the key is known as an asymmetric key. In our days, the banking transactions and confidential messages are hidden using an asymmetric cryptographic system. One of the earliest cryptographic systems called *Scitola Lacedemone* [2] can be traced back to 400 B.C. In this system, the message was written on a leather tape wrapped on a cylinder as shown on Figure 1.1. The sender sent only a leather tape to the receiver. Then, the receiver wrapped the leather tape on a cylinder with the same diameter of the cylinder used to encrypt the message. In the *Scitola Lacedemone* the key was the diameter of the cylinder.



Plain text (prior to encryption) Ciphertext Plaintext

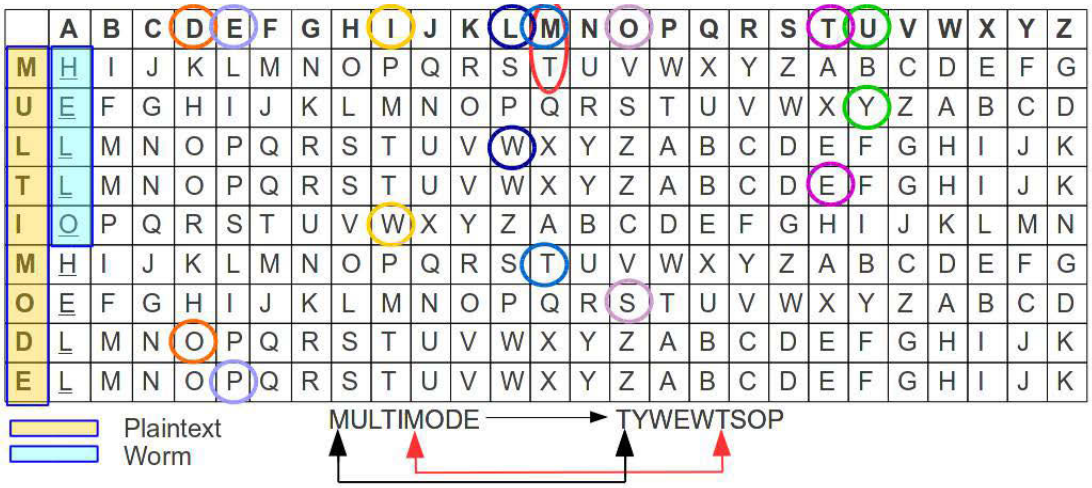
Figure 1.1: *Scitola lacedemone:* The message is written along the hight of the cylinder on the leather tape. The leather tape is sent as cyphertext as shown in the second picture. The receiver wraps the leather tape on a cylinder of the same diameter used for encrypting the message and it is possible read the plaintext.



Plaintext	w	e	s	t	v	i	l	l	e	u	n	i	v	e	r	s	i	t	y							
Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Shift 5 positions (e)	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
Ciphertext	b	j	x	y	a	n	q	q	j	z	s	n	a	j	w	x	n	y	d							

Table 1.1: *Caesar cipher:* The ciphertext is made by the looped traslation of the characters of the alphabet. In this case, the alphabet starts with the letter a, and is shifted by five positions to letter f. After the letter z, the alphabet starts from a until e. For each letter a number is assigned (a=0,b=1,...,z=25). This translation can be considered as a summation mod 26 between the alphabet and the key.

This system is easy to compromise and once the eavesdropper knows the diameter of the cylinder the code is broken. A cryptosystem that forms the base for the quantum cryptography is called *Vigenere cipher*. Vigenere cipher is a generalization of the *Caesar cipher*, where the characters of the alphabet are changed by a translation of it. For example, in order to send a plaintext e.g., *"westville university"* to the receiver, we need to choose the number of translations of the alphabet. The Caesar algorithm is shown in Table 1.1. The *Caesar's* cipher uses only one translation of the alphabet for the entire plaintext and the key is the number of shifts of alphabet's letters. On the other hand, the *Vigenere's cipher* uses a word called "worm" as a key. The worm is repeated for the full length of the plaintext. The result is presented in Table 1.2. The plaintext to send is "MULTIMODE" and the worm is "HELLO". Alice and Bob have to decide the secret key in advance before they share the message. Mathematically speaking, given an alphabet with n characters, once a number



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
U	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
T	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
I	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
M	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
O	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
D	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
E	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Plaintext
Worm
MULTIMODE
TYWEWTSOP

Table 1.2: Vigenere's cipher representation: The black and the red arrow indicate the recurrence due to the repetition of the key in the plaintext. By the periodical repetition of the letters, Eve can be able to decrypt the message and found the key.

mod n is assigned per each character, it is possible to combine the characters of the plaintext with a sum $\mod n$ of the characters of the key. In the Vigenere's cipher, the recurrence of the worm produces a repetition of the letters in the cipher text. Using the recurrences, the eavesdropper may be able to decrypt the message.

The Vernam cipher, also known as one time pad (OTP), follows the same algorithm of the Vigenere cipher, where the length of the key (worm) is the same as the plaintext. The key consists of a series of bits which are randomly chosen. In this cipher, the bit of the key and the bit of the message are combined by an XOR operation. This is shown in Figure 1.2. In order to decrypt the message, the XOR operation between the ciphertext and the key must be done. In order for the *Vernam's* cipher to be a perfect cryptographic system, Alice and Bob must share a key which is as long as the message to be encrypted and Alice and Bob should also transmit the secret key using a public untrusted channel. A flexible way for Alice to send the key is a public key system. Modern algorithm uses a public key to share a hidden message. A public key is generated from a private key by using a particular algorithm. If an eavesdropper intercepts the public key, it is not possible to calculate the private key in a short time.

The first public key algorithm was proposed by Diffie, Hellman and Merkle (DHM) in the 1970's. This protocol uses a symmetric key which means that the key used to encrypt the message is the same used for decryption. The algorithm uses the modulus and it permits an

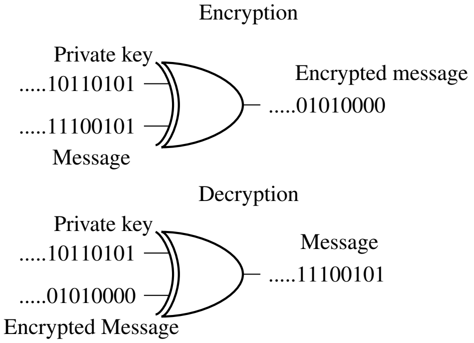


Figure 1.2: Example of a symmetric key encryption and decryption: The plaintext .....10110101 is encripted by a summation $\mod 2$ with a random key .....11100101. The receiver by a summation $\mod 2$ of the cyphertext and the key is able to decrypt the message.

exchange of a secret key. The unidirectional function used is:

$$N = Y^x \mod (p). \tag{1.1}$$

The variables Y and p are agreed to by Alice (A) and Bob (B) and N is equal to α for Alice or β for Bob, p is a prime number and $Y < p$. The flow chart of the algorithm is presented in Figure1.3. The number Y and the modulus p are chosen by Alice and Bob via a public channel. As an example Alice chooses a value $A = 6$ and she keeps it secret. Bob chooses $B = 8$ and also keeps it secret. Then, Alice will calculate the number $\alpha = 11^6 \mod (29) = 9$. Similarly, Bob calculates $\beta = 11^8 \mod (29) = 16$. Alice then transmits to Bob the number α and then receives β from Bob. The key for Bob becomes $9^6 \mod (29) = 20$ and the key for Alice will be $16^8 \mod (29) = 20$. It is not possible for an eavesdropper to know the key because it is computationally difficult to calculate the private key, but on the other hand, Alice and Bob need to share the value of p, Y, α and β before they share the message. The RSA protocol uses asymmetric keys. The encryption is made by using a public key and the decryption is achieved by using a private key. The private key is only known to the transmitter of the key. The RSA protocol exploits the prime number property. Alice chooses two random prime numbers p and q in order to obtain a number $N = p \cdot q$ called modulus [1]. She chooses another prime number $e < N$, with respect to the Euler function $\phi(N) = (p-1)(q-1)$. A private exponent called d is calculated by the condition $d \cdot e \equiv 1 \mod [(p-1) \cdot (q-1)]$. The couple (N, e) is called a public key while the couple (N, d) is a private key. Alice sends the

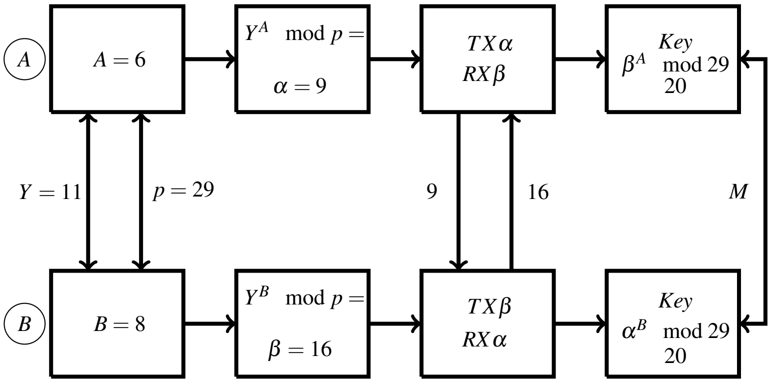


Figure 1.3: Block scheme of Diffie, Hellman and Merkel algorithm: A- Alice; B- Bob; M-Message. Alice and Bob agreed on the values $Y = 11$ and $p = 29$. Alice Chooses $A = x = 6$ and she kept it secret and by using the Equation (1.1) calculates the number $\alpha = 9$. Bob chooses $B = x = 8$ and calculate the number $\beta = 16$. Alice transmits to Bob the number α and Bob, the number β to Alice. The secret key for Alice become $16^A \mod 29 = 20$ and for Bob $9^B \mod 29 = 20$. Alice and Bob share the same key. This method is computationally secure.

Table 1.3: Message to be encrypted: Each character corresponds to a decimal number. The number are encrypted using the RSA protocol.

Letter	H	e	l	l	o		W	o	r	l	d
ASCII	72	101	108	108	111	32	87	111	114	108	100

public key to Bob, which is used to encrypt the message m by using the

$$c = m^e \mod (N). \tag{1.2}$$

Alice receives the ciphertext c from Bob and by using

$$m = c^d \mod (N), \tag{1.3}$$

she decrypts the message. Suppose that Bob wants to send a message *Hello World* to Alice. The ASCII code of this word is composed by decimal numbers shown in Table 1.3.

Alice chooses the prime number $p = 11$ and the prime number $q = 13$ to obtain $N = 11 \cdot 13 = 143$. The Euler function is $\phi(N) = (p-1)(q-1) = 10 \cdot 12 = 120$. Choses a number e, such that $e < N$, $e = 7$. Alice found a number d such that $e \cdot d \equiv 1 \mod \phi(N)$. The number $d = 103$. The public key is (7,143) and the private key is (103,143). Using the Equation (1.2)

Table 1.4: Encrypted message: Each character corresponds to a decimal number. The number is encrypted by using the RSA protocol.

Letter	!!	>	⧫	⧫	–	b	W	-	1	⧫	d
ASCII	19	62	4	4	45	98	87	45	49	4	100

the message is sent as shown in the Table 1.4.

In the previous Section an example of an encrypted message was shown. Regarding the encrypted message, if a single key bit is used for all letters, it is possible to decrypt the message by a statistical analysis i.e., using the recurrence for each particular language as shown in Figure 1.4. For Eve, it is theoretically possible to decrypt the RSA protocol message by a factorization of the public key, but with modern calculators it is not possible to calculate the private key in reasonable time. This problem of finding the key in a reasonable time can made by a quantum computer. The quantum computer will be able to factorize the key in a polynomial time [3] and the RSA protocol can be broken.

1.2 Attack methods

The eavesdropper can perform the following six categories of attacks;

- Ciphertext-only: Eve can try to obtain the information about the plaintext or the key given only the plaintext.

- Know-plaintext: Eve has a collection of plaintexts and the corresponding ciphertexts, and she may try to calculate the key or decrypt other ciphertexts.

- Chosen-plaintext: Eve is able to obtain the ciphertext of a chosen plaintext.

- Adaptative chosen plaintext: Eve is able to decrypt the ciphertext and can change the plaintext by using the knowledge of the ciphertext and tries to find the key.

- Chosen-ciphertext: Eve is able to obtain the plaintext of the chosen ciphertext.

- Brute force: Eve tries to decrypt the message using all possible combinations of the key.

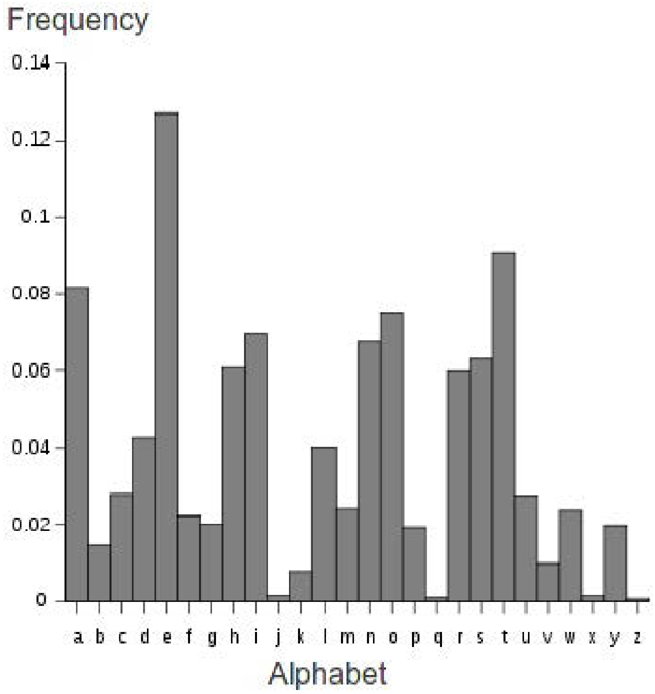


Figure 1.4: Histogram of the occurrences of the letters in the English language: If in a plaintext, the message is encrypted using a key of the length one, the ciphertext we will observe the same behavior of the recurrence but with different letter. If the letter “e” after the encryption corresponds with the letter “b”, the message contains more of the letter “b“ than others. Eve, by the knowledge of the language used, she is able to know that the letter of the plain text is “e” . This method is also used to decrypt the historical manuscripts. This figure is inspired from [4].

1.3 Evaluation of a cryptographic system

In a cryptographic system, it is possible to define the different kinds of security. These are

- Computational security: A crypto system is computationally secure if the best known algorithm that permits the violation of the ciphertext has complexity greater than a certain limit N, which is large enough. At the moment there exists no cryptographic system which is computationally secure.
- Demonstrably safe: the security of a cryptographic system is equivalent to the challenge required to solve the problem.
- Unconditionally safe: there exists a formal proof of security that is theoretically sound and technology independent.

1.4 The perfect cryptosystem

The attack methods of an eavesdropper have been defined in the Chapter 1.2. An invulnerable cryptosystem is defined as a perfect cryptographic system. Given a set of the plaintext M, and a set of the ciphertext C, it is possible to evaluate the probability to find a plaintext by the knowledge of the ciphertext. The definition of perfect cryptosystem was done by Shannon using the following equation:

$$P(M = m|C = c) = P(M = m). \tag{1.4}$$

Equation 1.4 said that the conditional probability to find a plaintext m from a ciphertext c is the same probability to find the plaintext m. The probability of the plaintext $P(M = m)$ and the probability of the cyphertext $P(C = c)$ are two independent events. The perfect cryptosystem requires that the length of key used, must be greater or the same length as the possible plaintext. For every new message, a new key must be used (one-time pad) [2]. The Vernam cipher uses a new key for every message, and the bits of the key are randomly chosen. The Vernam cipher is a perfect cryptographic system [5]. In this cryptosystem, the message and the key are transmitted as a series of bits according to a particular character code (e.g., Baudot or ASCII). The summation between the bit of the key and the bit of the plaintext is modulated by the length of the alphabet. To obtain a perfect cryptosystem, the bits of the key must be random and shared before the transmission of the message between Alice and Bob. The main problem with this scheme or cryptosystem is to send the key between Alice and Bob who are separated by a distance.

1.5 Quantum cryptography.

In Chapter 1.4, it was mentioned that the *Vernam* cipher can be a perfect cryptographic system if and only if the key is as long as the message and if its bits are randomly chosen. The problem is to distribute the secret key between Alice and Bob through an un-secure channel. Quantum key distribution (QKD), exploits the laws of quantum physics in order to afford security to the key. These laws include the uncertainty principle and the no-cloning theorem [6, 7]. In QKD, the key is transmitted as property of quantum state, where the value of the bits depends on a particular quantum state. Therefore, by the uncertainty principle, it is not possible for Eve to measure the quantum state of a particle being sent by Alice to Bob without perturbing the state. Again, by the no-cloning theorem, it is not possible to make a copy of the quantum state. This means that Eve cannot intercept the qubit being sent by Alice to Bob and make a perfect clone, and then send the copy to Bob without being detected.

1.5.1 No-cloning theorem

The state of a quantum system such as the polarization state of a single photon cannot be cloned in general by a quantum machine. Suppose that we have a cloning machine with an initial state $|M\rangle$, and we would like to copy the polarization state of a single photon in a known quantum state $|0\rangle$. In our context, we will indicate vertical polarization by using $|v\rangle$ and the horizontal polarization by $|h\rangle$. By applying a unitary transformation U, to copy a vertical quantum state $|v\rangle$, we have

$$U(|M\rangle|v\rangle|0\rangle = |M_v\rangle|v\rangle|v\rangle, \tag{1.5}$$

where $|M_v\rangle$ is the quantum state of the cloning machine after the measurement. The same process can be done in order to copy a horizontal state. This is expressed as

$$U(|M\rangle|h\rangle|0\rangle) = |M_v\rangle|h\rangle|h\rangle. \tag{1.6}$$

If the quantum state of the single photon is a superposition $|\psi\rangle = \alpha|v\rangle + \beta|h\rangle$, then by following Equation (1.5) and (1.6) we obtain

$$U(|M\rangle(\alpha|v\rangle + \beta|h\rangle)|0\rangle) = \alpha|M_v\rangle|v\rangle|v\rangle + \beta|M_o\rangle|h\rangle|h\rangle. \tag{1.7}$$

If $|M_v\rangle = |M_o\rangle = |M_f\rangle$, it is possible to factorize the result of the previous equation as

$$U(|M\rangle(\alpha|v\rangle + \beta|h\rangle)|h\rangle = |M_f\rangle(\alpha|v\rangle|v\rangle + \beta|h\rangle|h\rangle. \tag{1.8}$$

The desired result is:

$$\begin{aligned} U(|M\rangle(\alpha|v\rangle + \beta|h\rangle)|0\rangle) &= |M_f\rangle(\alpha|v\rangle + \beta|h\rangle)(\alpha|v\rangle + \beta|h\rangle) = \\ &\quad |M_f\rangle(\alpha^2|v\rangle|v\rangle + 2\alpha\beta|h\rangle|v\rangle + \beta^2|h\rangle|h\rangle). \end{aligned} \tag{1.9}$$

By comparing Equations (1.8) and (1.9), we recognize that α or β must be equal to zero. This means that copying is not possible if the quantum state is in a superposition.

The previous example of the cloning machine can be generalized by the No-Cloning theorem.

Theorem 1. *No-Cloning theorem. Let $|\phi\rangle$ and $|\psi\rangle$ be two generic states, $|0\rangle$ a state belonging to a known basis and U a unitary operator such that [8]:*

$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{1.10}$$

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{1.11}$$

Then, it must be $\langle\phi|\psi\rangle = 0$ or $\langle\phi|\psi\rangle = 1$

Proof: By the inner product of Equations (1.10) and (1.11) we obtain

$$(\langle 0| \otimes \langle\phi|)U^{\dagger}U(|\psi\rangle \otimes |0\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle), \tag{1.12}$$

$$\langle 0|0\rangle\langle\phi|\psi\rangle = \langle\phi|\psi\rangle\langle\phi|\psi\rangle, \tag{1.13}$$

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2 \tag{1.14}$$

This relation is valid if the states $|\psi\rangle$ and $|\phi\rangle$ are orthogonal or parallel.

1.5.2 BB84 protocol

Quantum cryptography is a symmetric key system, where the private key is used to encrypt and decrypt the message. The power of quantum cryptography is the capacity to recognize the presence of the eavesdropper during the transmission of the key. QKD was proposed by Bennett and Brassard in 1984 and therefore the first protocol is known as BB84 [9]. In this protocol, Alice sends to Bob a private key as a series of single polarized photons. The protocol uses two nonorthogonal bases. The polarization state of the single photons represents the value of the bit of the private key. For each single photon, Alice randomly chooses the polarization basis and the value of the quantum bit. Bob randomly chooses the measurement basis for the single photons. One basis is indicated with the symbol $+$ and represents the vertical and horizontal polarization. The photon sent with the vertical polarization ($\uparrow$) corresponds to the bit "1", and the photon sent with the horizontal polarization ($\rightarrow$) corresponds to bit "0". The second is a diagonal basis, indicated with the symbol $\times$ is tilted by 45° with respect to

Table 1.5: Representation of key exchange process for BB84 protocol: Alice sends the key to Bob by using a rectilinear basis and a diagonal basis indicated by $+$ and $\times$ respectively. The symbols $\rightarrow$ and $\uparrow$ are equivalent to the bit 0 and 1 respectively, for the rectilinear basis. The symbols $\nwarrow$ and $\nearrow$ are equivalent to the bit 1 and 0 respectively, for the diagonal basis. Alice randomly chooses the bases and the bits to transmit to Bob. Bob randomly chooses the bases to measure the single photons. When Alice and Bob choose different bases, Bob receives a correct bit with a 50% of probability. Once the key is transmitted, by the public channel Alice transmits the bases used to Bob, and the final key is composed by the bits, received and transmitted by using the same bases. Others error may occur during the transmission that will be removed from the key by the process called key distillation [10]. This table is inspired from [9].

Alice	Basis	$+$	$+$	$\times$	$\times$	$\times$	$+$
	Quantum bit	$\rightarrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\uparrow$
	key bit sent	0	1	1	0	0	1
Bob	Basis	$+$	$+$	$\times$	$\times$	$\times$	$+$
	Quantum bit	$\rightarrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\uparrow$
	key bit received	0	1	1	0	1	1
	Final key	0	1	1	0	1	1

the first one. The photon polarized with the direction $\nwarrow$ corresponds to the bit "1", otherwise the bit sent with the direction of polarization $\nearrow$ is "0". Once the key is transmitted, Alice sends the list of bases used to Bob via a public channel. The final key is composed of the bits transmitted and received with the same basis. The process of the key exchange is represented in Table 1.5. If there is a misalignment in the measurement bases, the number of errors increase, therefore Alice and Bob register the presence of Eve in the channel. However, even though Alice and Bob choose the same measurement bases, errors may still occur. In order to remove these errors a process called key distillation is implemented. In this process, Bob should know the timing of the photon transmission and the bases must be aligned. The timing can be obtained by radio or optical synchronization [11]. Further error correction and privacy amplification can be used to increase the confidentiality of the key.

1.5.3 Quantum bit error rate

The quantum bit error rate (QBER) is defined as the ratio of the error rate to the key rate [12]. QBER represents the scale of the amount of the information that an eventual eavesdropper knows. It is possible to estimate the quantum bit error rate by

$$QBER = p_f + \frac{p_d \eta q \Sigma f_r t_l}{2} \mu, \tag{1.15}$$

where p_f represents the probability of a false reading. P_d is related to the detector and represents the probability for a wrong photon signal, n is the number of detections, q is a coefficient related to the type of encoding, Σ is the detector efficiency, f_r is the pulse repeat frequency and the term t_l is the transmission rate. The value $\mu = 1$ represents the attenuation for the pulse of the light. For the same condition presented in [12], for the BB84 protocol, if the $QBER = 11\%$ the transmission is safe. By the Equation (1.15) it is possible to observe that the characteristic of the measurement setup is critical in order to mitigate the QBER, and it is the only way to estimate the presence of Eve. Other errors can occur if the basis of Alice and Bob are not correctly aligned. Considering for example that Alice sends a vertical polarized photon to Bob, while Bob prepares the orthogonal bases to receive the single photon. The single photon sent by Alice is

$$|V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.16}$$

Referring to the scheme shown in Figure 1.5, Bob measures the vertical and horizontal polarization by using a PBS and an avalanche photo diode. If a bases misalignment of an angle θ occurs, Bob measures a single photon in the following superposition state:

$$|\phi\rangle = \cos^2\theta|V\rangle + \sin^2\theta|H\rangle. \tag{1.17}$$

This means that the probability to obtain the correct measurement is related to the angle θ and this is reflected in the value of the QBER. It is necessary to have a system able to align the polarization bases.

1.5.4 Quantum cryptography in fiber optics

The transmission of the secret key, using the BB84 or other protocols, can be done using fiber optics or free space. In the previous section, the polarization of a single photon was considered as a quantum state. This method is recognized as polarization encoding. In this section we describe the polarization encoding in fiber optics and another system that exploits the phase between two pulses. In the polarization encoding, the transmission of the secret key, according to the BB84 protocols, is made by the scheme proposed in Figure 1.5. In this scheme fiber optics is used as a channel. Alice randomly chooses to transmit the quantum bit (qubit) with vertical or horizontal polarization using the laser L1 or L2, respectively. If Alice chooses to transmit the single photon using the diagonal basis, she uses the laser L3 and L4. Supposing that Alice chooses to transmit a horizontally polarised single photon to Bob. An

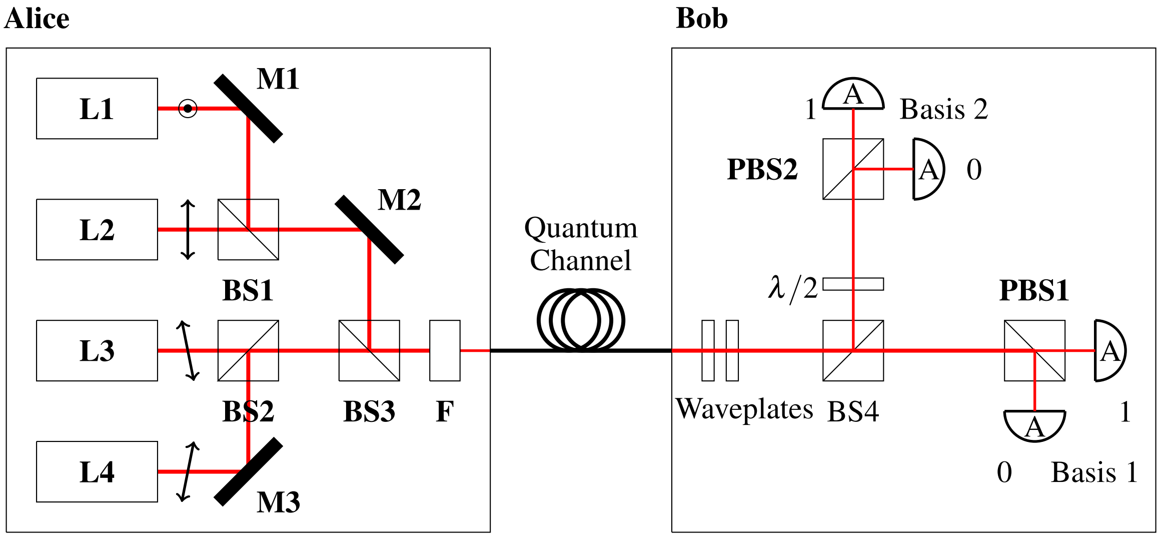


Figure 1.5: Optical scheme in fiber optics for BB84 protocol: Supposing that Alice wants to send a vertical polarised photon to Bob using the laser **L2**. The pulse crosses the beam splitter **BS1** and is reflected from the mirror **M2** and **BS3**. The pulse crosses the filter **F** in order to obtain less than one photon per pulse for 30 cm of path in free space [13]. The single photon loses the polarisation state which is recovered by Bob through the waveplates. The single photon now can "choose" to be reflected to the diagonal base or cross the **BS4** in order to be measured by a rectilinear base. The $\lambda/2$ plate is used to rotate the polarization of the single photon in order to measure with standard equipment [13]. The letter A describes the Single-Photon Avalanche Photo Diode detector, the "Basis 2" represents the diagonal basis and "Basis 1" the orthogonal basis. This figure is inspired from [13].

impulse from the Laser L1 is reflected by the mirror M1 and through the beam splitter BS1 is reflected in the direction of the mirror, M2. The mirror, M2, reflects the impulse to the beam splitter BS3 and in the end the laser impulse crosses the filter F. This filter is used to obtain an average photon lower than 1 per pulse over a distance of $30cm$ in free space [13]. Finally the single photon can be transmitted along fiber optic. During the way, the single photon loses the polarization state due to the fiber. When Bob receives the single photon it is necessary to recover the initial polarization using a series of waveplates. As shown in Figure 1.6(a), when a laser source crosses an ideal beam splitter (BS), there is a 50% probability that the photons cross the BS while the other 50% will be reflected. By referring to Figure 1.5, when a single photon is measured by Bob, he has a 50% probability of measuring a single photon on Basis 1 (direction **D1**) and 50% on Basis 2 (direction **D2**) according to Figure 1.6(b). If the single photon is not reflected Bob chooses the orthogonal basis, and in this particular case the measure is 0 since the photon was horizontally polarized. The measurement is made by Single-Photon Avalanche Photo Diode (SPAD) indicated with the letter A. When the errors

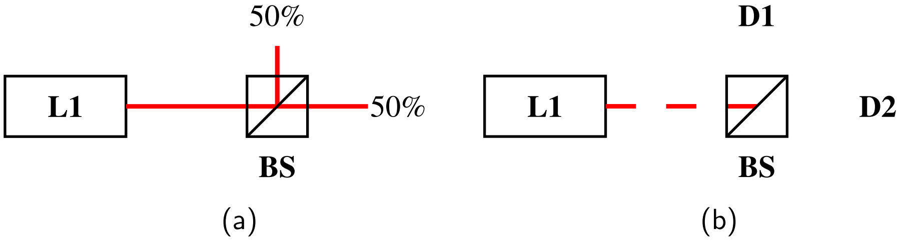


Figure 1.6: Measures the beam splitter output signal for a continuous laser source (a) and single photon (b): (a) For a continuous laser source it is possible measure 50% of the photons reflected and 50% cross the beam splitter. D1 and D2 represents the detectors of the single photon.(b) For a single photon source, the probability at measuring a reflected signal is 50% as well as the probability of measuring a non reflected single photon ; When Alice sends a single photon, Bob chooses the measurement bases as a function of the path taken by the single photon on the beam splitter BS4 in Figure 1.5.

of alignment occur, the quantum bit error rate (QBER) increases, and this can induce Alice and Bob to believe that Eve is present in the channel and the polarization encoding for a long link distance is stable only for a couple of minutes due to the thermal and mechanical stress of the fiber optics [13]. The polarization encoding in fiber optics is not an ideal method.

Phase encoding exploits an optical fiber Mach-Zehnder interferometer. Alice and Bob have a phase modulator respectively called $PM\phi_A$ and $PM\phi_B$. A coherent laser source “L” is split along the “Path 1” and along “Path 2”. On “Path 1” the signal has a phase ϕ_A and along “Path 2” has a phase ϕ_B. The conceptual scheme is shown in the Figure 1.7. By using the phase modulator, it is possible to change the phase of the pulse of both paths. Considering a different length ΔL between “Path 1” and “Path 2”, on the sensor labeled with 0, it is possible to measure the intensity:

$$I_0 = I \cdot \cos^2 \frac{\phi_A - \phi_B + k\Delta L}{2}, \tag{1.18}$$

and on the sensor labeled with 1, it is possible measure the intensity

$$I_1 = I \cdot \sin^2 \frac{\phi_A - \phi_B + k\Delta L}{2}, \tag{1.19}$$

where k is the wave number and I is the intensity of the source. If the difference of phase $\phi_A - \phi_B = \pi/2 + n\pi$ the measure on the photo detector “0” is $I_0 = 0$ and a maximum signal is collected from the sensor 1. The bit of the key depends on which sensor has measured the maximum intensity. The photo detectors are single photon avalanche diodes and Alice transmits single photons. The avalanche photo diode gives a TTL output signal when measuring a single photon. In other words, by the difference of phase $\phi_A - \phi_B$ the TTL signal can be

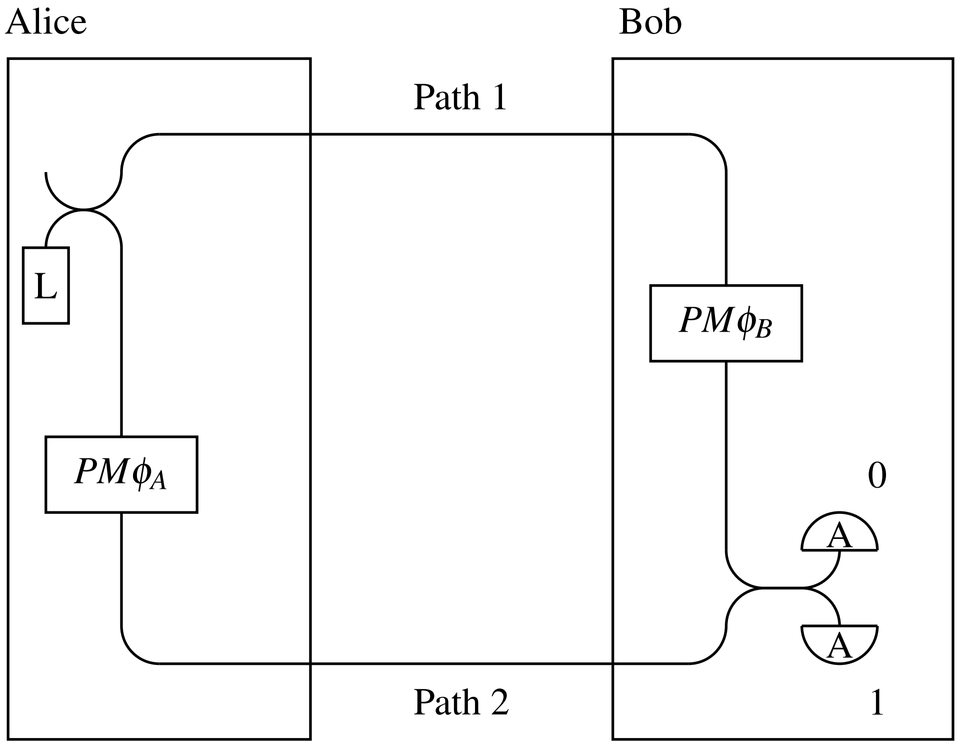


Figure 1.7: Representation of the conceptual scheme for phase encoding: This scheme is a fiber machzender interferometer. $PM\phi_A$ and $PM\phi_B$ are the phase modulators used to determine the base and the value of the quantum bit. This figure is inspired from [13].

measured by the sensor “0” or “1” according to the Equations (1.18) and (1.19). We consider now the BB84 protocol using the phase encoding. Alice sends a pulse that is split along “Path 1” and “Path 2”. By phase modulator $PM\phi_A$ Alice changes the phase $\phi_A = 0$ and $\phi_A = \pi$ to encode 0 and 1 respectively and the phase $\phi_A = \pi/2$ and $\phi_A = 3/2\pi$ to encode the bits 0 and 1 respectively; Bob chooses the basis by using the phase modulator $PM\phi_B$ with $\phi_B = 0$ or $\phi_B = \pi/2$. Table 1.6 shows an example of key transmission using the phase encoding[13]. Considering $\Delta L = 0$ and the output I_1 and I_2 normalized with respect the initial intensity I. Alice sends bit 0 to Bob with a phase 0. Bob prepares his phase $\phi_B = 0$ and received the pulse. In this case Bob choses the same basis as Alice and he hence measures:

$$I_0 = I\cos^2\frac{0-0}{2} = 1 \tag{1.20}$$

$$I_1 = I\sin^2\frac{0-0}{2} = 0. \tag{1.21}$$

Table 1.6: BB84 protocol using phase encoding: The protocol uses two bases in order to send the bits 0 and 1. One basis for Alice is 0 and π to send a bit 0 or 1 respectively, and the other basis is $\pi/2$ to send the bit 0 and $3/2\pi$ to send the bit 1. For Bob the bases are chosen using the phase 0 or $\pi/2$. The Mach-Zehnder interferometer works as an optical switch and if Alice and Bob choose the same basis, Bob is able to measure the exact bit sent from Alice. If the bases chosen are different, Bob measures a coincidence on the sensor 0 and 1 according to the Equation (1.18) and (1.19). This table is inspired from [13].

Alice		Bob		
Bit value	ϕ_A	ϕ_B	$\phi_A - \Phi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

If Alice sends a bit 0 ($\phi_A = 0$) to Bob and Bob chooses the phase $\phi_B = \pi/2$, corresponding with a different basis of Alice, Bob measures

$$I_0 = I\cos^2\frac{0-\pi/2}{2} = \frac{1}{2}, \tag{1.22}$$

$$I_1 = I\sin^2\frac{0-\pi/2}{2} = \frac{1}{2}. \tag{1.23}$$

This means that the bases are incompatible. From the Equations (1.18) and (1.19) if follows that the length of the paths changes, the measurements are affected by the errors. In practical applications, where the length of the path can be of the order of kilometers, the length of the path due to the thermal or mechanical stresses can change during the key exchange. This can affect the measurement because the changes cannot be more than a fraction of the wavelength of the photons. Commercial systems are more reliable and use particular strategies that are not discussed here since it is beyond the scope of this study [14, 15] .

1.5.5 Quantum cryptography in free space

The distribution of the quantum key is attached via by an optical link between two parities. According to the theory of propagation of a laser in the atmosphere [16, 17], the effects of the atmospheric media, on the polarization of the light can be neglected. For this reason in free space polarization encoding is preferable. On the other hand, in the atmosphere, due to turbulence along the laser beacon is affected by wandering and scintillation. As mentioned in Section 1.5.2, considering a set of the bits of the key, the presence of Eve is recognized by Alice and Bob by the mismatch of the bit transmitted and received. Due to the nature of the communication, it is necessary that the polarization bases of Alice and Bob must be aligned and the optical link between Alice and Bob needs to be stable in order to decrease the quantum bit error rate (QBER). In order to check a set of the bits of the key it is also necessary to keep the time stamping of each bit transmitted and this is made by a synchronization system. Quantum cryptography in free space allows maximum flexibility. Quantum cryptography in free space can be used to link two non stationary points as well as an aerospace system or for terrestrial application where it is not possible to use fiber optics. The parts of the system considered in this thesis for free space quantum cryptography can be summarized as follows:

- Synchronization system.
- Polarization alignment system
- Tracking system for optical alignment of Alice and Bob.

To synchronize the transmission it is possible to use a signal from the Global Positioning System (GPS), radio signal [18] or by temporal filtering [19]. Temporal filtering can be realised using the same clock for Alice and Bob, and adjusting the synchronization manually. When Alice or Bob are located on a satellite the time filtering cannot be done due to Doppler effects [20]. GPS synchronization for satellite communication can be used for satellites only if the Doppler effect is compensated. The GPS is a USA property and quantum cryptography can be used for military purposes. For this reason it is necessary have an autonomous system able to work without support of another country's systems. Thus in this work the synchronization using GPS is not considered.

The polarization bases of Alice and Bob must also be aligned in order to transmit and receive the single photon correctly. A recent system [21], proposed the system shown in Figure 1.8. Alice sends a polarised laser beacon to Bob, and she changes the angle of polarization through a polarization modulator. The polarisation direction changes between an angle θ_1 and θ_2. Bob receives the laser beacon and according to the polarization received, the intensity measured from the photodetectro (PD) depends on the direction of the polarisation of the polariser. Figure 1.9 shows the general wave form measured when alignment and misalignment is present. Alice sends a laser beacon with a polarisation direction $\theta_1 = 0°$ and

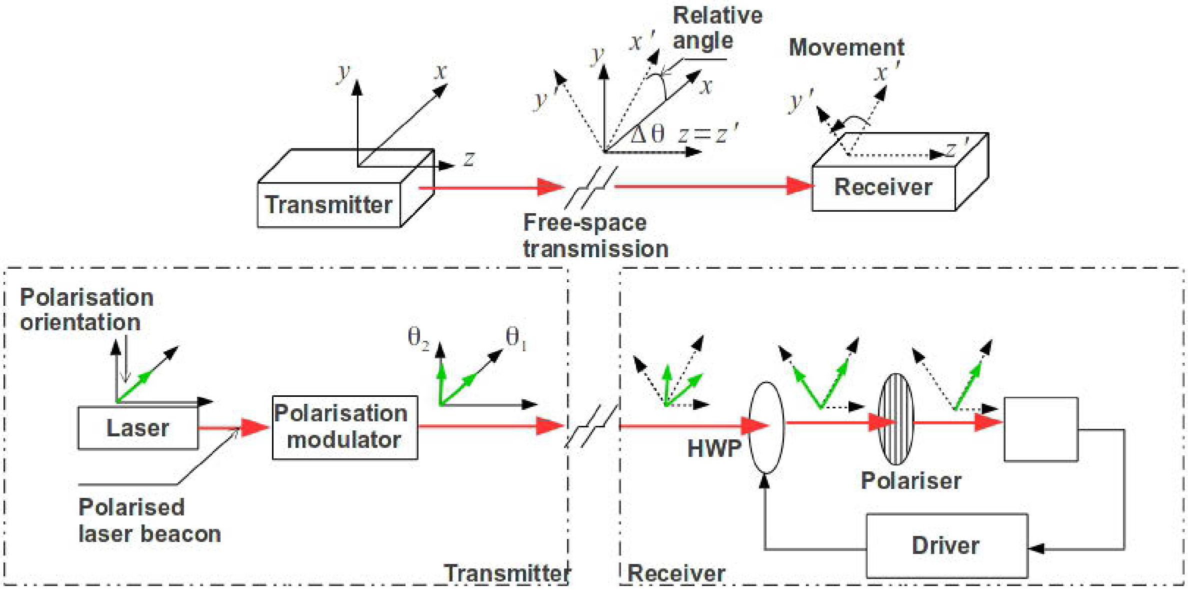


Figure 1.8: Polarization tracking scheme: In this system Alice, sends the single photon and a polarised laser beacon to Bob. The laser beacon through a polarization modulator, changes its polarisation between an angle θ_1 and θ_2. When Bob receives the laser beacon he receives a signal with an intensity that changes according to the angle θ_1 and θ_2. By the difference of the intensity, the system can align the bases by acting on the Half Wave Plate (HWP). The figure is inspired from [21].

$\theta_2 = 90°$. If the bases are aligned $\Delta\theta = 0$, Bob measured a square signal as shown in Figure 1.9(b). If misalignment is present, Bob measures the signal as shown in Figure 1.9(c). By a rotation of half wave plate (HPW), Bob is able to align the bases. In this system the laser beacon can be used for synchronization.

To align the transmitter and the receiver a tracking system is required. The systems for optical communication subdivides the tracking system in two subsystems. A first subsystem is a coarse alignment and second one is a fine alignment system. The coarse alignment system can be done by using the geographical coordinates measured by a GPS of the transmitter and receiver and the alignment can be done by using an electronic compass or by calibration with the stars as reference point [22, 23]. Coordinates measured by the GPS are affected by error and it is not possible to have an accurate alignment for optical communications. A fine alignment system, can function by using a camera or photodetector to hold the signal from the laser beacon and follow the displacement of the aircraft or any mobile system. By the knowledge of the errors from the coarse alignment, it is possible to use a scanning algorithm able to find and track the position of the laser beacon as shown in Figure 1.10. Once the transmitter and the receiver knows the alignment direction and the errors that occur, the

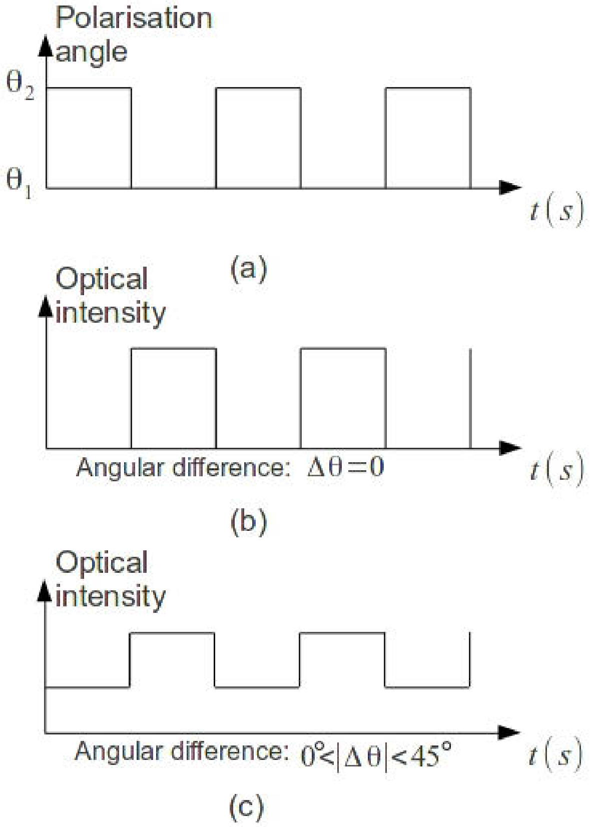


Figure 1.9: Tracking polarisation signals: (a) The polarisation of the signal changes between $\theta_1 = 0°$ and $\theta_2 = 90°$. If the bases are aligned $\Delta\theta = 0$ the signal measured from Bob is (b). If a misalignment occurs the signal measured is (c). By the wave forms, the system is able to recognize the misalignment. The figure is inspired from [21].

scan algorithm provides the fine alignment by searching for the laser beacon. According to [22] the raster scan requires a long time to acquire the position and the spiral scan algorithm does not cover the entire search area, especially if the search area increases. In [22] a binary scan algorithm is proposed. This algorithm considers an area as large as the error due to the coarse alignment system. This area is split in two sub areas and the power, per each area is measured. The portion of the area from which less power is measured is excluded from the next iteration. The remaining area is also split in two parts and another power measurement is done. In this operation the area from which we measure the lower power is excluded from the other iteration. In other words, the position of the laser beacon is found by the exclusion of the area from which less power is measured over a course of iterations.

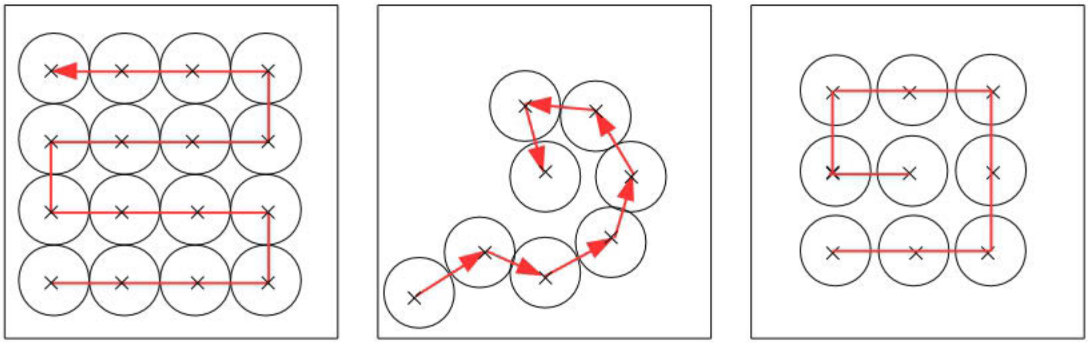


Figure 1.10: Scan algorithm: The pictures show from left to right, the Raster, Spiral and Raster spiral scan algorithm. By the photodetector this algorithm must be able to intercept the laser beacon and hold the alignment between the transmitter and receiver. By the red line is shown the scan methods to track the laser beacon. The figure is inspired from [22].

1.6 Contributions

In the previous section the importance of the tracking system in quantum cryptography in free-space was made evident. From the literature we learnt that a tracking system can be formed using a laser beacon and the coordinates from GPS. The laser beacon can be used for fine alignment between Alice and Bob and to align the polarization bases. In this dissertation we focus on a coarse alignment system and a polarization alignment system. Since quantum cryptography in free-space, might be done for two stationary points or for aerospace vehicles, it was necessary to first study the different scenarios where we intend to operate. Doppler effect, base misalignment due to the reciprocal rotation between Alice and Bob and atmospheric effects were studied. Our system was tested between two stationary points, and from the experiments performed in our laboratory and in free space, we are confident that our systems will also work on mobile vehicles in the future. In this thesis we will discuss the design of a coarse alignment and polarisation alignment system in detail and will touch on a fine alignment system that uses a position sensitive device and a camera.

1.6.1 Synchronization and tracking for satellite communication

Synchronization is an important feature for practical quantum cryptography in order keep the time stamp between the transmitter and receiver. Currently synchronization is achieved using GPS signals, but this is exclude in our project for satellite communication in order to have an autonomous system. A radio signal can be synchronized to the transmitter and receiver and can be used for coarse alignment. The effects of the polarization drift due to the motion of the satellite along the orbit. This work is based on the manuscript **CP1** and **CP2**.

1.6.2 Polarization alignment system

Quantum cryptography in free space exploits polarization coding and for this, Alice and Bob must use a base alignment system in order to reduce the quantum bit error rate. To achieve this system two way solutions that use a polarized laser beacon are proposed. The first solution uses one polariser and a feedback algorithm to track the bases, the second system consists of a polarizing beam splitter and the electronics to measure the misalignment between the polarization bases of Alice and Bob. The collected data was used to find a correction algorithm to minimise misalignment. This system has a provisional patent as a general purpose angular sensor. The experimental result was used to simulate the electronic devices designed for tracking. This work is based on the manuscript **CP2**, **CP3**, **CP4** and **M1**.

1.6.3 Tracking system using the GPS coordinates

Alice and Bob must be optically aligned through a line-of-sight link. Some systems use an electronic compass but in various areas of the Earth strong magnetic deviation exists due to the geology of the land. Other systems use the stars as a reference frame. Our tracking system uses the GPS coordinates of the transmitter, receiver and one reference station. This is an inexpensive and accurate system . The algorithm used to calculate the direction of the receiver was tested experimentally and via cartographic software. It was confirmed that the best accuracy can be obtained with a differential global positioning system (DGPS). This algorithm is used for the coarse alignment system for quantum cryptography and can be used as a fine alignment system for radio communication. The algorithm was used in a microcontroller for our “Plug and Play System”. This work is based on the manuscript **CP1**, **CP2**, and **M3**.

1.6.4 Plug and play system

The coarse alignment and the polarization alignment system was implemented in an electronic circuit board. This board was helpful during the experiments in free space and future improvements can be made to obtain an autonomous system for quantum cryptography. The circuit was simulated and tested experimentally. This work represents a design of a system based from the manuscript **CP2**, **CP3**, **CP4** ,**P1** , **M1**, **M2** and **M3**.

Chapter 2

Tracking and synchronization system for quantum key distribution

Recent experiments have shown that it is possible to share a secret key using quantum cryptography in free space over long distances between two stationary points on the Earth's surface [18]. One benefit of quantum cryptography is that it allows one to share a secret key between two non stationary points in free space. Due to the nature of transmission a reliable system must guarantee the optical link between Alice and Bob. This can be achieved by the GPS or a system that uses radio or laser signals. As described in the previous chapter the alignment requires a coarse alignment subsystem and a fine alignment subsystem. Recent tracking systems exploit the GPS coordinates of the transmitter and receiver combined with the position of the stars, or the GPS coordinates combined with an electronic compass. The sky is not always clear and a coarse alignment using the electronic compass can be affected by errors due to local magnetic deviation. In this chapter an accurate coarse alignment system that only exploits three GPS coordinates is presented. In this system a laser beacon was used. The tracking system was designed through the open-source electronics in order to reduce the cost of the system. Quantum cryptography requires a synchronization system to keep the time stamping of each photon transmitted in order to recognize the correlated base. For satellite communication, when Alice is a satellite and Bob is located on the Earth's surface, the Doppler effect is present, and it is necessary to mitigate this effect [20]. To synchronize the transmission of the quantum bit between Alice and Bob, a phase-locked loop is used. The synchronization signal can be optical or radio. This work is based on the manuscripts **CP1**, **CP2**, **CP3** and **M3**.

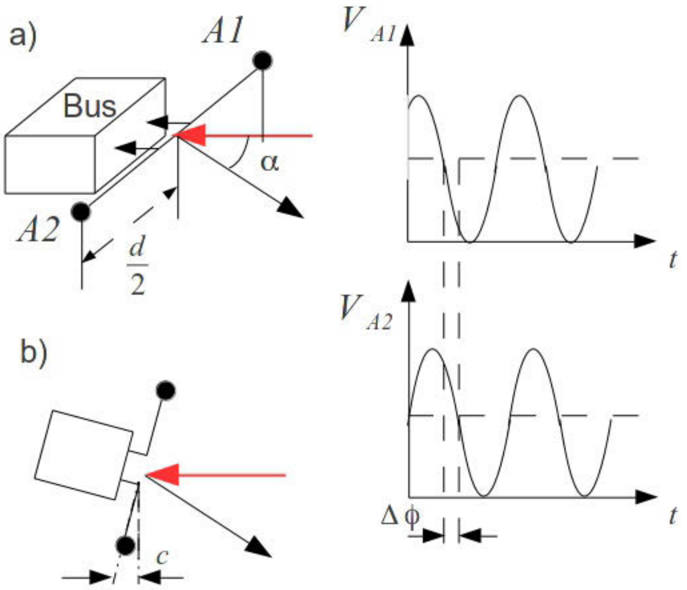


Figure 2.1: Alignment system using a modulated radio signal: $A1$ - First aerial; $A2$ - Second aerial; d - distance between the aerials. As shown in the picture a), if the system is not aligned with the wavefront of the radio signal $(\alpha \neq 0)$ the signal detected from the aerial A1 has a different phase with respect to the signal detected from the aerial A2. By the difference of phase it is possible to calculate the tilt angle α. The picture (b) shows the planar projection of the system. If c has the same order of the wavelength of the radio signal, it is possible to have ambiguities in the measurement, because the signal measured from $A1$ and $A2$ can have the same phase if $c = \lambda$, where λ is the wavelength of the modulating signal. The wavelength of the radio signal needs to be comparable with the length d.

2.1 Tracking system for aerospace system

The system that we will discuss, can be used as coarse alignment between two aerospace system or for up and down link. The system exploits a radio signal received from two different aerials as shown in Figure 2.1. The transmitter sends a modulated radio signal via these two antennas to the receiver with a frequency f. Referring to Figure 2.1, the direction of propagation of radio waves is indicated by the red arrow and the value V_{A1} and V_{A2} is the modulating signal received with different phase. If the receiver is not aligned with respect to the radio propagation, the signal from the aerial $A1$, is received in advance with respect to the aerial $A2$. This difference can be measured as difference of phase according to the Equation

$$\Delta\phi = \frac{2\pi}{\lambda}(d \sin\alpha). \tag{2.1}$$

The carrier is modulated by the signal used for the tracking. In order to obtain a good measurement the wavelength of the signal used for tracking must be comparable with the length d because, if $c = \lambda$, $A1$ and $A2$ measure the same phase.

2.2 Refractive index for the Radio signal

The trajectories of signals are dependent on the atmospheric conditions. The state parameter of atmospheric gas like pressure, temperature and humidity change in function of the altitude and consequently also the refractive index changes [24]. The trajectory will be a curve and the angle of tracking will thus be different from the real position of the satellite. An estimation of the refractive index is therefore made from the average annual atmospheric condition. The refractive index equation is [25]:

$$n = 1 + N10^{-6} \tag{2.2}$$

where:

$$N = \frac{77.6}{T}\left(P + 4810\frac{e}{T}\right) \tag{2.3}$$

and P and T is the pressure and temperature, respectively and they are functions of the altitude. The behavior of these parameters is calculated by the Recommendation Rec. ITU-R 835-3 and for the vapour pressure we have [26]:

$$e = \frac{\rho T}{216.7}, \tag{2.4}$$

Where ρ is the density of the atmospheric gas. Equation (2.2) can be used only for altitudes between 0 km to 50 km. Over 50 km of altitude, the solar activity ionizes the gas leading to the presence of free charges. Calling gyrofrequency f_b, critical frequency f_c and the transmission frequency of the satellite f, the equations of the refractive index in the ionosphere are expressed as [24]:

$$n_{os}^2 = 1 - \frac{f_c^2/f^2}{1 + (f_b/f)\cos\theta}, \tag{2.5}$$

and

$$n_{xd}^2 = 1 - \frac{f_c^2/f^2}{1 - (f_b/f)\cos\theta}, \tag{2.6}$$

where n_{os}^2 and n_{xd}^2 are the refractive index for the characteristic wave propagation in respect to the angle of terrestrial magnetic field θ. The refractive index depends on the solar activity and for that we have periodical changes every eleven years and also changes in the refractive index

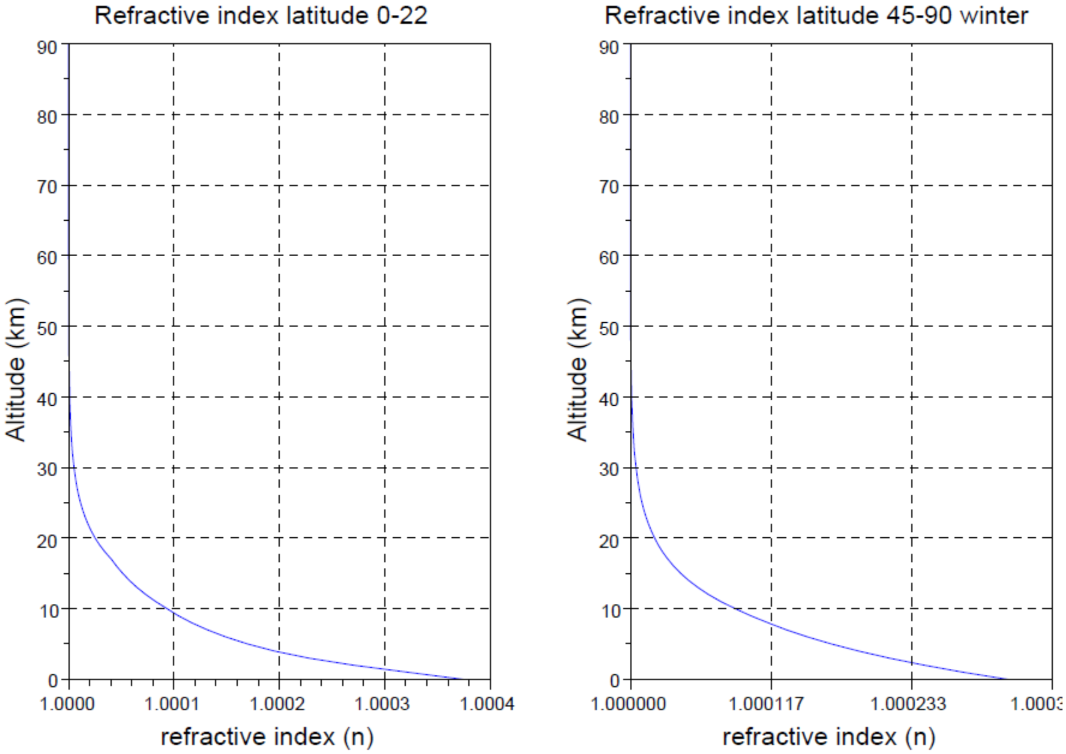


Figure 2.2: Refractive index vs altitude: The graph shows that the index of refraction is a function of altitude, latitude and season. All variables are calculated by the simulation software when we know the altitude of the aircraft. Using the Equation (2.2) it is possible calculate the refractive index for altitudes between 0 to 50 km from the sea level. For spacecrafts it is necessary to consider the Equations (15) and (2.6). Model taken from [26].

of day and night. We can make an estimation regarding electronic charge in the atmosphere using the ionograms from different institutes of research. In the first approximation, we use the data from the latitude of Rome and obtain the diagrams in Figure 2.3 [27]. The gyrofrequency at 90 km altitude can be determined from Figure 2.4 [28]. By Equation (2.2), for low atmosphere, the frequency of the radio signals is not considered in the equation. Only Equation (2.5) and (2.6) considers the change of the refractive index as a function of the frequency. For optical signals it is important to consider the wavelength of the laser. The radio channel can be used as a coarse alignment to track the satellite and for synchronization because the path followed by the laser is different from the path followed by the radio signal.

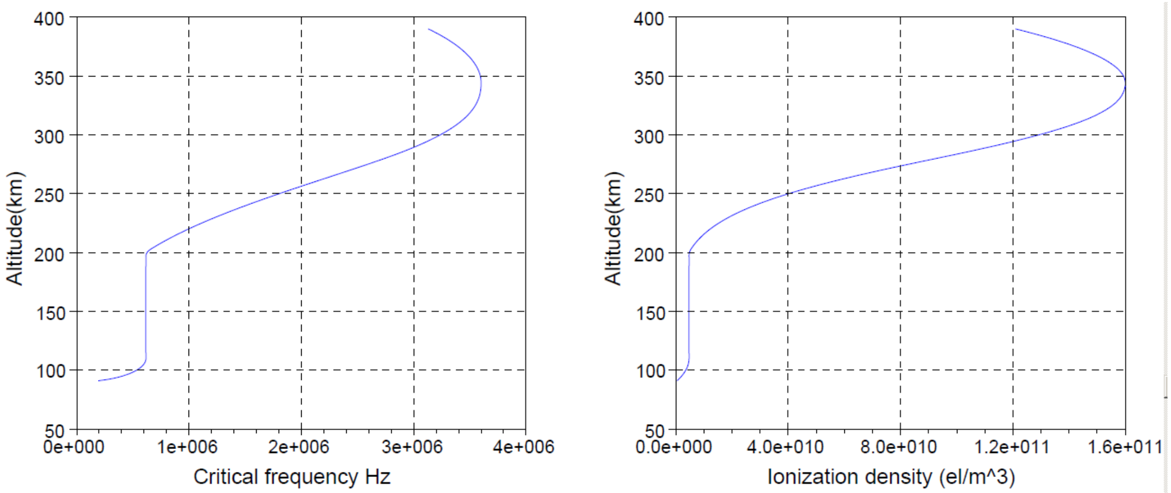


Figure 2.3: Ionograms: Reconstruction of the ionogram of the ionosphere from experimental data gathered in Rome. These trends will be used in our simulation program [24].

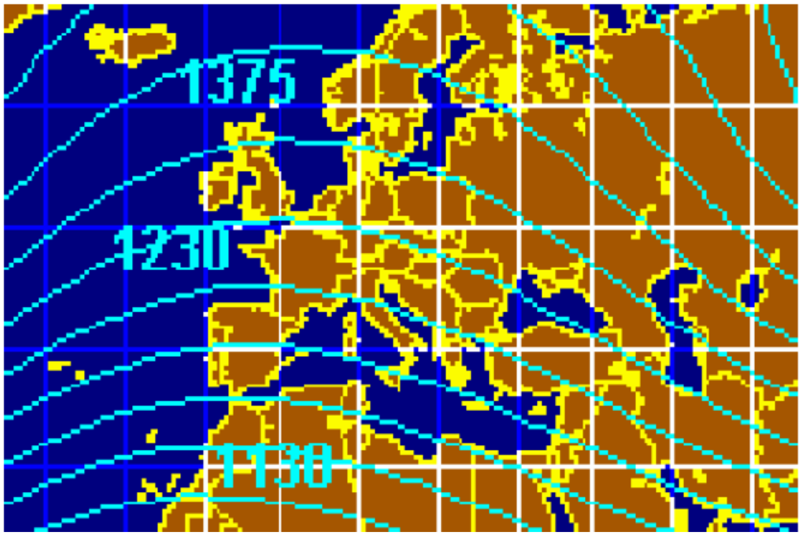


Figure 2.4: Map of the gyrofrequency (kHz) for 90 km in altitude sourced from [28]: This chart is used to calculate the first approximation feasibility simulation of the proposed system. The magnetic field will be modeled in our simulation program, using the data for each altitude.

2.2.1 Laser tracking system

The system uses a laser with a different wavelength to the laser used for the qubit exchange. This tracking laser signal is sent from Alice and received by Bob. In the system shown in Figure 2.5, the laser signal will be detected at Photodetector 2 and Photodetector 1 at different

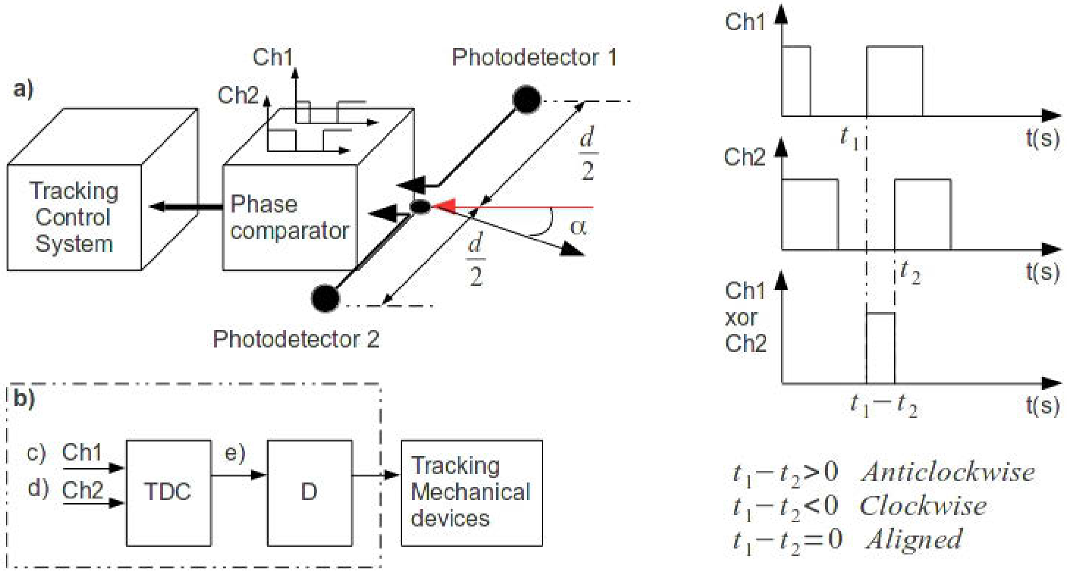


Figure 2.5: Tracking system using a laser: The figure shows the principle scheme for tracking between Alice and Bob using a laser beacon. Ch1 - Channel of the Photodetector 1; Ch2 - Channel of the Photodetector 2; TDC - Time to digital converter; D - Control device designed to control the tracking mechanical devices; The phase comparator indicates the TDC. Bob sends a pulsed laser beacon to Alice that has two avalanche photodiode, indicated with Photodetector 1 and Photodetector 2. If the system is not aligned with respect to the laser beacon of an angle α, Photodetector 1 received the signal before than Photodetector 2. Using a TDC it is possible for the system to know if misalignment exists, requiring rotation of the system. The time digital converter, rotates the communication system until it is able to measure the coincidence from Photodetector 1 and Photodetector 2.

time if misalignment α is present. The device, called a phase comparator, is a Time to Digital Converter (TDC). From Figure 2.5, the signal timing at Photodetector 1 is indicated with Ch,1 and with Ch2 we indicate the timing of the signal received at the Photodetector 2. The output e) represents the TDC output. The difference of the “click” $t_1 - t_2$, gives the command to a controller “D” to rotate, by the Mechanical device the system in order to aim the transmitter. The laser used for the tracking can also be used for the synchronization of the key exchange and also as a beam reference for the alignment of the polarization basis.

2.3 Beam spread and wandering

The atmospheric refractive index is not constant due to the local changes of the wind speed. The relation between the wind speed and the refractive index n is given by [16]

$$n_1(\vec{r},t) = n_1[\vec{r} - \vec{V}(\vec{r})t], \tag{2.7}$$

where $n_1(\vec{r},t)$ is the fluctuation of the refractive index, $\vec{r}$ is the vector of the spatial position, $\vec{V}$ is a local speed of the wind and t is the time. The refractive index is given by

$$n(\vec{r},t) = 1 + n_1(\vec{r},t). \tag{2.8}$$

To design the tracking system it is necessary to consider beam wandering and reciprocal movements between Alice and Bob. The tracking system is required to align Alice and Bob and their polarization bases. The effects of turbulence on the polarization of the beam is negligible [16, 17]. If the turbulent eddies are small compared to the diameter of the laser beam, the beam is not deflected significantly, while if the turbulent eddies are larger than the diameter of the laser beam, the beam is significantly deflected. In the absence of turbulence the angular spread of the laser is in the order of λ/D, where λ is the wavelength of the photon and D is the initial diameter of the laser beam. According to Equation 2.7, the refractive index changes with time. If we compare pictures in different temporal steps it is possible to observe the change in position of the laser spot. The single spots are inside a circle with average radius ρ_l as shown in Figure 2.6. In the case of strong turbulence the spot does not wonder significantly, instead the beam is broken down into multiple spots that are contained in a circular area approximatively of the radius ρ_l. The weighted average point of the spatial positioning of the laser beam is defined as centroid. The tracking system must be able to follow the wandering of the centroid.

2.4 Atmospheric effect on the tracking system

From section 2.2 the refractive index changes according to the frequency of the transmitted signal and the atmospheric conditions a radio signal can not follow an horizontal path. The same problem exists for a laser signal. The radio tracking system can be considered as a coarse alignment. The wavelength of a laser beacon is $532nm$ and the wavelength of the single photon is $780nm$. The difference of the wavelength can produce different paths as shown in

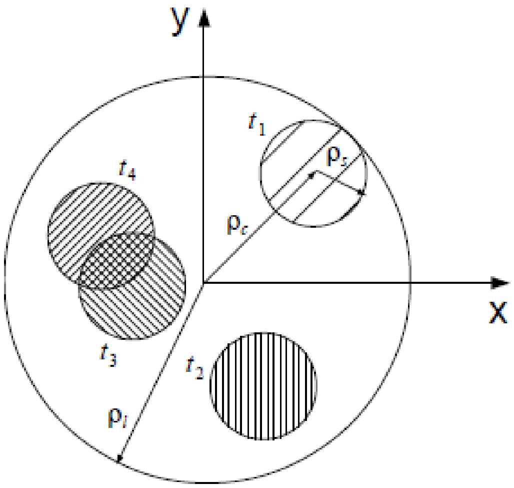


Figure 2.6: Spot of the laser received through a strong turbulence media: With time, the position of the laser spot changes. The origin of the reference frame x,y represents the centroid of the spot. ρ_s is the spot of the laser, ρ_l is the average radius contained the single spots and ρ_c is the position of single spot at time t. This figure is inspired from [16].

Figure 2.7. For a vertical path, e.g Earth station to satellite, it is possible to characterize the refractive index by the atmospheric condition on the Earth station, given the local values of pressure and temperature. If the path is not vertical we perform a characterization of the channel.

2.5 Tracking using GPS for coarse alignment

Telecommunication systems in free space, radio or optical, require a geometrical alignment system in order to maximize the transmission gain. Here, a system which uses three GPS coordinates in order to align the transmitter with the receiver is presented. The algorithm is optimized for a micro-controller. The algorithm was simulated with the help of cartography software tools and the average error of alignment between the transmitter and the receiver was 0.34 degrees. The micro-controller algorithm uses single precision. The calculation time of the micro-controller was measured at $4966\mu s$ making it suitable for plug and play mobile applications. Where GPS position is used, the accuracy of the alignment increases if a Differential Global Positioning System (DGPS) is used [29]. In some geographical areas, strong magnetic deviations due to the geological morphology are measured, as shown in Figure 2.8 and a tracking system using a compass can be affected by large errors. The system

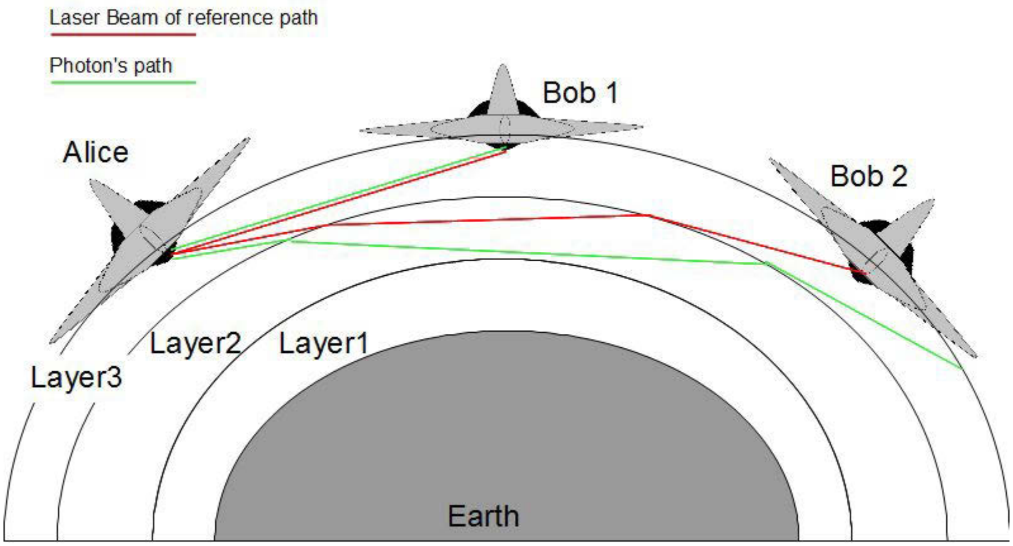


Figure 2.7: Effects of the chromatic dispersion: Consider the link between Alice and Bob. If the link propagates through a single layer of the atmosphere, minimal diffraction occurs, hence the green laser and the red laser (Single photon) have the similar paths as illustrated with Bob 1. The link to Bob 2 propagates through various layers of the atmosphere and due to chromatic dispersion the lasers follow different paths.

Figure 2.8: Magnetic deviation in Reunion Island: During an experiment, using a theodolite and one compass. The magnetic deviation in Piton Textor was greater than 20 degree. Own photo.

proposed in this thesis uses the GPS coordinates of the transmitter, receiver and one reference point called the reference station. Each position is identified by the position vectors with

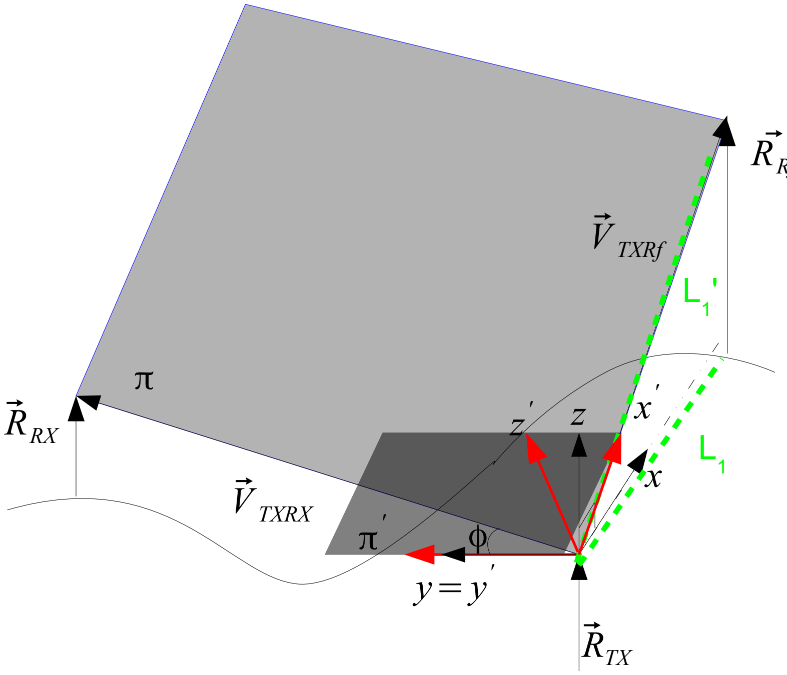


Figure 2.9: First alignment step: The initial direction of the laser L_1 is aligned with the x axes and also the same direction of the maximum gain of the aerial or the laser for used for the transmission. The x axis is aligned with the direction of the position vector $\vec{R_{TX}}$ (position of the transmitter). In the first step the x, y and z is rotated around the y axis until the x axes aims the position of the reference station. The new reference frame become x', y' and z'.

respect to an origin in the center of the Earth. The position vector of the transmitter, receiver and the reference station are called $\vec{R}_{TX}$, $\vec{R}_{RX}$ and $\vec{R}_{Rf}$ respectively. The reference station coordinates are sent to the transmitter station. The receiver also sends its coordinates to the transmitter. The algorithm uses the standard Cartesian coordinates to define the position vectors. The local reference frame of the transmitter is x, y and z. The position vectors are referred to another reference frame X, Y and Z that rotates accordingly with the rotation of the Earth. Initially the z axis is aligned according to gravity in the direction of the weight force parallel to the position vector $\vec{R}_{TX}$ as shown in Figure 2.9 and the x axis is aligned with a collimation laser L_1 in the direction of the reference station. The direction of the laser L_1 is the same as the maximum gain of the aerial or the direction of the laser used for the communication. By undergoing a rotational transformation about the y-axis, the local reference frame becomes x', y' and z', where x' aims at the position of the reference station on the Earth's surface. The plane where the x' and y' lie is called π', it is not coplanar with plane π which is identified by the position $\vec{R}_{TX}$, $\vec{R}_{RX}$ and $\vec{R}_{Rf}$. Through a rotation ϕ around

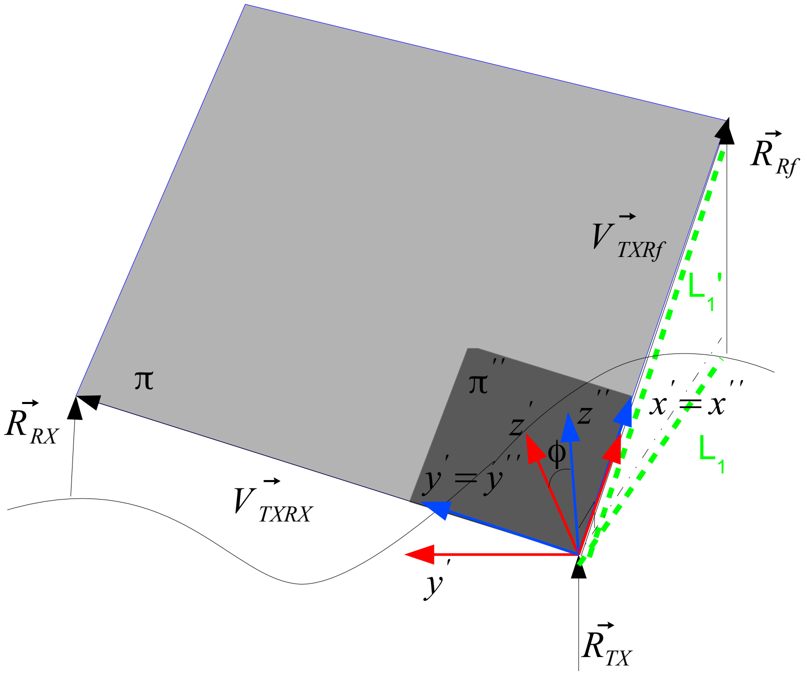


Figure 2.10: Second step followed by the algorithm: The new reference frame x', y' and z' is rotated by an angle ϕ in order to obtain a new reference frame x'', y'' and z'', where the plane y'' and x'' lie on the plane π.

the axis x' the plane π and π' become coplanar. The z'' axis of the new reference frame x'', y'' and z'' is orthogonal with the plane π as shown in Figure 2.10. Another rotation of an angle θ around z'' ensures the alignment of the transmitter and the receiver as shown in Figure 2.11.

2.5.1 3-point GPS alignment system

In order to build a portable alignment system, the following algorithm is implemented in a micro-controller [30]. In radio and optical communication the Sagnac effect due to the rotation of the Earth is neglected as well as the deviation of the weight force due the rotation of the Earth. An orthogonal reference frame, X,Y and Z is chosen. The origin of the reference frame is located on the center of the Earth where the X axis has the direction of the Greenwich meridian and the Z axis through the geographical north pole as shown in Figure 2.12. The reference frame X, Y and Z, rotates according to the rotation of the Earth. From now on, the vectors are identified and calculated on the reference frame X,Y and Z using the GPS coordinates. The position of the reference station is identified by the vector $\vec{R}_{Rf}$. We identify the position of the transmitter and receiver by the vectors $\vec{R}_{TX}$ and then $\vec{R}_{RX}$ respectively. The standard WGS-84 is used to locate the position. This standard considers the

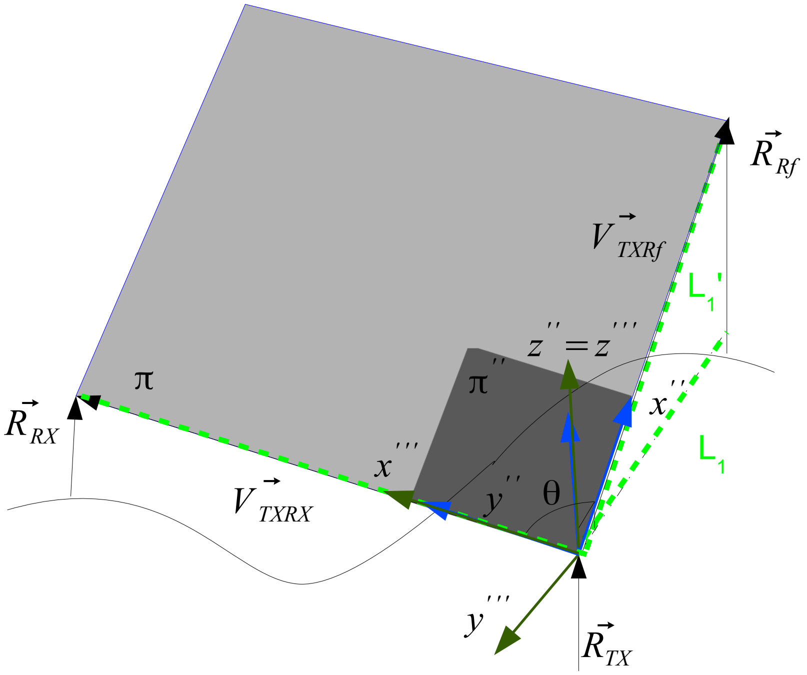


Figure 2.11: Last step to align the transmitter to the receiver: After the previous rotation, the laser will aim in the direction of the reference station. By the rotation around z'' of an angle θ, the transmitter aims the receiver.

Earth as an ellipse with the semi-major axis of $a = 6378137$ m and the semi-minor axis of $b = 6356752.3142$ m [31] [31]. The altitude from the GPS are given from the ellipsoid of reference. The eccentricity e is expressed as:

$$e^2 = \frac{a^2 - b^2}{a^2} = 0.006694. \tag{2.9}$$

The curvature of the first vertical is expressed as:

$$N = N(\lambda) = \frac{a}{\sqrt{1 - e^2 \sin^2 \lambda}}. \tag{2.10}$$

The coordinates of the position vector of the reference station are expressed as

$$\begin{aligned} X_{Rf} &= [N + h_{Rf}] \cos \lambda_{Rf} \cos \mu_{Rf}, \\ Y_{Rf} &= [N + h_{Rf}] \cos \lambda_{Rf} \sin \mu_{Rf}, \\ Z_{Rf} &= [N(1 - e^2) + h_{Rf}] \sin \lambda_{Rf}. \end{aligned} \tag{2.11}$$

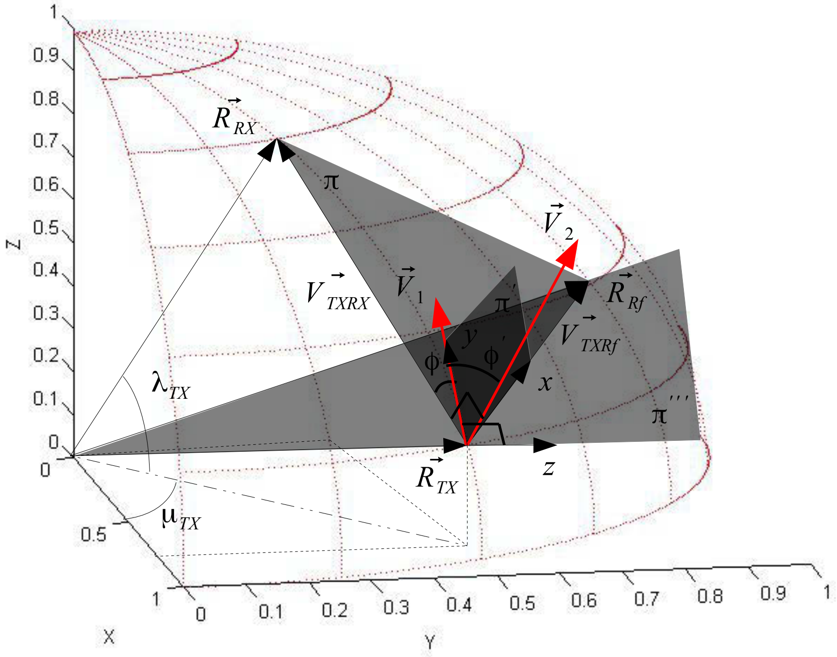


Figure 2.12: The picture shows the planes and the relative angle, used to calculate the direction of rotation: The position vector are taken with respect to the center of the Earth, and are calculated by the WGS84 standard. By the GPS it is possible measure the position on the Earth surface, altitude from the geoid and from the ellipsoid.

Here, h_{Rf} represents the altitude from the ellipsoid to the Earth surface. The position vector of the transmitter R_{TX} has coordinates:

$$\begin{aligned} X_{TX} &= [N + h_{TX}] \cos\lambda_{TX} \cos\mu_{TX}, \\ Y_{TX} &= [N + h_{TX}] \cos\lambda_{TX} \sin\mu_{TX}, \\ Z_{TX} &= [N(1-e^2) + h_{TX}] \sin\lambda_{TX}, \end{aligned} \tag{2.12}$$

and the coordinates of the receiver are,

$$\begin{aligned} X_{RX} &= [N + h_{RX}] \cos\lambda_{RX} \cos\mu_{RX}, \\ Y_{RX} &= [N + h_{RX}] \cos\lambda_{RX} \sin\mu_{RX}, \\ Z_{RX} &= [N(1-e^2) + h_{RX}] \sin\lambda. \end{aligned} \tag{2.13}$$

The subscripts RX,TX and Rf represent the position of the receiver, transmitter and the reference station respectively. The vector $\vec{R}_{TX}$ is the position vector of the transmitter with respect to the chosen reference frame. The vectors $\vec{R}_{Rf}$and $\vec{R}_{RX}$ are the position vectors of the reference station and the receiver, respectively. The angle θ, is calculated by the inverse of the following equation:

$$\vec{V}_{TXRf} \cdot \vec{V}_{TXRX} = |\vec{V}_{TXRf}||\vec{V}_{TXRX}|\cos\theta. \tag{2.14}$$

The direction of rotation (clockwise or anticlockwise) is calculated by the component Z of the cross product $\vec{V}_3 = \vec{V}_{TXRf} \times \vec{V}_{TXRX}$, where $\vec{V}_{TXRf} = \vec{R}_{Rf} - \vec{R}_{TX}$ and $\vec{V}_{TXRX} = \vec{R}_{RX} - \vec{R}_{TX}$ as shown in the Figure 2.12. If the transmitter is located on the Northern Hemisphere and the component of $\vec{V}_3$ long Z is positive the direction of rotation is clockwise. If the transmitter is located on the Southern Hemisphere and the component of $\vec{V}_3$ along Z is negative, the direction of rotation is anticlockwise. Initially the direction of the laser pointer L_1 is orthogonal to the vector $\vec{R}_{TX}$ and is subsequently is tilted in order to aim to the reference station. The local reference frame x,y and z changes to x', y' and z'. The x' axis has the same direction of $\vec{V}_{TXRf}$ as shown in Figure 2.12 . For the transmitter to aim at the receiver, it needs to be rotated around the vector $\vec{V}_{TXRf}$ once the angle θ is calculated. By the cross product, the vector $\vec{V}_1 = \vec{R}_{TX} \times \vec{R}_{Rf}$ is orthogonal to the plane π''' (see Figure 2.12). By the cross product $\vec{V}_2 = \vec{V}_{TXRf} \times \vec{V}_{TXRX}$ the vector $\vec{V}_2$ is orthogonal to the plane π. The angle ϕ' between the vectors $\vec{V}_1$ and $\vec{V}_2$ is calculated by the rules of the inner product. The plane π''' is aligned with the plane given by the x, z axes (see Figure 2.9). The plane π' is coplanar with π when the vectors $\vec{V}_1$ and $\vec{V}_2$ are orthogonal. The angle of rotation around the vector $\vec{V}_{TXRf}$ is $\phi = 90 - \phi'$. In the algorithm, the component Z of the vector $\vec{V}_1$ must be the same as the component Z of the vector $\vec{V}_2$. During the calculation, if the condition is false the cross product $\vec{V}_2$ becomes $\vec{V}_2 = \vec{V}_{TXRX} \times \vec{V}_{TXRf}$.

2.6 Test for short distance

The test was done using a classical GPS, a laser pointer ($532nm$) and one tripod with a protractor for civil construction. On top of the protractor we fixed a laser and using a GPS we measured the position that represents the position of the transmitter TX. A second GPS position was taken at reference station R_{Rf} and another was taken at the position of the receiver RX. We calculate the angle θ shown in the Table 2.1. The experiment was performed, using a GPS aerial that transmits the coordinates to the transmitter side via a radio channel (See Appendix A.3). Once the coordinates were acquired, the angle θ between the line, transmitter to reference station and transmitter to receiver was calculated by the algorithm proposed in the previous section. The position of the reference station and the transmitter was fixed,

Table 2.1: Results of the tracking experiment, using three GPS coordinates for a short distance: λ_β and μ_β are the latitude and longitude respectively, where β represents the position of the transmitter, receiver and reference station. T 1 and T 2 represents the test number 1 and 2 respectively. The coordinates were transmitted to the computer by an GPS antenna. Using the collected data it was possible to calculate the angle θ. The same system can work autonomously if the position is transmitted to the transmitter by a radio or Internet connection. Figure 2.13 shows that the algorithm is able to align the transmitter with the receiver.

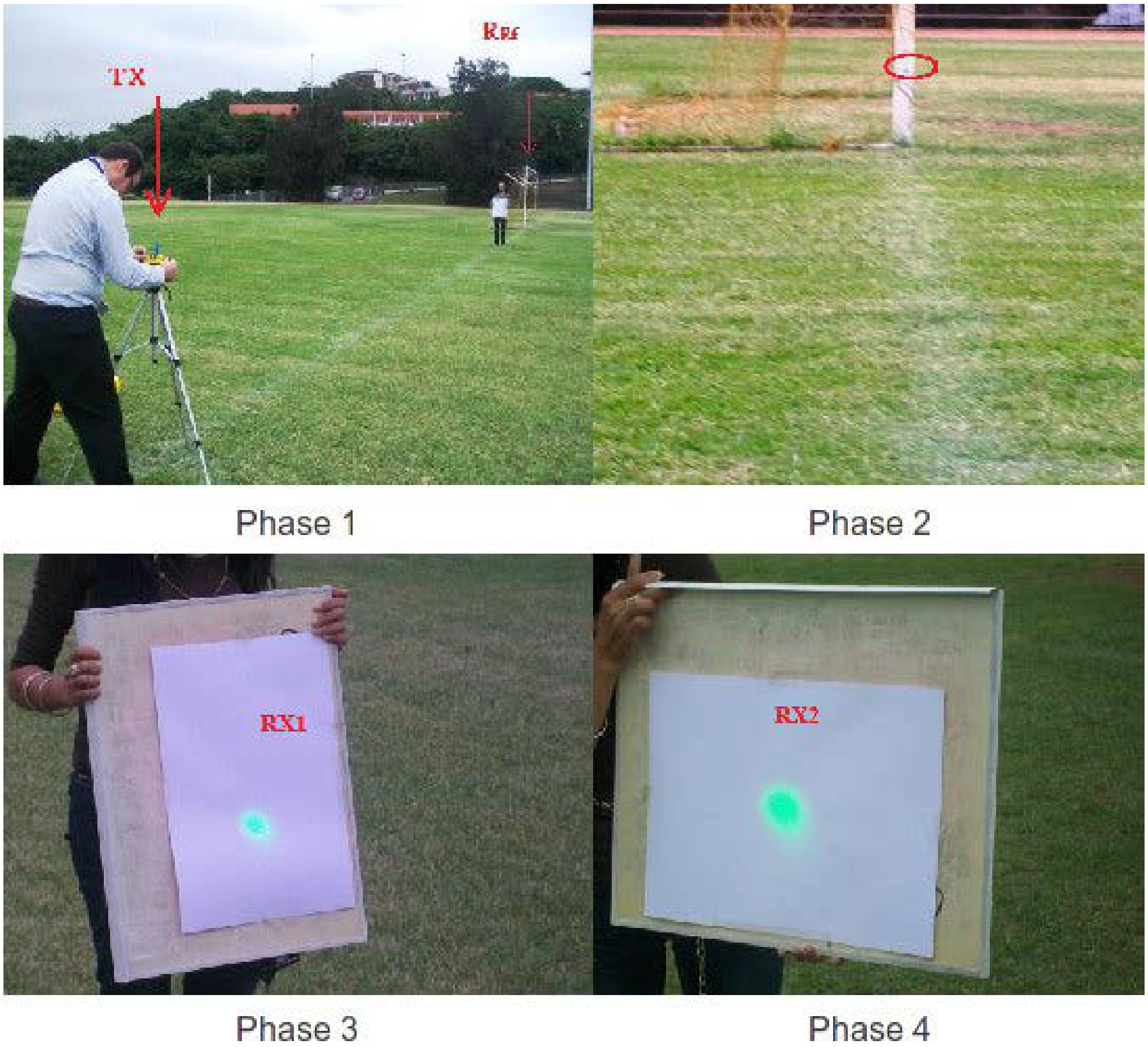
	λ_{TX}	μ_{TX}	$\lambda_{R_{RF}}$	$\mu_{R_{rf}}$	λ_{RX}	μ_{RX}	θ
T 1	-29.821365	30.94651	-29.821145	30.94636	-29.820775	30.946901667	60.798
T 2	-29.821365	30.94651	-29.821145	30.94636	-29.82080375	30.9472297917	78.926

while the receiver was moved once in order to test the algorithm for two different positions of the receiver. The results of the two measurements are shown in the Table 2.1. Figure 2.13 shows the accuracy of the system and algorithm. This experiment shows the feasibility of coarse alignment using GPS. In this experiment, the distance between the transmitter and the reference station was $18.91m$.

Point A of the transmitter is located at one point on the fuselage where it is possible to measure the coordinates via the terrestrial reference frame and similarly for point B. Point A represents the position of the transmitter and point B represents the position of the reference station as represented in Figure 2.14. Following the algorithm proposed it is possible align the transmitter, located on the aircraft and the receiver located on the Earth station. With a distance from the transmitter to the reference station as tested 18.92 m is realistic size for setting up the system in a small airplane such as Learjet 85, where the total length of the airplane is 21 m [32].

2.7 Test of the Algorithm in a single precision using a micro-controller

Simple mathematical operations were used in a micro-controller in order to create a plug and play tracking system for optical and radio communication. The proposed algorithm was loaded into a Harvard architecture 8 bit micro-controller, with operating frequency at 16MHz. The angle θ was calculated in single precision and checked these measurements in double precision. Because the system can be used for mobile applications, the calculation time was measured. The goal of the system was to find geometrical alignment between the transmitter



Phase 1

Phase 2

Phase 3

Phase 4

Figure 2.13: Tracking system experiment for short distance: This experiment was done in a soccer field of the University of KwaZulu-Natal. Phase 1: Alignment of the transmitter RX with the reference station R_{Rf}. Phase 2: The laser beacon was aligned with the reference station located on the goal post. Phase 3: We aim the laser in the calculated direction θ, where the receiver $RX1$ was located. Phase 4 : we change the position of the receiver and following the same step of Phase 3 we aim the receiver position $RX2$. As it possible observe from the picture, also without using the DGPS the system is very accurate as coarse alignment.

and receiver for long distance. For this purpose it is possible to use Google Maps software in order to measure the angle θ and compare the results calculated by our algorithm. From Table 2.2 it is evident that the difference of calculation between double precision and single precision can be neglected for radio communications since the angle of maximum gain aerial

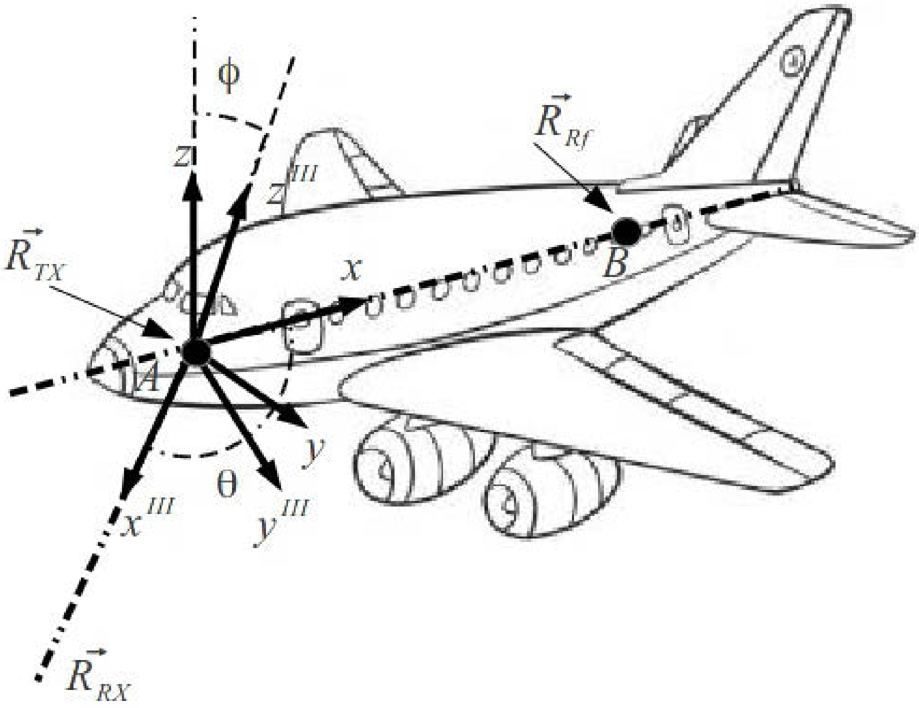


Figure 2.14: Application of the coarse alignment system for aircraft: Two GPS location can be received along two known points on the fuselage (A and B). Following our coarse alignment algorithm, the system can be able to aim the transmitter.

is generally greater than the error calculated [33]. The system uses a GPS receiver and the accuracy depends on many factors and may fluctuate between 15 to 30m if the DGPS is not used.

Using Google maps the locations for the transmitter, receiver and the reference station. The coordinates were converted in decimal degrees and by the Equation (2.11), (2.12) and (2.13) the components of the vectors were calculated. The experiment was done twice on the Northern Hemisphere and twice on the Southern Hemisphere. In the beginning, by using the graphical tools of Google Maps, we measured the angle θ_G between the direction transmitter-reference station and transmitter-receiver. The angle θ_M was the angle θ_G calculated using the double precision of Matlab and θ_{MCU} was the angle calculated by the microcontroller. The calculation time t of the microcontroller to calculated both the angles, ϕ_{MCU} and θ_{MCU}. It was possible to observe the small difference between the single and double precision of the angle $\varepsilon_{\theta_{MCU}} = |\theta_G - \theta_{MCU}|$. The direction of rotation is calculated by the cross product $\vec{V}_3 = \vec{V}_{TXRf} \times \vec{V}_{TXRX}$ as shown in the Table 2.2. The calculation also confirmed that the sys-

Table 2.2: Test of the algorithm loaded in a microcontroller, in single precision: In order to check the calculation accuracy for long distance, the results calculated by the microcontroller was compared using the double precision of Matlab. λ - Latitude; μ - Longitude; θ_G - Angle measured using Google maps; θ_M - angle calculated by Matlab (Double precision); θ_{MCU} - angle calculated by the micro-controller (single precision); Direction - Direction of rotation of the angle θ calculated by the micro-controller and Matlab; ϕ_M - angle of rotation around the vector $\vec{V}_{TXRf}$ calculated by Matlab; ϕ_{MCU} - angle of rotation around the vector $\vec{V}_{TXRf}$ calculated by micro-controller; t(μs) - calculation time of the micro-controller;ε_{θ_M} - Difference of the calculate angle θ in double precision and the angle measured using Google maps; $\varepsilon_{\theta_{MCU}}$ - Difference of the calculate angle θ in single precision and the angle measured using Google maps; Distance - distance between the transmitter and the receiver.

	TEST 1	TEST 2	TEST 3	TEST 4
λ_{TX} (Deg.)	-29.06006944	-32.60886667	42.50960278	41.43288333
μ_{TX} (Deg.)	27.24506667	27.60504444	11.56986389	12.83350833
λ_{Rf} (Deg.)	-29.05515000	-32.60844444	42.50969167	41.43427500
μ_{Rf} (Deg.)	27.23995833	27.60464444	11.56978611	12.83227778
λ_{RX} (Deg.)	-29.00026667	-32.60220833	43.75004556	41.48340278
μ_{RX} (Deg.)	27.30960833	27.61673611	12.24766389	13.32911667
θ_G (Deg.)	85.6100	94.1800	54.1200	115.6700
θ_M (Deg.)	85.8797	94.7938	54.5021	115.7600
θ_{MCU} (Deg.)	85.8719	95.0355	53.9950	115.7889
Direction	Clockwise	Clockwise	Clockwise	Clockwise
$\phi_M(Deg.)$	0.0690	0.1031	0.9243	0.3142
$\phi_{MCU}(Deg.)$	0.0722	0.0153	0.8387	0.3794
t(μs) MCU	5072.00	5124.00	4472.00	4504.00
ε_{θ_M} (Deg.)	0.2697	0.6138	0.3821	0.0900
$\varepsilon_{\theta_{MCU}}$ (Deg.)	0.2619	0.8555	0.125	0.1189
$\phi_{MCU} - \phi_M$	0.0032	0.0877	0.0856	0.0652
Distance (km)	9.1357	1.3227	148.4300	41.7860

tem rotates in the correct direction. In the simulation the altitude of the transmitter, receiver and reference station was considered at the same level of the ellipsoid ($h_\alpha = 0$), for short distances the calculation of the angle ϕ is not accurate in single precision, because the difference of the altitude between the three points it is not appreciable. For long distance the effects of the error on the terrestrial coordinates measured by GPS, is relatively small. Consider the Figure 2.15, where the position of the transmitter and the reference station are accurate (using the DGPS) and the position of the receiver is affected by an error of $30m$. The distance between the transmitter and the receiver is 10 km. The error on the angle θ_{err} can then be

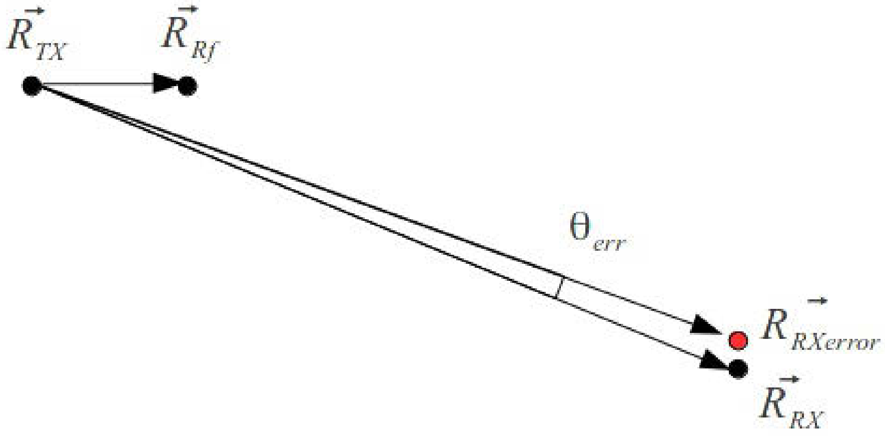


Figure 2.15: Effects on the GPS error on the tracking angle: Using the red point is indicated the "virtual" geographical position measured by the GPS and affected by an error of $30m$. Considering the distance between the transmitter and receiver of $10km$, the angle θ_{err} is the error of misalignment. For long distance this error decreases.

calculated approximatively as:

$$\theta_{\mathrm{err}} = \frac{30}{10000} = 0.003. \tag{2.15}$$

If the distance between the transmitter and receiver is $1km$ the misalignment is $\theta_{err} = 0.03$. For long distance the misalignment error can be neglected for radio communication [33] and decreases inversely with the distance. For optical communication a fine alignment system is necessary and for long distance it is necessary have an accurate equatorial mount able to follow the small changes of angle.

2.8 General methods for synchronization

In section 1.5.5 we emphasized that quantum cryptography requires a synchronization system in order to keep the time stamping of each single photon sent. When Alice and Bob are located in two stationary points, the synchronization can be done by using the radio signal from the GPS [18]. In this section we describe an autonomous synchronization system using a radio signal, transmitted from Alice. Theoretically it is possible to synchronize Alice and Bob using a laser signal, but if an obstacle lies between the transmitter and receiver, synchronization may be lost. A radio signal ensures the synchronism and it is possible to use the same signal as public channel.

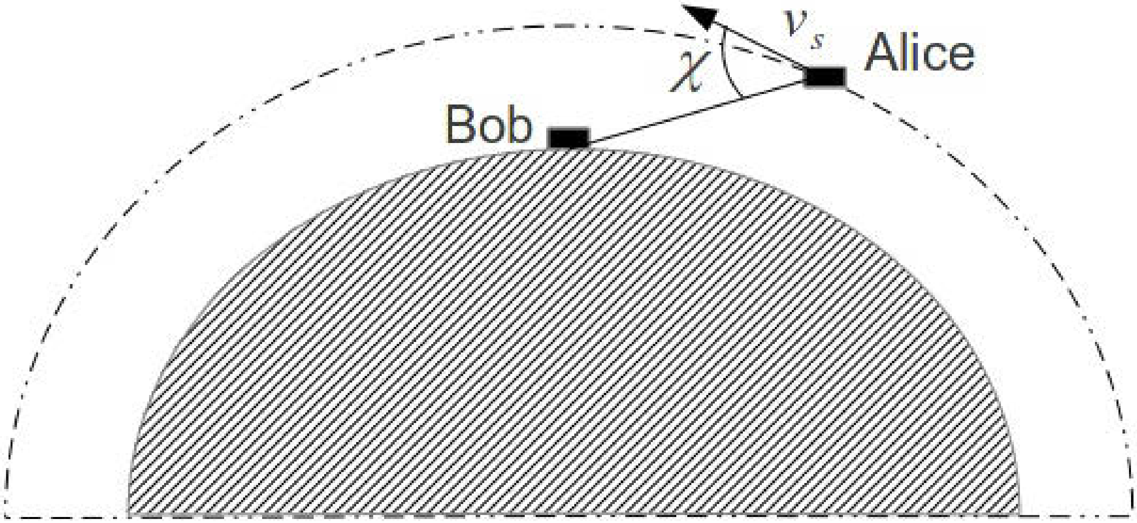


Figure 2.16: Doppler effect scenarios: Alice transmits the radio signal to Bob in order to synchronize the key exchange. Due to the high speed of the spacecraft Bob receives the synchronization signal with a frequency higher or lower with respect to the carrier sent from Alice. The Doppler effect depends of the direction of the satellite and its speed. The velocity to be considered is the component of the speed with respect to the link. If the clock used to transmit the quantum bits is a fraction of the frequency of carrier signal, the clock frequency at the quantum bit measured by Bob changes by the same ratio as the carrier signal.

2.8.1 Doppler effects

In this scenario, Alice is located on the satellite and Bob is located on the Earth station. Once Alice is aligned with Bob, she transmits a carrier to Bob and the quantum bit is synchronized with the frequency of the carrier. The quantum bit rate, can be a fraction of the carrier signal. Due to the high speed of the spacecraft, the carrier signal is received by Bob with a different frequency according to the Doppler effect. Figure 2.16 represents this situation. Alice transmits the synchronization signal with a frequency f_T and Bob received the same signal with a frequency f_R. The frequency shift Δf is [24]:

$$\Delta f = v_s \cos\chi \frac{f_T}{c}, \tag{2.16}$$

where v_s is the speed of the satellite, c the speed of propagation of the signal and χ is the angle between the direction of the link and the vectorial speed of the spacecraft. The ratio of the frequency shift Δf and the frequency f_T depends on the angle χ and the speed v_s. The same ratio is observable for the transmission frequency of the single photon. If the synchronization

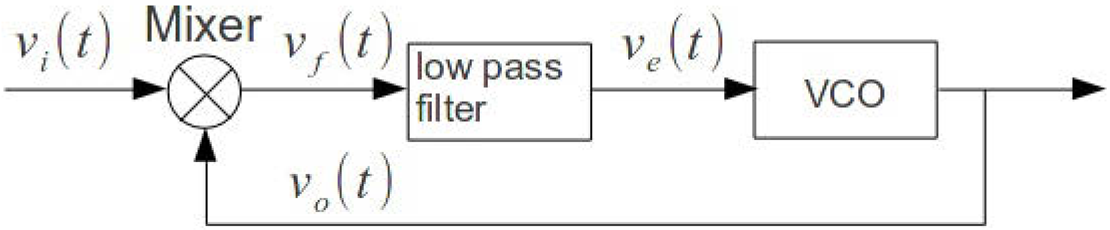


Figure 2.17: PLL conceptual scheme: The Phase Locked Loop (PLL) is a device used to lock the frequency of carrier indicated by $v_i(t)$. The carrier with frequency f_i is multiplied by a mixer with the local frequency given to the Voltage Controlled Oscillator with frequency f_o. The output of the mixer $v_f(t)$ is composed of two signals, one signal has the frequency $(f_i + f_o)$ and the other has frequency $(f_i - f_o)$. In the output of the filter , the signal $v_e(t)$ has frequency $(f_i - f_o)$ and represents the signal control for the VCO. Once the frequency is locked the PLL is able to lock the phase. The signal is now ready to synchronize the transmission between Alice and Bob by the clock recovery. It is probably necessary add a delay between the clock recovered and the time for which the quantum bit arrives to the detectors because the path of the radio signal and the single photon are different [34].

detection of the single bit is synchronized with the radio frequency, the Doppler effect does not effect the transmission of the single photon.

2.9 Synchronization using a Phase-Locked Loop

One way to synchronize the communication is to use a Phase Locked Loop (PLL) [34]. The scheme of the PLL is shown in Figure 2.17. The most simple model of an analog PLL is composed by a mixer, one low pass filter and one voltage controlled oscillator (VCO). The signal $v_i(t)$ received by Bob and transmitted from Alice, is mixed with the signal v_o from the VCO. Given

$$v_i(t) = V_i \cos(\omega_i t) \tag{2.17}$$

and

$$v_o(t) = V_o \cos(\omega_o t + \phi), \tag{2.18}$$

where ϕ is the difference of phase between $v_o(t)$ and $v_i(t)$, in output of the mixer we obtain:

$$\begin{aligned} v_f(t) &= K \cdot V_i \cdot V_o \cos(\omega_i t) \cos(\omega_o t + \phi) = \\ & K \frac{V_i \cdot V_o}{2} \left(\cos((\omega_i + \omega_o)t + \phi)\right) + \cos((\omega_i - \omega_o)t - \phi)\right) . \end{aligned} \tag{2.19}$$

The low pass filter excludes from the signal $v_f(t)$ the terms where the frequency is $\omega_i + \omega_o$ and the error signal $v_e(t) = K(V_i \cdot V_o)/2\,(\cos((\omega_i - \omega_o)t - \phi))$ is obtained. This signal is used to control the frequency of the VCO. If $\omega_i > \omega_o$ the signal $v_e(t)$ control the VCO in order to increase the frequency ω_o until the frequency $\omega_i(t) = \omega_o(t)$. Once the frequency is locked, from Equation (2.19), output of the filter is

$$v_e(t) = K\frac{V_i \cdot V_o}{2}\cos\phi \tag{2.20}$$

and this signal is used to lock the phase. This scheme can be used for terrestrial application between two stationary points.

2.10 Open-Source electronics for tracking system

The design of a new system, often requires a team in order to optimize the time and decrease the price of the final product. Open-Source programmable units are a user friendly way to design systems for quantum cryptography, for the experimentation and for prototyping. Following this ideology, the microcontroller “Arduino uno” and the micro-computer “Raspberry Pi” were utilised. The Arduino microcontroller has six analog inputs, thirteen digital lines of input/output and is easily programmable in C language. The Analog to Digital Converter (ADC) is able to convert an analog sample in 100 μs. The clock frequency is 16 MHz. The performance of Arduino is adequate for our system. Arduino can be controlled via the USB ports of a personal computer and that permits the use of Arduino together with Raspberry Pi. The operating system of the Raspberry Pi is Linux based.

2.10.1 Raspberry Pi

Raspberry Pi was designed by the Raspberry Foundation in 2012 as a didactic micro-computer. The Central Processing Unit (CPU) is an ARM1176JZF-S at 700 MHz, and a video board BroadCome Videocore IV is included. The micro-computer has two USB ports, one Ethernet port and the video output. General-Purpose Input-Output port (GPIO) that can be used for digital controls for external apparatuses or to acquire the digital values from an ADC is potentially interesting. Figure 2.18 shows the hardware diagram of the board. Since the operating system is Linux, the micro-computer can be programmed natively in C/C++ or Python. Eventually, to fully exploit the power of this programmable system, it is optimal to write the program in assembler without using the operating system [36]. For our purpose, Raspberry

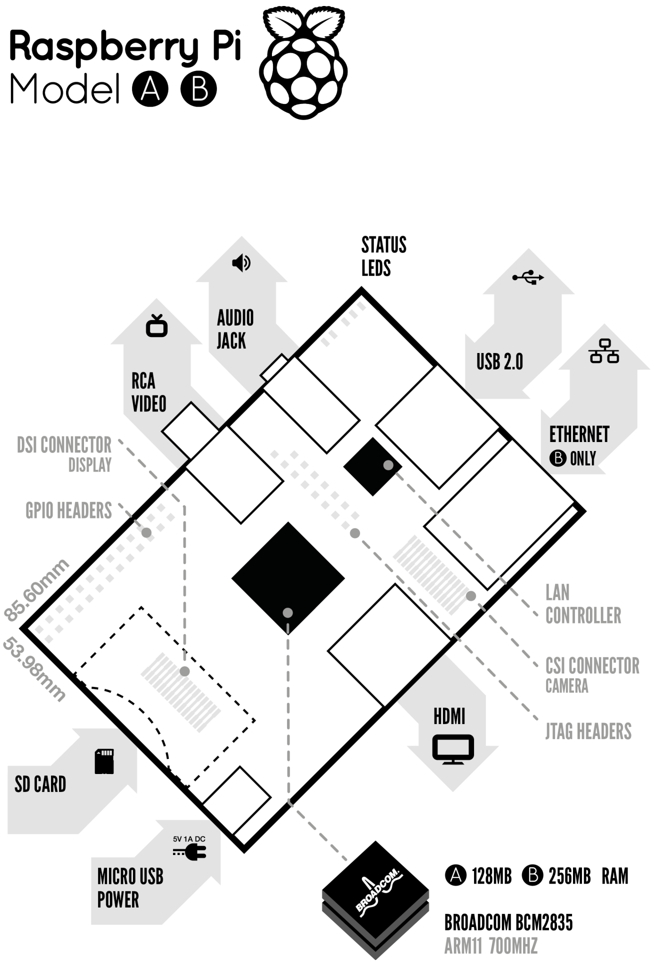


Figure 2.18: Scheme of Raspberry Pi: The picture shows the position of the output ports as the video outputs and the useful ports GPIO. The figure is sourced from [35].

Pi can be use for fine alignment tracking using a CCD camera. The Raspberry Pi is not a micro-controller and cannot communicate autonomously with the external world, but it is required an input/output interface.

2.10.2 Arduino

Arduino uno, from here on referred to as Arduino, can be considered a microcontroller. The power budget for an Arduino is less than for a Raspbery Pi, and the internal ADC permits acquisition at the analog data with less or no external circuitry. The core of Arduino is a microcontroller Atmega328P with an internal boot-loader and is programmable by an Integrated Development Environment (IDE) supplied by Arduino company [37]. The user can program the microcontroller by using the IDE with a simplified version of C language or using avr-C [38]. The IDE has a set of black-box subroutines of which it is not possible to know the amount of RAM used and is not possible to know the exact number of clock cycles required to follow the instructions. However, when it is not necessary to optimize the timing, and when the program does not require a large amount of memory, the IDE represents the shortest way to produce a prototype. The following example shows how it is possible improve a program by using avr-C instead of Arduino C.

Considering a system that sends a TTL signal with a frequency proportional to an analog value converted from the internal ADC of the micro-controller. The program written with the Arduino C is:

```
void setup(){
  // Set the pin number 2 as output
  pinMode(2,OUTPUT);
}
void loop(){
  int waiting;
  while(1){
      waiting=analogRead(0);
      digitalWrite(2,1);
      delay(waiting);
      digitalWrite(2,0);
      delay(waiting);
  }
}
```

The same program written in avr-c is:

```
#include<avr/io.h>
#include<util/delay.h>
int main(void){
  unsigned int waiting,counter;
  //set PB0 pin as output
  DDRB|=(1<<PB0);
  // Set of the frequency of the clock by theprescaler for the ADC
  ADCSRA=(1<<ADEN)|(1<<ADPS2)|(1<<ADPS1)|(0<<ADPS0);
  ADMUX=(0<<REFS1)|(1<<REFS0)|(0<<MUX3)|(0<<MUX2)|(0<<MUX1)|(0<<MUX0);
```

```
 // Set the input pin
  while(1){  // Loop
    ADCSRA|=(1<<ADSC);    //Start the conversion
    while((ADCSRA & (1<<ADSC))){};
    // Waiting until the end conversion signal is present
    waiting=ADC;   // Reading the converted analog value
    PORTB=0b00000001; // Set the pin PB0 at logic level 1
    for (counter=0;counter<=waiting;counter++){
      _delay_ms(1);
    }
    PORTB=0b00000000; // Set the pin PB0 at logic level 0
    for (counter=0;counter<=waiting;counter++){
      _delay_ms(1);
    }
  }
  return(0);
}
```

The program written in avr-C, requires an amount of memory of 228 byte against the Arduino C, that require 1122bytes. Using the avr-C is also possible, through the prescaler, set the clock of the internal ADC of the microcontroller. However, for our purpose Arduino C was used because the mathematical algorithm does not require more storage memory used than for a program written in avr-C, and the total storage memory was only 1/3 of the total space.

2.10.3 Fine alignment system using a PSD

The laser beacon is received through a telescope and the spot is concentrated on a Position Sensitive Device (PSD) [40]. The PSD is a plate of doped silicon that has four output terminals. The beacon spot activates the surface of the sensor and provides the position of the spot. In the output there are different current values for each terminal. Using this current signature it is possible to determine the position of the centroid as shown in Figure 2.20. The automatic tracking control can be performed using the open-source microcontroller Arduino. The signal from the PSD is amplified and iteratively enhanced by the micro-controller. The microcontroller performs measurement of the position of the spot and at the same time it controls the power system that moves the mechanics for tracking.

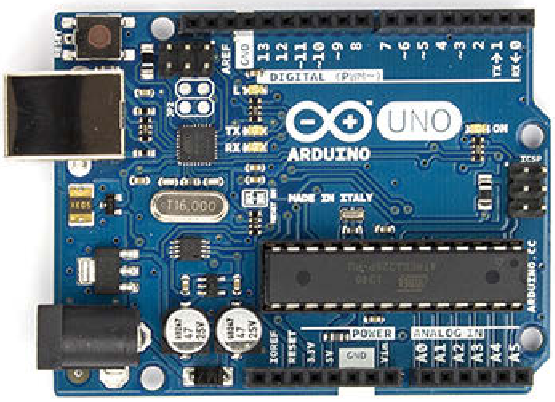


Figure 2.19: Arduino mocrocontroller: The numbered pins from 0 to 13 indicate the digital pins and the analog input are indicated using the letter A. The figure is sourced from [39].

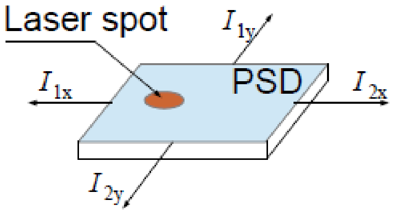


Figure 2.20: Scheme of the positioning sensitive device: The laser is received by a PSD. When the laser spot changes from the central position the values of the current I_{1x}, I_{2x}, I_{1y} and I_{2y} change. This figure is inspired from [40].

2.10.4 Fine alignment system using a camera

As discussed in subsection 2.10.3 the tracking system uses a PSD sensor to follow the laser spot. The system is completely autonomous and it is not necessary to use a computer, however it is not entirely accurate. It is also possible to follow the laser spot with a camera plugged into a computer. The spot of the laser is visualized using a camera. The position of the centroid can be computed and consequently the command can be sent to the electromechanical tracking unit. The computer receives the images as a matrix of numbers. The dimension of the matrix depends on the number of pixels of the camera. The color of a single pixel is represented by a number. When the image spot is received from the camera, the computer acquires the position of the single pixel which corresponds to the color of the laser and computes the centroid position. The program was tested using SCILAB [41] and the result is shown in Figure 2.21. The same algorithm proposed in SCILAB can be rewritten in

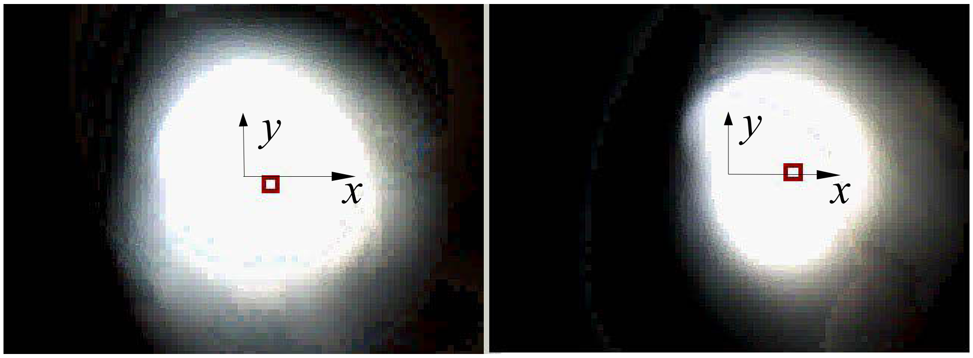


Figure 2.21: Experimental picture of the fine alignment test, using a CCD camera: The red square follows the movement of the spot with respect the center of the camera indicated by the axes x,y. The same coordinates used to follow the centroid with the red square can be used to move the mechanics of the tracking system.

Phyton to be used in a Raspberry Pi. Raspberry Pi and Arduino utilised together will permit an integrated autonomous system.

2.10.5 Summary

As explained in the Section 1.5.5 a tracking system consists of a subsystem for coarse alignment and a subsystem for a fine alignment. This chapter focused on coarse alignment and briefly discussed a fine alignment system using a PSD and CCD camera. The coarse alignment proposed here used three coordinates measured by a GPS. The GPS system, due to the factors discuss in subsection 2.7, can not track aprecise position. Better precision can be obtained using a differential global positioning system. Other systems use an electronic compass, but in particular positions on the Earth a strong magnetic deviation as shown on Figure 2.8 can give a large misalignment between the transmitter and receiver.

Our system is not affected by magnetic deviation and the experiment done for short distance shows that our system is accurate for radio-telecommunication and is very accurate as a coarse alignment system. The necessary distance between the transmitter and the reference station can be small enough to allow placement at the system on an aircraft. Using the GPS tracking, and the scan algorithm [22], it is possible to have a reliable tracking system for optical communication. The algorithm proposed is suitable for commercial microcontroller or for an open-source prototyping platform such as Arduino. On the other hand, to apply our tracking system in an aircraft it is necessary to reduce processing time. The timing can be reduced using a more optimize microcontroller or FPGA. Our system uses a laser beacon that can be used to synchronize the transmission, but a radio channel can also be used for this purpose. A radio channel would guarantee synchronization better than the optical system, since if an obstacle were present between Alice and Bob, synchronization would still be ensured.

Chapter 3

Polarisation alignment

One of the challenges to obtain quantum cryptography in free space is the relative orientation of the polarisation bases between Alice and Bob. In this chapter we present various methods to obtain good basis alignment in free space. The first system uses one polariser and represents the solution for Alice and Bob when they are located in two stationary positions. The second and the third method represent solutions for aerospace applications as well as for two stationary position. For an aerospace system we study the polarisation direction for a spacecraft as a function of its orbital parameter, considering an optimal attitude control system. Each polarisation alignment system proposed is designed to measure the polarisation of a polarised laser beacon. The direction of polarisation of the laser beacon is measured as a function of the polarisation direction of the polarisation bases used for quantum cryptography. The systems proposed measure the polarisation orientation of the laser beacon and this measure is used to rotate the bases used for quantum cryptography.

3.1 Quantum cryptography for satellite communication

The tracking scheme proposed in the previous chapter can be used for any kind of aerospace system. Once the systems are accurately tracked, it is necessary to adjust the angle of the polarisers of the receiver and the transmitter. The polarisation of a photon in free space does not change substantially [16]. By considering Alice as a satellite, and the horizontal basis of the polariser parallel at the orbital plane, it is possible to know the polarisation received at the ground station by using a function of the longitude μ and latitude λ. In this simulation we consider a low orbit of 300 km and 0 degrees between the Greenwich meridian and the Aries constellation. These conditions are at the initial time when the satellite crosses over the

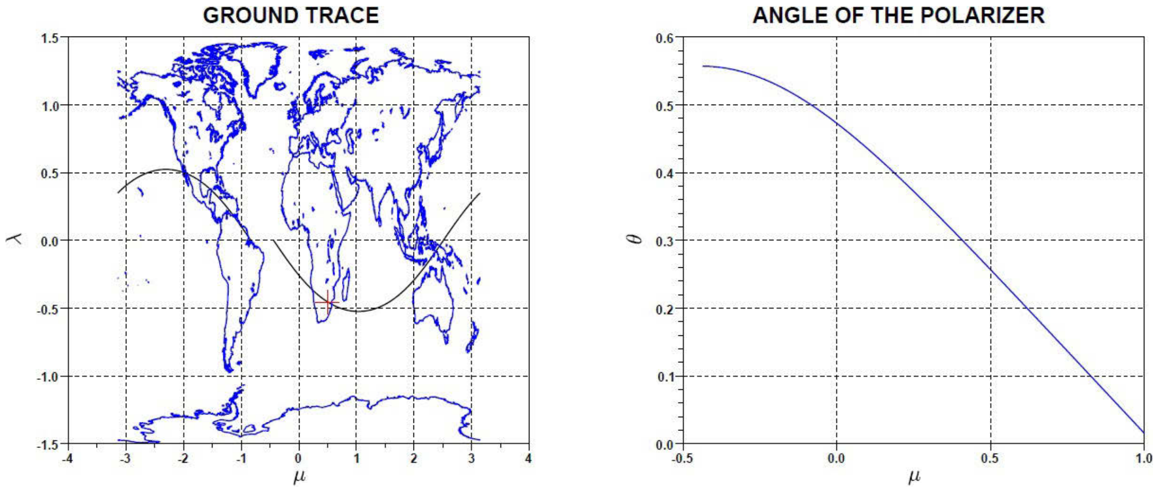


Figure 3.1: Orbit propagation and direction of the polarisation bases: Angle of polariser θ as a function of the longitude μ. It is possible to observe from the first chart the simulation which considers the satellite that crosses the geographical position of Johannesburg. Johannesburg is shown as a red cross on the Ground Trace chart. (See Appendix A.1 and A.2)

descendent node. The ground trace is calculated by considering the rotation motion of the Earth. The ground trace is given by the equations:

$$\sin\lambda = \sin(\phi)\sin(\beta), \tag{3.1}$$

where $\phi = \phi(t)$ is the angle between the position of the satellite and the line of nodes, β is the angle between the equatorial plane and the projection of the satellite's orbit on the Earth's surface. The longitude, μ, is given by [42],

$$\mu = \mu_\Omega + \omega_E \Delta t - \arcsin\frac{\cos(\phi)}{\cos(\lambda)}, \tag{3.2}$$

where $\mu_\Omega = -25$ degrees is the angle between the line of nodes and Greenwich, Δt is the change in time, and ω_E is the Earth's angular speed. In Figure 3.1 the polariser's angle θ is calculated from the nodes line up to 1 rad. The angle θ represents the angle between the line of horizontal basis of the polariser (parallel to the orbital plane) and the equatorial plane. The simulation considers the equatorial plane as the reference plane. On the ground trace, there is an additional phase per period is due to the rotation of the Earth.

3.2 Aircraft to Aircraft links

A link between two aircraft is realizable without using a complicated orientation control system of the aerospace system because it is possible to exploit the aerodynamic forces. The synchronisation of the laser is particularly easy to perform if two vehicles fly at the same altitude and are sufficiency close, since this will prevent the deviation of the laser beacon due to the chromatic dispersion [43]. In the previous section, it was possible to calculate the polariser's angles during the orbit evolution, but in this case the change in relative position between Alice and Bob is random and it is therefore impossible to predict the orientation of the polarisers for Alice and Bob during the flight. To resolve this problem, the communication systems must have appropriate polarisation compensation controls.

3.3 Satellite to satellite links

Since the satellite orbit is predictable, it is possible to know the relative position of the satellites. In a satellite to satellite link, the direction of the link and the position of the polarisers are either known, or they can be determined by using an appropriate system for tracking and collimation.

3.4 Polarisation alignment system using Polaroid foil

Previous experiments have shown the possibility of using a beam laser reference which is able to hold a correct polarisation angle between Alice and Bob [21]. A possible optical scheme for polarisation alignment system is shown in Figure 3.2. Bob has one optical receiver for the quantum channel and a laser of 532*nm* for the polarisation alignment control. The intensity of the polarized light I_0 through the Polaroid foil at an angle of θ from the polarisation axis has a final intensity according to the equation [44]:

$$I(\theta) = I_0 \cos^2(\theta). \tag{3.3}$$

The hypothetical scheme shown in Figure 3.2, supposes that Alice receives a polarized laser beacon from Bob with an angle α between $\pm\frac{\pi}{4}$ with respect to the vertical polarisation. The polarisers "Pol 1" and "Pol 2" have the polarisation direction tilted $\pm\frac{\pi}{4}$ with respect to the vertical polarisation of the quantum channel. The intensities received at P1 and P2 are

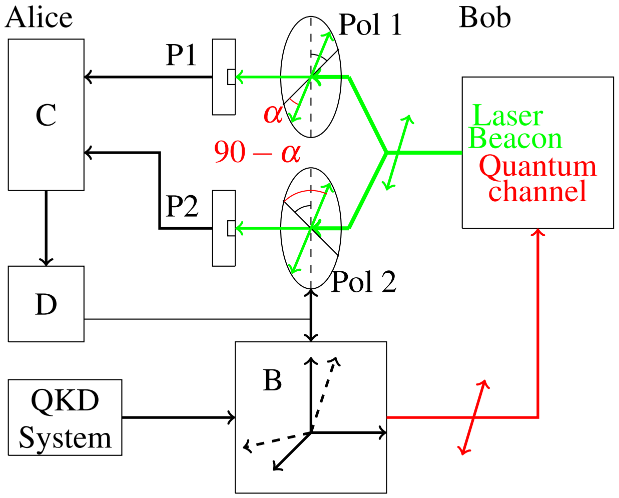


Figure 3.2: Polarisation tracking scheme: B - Polarisation bases of the quantum channel; C - Comparator; P1 - photodetector 1; P2 - photodetector 2; Pol 1, Pol 2 - polarisers; D - Mechanical devices to turn the bases (can drive a half wave plate). The polariser "Pol 1" is tilted 45° with respect to the vertical polarisation basis of the quantum channel and the polariser "Pol 2" is tilted −45° with respect the vertical polarisation of the quantum channel. In this case the polarisation of the laser beacon, indicated using the green line, is closer with the polarisation direction of the polariser "Pol 1". The signal received on the sensor "P1" is greater than the signal measured from the sensor "P2". The system is able to instantaneously recognize the direction in which the bases need to rotate. In this case the bases need to be rotated in an anticlockwise direction.

respectively expressed as:

$$I_{P1} = \cos^2(\alpha), \tag{3.4}$$

and

$$I_{P2} = \cos^2(\frac{\pi}{2} - \alpha). \tag{3.5}$$

The output is measured as a proportion of voltage to the intensity of light. The signal difference $V_{OUT} = V(I_{P1}) - V(I_{P2}) > 0$ dictates the drive turn of the polariser until the difference is zero. The polariser must be geometrically close in order to collect the same signal. In this system it is necessary that the divergence of the spot is big enough to hit both polarisers. If the channel is affected by strong turbulence due to the non-uniform spot, the intensity measured from the sensor P1 and P2 may be different although the system is aligned.

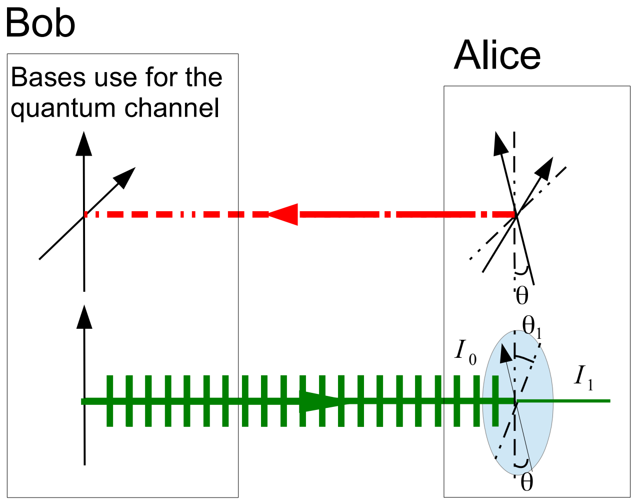


Figure 3.3: Conceptual scheme of a polarisation tracking scheme using one polariser: The black dashed line represents the polarisation direction of the polariser. The green lines represent the polarisation direction of the laser beacon. θ is the angle between the directions of polarisation of the laser and the polariser. When the laser crosses the polariser the intensity in output follows the Equation (3.6). This simple scheme supposes the knowledge of the power received. Equation (3.6) does not give the information of the direction in which the bases need to be rotated. For this system it is necessary to use an algorithm able to find the maximum signal in output of the polariser.

3.5 Polarisation alignment system using one laser beacon and one polariser

In order to align the polarisation bases of the transmitter and receiver, the system uses a vertical polarized laser beacon [43] and one polariser. The wavelength of the laser beacon and the wavelength of the single photons are different. The polarisation direction of the laser beacon is aligned with the polarisation bases used by Bob for quantum transmission. The polariser is mounted on Alice's side, and the direction of polarisation is aligned with Alice's polarisation bases for quantum transmission. The system is shown in Figure 3.3. Bob transmits the laser beacon to Alice. Alice receives the signals affected by scintillation and wandering due to atmospheric turbulence. The turbulence effects on the polarisation of the laser beacon can be neglected [16]. When a polarized laser beacon with the intensity I_0 crosses a polariser, the output intensity follows the Malus' law which is expressed as:

$$I_1 = I_0 \cos^2(\theta), \tag{3.6}$$

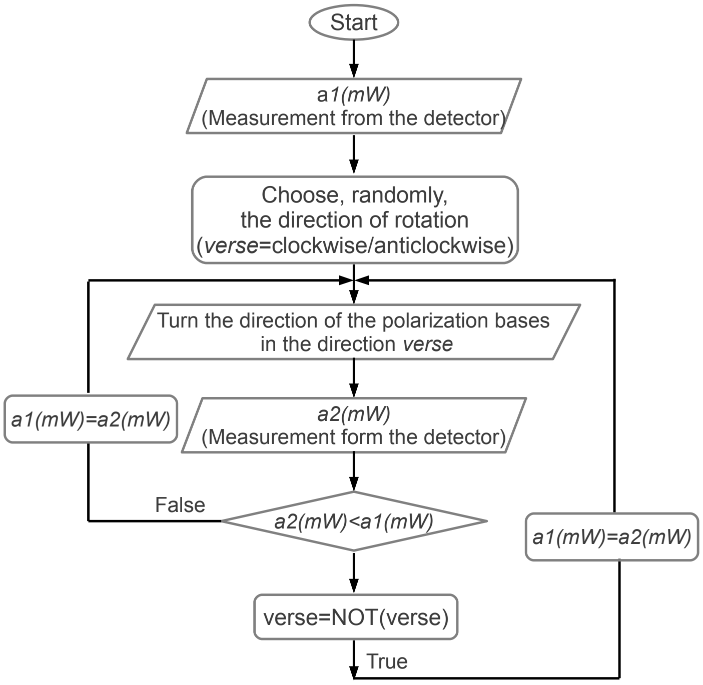

Start
a1(mW)
(Measurement from the detector)
Choose, randomly,
the direction of rotation
(verse=clockwise/anticlockwise)
Turn the direction of the polarization bases
in the direction verse
a1(mW)=a2(mW)
a2(mW)
(Measurement form the detector)
False
a2(mW)<a1(mW)
a1(mW)=a2(mW)
verse=NOT(verse)
True

Figure 3.4: The flowchart shows the algorithm used to determine the direction of vertical polarisation: The power received from the sensor, is measured using a microcontroller that stores this value in the variable $a1$. The microcontroller randomly chooses the rotation of the polarisation basis of the polariser and the bases of the quantum channel and gives the command to a step motor, for example clockwise. According to the Malus Law, once the bases are rotated, the sensor receives another value of power. This value of power is stored in the variable $a2$. If $a2 < a1$, the value of $a2$ is stored in the variable $a1$ and the verse of rotation is still clockwise. The microcontroller measures the power again ad store the value in the variable $a2$. If $a2 > a1$ means that the vertical polarisation was measured in the previous step. The direction of rotation must be changed to anticlockwise and the value of $a2$ is stored in the variable $a1$. (See Appendix A.4).

where I_0 is the intensity of the spot in the input of the polariser and I_1 is the intensity of the spot in the output. θ is the angle between the direction of the polarisation of the laser and the direction of the polarisation of the polariser. When $\theta = 0$, it follows that $I_1 = I_0$. Since the intensity changes with time due to atmospheric turbulence, it is not possible to know the value of I_0 in advance. As shown in Figure 3.3, there is an ambiguity between θ and θ_1. In order to find the correct direction, the polariser can be rotated until the maximum value of intensity is measured. The algorithm is shown in Figure 3.4. Alice's tracking system measures the intensity I_1 stored in the variable *a1(mW)*. The system for example randomly chooses a clockwise bases rotation and the power drive, mechanically turns the bases of the quantum channel and the polariser. Alice measures the intensity of the laser beacon and stores

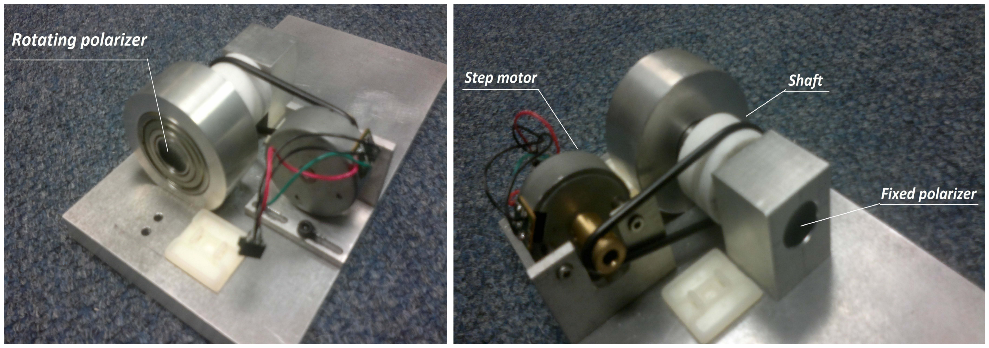


Figure 3.5: Mechanical experimental devices, used to track the polarisation bases: The stepper motor moves the rotating polariser mounted on the shaft. The rotating polariser, represents the Alice's side. The laser is incident on the fixed polariser to create a reference signal. The fixed polariser represents Bob's side. The signal is acquired from the detector fixed to the rotating polariser. The microcontroller acquires the signal from the detector, and rotates the shaft until the polarisers are aligned.

this value in variable *a2(mW)*. If *a2* is smaller than *a1*, Alice changes the verse of rotation anticlockwise. If *a2>a1* the direction of rotation does not change from clockwise. This kind of system cannot work properly when atmospheric turbulence is strong. The bases cannot be stable in one direction and an oscillation about the vertical position occurs. The experimental setup is shown in the Figure 3.5. The side where the fixed polariser is mounted represent the position of Bob. The fixed polariser is used in order to create a polarized laser beacon. Initially the polarisers are not aligned and the shaft starts to rotate as per the micro-controller command. For our experiment, a step motor was used. The step motor is used to control the speed and the extent of rotation. At each step the micro-controller measures the intensity of the signal output from the rotating polariser and decides the direction of rotation by using the algorithm in Figure 3.4. This system can be modified as shown in Figure 3.10 in order to calculate the angle θ.

Bob sends the laser beacon to Alice. A beam splitter divides the signal in the directions of detector P1 and detector P2. The signal measured from the detector P1 can be used to calculate the initial intensity I_0 and by the inverse Equation (3.6), it is possible to calculate the angle θ because the initial intensity is measured by the sensor P2. Regardless of the ambiguity regarding direction of rotation, it is still possible to follow the algorithm shown in Figure 3.4 and find the polarisation direction. Instead of using the intensity, the algorithm can use the angle θ. The angle θ can be calculated by the inverse of Equation (3.6). The last configuration is the best way if the alignment system works in a turbulent environment because the total power I_0 is known by the measurement of P1 after previous corrections.

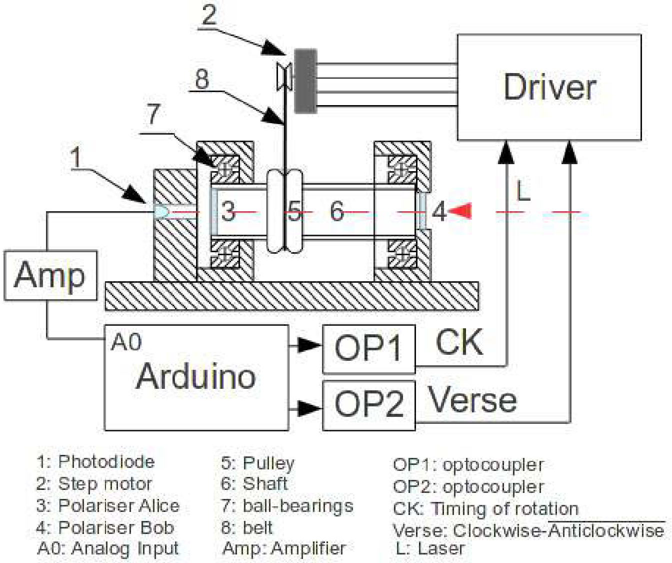


Figure 3.6: Mechanical drawing and electronics of polarisation tracking: The fixed polariser is indicated by number 4. The rotating polariser 3 is fixed on the shaft, and represents the direction of the polarisation bases of Alice. The shaft is rotates via by a stepper motor through a belt. The output signal from polariser 3 is measured by a photodiode and it is amplified. The Arduino microcontroller measures the amplified signal and by the algorithm shown in Figure 3.4 controls the extent of rotation. The microcontroller does not control the driver for the stepper motor, but is separated using two optocouplers "OP1" and "OP2". In this way the Arduino is electrically isolated from the power system used to control the stepper motor. The driver is controlled using two signals. One signal is "CK" and is the timing to control the speed of rotation, and "Verse" controls the direction of rotation.

3.6 Polarisation base alignment system using a polarizing beam splitter

The system in Figure 3.6 is able to work when Alice and Bob are located two fixed points. In our recent system (Patent **P1**), a polarizing beam splitter as shown in Figure 3.11 and is able to work in non-stationary conditions [45]. If the polarisation of the beam is not aligned with the bases of Alice, Detector 1 receives the intensity, $I_1(\theta) = I_0 \cos^2 \theta$, where θ is the angle of misalignment. The detector 2 receives the intensity, $I_2(\theta) = I_0 \sin^2 \theta$. Theoretically, we obtain the graph shown in Figure 3.12 where we plot I_1 and I_2 as a function of the angle θ. In order to align the system, the laser beacon is sent with a polarisation of 45° with respect to the vertical polarisation. Alice by the measure of the intensity $I_1(\theta)$ and $I_2(\theta)$ is able to know the degree and direction of rotation. The system is aligned when $I_1 = I_2$. It is possible to calculate the angle without ambiguity. By comparing the signals, it is possible

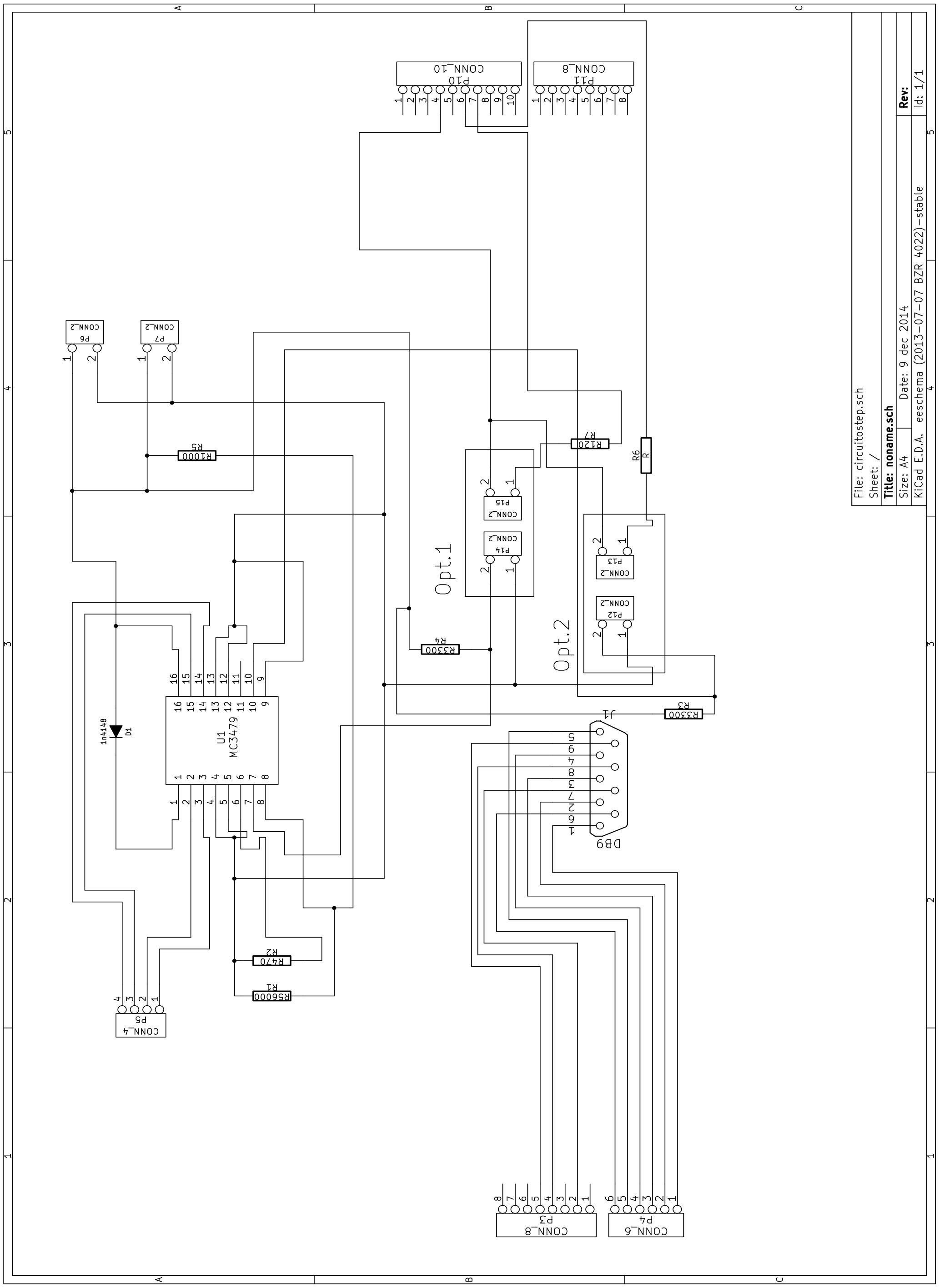


Figure 3.7: Electronic scheme adapted to Arduino to drive the step motor: An IC MC3479 is the driver for the step motor. This driver uses one clock impulse to increase the step and another is used to change the direction of rotation. Arduino is electrically isolated from the IC, using two optocouplers Opt.1 and Opt.2.

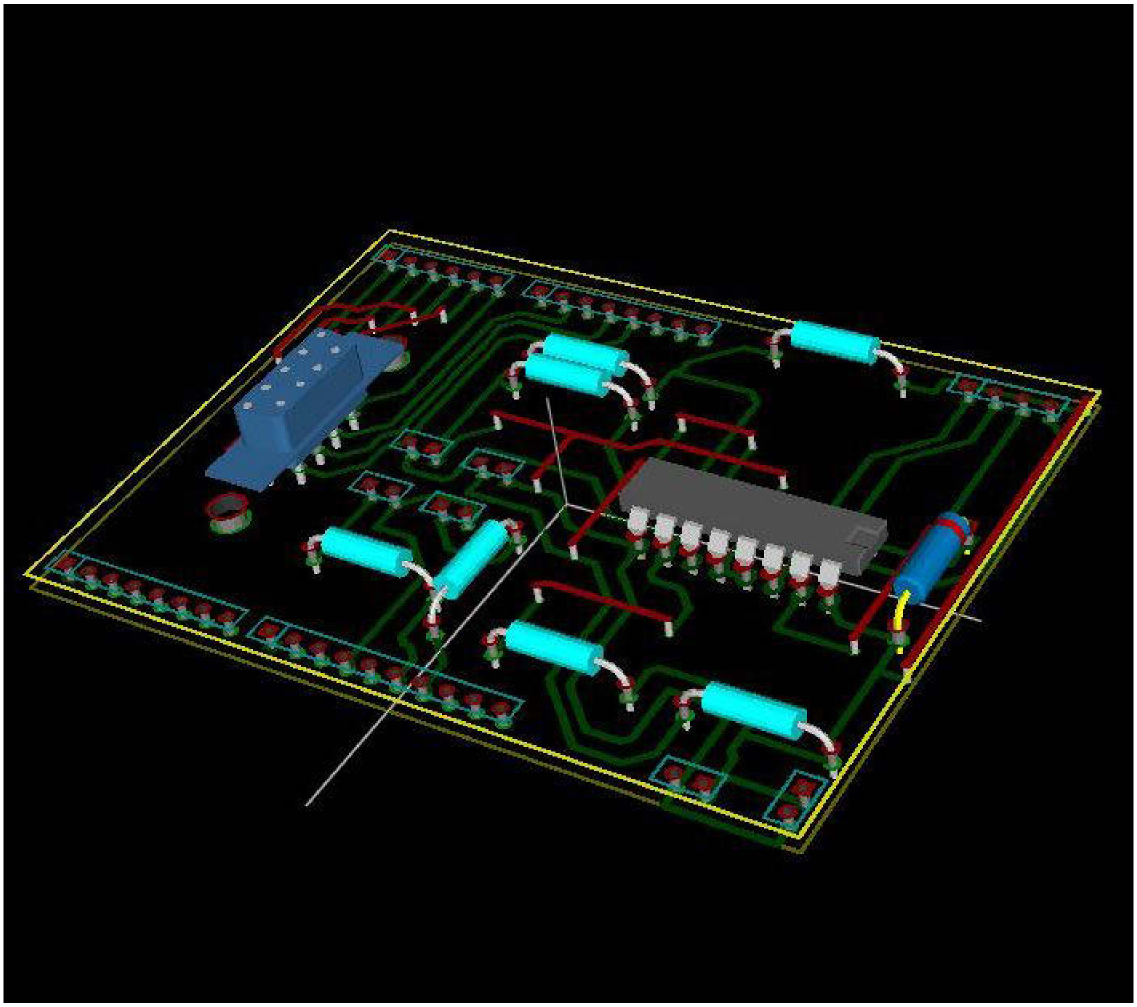
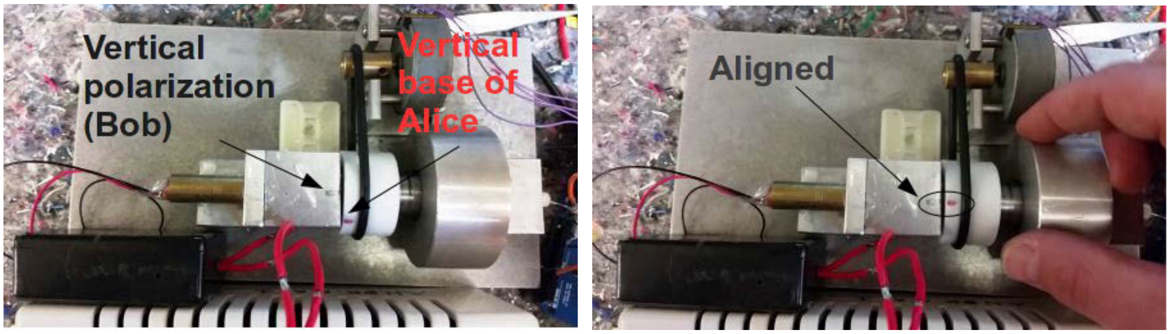


Figure 3.8: 3D rendering of printed circuit board of the scheme shown in Figure 3.7.



(a) Misalignment at the start

(b) Alignment

Figure 3.9: Test of the alignment system using one polariser: The black mark is the vertical polarisation direction of the fixed polariser while the red mark is the direction of polarisation of the rotating polariser fixed on the shaft. Initially, as shown in (a) the polarisation bases are not aligned. Once the system is on, the microcontroller is able to align the bases as shown in (b).

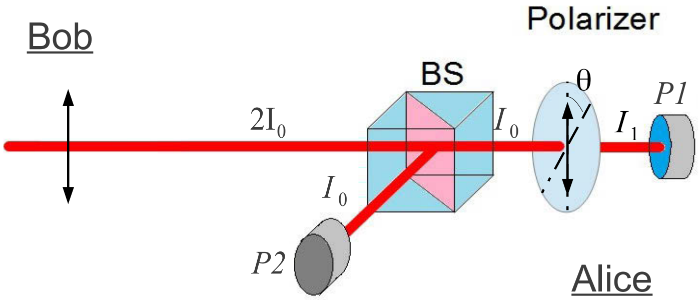


Figure 3.10: Improvement of the alignment system using one polariser: The beam is split at the beam splitter (BS), the value of I_0 can be determined from the value measured in detector P1. The angle can be calculated by the equation $\theta = \arccos \sqrt{\frac{I_1}{I_0}}$.

to know in which direction the systems should be rotated. This system can work by using a programmable logic unit or using analog controls.

3.7 Implementation of the alignment bases system using a polarizing beam splitter

As discussed in Section 1.5.2, the presence of Eve is detected through the analysis of errors in the transmitted key. If the polarisation bases of Alice and Bob are not aligned, the number of errors in the key might cause Alice and Bob to believe that Eve is in the channel. In

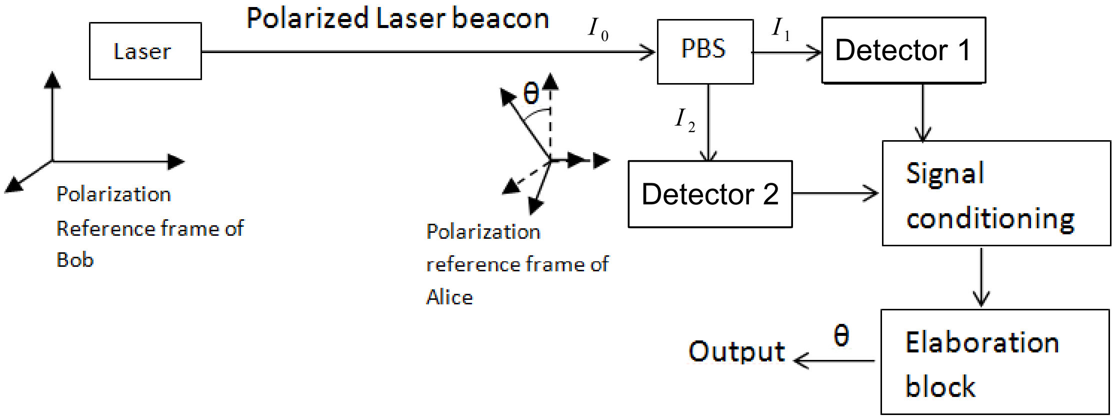


Figure 3.11: Provisional patent no. 2014/03405: The laser beacon is sent from Bob to Alice. Alice receives the signal from Bob and measures the intensity $I_1 = I_0 \cdot \cos^2\theta$ and $I_2 = I_0 \cdot \sin^2\theta$. The angle θ can be calculated as arctan $\sqrt{\frac{I_2}{I_1}}$. Once the angle θ is calculated, it is possible to know in which direction we need to rotate to align the bases. The rotation occures for the bases used for the quantum channel and for the bases of the PBS.

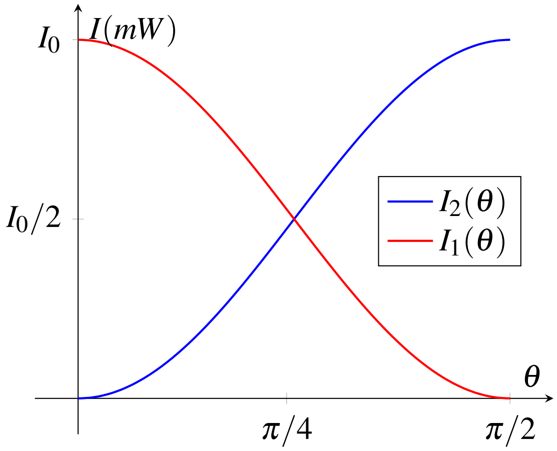


Figure 3.12: Output intensities for an ideal PBS: I_1 and I_2 are the theoretical intensity to be measured from the Detector 1 and Detector 2 according to the Figure 3.11. The measurements of both channels make it possible to calculate the angle θ.

this section, we describe a practical scheme which can be used to align the measurement bases. The bases are aligned by using a laser beacon and a polarizing beam splitter (PBS) as proposed in section 3.6. The chapter is based on the manucripts **P1**and **M1**.

3.7.1 The system

As described in section 3.6 the principal component of our proposed system is a PBS. In our system, Bob sends a polarized laser beacon where the direction of polarisation is 45° with respect to the vertical bases of the quantum channel. The vertical basis of the PBS is also aligned with the vertical basis of the quantum channel. Once Alice receives the signal from Bob, on the sensor $P1$ and $P2$ we measure the following intensities:

$$I_1 = I_0 \cos^2 \alpha, \tag{3.7}$$

and

$$I_2 = I_0 \sin^2 \alpha, \tag{3.8}$$

where I_0 is the intensity of the input light for the PBS, I_1, I_2 are the intensities measured from the sensor P_1 and P_2 (see Figure 3.13). According to the Malus Law, the bases of the quantum channel will be aligned when $I_1 = I_2$. The tilt angle α can be determined by using

$$\alpha = \arctan \sqrt{\frac{I_2}{I_1}}. \tag{3.9}$$

From here on, we indicate I_0, I_1 and I_2 using units of (mW). From Table 3.1 we observe that the PBS is close to the ideal behavior when $\alpha = 45°$. This shows that it does not follow a theoretical behavior. Therefore it is necessary to characterize the PBS that one wants to use.

3.7.2 The experiment

The optical scheme for polarisation tracking is shown in Figure 3.13. The experiment was performed by using a polarised laser beacon $L1$, initially polarized at an angle $\alpha = 90°$ with respect to the vertical polarisation of the PBS. The wavelength of the laser is $780nm$. A half wave plate is used to change the polarisation direction of the laser beacon. Based on the experiment, it was observed that the Equations (3.7) and (3.8) become:

$$I_1 = (I_0 - I_{Br} - I_{Lr}) \cos^2 \alpha + I_{OFF}, \tag{3.10}$$

$$I_1 = (I_0 - I_{Br} - I_{OFF}) \sin^2 \alpha + I_{Lr}, \tag{3.11}$$

Table 3.1: Experimental measurement taken form the optical scheme shown in Figure 3.13: $I_1(mW)$ is the power measured from the sensor P1; $I_2(mW)$ is the power measured from the sensor P2. "Cal. Angle" is the calculated angle using the Equation (3.9). The laser L_1 is a vertical polarised laser beacon. By using the HWP the direction of polarisation was rotated from 0° to 90°, using a step of 4°. For each step the powers $I_1(mW)$ and $I_2(mW)$ were measured. From these measurements the minimum error occurs around 45° where the PBS output is optimal. For an angle of 45° the calculated angle has an error of 0.64°.

Angle (Degrees)	$I_1(mW)$	$I_2(mW)$	Cal. Angle
90	0.01	2.64	86.52
86	0.04	2.60	82.97
82	0.08	2.57	80.03
78	0.15	2.50	76.28
74	0.24	2.42	72.56
70	0.36	2.29	68.41
66	0.47	2.19	65.18
62	0.62	2.03	61.10
58	0.76	1.89	57.65
54	0.96	1.70	53.10
50	1.10	1.57	50.09
46	1.26	1.41	46.63
42	1.45	1.23	42.67
38	1.61	1.07	39.21
34	1.79	0.90	35.36
30	1.92	0.77	32.36
26	2.06	0.64	29.15
22	2.17	0.52	26.10
18	2.28	0.42	23.24
14	2.36	0.35	21.07
10	2.42	0.28	18.80
6	2.46	0.25	17.69
2	2.47	0.24	17.32

where I_{Br} is the intensity that is back reflected from the PBS, I_{Lr} is a fraction of the intensity that is laterally reflected from the side of the sensor $P2$ for any angle of polarisation. I_{OFF} is a fraction that crosses the PBS for any polarisation angle. The power fraction is visible from Figure 3.14: The measured total power is given by $I_{TOT} = I_1 + I_2$. The average value of I_{Lr} is 10% of I_{TOT} and I_{Br} is the 1% of I_{TOT}. Due to the accuracy of the measurement devices, other errors may occur. In order to align the bases, we can follow the two methods described

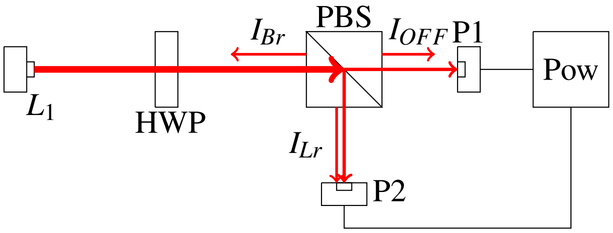


Figure 3.13: Optical setup of the polarisation alignment system using a PBS: P1, P2 - photodiode; Pow - Power meter; I_{OFF} - Frontal offset; I_{Lr} - Lateral offset; I_{BR} - Back reflection; L_1 - Laser beacon; the laser, indicated with L_1 is polarized and represents the laser beacon. Using a half wave plate (HWP) it is possible to change and measure the polarisation direction of the laser beacon. For each angle the power was measured and the results shown in Table 3.1 were obtained. The experiment was performed for different values of power of the laser beacon.

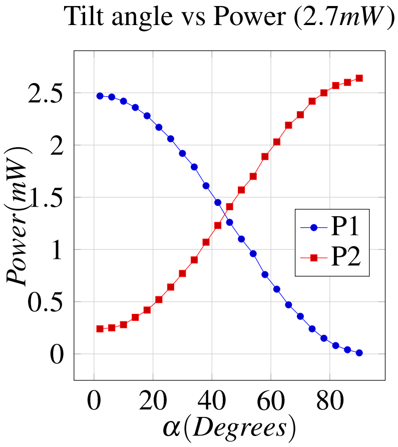


Figure 3.14: The power $I_1(mW)$ and $I_2(mW)$ measured for different polarisation angles: It is possible to observe the amount of power lateral reflected I_{Lr} and the amount of power that crosses the PBS for 90° of polarisation I_{OFF}.

in subsection 3.7.3 and 3.7.4.

3.7.3 Alignment by comparing I_1 and I_2

We can observe fro1m the experimental results shown in Figure 3.14 that there is a point where the power detected from the sensor $P1$ is equal to the power measured on the sensor $P2$. It is possible to fix one of the nodes and rotate the laser beacon to an angle of $45° \pm \Delta\alpha$ with respect to the vertical polarisation of the quantum channel. The angle $\Delta\alpha$ is sufficient to obtain $I_1 = I_2$ when the polarisation bases of Alice and Bob are aligned. If a misalignment occurs between Alice and Bob by a clockwise rotation, the signal received on the sensor $P1$ is bigger than the signal received on the sensor $P2$ (See Figure 3.14. By a comparator device, the system is able to rotate rapidly in an anticlockwise direction until the condition $I_1 = I_2$ is met. The device for achieving this can be made from an analog circuit that has a fast response in function of the input signals I_1 and I_2.

3.7.4 Correction algorithm

Theoretically, it is not possible to use the Malus Law from Equations (3.7) and (3.8) because the real behavior of the PBS is not ideal. To know the tilt angle between the polarisation bases α of Alice and Bob, it is possible to add a correction function to calibrate the PBS once it has been characterized. Each measurement from the Channel P1 (I_1) and Channel P2 (I_2) is normalized with respect to the total power, $I_{TOT} = I_1 + I_2$ and are indicated as I_{1N} and I_{2N}. The test was done for a power of $2.7mW$. The angle α was calculated by using Equation (3.9). The correction function is a polynomial function which is found by fitting the error measured from the half wave plate subtracted from the calculated angle. The function of the curve of the error $\Delta\alpha$ is shown in equation (3.12).

$$\begin{aligned}\Delta\alpha_{err}(I_{2N}) \quad = \quad & -4.4183529 \cdot 10^3 \cdot I_{2N}^{10} + 2.6516046 \cdot 10^4 \cdot I_{2N}^{9} - 6.9067889 \cdot 10^4 \cdot I_{2N}^{8} + \\ & 1.0242461 \cdot 10^5 \cdot I_{2N}^{7} - 9.5322069 \cdot 10^4 \cdot I_{2N}^{6} + 5.7860943 \cdot 10^4 \cdot I_{2N}^{5} + \\ & -2.3060932 \cdot 10^4 \cdot I_{2N}^{4} + 5.9228588 \cdot 10^3 \cdot I_{2N}^{3} - 9.3386548 \cdot 10^2 \cdot I_{2N}^{2} + \\ & +8.1854136 \cdot 10^1 \cdot I_{2N} - 3.13918375. \qquad (3.12)\end{aligned}$$

The final equation used to calculate the angle is then expressed as :

$$\alpha = \arctan\sqrt{\frac{I_2}{I_1}} + \Delta\alpha_{err}. \qquad (3.13)$$

Using the Equation (3.13) the mismatch angle between the calculated and the measured angle is shown in the table 3.2 for an average total power of $2.67mW$. The polarisation bases of Alice and Bob are aligned with the vertical polarisation bases of the quantum channel when Alice measures 45° with respect to the vertical polarisation of the PBS. This system can be used in free space communication, we can consider Alice and Bob to be located on two non-stationary points. The mutual displacement of Alice and Bob can be simulated by varying the laser power. Table 3.3 shows the error between the calculated error and the angle measured

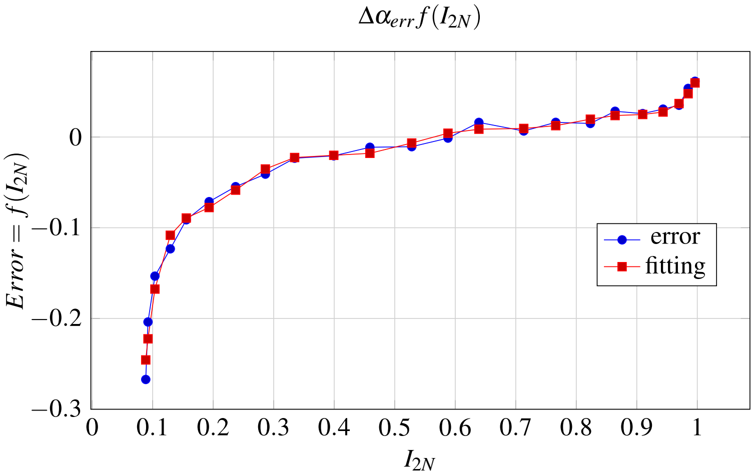


Figure 3.15: Error on the angle due to the non ideal behavior of the polarizing beam splitter: The curve indicated with the red line, represents a polynomial function that is the best approximation of the error between the measured polarisation angle and the system calculated angle. This value is found by the normalization of the power I_2. The approximation of the error is added to the value calculated by the Equation (3.9) in order to approximate an ideal behavior of the PBS.

by the half wave plate at 45°, for different values of average power.

3.8 Summary

The proposed system is able to align the polarisation bases in two different ways. The alignment can be done by comparing the signals from the sensor P1 and P2. When the signal from the sensor P1 is different from the sensor P2, the system rotates the bases until the signal $I_1 = I_2$. This system can be implemented using an analog or digital comparator and does not require a correction equation. Figure 3.16 shows that the system is able to follow polarisation changes. In this experiment, by using an HWP, the polarisation was changed, and the system was able, by Equation (3.13), to follow the rotation immediately. In this experiment the values of power were measured by the Arduino, and the data was sent to the computer in order to visualize it. This system can work without a computer because the microcontroller is able to control polarisation through a power interface to the mechanics. The correction, using Equation (3.12), can be used to determine the real angle of the polarisation basis tilt. In the final section a portable tracking system is presented. In our case the alignment was done by comparing the signal I_1 and I_2.

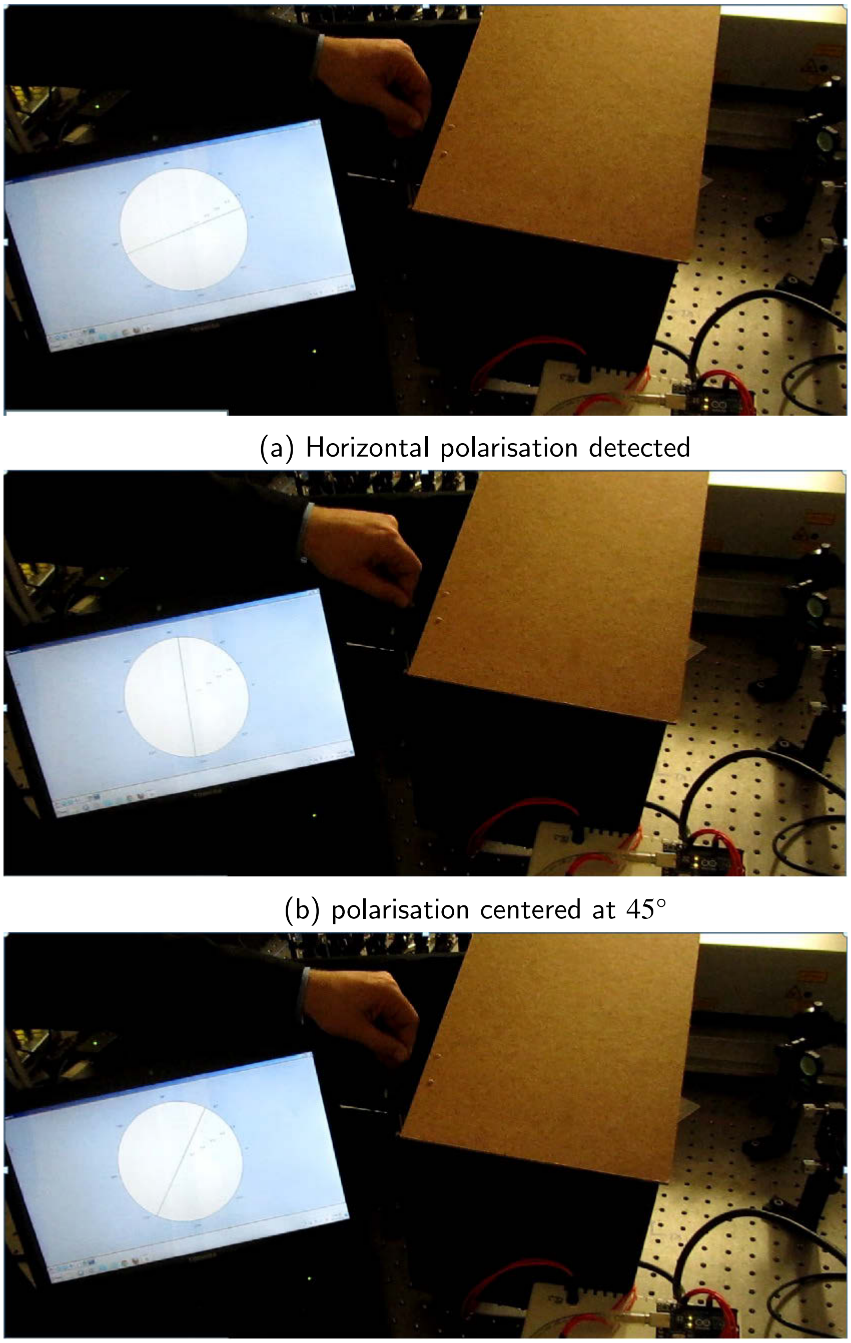
An important issue is the amount of information that Eve can leak due to transmission errors. With a tilt angle of the polarisation bases lower than 20°, the number of errors during the key exchange does not allow Eve to obtain too much information about the key [46]. If Bob sends the polarised laser beacon to Alice, and Alice measures the polarisation bases using the system proposed, the error is lower than 1° as depicted on Table 3.3 and does not require feedback to Bob.

Table 3.2: Calculation of the angle using the corrected Equation (3.13): A - Angle calculated by the Equation (3.9); B - Difference between the measure and calculated angle; C - Calculated angle added with the value of the function of error $\Delta\alpha_{err}$; D - Corrected angle indicated in Degrees; E - Error after correction

Angle (Deg.)	Ang.(rad)	A	B	C	D	E
90.0000	1.5708	1.5093	0.0615	1.5689	89.9398	0.0602
86.0000	1.5010	1.4474	0.0536	1.4951	85.7079	0.2921
82.0000	1.4312	1.3962	0.0350	1.4331	82.1497	-0.1497
78.0000	1.3614	1.3306	0.0308	1.3581	77.8540	0.1460
74.0000	1.2915	1.2657	0.0258	1.2906	73.9811	0.0189
70.0000	1.2217	1.1933	0.0284	1.2170	69.7631	0.2369
66.0000	1.1519	1.1370	0.0149	1.1566	66.3039	-0.3039
62.0000	1.0821	1.0659	0.0162	1.0784	61.8219	0.1781
58.0000	1.0123	1.0057	0.0066	1.0151	58.1916	-0.1916
54.0000	0.9425	0.9264	0.0161	0.9350	53.5972	0.4028
50.0000	0.8727	0.8739	-0.0012	0.8781	50.3365	-0.3365
46.0000	0.8029	0.8135	-0.0107	0.8069	46.2556	-0.2556
42.0000	0.7330	0.7443	-0.0113	0.7264	41.6381	0.3619
38.0000	0.6632	0.6840	-0.0207	0.6638	38.0519	-0.0519
34.0000	0.5934	0.6168	-0.0234	0.5942	34.0622	-0.0622
30.0000	0.5236	0.5645	-0.0409	0.5293	30.3421	-0.3421
26.0000	0.4538	0.5085	-0.0547	0.4499	25.7920	0.2080
22.0000	0.3840	0.4552	-0.0713	0.3775	21.6396	0.3604
18.0000	0.3142	0.4054	-0.0913	0.3161	18.1228	-0.1228
14.0000	0.2443	0.3676	-0.1233	0.2593	14.8653	-0.8653
10.0000	0.1745	0.3279	-0.1533	0.1602	9.1859	0.8141
6.0000	0.1047	0.3086	-0.2039	0.0862	4.9392	1.0608
2.0000	0.0349	0.3022	-0.2673	0.0565	3.2360	-1.2360

Table 3.3: Alignment error for different laser powers: The table shows the error alignment at 45° without using the correction and by using the correction algorithm.

Total power (mW)	1.28	1.93	2.67	3.30	4.06
Error at 45° corrected	0.17	0.11	0.10	0.24	0.06
Error at 45° no corrected	0.41	0.47	0.64	-0.36	0.61



(a) Horizontal polarisation detected

(b) polarisation centered at 45°

(c) Vertical polarizarization detected

Figure 3.16: Experiment of the bases tracking using Arduino: The direction of polarisation of the laser beacon is rotated from 90° to 0° with respect the vertical polarisation, by using a half wave plate. The measurement was done by two photidiodes, and one microcontroller. Once the microcontroller calculated the angle, it was transmitted to the computer in order to visualize the tilt with respect to the vertical base.

Chapter 4

Portable tracking system for quantum cryptography and radio communication

In the previous chapters was analyzed different methods for fine alignment the bases of the transmitter (Alice) and the receiver (Bob), as well as the methods which implement the GPS coordinates for coarse alignment of the transmitter and the receiver. In this Chapter we will analyze the electronic systems implementing the algorithms proposed in Chapter 3 and 4.6 are analyzed. In order to perform our analysis we exploit the Open-Source tools which are described in Chapter 2.10.

4.1 Block scheme of the embedded system

The portable tracking system was built using several blocks, as shown in Figure 4.1. The system consits of four different voltage regulators $(+5V, +5V, \pm V)$ which are connected to the rectifier. The microcontroller is powered by a single 5V voltage regulator while the other 5V regulator provides power for a stack of the shift register, the liquid crystal dispaly (LCD) and the analog keyboard. Two variable voltage regulators provide +12V and -12V for the amplifiers of the photo-diodes. The outputs of the voltage regulator can be varied accordingly using a potentiometer. The microcontroller which we use in our system is an ATMEGA328P and is programmed by using an Arduino IDE. The microcontroller consists of a fourteen digital Input/Output (I/O) line and six multiplexed analog input lines linked with a successive approximation analog to digital converter indicated with the letter “A” on the block scheme. The clock frequency of the Micro-controller was set to 16MHz. In the scheme, V_{ref} indicates the reference voltage for the analog to digital converter. The analog input “A0”, is used for

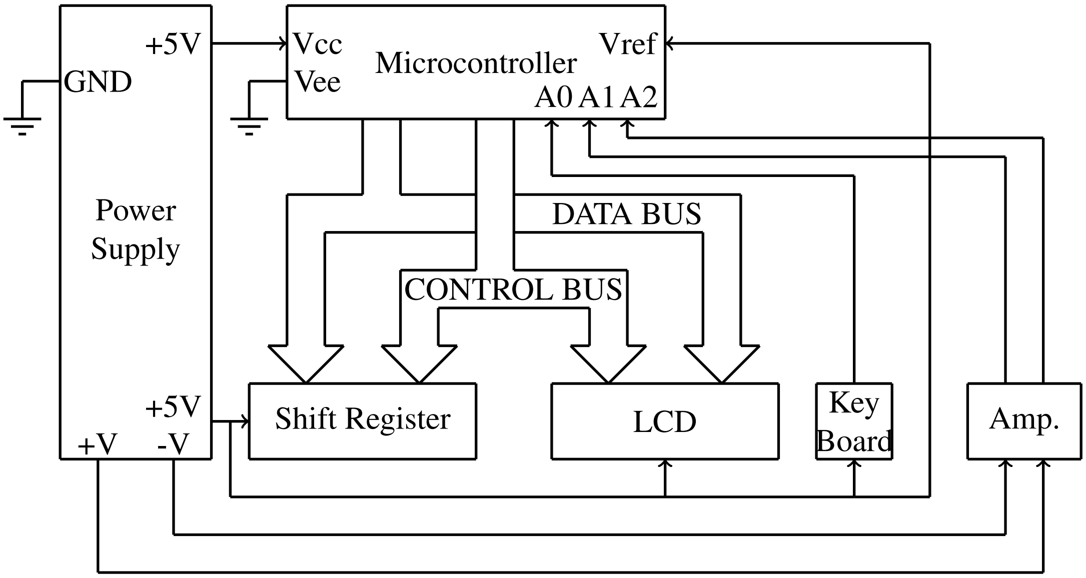


Figure 4.1: Scheme block of the portable tracking system: The microcontroller has an independent power source of $5V$. The CONTROL BUS and the DATA BUS are unidirectional and are used for the Shift register and for the LCD. Only three of the six analog to digital converter are used for the keyboard and the for the amplifiers output. The keyboard used a $5V$ voltage regulator which was also connected with the LCD and the shift register. The system has a double voltage regulator for the external amplification circuits.

the analog keyboard while the inputs “A1” and “A2” are used for photodiode amplifiers. It is also important that the keyboard is powered from the regulator which is linked to the voltage reference pin of the microcontroller. This forms a condition for our keyboard to function properly. The variable voltage regulator ($\pm V$) in the system is used to protect against short circuiting. The amplifier circuit is not part of the final system one could utilise a different amplifier with the system.

In order to accommodate future application of the digital outputs such as using a stepper motor for the bases alignment or tracking, we use a stack of shift registers. They provide an extension of 32 output digital pins. The shift register is controlled by a five digital I/O line. The microcontroller has three free lines for analog to digital conversion and these can also be used as digital I/O lines if necessary.

4.1.1 Main algorithm

Once the system has been turned on, the menu will be displayed on the LCD. The microcontroller sets the analog pin wired with the keyboard and continuously reads the output of the keyboard until a drop of voltage between the analog input pin and ground occures as

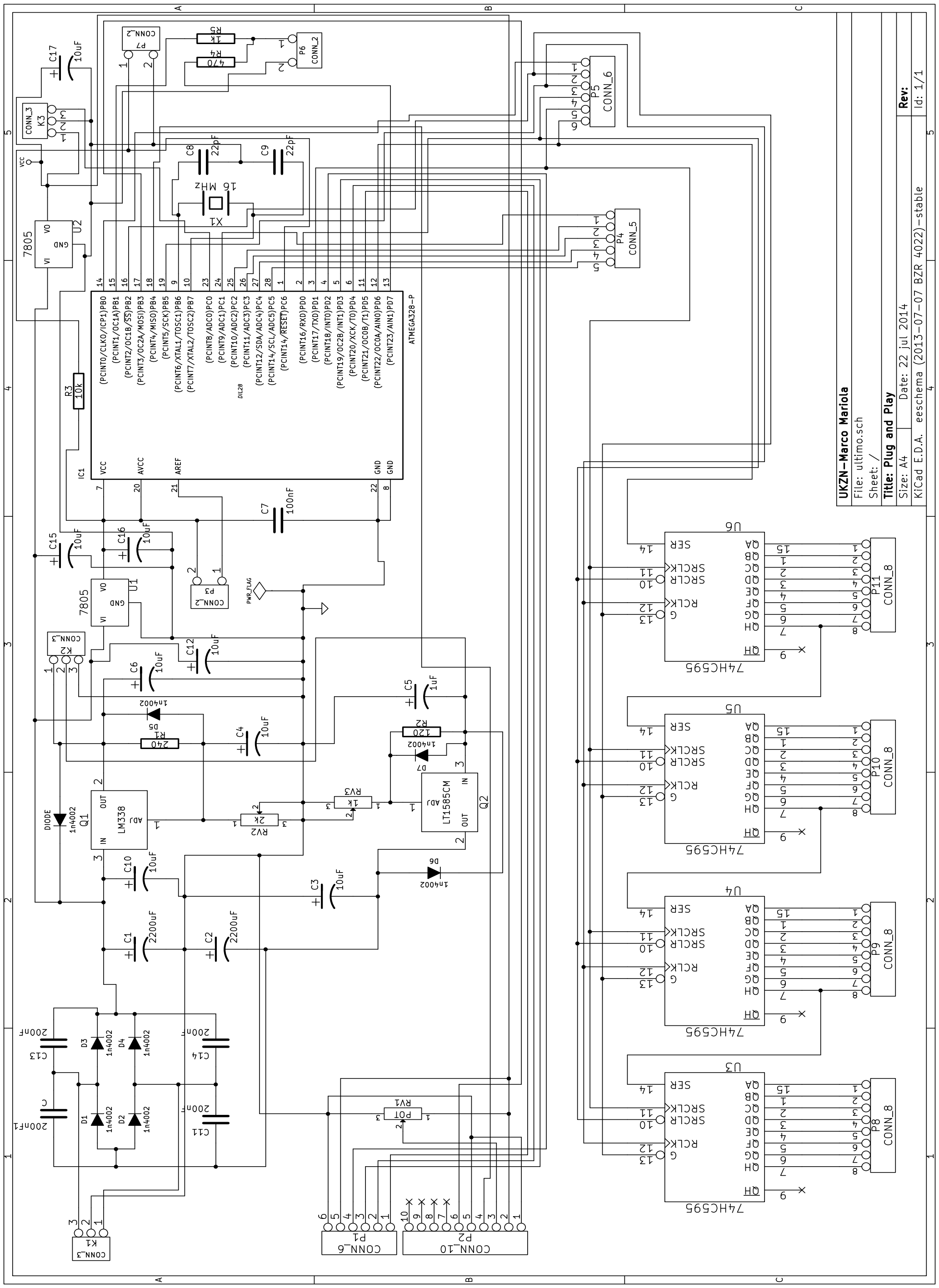


Figure 4.2: Scheme of the portable tracking system.

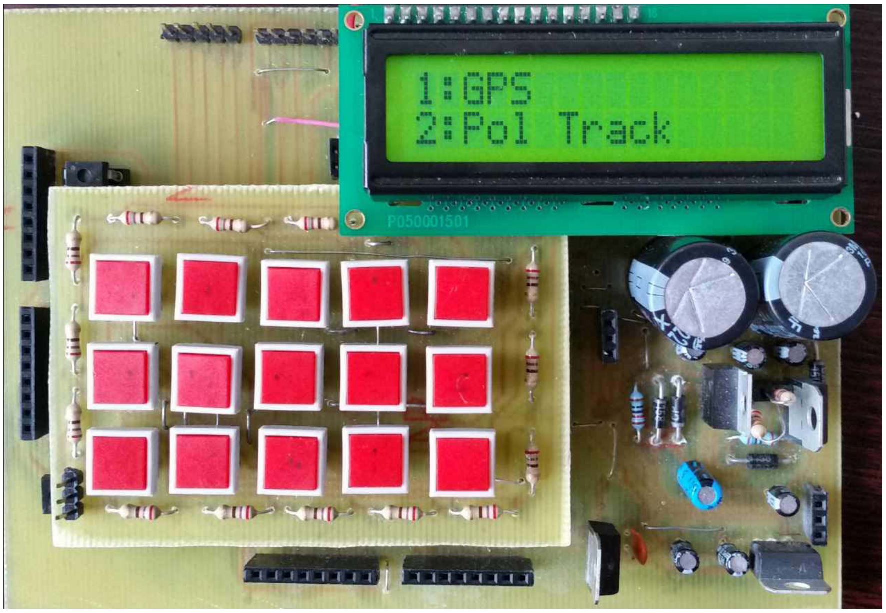


Figure 4.3: Complete scheme of the portable tracking scheme.

evaluated by Equation (4.13) gives number $n = 1$ or $n = 2$. If $n = 1$, runs the algorithm for the GPS tracking system and once the subroutine is processed, the angles θ and ϕ are shown. If $n = 2$, the system runs the algorithm for polarisation alignment. After this algorithm is completed, the system will be frozen until another button on the keyboard is pressed. The main algorithm is shown in Figure 4.4(a). Each subroutine (GPS or polarization alignment) contains the local variables that are cleared from the random access memory (RAM) once the calculation is finished.

4.1.2 GPS subroutine

The micro-controller will sequentially request the latitude, longitude, and altitude of the reference station of both the transmitter and receiver as shown in Figure 4.4(b). The coordinates are transformed into Cartesian coordinates according to the Equations (2.11), (2.12) and (2.13). In order to simplify the insertion of data from the user, the coordinates are inserted as decimal degrees. The microcontroller follows process the data according to the algorithm proposed in Section 2.5.1.

4.1.3 Polarization tracking subroutine

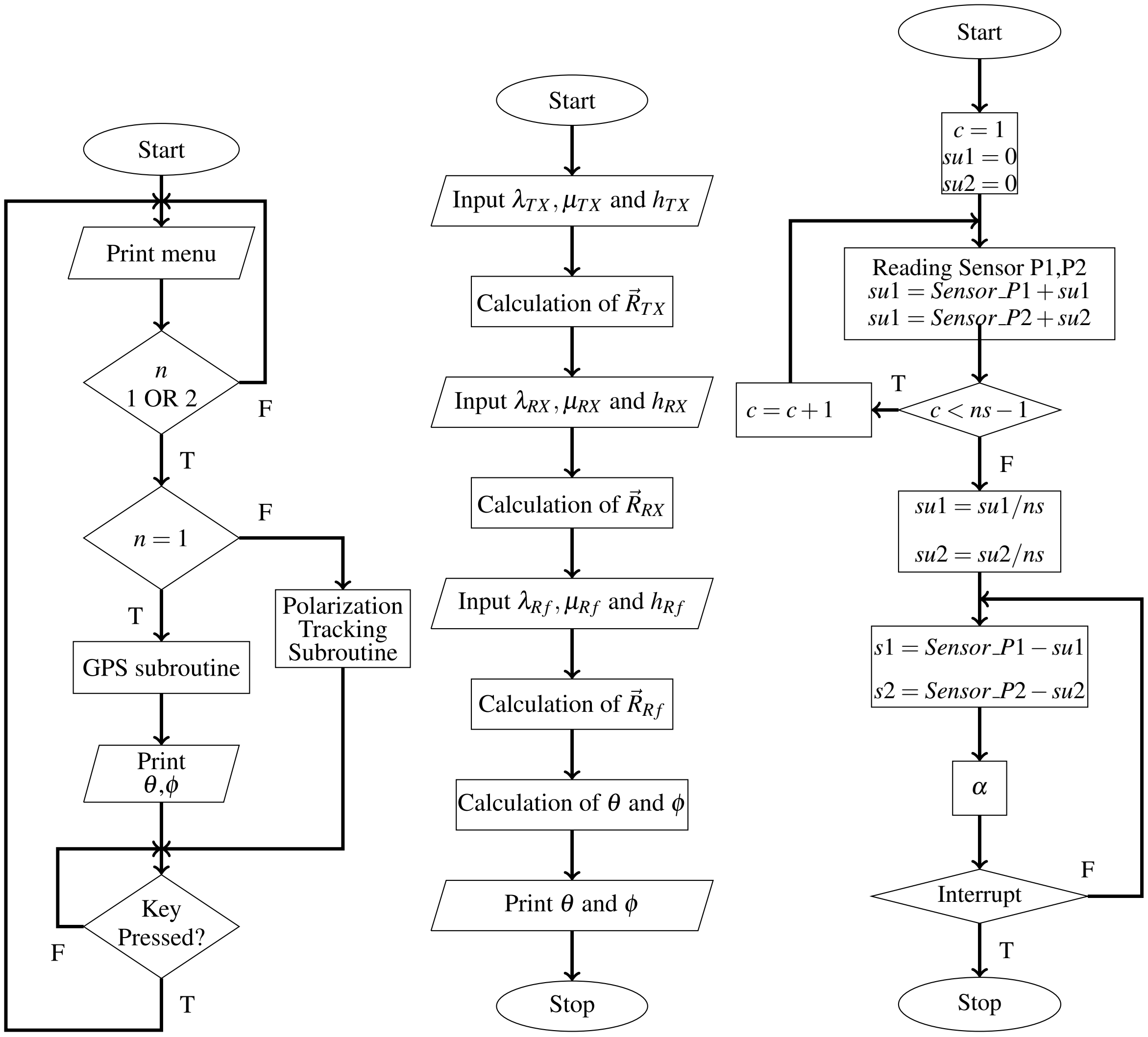
The signal from the photo diodes are amplified by the use of operational amplifiers. In our scheme, the circuit for compensating the offsets is not going to be regulated. We intend to remove the errors numerically as shown in Figure 4.4(c). Before a laser beacon is sent to the receiver, the micro-controller measures several samples of signal from the amplifiers. The number of samples are defined with the variable ns. The average value of the samples are stored in the variable $su1$ and $su2$. The variable $Sensor\_P1$ and $Sensor\_P2$, represent the analog signal from the amplifier of the $Sensor\_P1$ and $Sensor\_P2$, respectively. The transmitter sends the laser beacon to the receiver and the microcontroller measures the analog values from the amplifier. The final values are $s1 = Sensor\_P1 - su1$ and $s2 = Sensor\_P2 - su2$. The reading of the analog values from the amplifier continues until a key on the keyboard is pressed. Therefore, according to the algorithm proposed in Chapter 3.7.4 it is possible align the polarization bases between the transmitter and the receiver.

4.2 Power supply

In the Section 4.1 it was mentioned that the power supply provides power for the three different subsystems. Each output of the power supply must be regulated and the circuit must be compact. The circuit is built by a monolithic integrated circuit in order to supply the different blocks of the circuit.

4.2.1 Bridge rectifier with the center-tapped transformer

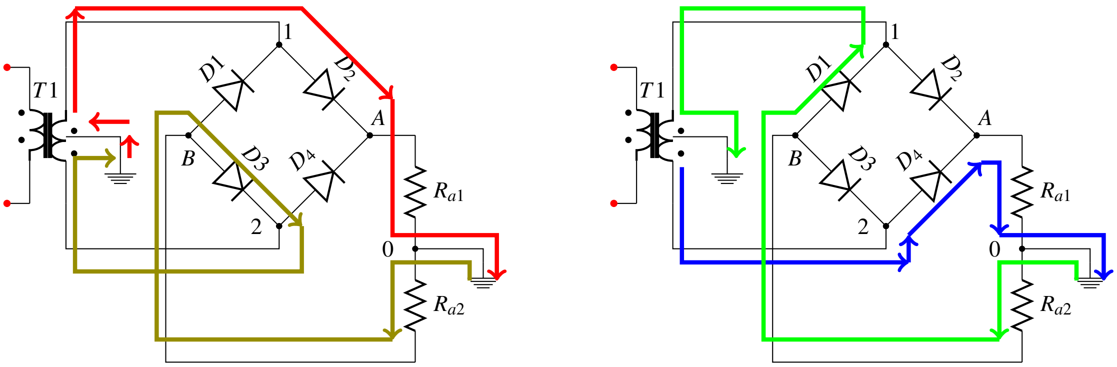
The electronic board was designed to supply energy to the photo-diode amplifier. Each amplifier is an operational amplifier $\mu A741$ that requires a dual voltage power supply. Figure 4.5 shows the conceptual scheme for obtaining a dual voltage power supply by using a center-tapped transformer and the Graetz bridge [47]. When the input of the Graetz bridge is $V_1 - V_2 = V_{12} > 0$ we have a positive half-wave. The drop of voltage is $V_{1A} > 0$ and the diode D_2 is forward biased and the current follows the path indicated by a red line, and the voltage drop, V_{A0} is positive. This is shown in Figure 4.5. In the meantime, the diode D_3 is also forward biased and the current is indicated by a brown line. This produces a drop of voltage, $V_{0B} < 0$. If $V_{12} < 0$ the diodes D_2 and D_3 are reverse biased and the diodes D_1 and D_4 are forward biased. The current indicated by a green arrow produces a voltage drop, $V_{A0} > 0$. The green arrow indicates the current through the diode D_1 that produced a voltage



(a) Main program (b) GPS subroutine (c) Pol. Trac. subroutine

Figure 4.4: Flow-chart of the algorithm loaded in the microcontroller: The microcontroller program contains one main algorithm and two subroutines. The variables contained in the subroutines, are cancelled from the SRAM once the calculations are finalized. This permits to save the space memory for other applications. (See Appendix A.5)

drop, $V_{0B} < 0$. If the load connected between the nodes A and 0 is different from the load connected between the nodes B and 0, the current on the diodes D_2 and D_4 will be different than the current through D_1 and D_3. The electronic scheme shown in Figure 4.8 has a capacitor filter to hold the drop voltage between the consecutive waves. The output of the capacitor filter produces an oscillation with a minimum voltage V_{MIN} and a maximum voltage V_M. This oscillation in output of the filter is knows as ripple. The ripple must be as small as possible and for this reason, using an electrolytic capacitor of $2200\mu F$ guarantees a low ripple for the



(a) Path of the current for the positive half-wave.

(b) Path of the current for the negative half-wave.

Figure 4.5: Path of the current for the negative and positive half waves: The differential of potential on the node V_{A0} and V_{B0} is determined by the path of the current. The red dots indicate the primary of the transformer $T1$ pugged in the electric network.

required average current. The presence of the filter increases the current peaks in the diodes for the reasons which follow in the sections below.

4.3 Full scheme of the power supply

The first part of the power supply consists of a center-tapped transformer, this is followed by a Graetz bridge (D_1, D_2, D_3, D_4). This scheme shown in Figure 4.8. For this numerical simulation of the center-tapped transformer T1 (See Figure 4.5), we used two sinusoidal voltage sources V_{s1} and V_{s2} which were set out of phase 180° at 50Hz. The effective value (rms) per power source was 12V. After the rectification there is a low-pass filter with a capacitance of $2200\mu F$. From Figure 4.6, it is possible to observe the behavior of the signal of the filter output, V_{40}. The amount of current required for the negative source is small because only the amplifier is supplied with negative voltage. The output voltage for the negative filter C_6, indicated with the green line, is affected by ripple but due to the low current required it is not observable. The positive output supplies most of the power from the board as compared to the negative output. In order to know the maximum value of the repetitive current needed by the rectifier diodes, we consider only the positive output of the filter. In order to build our circuit, the discharge of the capacitor can be estimated for a period of $T/2$, where T is the period of the electric current from the mains supply. In this lapse of period, the capacitor C_5

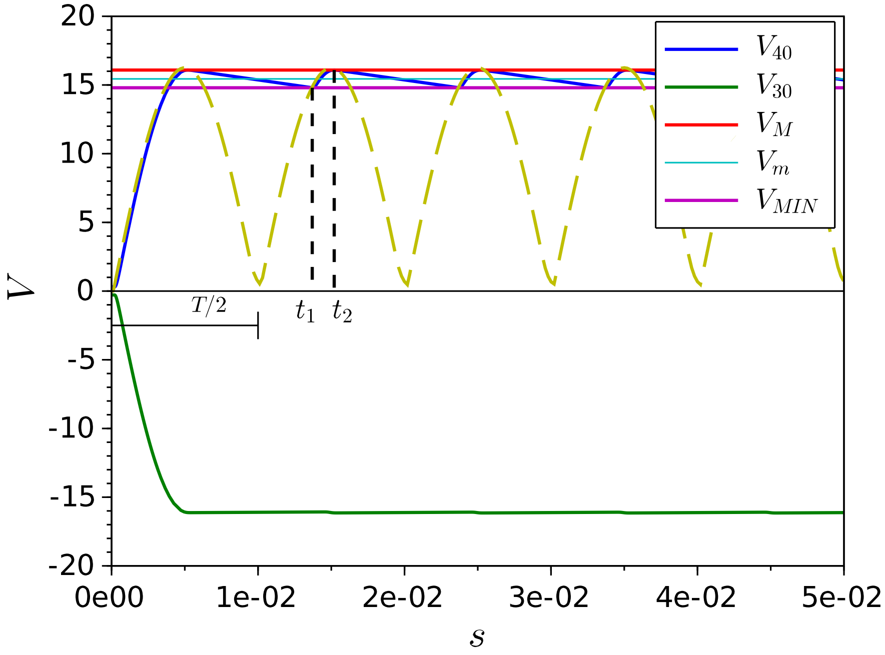


Figure 4.6: The negative and positive outputs in output of the filter: The chart only shows the positive output in order to show the effects of the load connected with the filter. The negative output is also affected by the ripple, but due to the low load applied it is not possible to observe. The yellow line indicates the waveform in the output of the Graetz bridge if the filter is not present.

releases a quantity of charge which is expressed as

$$\Delta Q = I \cdot \frac{T}{2}, \tag{4.1}$$

where I is the average current required from the circuits board. This quantity of charge must be replaced by the current that crosses the diodes I_{FRM} in a time $\Delta t = t_2 - t_1$

$$\Delta Q = I_{FRM} \cdot \Delta t. \tag{4.2}$$

Comparing Equation (4.1) and (4.2), we have

$$I_{FRM} = \frac{I \cdot T}{2 \cdot \Delta t}. \tag{4.3}$$

The terms $\Delta V = V_M - V_{MIN}$ shown on Figure 4.6 is

$$\Delta V = \frac{I}{2 \cdot f \cdot C}. \tag{4.4}$$

Because $T/\Delta T = \pi \cdot \sqrt{2 \cdot V_M/\Delta V}$, the current that crosses the forward bias diode is expressed as

$$I_{FRM} = I \cdot \pi \cdot \sqrt{f \cdot R_L \cdot C}. \tag{4.5}$$

The current across the forward bias diode is greater than the average required current I. For this reason the diodes D_2 and D_4 will be the ones mostly affected by the repetitive current peaks (I_{FRM}). The current necessary for the system is less than 0.5 A but the peak currents on the diodes D_2 and D_4 are above 3.5 A. On node 4 in Figure 4.8, voltage regulators U1, U3 and U4 are connected together. Node 3 is connected to the input of the negative-voltage regulator U2. The integrated circuits U3 supplies 5V to the micro-controller and U4 supplies a voltage of 5V to the LCD, the shift register and the keyboard. U1 is a variable positive voltage regulator LM317, and U2 is a variable negative voltage regulator LM337 while U3 and U4 are two voltage regulators LM7805. U1 and U2 are used to build a power supply for an external amplification circuit and require protection against short circuit in input and output. The 5V voltage regulators are only used the board and they don't need protection. The monolithic voltage regulators have an internal protection against short circuit as well as thermal protection. The diodes D_5 and D_7 are bypass diodes in case there is a short circuit between nodes 4 and 0 and between nodes 3 and 0, respectively. For our PCB, shown in Figure 4.7, the capacitors C_7 and C_8 can be neglected because the capacitors C_5 and C_6 are close to the input of U1 and U2 but are considered in the simulation for further changes in the circuit configuration. The capacitor C_{12} and C_{14} are wired close to the IC U3 and U4 because the distance from the filter is more than 5cm [47]. The diodes D_6 and D_8 are used to save the regulator in case of a short circuit in output between the nodes 7 and 0 or nodes 10 and 0. The capacitors C_{13} and C_{15} belong to a family of high frequency filters. The amplifiers form an external circuit for our PCB, but in order to check the behavior of the circuit the entire simulation was done by using the experimental values from Chapter 3.7. The resistor R_{L1} is a dummy load representative of the micro-controller unit while R_{L2} is a dummy load representative of the LCD shift register and the keyboard.

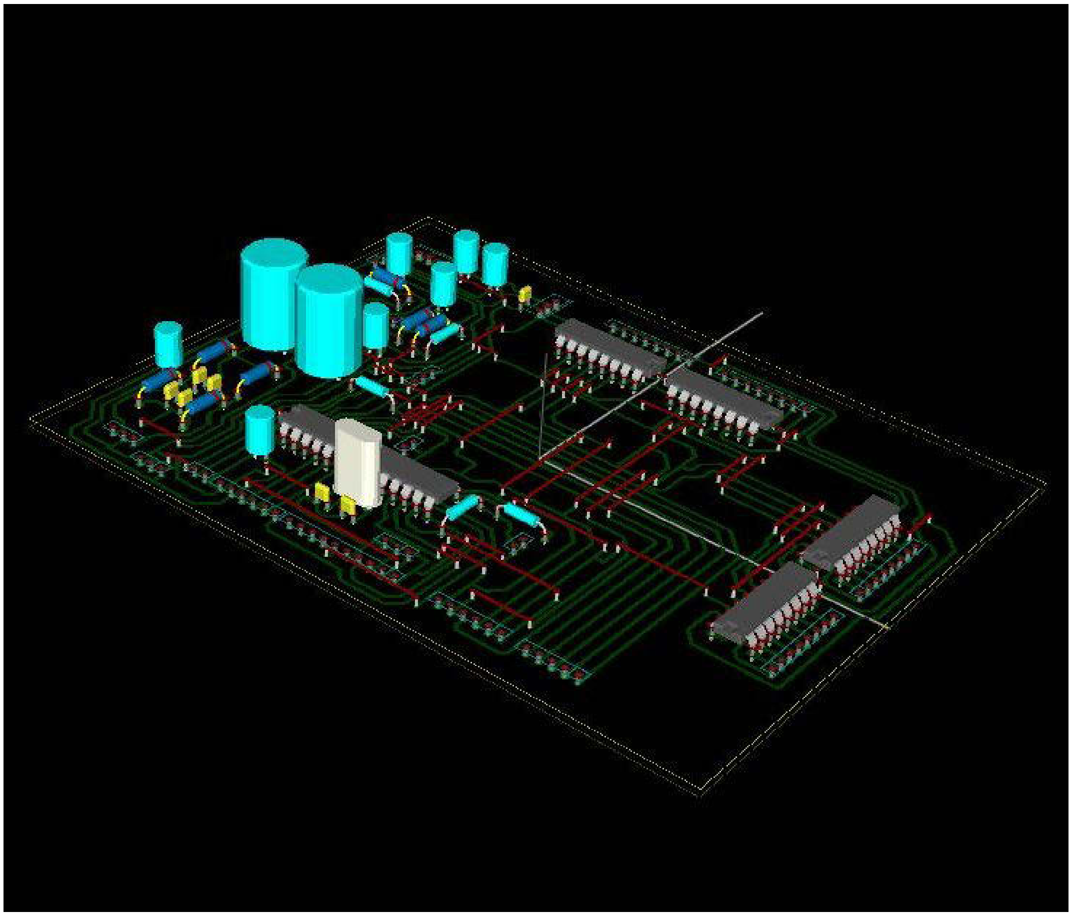


Figure 4.7: PCB of the portable tracking system excluding LCD and keyboard.

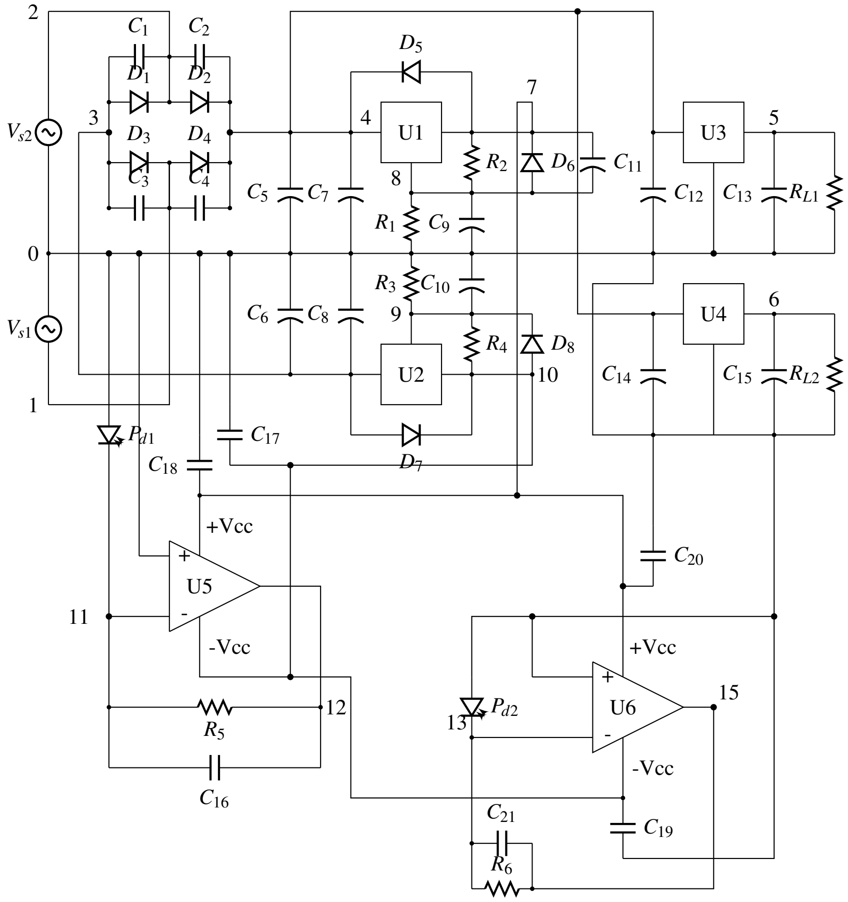


Figure 4.8: Circuit used to simulate the portable tracking system with the photodiode as explained in Section 4.4: In order to simulate the behavior of the circuit, a dummy load R_{L1} is used instead of the microcontroller, and the dummy load R_{L2} is used to simulate the load to the shift register the LCD and the Keyboard. The photodiodes are replaced with a current generator, and the center-tap transformer is replaced by two sinusoidal voltage generators. The symulation program used was ngspice.

4.4 Photodiode

The photodiode is a doped-PN semiconductor. When the photons hit the junction a photo-current is generated. The characteristic equation of the photo-diode is [48]:

$$I_D = I_0(e^{V_d/V_T} - 1) - I_{ph}, \tag{4.6}$$

where I_0 is the leakage current of the diode, V_T is the thermal voltage, V_D is the voltage applied on the photo-diode and I_{ph} is the photo-current. If $V_D < 0$ is the current through the

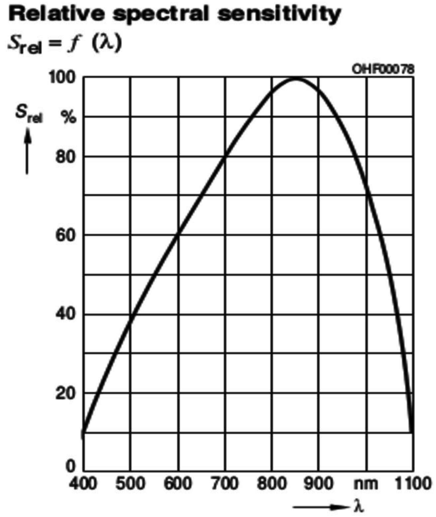


Figure 4.9: Relative spectral sensitivity of the photodiode used: From this chart it is possible to extract the value of the sensitivity for different λ

diode is then

$$I_D = -I_0 - I_{ph}, \tag{4.7}$$

where the I_0 is defined as dark current. If the voltage applied on the photo-diode is $V_d = 0$ the current through the diode becomes

$$I_d = -I_{ph}. \tag{4.8}$$

The photo current I_{ph} is given by

$$I_{ph} = S \cdot P = \frac{\eta e}{h\nu} P, \tag{4.9}$$

where S is the sensitivity, η is the quantum efficiency, e is the charge of the electron and h is the Plank constant. The parameter ν refers to the frequency of the incident electron on the surface of the photo-diode and P is the power of the wave. In section 3.4 we mentioned that a $532nm$ laser beacon is used to align the polarization bases of Alice and Bob. This experiment was conducted by using a laser with a wavelength, (λ) of $780nm$. In Figure 4.9, the sensitivity as a function of λ for the photodiode SIEMENS BPW 34 is shown. For this photo-diode the maximum value of the sensitivity is $0.62A/W$ at $850nm$. The sensitivity for the wavelength (λ) of $780nm$ extracted from the chart is $S(780nm) = 0.589A/W$, corresponding to 95% of $0.62A/W$. In the circuit of the Figure 4.8, the photo-diode was replaced with a current

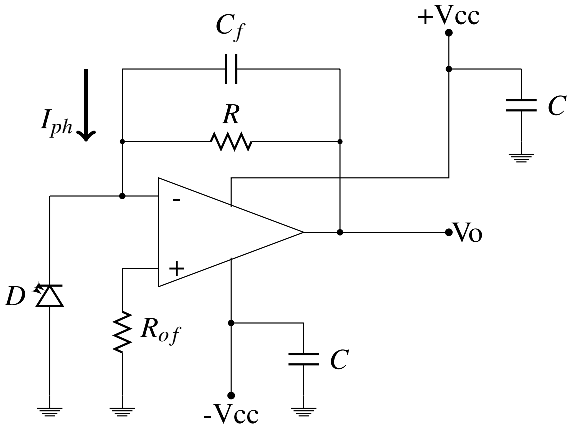


Figure 4.10: Amplifier circuit used for the photodiode: The capacitor C is used to avoid the self oscillation of the operational amplifeir. The capacitor C_f is used as a filter and the resistor R_{of} is used to decrease the offset current. The resistor R_{of} is deleted from the system because it gives negative output when the signal from the sensor P1 is close to zero.

generator called P_{d1} and P_{d2}. The value of the current is evaluated by using Equation (4.9) per each value of incident power measured in section 3.7.

4.5 The amplifier

Our system is designed to supply power to an external amplifier circuit and also to measure its output signal. In our simulation, we consider the simple scheme shown in Figure 4.10. The capacitors indicated with C are used to prevent oscillations of the operational amplifiers, while the capacitor C_f works as a filter. The resistor R_{of} is used to reduce the offset current. The voltage drop on the photodiode is indicated by $V_d = 0$ for the virtual ground. In order to simulate the photodiode as a current source in our simulation we can use Equation (4.8). The photo current I, moves from the output to the inverting input of the amplifier. The path taken by the photo current is indicated in Figure 4.10. By considering an ideal operational amplifier, the output Vo is given by the relation

$$Vo = -R \cdot I_{ph}. \tag{4.10}$$

The values of I_{ph} are calculated by using measurements from the experiment discussed in Section 3.7 and also in combination with Equation (4.9). In order to evaluate the effect of the resistor R_{of}, we performed two simulations which are explained below.

4.6 Analog keyboard for a microcontroller

A keyboard usually uses a serial protocol in order to communicate with a microprocessor or microcontroller unit. Serial protocols usually require a proper program and a minimum of two connections between the microcontroller and the keyboard [49]. Using the internal analog digital converter (ADC) of the microcontroller it is possible to use an analog keyboard in order to reduce the code line stored in the flash memory of the microcontroller. The analog to digital conversion is made by the ADC of the microcontroller. This kind of keyboard permits one to exploit the flexibility of the microcontroller by reducing the necessary input/outout ports, for the connection between of the microcontroller and the keyboard. The simple algorithm uses the approximation of an integer division. This section is based on the manuscript **M2**.

Often, an embedded system requires a keyboard to input the data from the user. Serial transmission requires one pin of the microcontroller for the synchronizations and another pin for the transmission of the characters. The standard serial communication requires a particular serial protocol program stored in the flash memory of the microcontroller. The most recent microcontroller generation contains an analog to digital converter (ADC) and an Electrically Erasable Programmable Read-Only Memory (E^{2}PROM) with a limited number of pins as well as the attny45 with 8 pins only [50].

In order to customize the numbers of pins of the microcontroller and the program memory, an analog keyboard can be used [51]. The circuit is composed by a resistor voltage divider, where the values of the resistors are: $R_1 = R_2 = R_3 = ... = R_N = R = 240\Omega$ with a 5% of tolerance as shown in Figure 4.11. The value of the resistor does not make a difference, but it must be scaled as a function of the entire circuit where the keyboard is used. For the experiment, a microcontroller ATMEGA328P was used [52]. The microcontroller contains a 10-bit successive approximation ADC. The voltage reference V_{ref} of the internal ADC converter must be connected to the node **1** of the voltage divider. The ADC of the microcontroller, measures the voltage on node **2**. In this discussion the values of the digital conversion are reported in decimal base. When no switch is pressed, the current is $I = V_{ref}/(N \cdot R)$ where N is the number of resistor used and V_{ref} is the ADC voltage reference. The voltage drop on the node **2** is

$$V_{OUT} = \frac{V_{ref}}{N \cdot R} R = \frac{V_{ref}}{N} = \frac{1023}{17}. \tag{4.11}$$

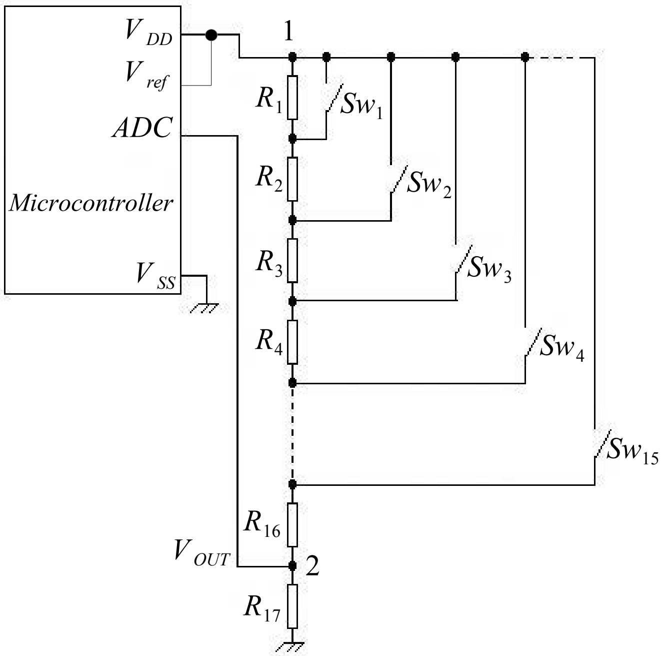


Figure 4.11: Customized analog keyboard for the portable tracking system: Sw_n is the key of the number, and the subscript n represents the number pressed; V_{DD} and V_{ref} is the differential of potential applied to the microcontroller and the voltage reference used for the analog digital converter of the microcontroller. V_{SS} is the ground reference. The keyboard is made by a voltage divider where the resistors values are the same, with a tolerance of 5%. The tolerance, due to the reading algorithm does not effect the character evaluated.

Where the maximum decimal value in output is 1023 of the ADC and corresponds to the reference voltage. The corresponding digital output converted from the ADC is 0000111100_b corresponding to 60 in decimal base. If switch number 1 is pressed (Sw_1) the Equation (4.11) becomes $V_{OUT} = (V_{ref}/((N-1)\cdot R))R$. With, n, the number of the switch pressed we derive at the following equation:

$$V_{OUT} = \frac{V_{ref}}{(N-n)\cdot R}R = \frac{V_{ref}}{N-n} \tag{4.12}$$

The decimal value for each button is shown in Table 4.1. These values, due to the noise or thermal effects may deviate by one unit. By the inverse of the Equation (4.12) it is possible to obtain an integer value corresponding to the switch pressed:

$$n = N - \frac{V_{ref}}{V_out} = N - \frac{1023}{V_{out}}. \tag{4.13}$$

In our case V_{out} is not the voltage measured, but the corresponding digital value. In terms of the digital values for any value of V_{ref}, the digital value is 1111111111 (1023), the values of V_{out} will therefore not change as a function of the resistors and the voltage reference. The only restriction is that the value of the resistors and their tolerances must be the same. The number n can be considered as an address for the E^2PROM where, for example, the ASCII code is stored.

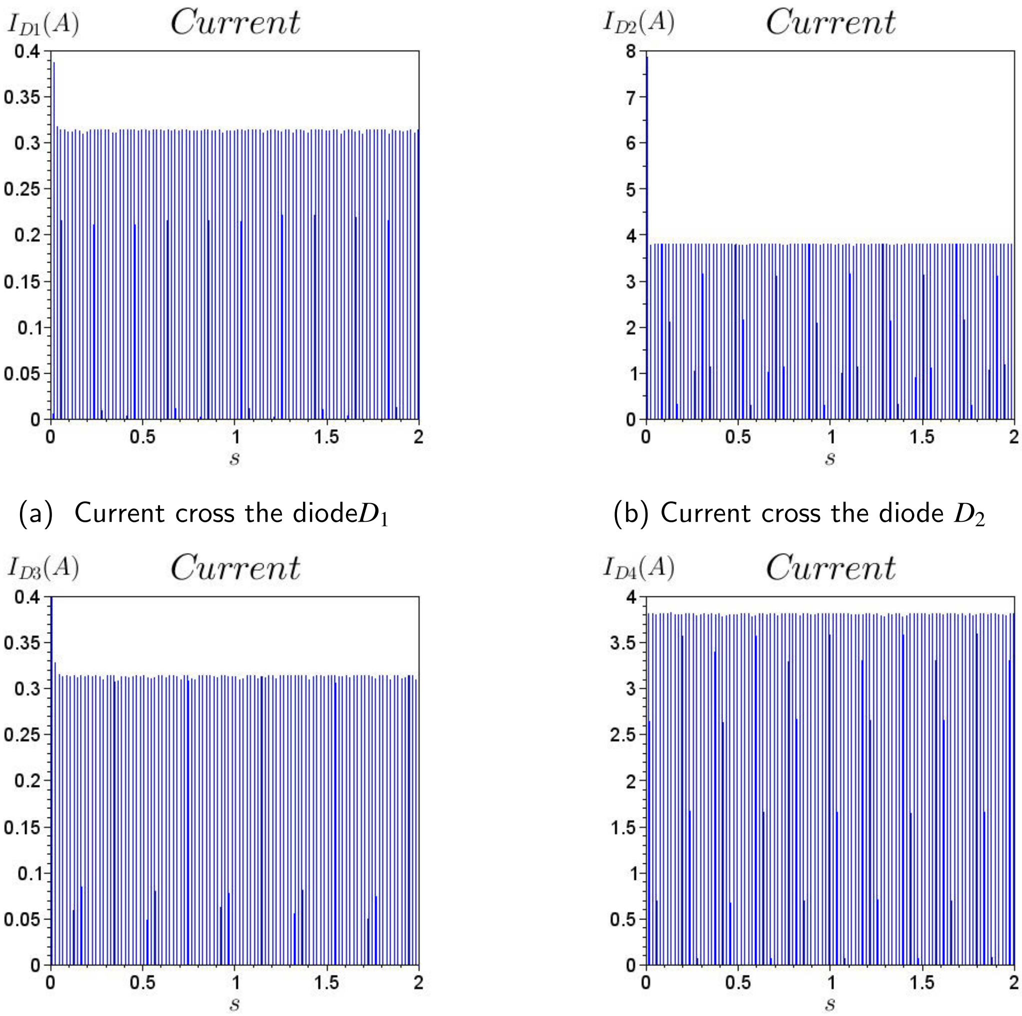
4.6.1 Numerical simulation and experimental considerations

It is possible that V_{OUT} is not stable around one value. Since in Equation (4.13) an integer division is made, the calculated address memory n, is stable for a certain value of the instability around the value V_{OUT}. The forth and fifth columns of Table 4.1 describe the admissible fluctuation around V_{OUT} allowable to obtain the same value n. In columns six and seven there are the corresponding voltage values when the reference voltage is 5 volt and the value of the resistors are 240Ω. The experimental keyboard was linked with the microcontroller, and the E^2PROM was loaded with the corresponding characters for each value n measured. By using an LCD, we saw that for each button pressed the value n did not change. This confirmed the reliability of the keyboard. In the Table 4.1 it is possible to observe that for the first five values the instability admissible is more critical but we did not observe changes in the values written to the LCD. By changing the values of the resistor tolerance, it is possible to improve the stability. In our case the algorithm continuously reads the analog value until a button is pressed and the character shown on the LCD. It is possible, using a Schmitt Trigger and one pin of the interrupt of the microcontroller to measure the value from the keyboard only when the button is pressed.

Using Equation (4.13), the values n, corresponding with the address memory of the character or an instruction, never changed during our experiment. The stability is given by numerical approximation of the integer division. This keyboard is flexible for any kind of application specifically when the microcontroller has limited numbers of input-output pins. The simplicity of the algorithm customizes the program memory of the microcontroller. Further by directly using the digital values from the conversion, it is possible to change the reference voltage without changing the program.

4.7 The simulation

The algorithm for the GPS tracking and the keyboard were tested on the final system. In order to verify our results, we also performed a simulation to study the behavior of the circuit with the amplifier. The polarization alignment system was tested utilizing an Arduino board in the optical laboratory. The behavior of the system with the amplifier was tested numerically by using the software called "*ngspice*" [53]. In the simulation, we consider an angular speed of $90°/s$ from 90° to 0° of the polarization direction. The first test was done with a resistor of $1M\Omega$ between the inverting input of the operational amplifier and the ground. This is indicated in Section 4.5 as R_{of}. The current passing through the diodes is shown in Figure 4.12. The current passing through diodes D_1 and D_3 is low because they only work for the negative voltage regulator as explined in section 4.3. This is necessary in order to supply power well regulated only for the polarization of the operational amplifiers. The current passing through diodes D_2 and D_4 is greater with respect to the current across D_1 and D_3, because they are applied at the input of the positive voltage regulators where more load is applied. When the simulation starts, the current increases because during the period $T/4$ of the wave shown in Figure 4.6, the capacitors are completely discharged. The non-repetitive current peaks (I_{FSM}) have a value of about $8A$ for the diodes D_2 and D_4 while for the diodes D_1 and D_3 the current is about $0.4A$. The value of the repetitive current peaks (I_{FRM}) is about $3.8A$ for the diode D_2 and D_4 and $0.31A$ for D_1 and D_3. For these conditions, it is possible to use the rectifier diode series 1N4004. After checking the amount of current passing through the diodes, we study the output of the amplifiers for different average power values of the laser beacon as explained in section 3.7.4. The effects of the resistor R_{of} is shown in Figure 4.13(a). The differential of potential called V_{12} refers to the signal collected from the photodiode P_{d1} relative to the sensor $P1$ according to the scheme shown in Figure 3.13. We indicate with V_{15} the signal collected from the photodiode P_{d2} relative to the sensor P_2. It is possible to observe that in the first $0.2s$ the value of V_{12} is negative. Because the voltage reference of the analog to digital converter works with a positive voltage drop, this configuration cannot be used. Another simulation was done without using resistor R_{of} and we obtained the final circuit as shown in Figure 4.8. With this configuration the output of the amplifiers V_{12} and V_{15} are positive for any value of the laser power collected from the photodiode. In our system we make sure that the average power of the laser beacon is kept at $4.06mW$. Our reference voltage reference V_{ref} is $5V$ and with this power in $5V$ is exceeded at the output of the amplifiers. Therefore, since it is required to measure this value, the circuit had to be altered by performing the following steps:



(a) Current cross the diodeD_1

(b) Current cross the diode D_2

(c) Current cross the diode D_3

(d) Current cross the diodeD_4

Figure 4.12: Currents cross the diodes: It is possible to observe that through the diode $D2$ and $D4$ it is higher with respect the diode D_1 and D_3 due to the load applied to the positive output of the circuit rectifier-filter. On the chart it is possible to observe the first peak of current due to the initial charge of the capacitor. Initially the charge Q of the capacitor is zero.

- Disconnect the keyboard and the V_{ref} pin of the microcontroller from the $5V$ voltage regulator.

- Connect the keyboard and V_{ref} pin of the microcontroller to another voltage regulator with the output voltage $V_0 > 5$.

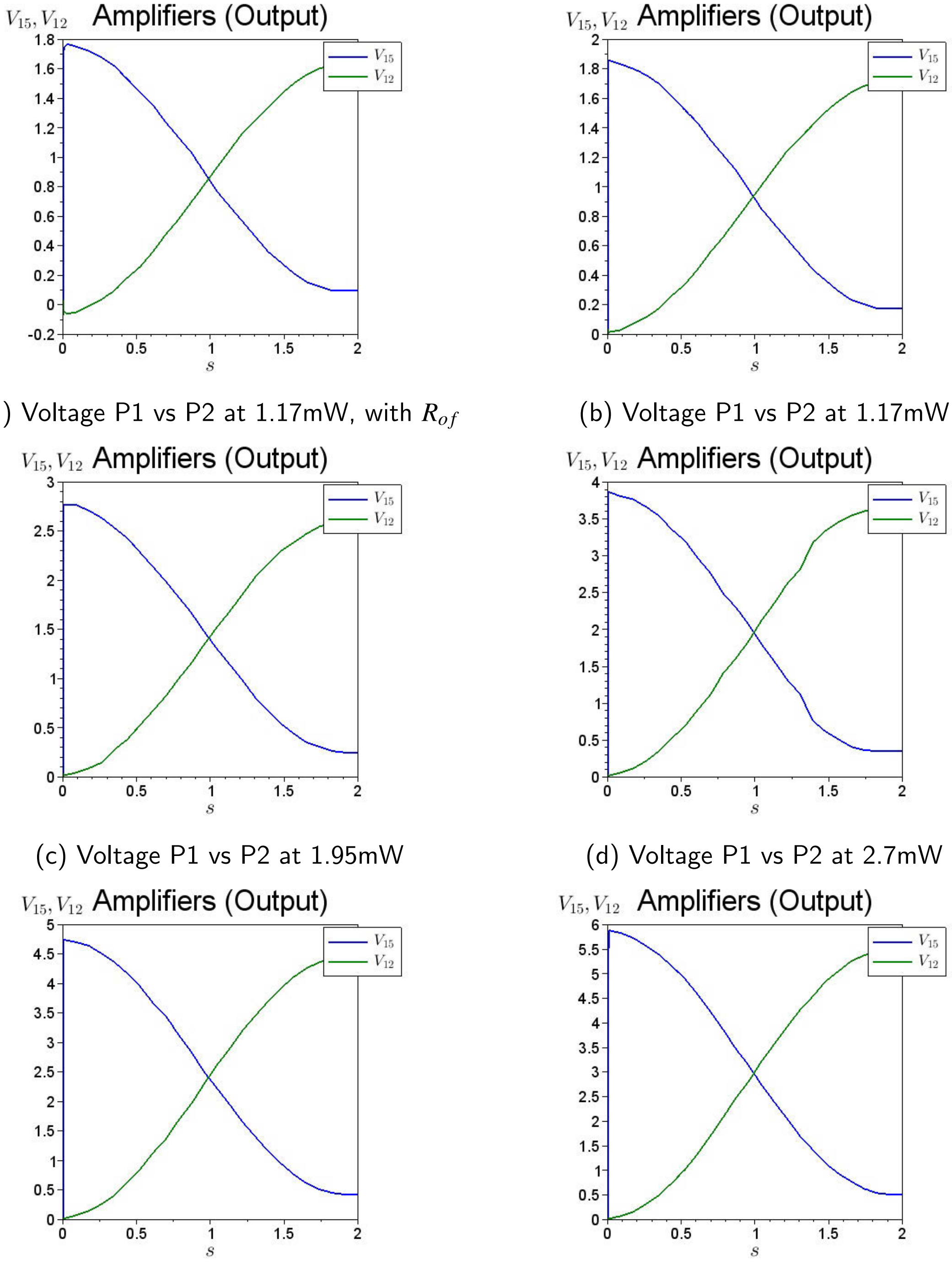
However, this change is not ideal because for a low power of the laser beacon, the quantization error of the ADC increases. When the printed circuit board changes from its original configuration, it is not necessary to change the software of the microcontroller.

4.8 Summary

In this chapter the design and implementation of a portable tracking system for quantum cryptography was discussed. The intention of the system was to guarantee the optical link between Alice and Bob and of their polarisation bases. The core of the system is a microcontroller programmed via the Arduino IDE. The GPS coordinates are inserted using a customized keyboard, but the microcontroller still has three analog input pins free that can be used as digital input/output devices to cooperate with other programmable devices or with a computer, for a fine alignment system. Using the shift register, it is possible to control the mechanical devices that move the optics and telescope by using external interfaces. The memory used by the program is one third of the total space, and for that reason the board can be reconfigured without changing the circuit, and using the IDE it is easy to work in a team.
From Figure 4.13(f), if the power received from the optical source generates an output above $4mW$ in the amplifier, the microcontroller is not able to measure the analog input correctly. This is because 5V is the voltage reference V_{ref}. The system is configured to measure a power of light lower than $4mW$. If it is necessary to measure more light power we can act on the gain of the amplifier manually or automatically by using a commercial instrumental differential amplifier, as for example the integrated circuit LH0084 [54], that can change the gain by the digital controls. In this case the inverting input must be linked with the ground.
In order to use the polarization alignment system, the transmitter and receiver need to be perfectly aligned. The future of this work requires the design of a fine alignment system integrated with the coarse alignment system. For a long distance link it is necessary to design a mechanical system because a small error in the measured angle, will result in several meters of misalignment between the transmitter and receiver.

Table 4.1: Numerical simulation of the keyboard per each switch pressed: In the first column, the number of the switch pressed is shown. The third column represents the address of the character stored in the E^{2}PROM. The forth and fifth column represents the maximum and minimum deviation due to the noise or different resistor tolerances admissible, in order to obtain the same memory address. The last two columns represent the corresponding admissible oscillation in volts, for a reference voltage of $5V$.

n	ADC	EEPROM ADDRESS	Max	Min	ΔV	$-\Delta V$
(Switch number)	conversion	(Decimal base)	Deviation	Deviation		
0	60	0	61	0	-0.00488	0.2928
SW_1	64	1	65	62	-0.00488	0.00976
SW_2	68	2	70	66	-0.00976	0.00976
SW_3	73	3	75	71	-0.00976	0.00976
SW_4	79	4	81	76	-0.00976	0.01464
SW_5	85	5	88	82	-0.01464	0.01464
SW_6	93	6	97	89	-0.01952	0.01952
SW_7	102	7	107	98	-0.0244	0.01952
SW_8	114	8	120	108	-0.02928	0.02928
SW_9	128	9	136	121	-0.03904	0.03416
SW_{10}	146	10	157	137	-0.05368	0.04392
SW_{11}	171	11	185	158	-0.06832	0.06344
SW_{12}	205	12	227	186	-0.10736	0.09272
SW_{13}	256	13	292	228	-0.17568	0.13664
SW_{14}	342	14	409	293	-0.32696	0.23912
SW_{15}	512	15	681	410	-0.82472	0.49776



(a) Voltage P1 vs P2 at 1.17mW, with R_{of}

(b) Voltage P1 vs P2 at 1.17mW

(c) Voltage P1 vs P2 at 1.95mW

(d) Voltage P1 vs P2 at 2.7mW

(e) Voltage P1 vs P2 at 3.2mW

(f) Voltage P1 vs P2 at 4.11mW

Figure 4.13: Output of the photodiode amplifiers: In Figure (a) R_{of} produce a negative output that cannot be measured from the microcontroller. (b),(c),(d),(e) amplifier output for different power received by the laser source. The amplifiers are able to follow the behavior of the power in input of the photodiodes. The Figure (f) shows that for a value of the power of the laser beacon of $4.11mW$ the microcontroler cannot measure the entire value of the amplifier output due to the voltage reference being fixed at $5V$.

Chapter 5

Conclusion

In addition to the use of optic fibre for transmission, quantum cryptography in free space presents a new potential spectrum of opportunity to achieve secure communications. In this thesis we analyzed different possible scenarios for quantum cryptography in free space, for two stationary points and for aerospace systems. In free space, the polarization bases of the single photon for Alice and Bob must be well aligned. However, this required alignment presents a challenge and requires resources. The main problem is due to turbulent effects of the media where the transmission of photons takes place. For example in a horizontal link to stationary points located on the Earth's surface, it is necessary to characterize the channel in terms of noise, beam wandering and scintillation of the laser beam. Fortunately, the turbulent effects on polarization can be neglected. This fact permits us to exploit this characteristic in order to create a polarisation alignment system that exploits a laser beacon. The laser beacon has a different wavelength from the single photon, from the receiver to the transmitter in order to reduce the noise on the receiver side. For this purpose, we created an angular sensor by using a polarising beam splitter with a proper correction algorithm. The correction function exploits the normalized signal measured from the sensor P1 or P2 indicated in Figure 3.13. In our case a polynomial function was used but it will be possible to find a complete function for the error once the beam splitter used is characterized. This system is very accurate for the purpose, but it requires a previous fine alignment between the transmitter and receiver.

We also showed that in the case of transmission between an Earth station and a satellite, it is possible to determine the polarization bases direction once the position of the satellite is known. In addition to the alignment, quantum cryptography also requires a synchronization system in order to keep the time stamp of the qubit received and this can be achieved via radio synchronization by using GPS or another radio source from the transmitter. The radio transmission may also be used for coarse alignment. However, this has some pit falls because one needs be to very careful that the path of the radio signal is not different from the path of the laser. Moreover, a coarse alignment system that exploits a compass can be affected by a strong error due to magnetic deviation in some geographical areas. Therefore, in order to solve the problem of the trade off between cost and accuracy, we developed an algorithm which utilises three physical positions including one laser beacon. Generally, for optical communication in free-space two systems are used, one for coarse alignment and another one for fine alignment. Here we solved the problem of coarse alignment. We determined that the system is able to achieve a coarse alignment to a good accuracy between the transmitter and receiver that are separated by a distance of up to 150km. Moreover, our system is also highly versatile. It is useful to provide a fine alignment for radio communication. Therefore, this system is a powerful tool to establish initial communication between the transmitter and the receiver. The tracking system developed is useful for quantum communication, but would also be an excellent system to align two radio transreceiver.

This thesis represents the first step in obtaining a tracking and alignment system for quantum cryptography in free-space. We are confident that this system represents a low-cost tracking system for quantum key distribution between two stationary points, and that further optimization of the system will enable it to function between two aircrafts or between a satellite and a ground station.

Appendix A

Codes

A.1 Scilab Code for ground trace and detemination of the direction of polarization basis of the satellite with respect to the equatorial line

```
// Constant variable initialization
clear
clc
counter=1;


re=6378*10^3; // Earth radius
mu_t =5.97*10^24*6.67*10^(-11); // Gravitational parameter
h=300*10^3; // Satellite Altitude
io=-30*%pi/180; // Orbit inclination
mu_greenwich=0//25*%pi/180;
mu_asc=-25*%pi/180;

// Earth map
xx=read('map.dat',-1,2)
x_x=xx(:,1)*%pi/180;
x_y=xx(:,2)*%pi/180;
```

```
r_tot=re+h; // Vector from the center of the Earth
omega_sat=sqrt(mu_t/r_tot^3);
omega_E=2*%pi/(24*3600); // Angular speed of the Earth
T_sat=2*%pi/omega_sat; // Orbit period
time=0;
phi(counter)=omega_sat*time;
lambda(counter)=asin(sin(phi(counter))*sin(io));
mu(counter)=mu_asc+omega_E*time-acos(cos(phi(counter))/...
        cos(lambda(counter)));
counter=2;
for time=T_sat/1000:T_sat/1000:T_sat
    phi(counter)=omega_sat*time;
    lambda(counter)=asin(sin(phi(counter))*sin(io));
    mu(counter)=-(mu_greenwich-mu_asc)-omega_E*time+...
           acos(cos(phi(counter))/cos(lambda(counter)));
    if (mu(counter)-mu(counter-1) <0) then break end
    counter=counter+1;
end

// maximum point of visibility
V1=[re*cos(26.2*%pi/180)*cos(28.06*%pi/180),re*cos(26.2*%pi/180)*...
            sin(28.06*%pi/180),re*sin(26.2*%pi/180)];
// V1 position vector of the earth station

// vector coordinates
x_coord=r_tot*cos(lambda).*cos(mu);
y_coord=r_tot*cos(lambda).*sin(mu);
z_coord=r_tot*sin(lambda);
V2=[x_coord,y_coord,z_coord]; // V2 vector position of the satellite
max_col=size(mu);
max_lamb=size(lambda);
counter1=1;
maximum=max_col(1,1);
for counter=2:max_col(1,1)
    l(counter1)=x_coord(counter)-x_coord(counter-1);
    m(counter1)=y_coord(counter)-y_coord(counter-1);
    n(counter1)=z_coord(counter)-z_coord(counter-1);
    counter1=counter1+1;
end
a=1; // planar coefficent
b=1; // planar coefficent
theta1=asin(abs(-1*n)./(sqrt(1)*sqrt(l.^2+m.^2+n.^2)))

// Visibility calculation.
// V1-V2
A=V1(1)-V2(:,1);
B=V1(2)-V2(:,2);
C=V1(3)-V2(:,3);
// Inner product V1 , V_diff.
count_vis=1;
for counter_v=1:maximum
    v_scalar=A(counter_v)*V1(1)+B(counter_v)*V1(2)+C(counter_v)*V1(3);
    if (v_scalar==0) then
        mu_vis(count_vis)=mu(counter_v);
        count_vis=count_vis+1;
    end
end
counter=1;
for time=time:T_sat/1000:T_sat
    phi2(counter)=omega_sat*time;
    lambda2(counter)=asin(sin(phi2(counter))*sin(io));
    mu2(counter)=(mu_asc-omega_E*time+2*%pi-acos(cos(phi2(counter))/...
                            cos(lambda2(counter))));
    if (mu2(counter) >= %pi) then break end
    counter=counter+1;
end
counter=1;
for time=time:T_sat/1000:T_sat
    phi3(counter)=omega_sat*time;
    lambda3(counter)=asin(sin(phi3(counter))*sin(io));
    mu3(counter)=(mu_asc-omega_E*time+2*%pi-acos(cos(phi3(counter))/...
                              cos(lambda3(counter))))-2*%pi;
    counter=counter+1;
end

scf(1)
subplot(1,2,1)
plot(mu,lambda,'g',mu2,lambda2,'g',mu3,lambda3,'g',x_x,x_y,28.06*...
                    %pi/180,-26.2*%pi/180,'+r')
title('GROUND TRACE','fontsize',4)
xlabel(prettyprint('\mu'),'fontsize',4)
ylabel(prettyprint('\lambda'),'fontsize',4)
xgrid()

subplot(1,2,2)
plot(mu(1:maximum-1),theta1)
title('ANGLE OF THE POLARIZER','fontsize',4)
xlabel(prettyprint('\mu'),'fontsize',4)
ylabel(prettyprint('\theta'),'fontsize',4)
xgrid()
xs2jpg(figure(1),'foo_1.jpg', 1); // best quality
```

A.2 Scilab code for video simulation of the orbit propagation

```
clear
clc
mu_t =5.97*10^24*6.67*10^(-11);
mutton=0
theta1=0
r=6378000;
r_tot=r+300000;
omegae=2*%pi/(24*3600); //
//della terra
```

```
omega_sat=sqrt(mu_t/r_tot^3);
xx=read('map.dat',-1,2)
lambdat=xx(:,2)*%pi/180;
mut=xx(:,1)*%pi/180;
count_frame=1
// Video construction
for time=0:80:(%pi/omega_sat)
    ii=omegae*time;
    is=omega_sat*time;
    lambda=xx(:,2)*%pi/180;
    mu=xx(:,1)*%pi/180+ii;
    x_coord=r*cos(lambda).*cos(mu);
    y_coord=r*cos(lambda).*sin(mu);
    z_coord=r*sin(lambda);
    u = linspace(-%pi/2,%pi/2,20);
    v = linspace(0,2*%pi,20);
    X = (r-100)*cos(u)'*cos(v);
    Y = (r-100)*cos(u)'*sin(v);
    Z = (r-100)*sin(u)'*ones(v);

    //Satellite trajectory
    xx_x=r_tot*cos(is);
    yy_x=r_tot*sin(is);
    zz_x=0;

    betas=-%pi/6;
    alpha=-25*%pi/180;
    A=[1,0,0;0,cos(betas),sin(betas);0,-sin(betas),cos(betas)];
    B=[cos(alpha),sin(alpha),0;-sin(alpha),cos(alpha),0;0,0,1];
    C=A*B;
    trasf=C^-1;
    // satellite coordinates
    x_sat(count_frame)=trasf(1,:)*[xx_x;yy_x;zz_x];
    y_sat(count_frame)=trasf(2,:)*[xx_x;yy_x;zz_x];
    z_sat(count_frame)=trasf(3,:)*[xx_x;yy_x;zz_x];
```

```
 // Latitude calculation
 lambdasat(count_frame)=atan(z_sat(count_frame)/...
(sqrt(x_sat(count_frame)^2+ y_sat(count_frame)^2)));

 if ((y_sat(count_frame)>0) & (x_sat(count_frame)>0)) then
     phip(count_frame)=asin(y_sat(count_frame)/(r_tot*...
               cos(lambdasat(count_frame))));
 end
 if ((y_sat(count_frame)>0) & (x_sat(count_frame)<0)) then
     phip(count_frame)=%pi-asin(y_sat(count_frame)/(r_tot*...
               cos(lambdasat(count_frame))));
 end
 if ((y_sat(count_frame)<0) & (x_sat(count_frame)<0)) then
     phip(count_frame)=-1*asin(y_sat(count_frame)/...
                (r_tot*cos(lambdasat(count_frame))))+%pi;
 end
 if ((y_sat(count_frame)<0) & (x_sat(count_frame)>0)) then
     phip(count_frame)=asin(y_sat(count_frame)/(r_tot*...
               cos(lambdasat(count_frame))));
 end
 // Longitude calculation
 musat(count_frame)=phip(count_frame)-ii;

 // Polariser direction
 x_satt(count_frame)=r_tot*cos(lambdasat(count_frame))*...
                cos(musat(count_frame));
 y_satt(count_frame)=r_tot*cos(lambdasat(count_frame))*...
               sin(musat(count_frame));
 z_satt(count_frame)=r_tot*sin(lambdasat(count_frame));

 if count_frame>1 then
     l(count_frame-1)=x_satt(count_frame)-x_satt(count_frame-1)
     m(count_frame-1)=y_satt(count_frame)-y_satt(count_frame-1)
     n(count_frame-1)=z_satt(count_frame)-z_satt(count_frame-1)
```

```
        theta1(count_frame-1)=asin(abs(-1*n(count_frame-1)/...
          (sqrt(1)*sqrt(l(count_frame-1)^2+ m(count_frame-1)^2+...
           n(count_frame-1)^2))))
        mutton(count_frame-1)=musat(count_frame)
    end

    clf()
    subplot(2,2,1)
    a=get("current_axes");
    param3d1(x_coord,y_coord,z_coord)
    param3d1(x_sat,y_sat,z_sat)
    plot3d2(X,Y,Z,flag=[12,4,4]);
    a.thickness = 0;
    a.rotation_angles=[90,0,0];
    a.background=-2;
    subplot(2,2,2)
    plot(musat,lambdasat,mut,lambdat)
    xlabel(prettyprint('\mu (rad)'),"fontsize",4);
    ylabel(prettyprint('\lambda (rad)'),"fontsize",4)
    subplot(2,2,4)
    plot(-25*%pi/180,0,3.14,0.56,mutton,theta1);
    xlabel(prettyprint('\mu (rad)'),"fontsize",4)
    ylabel(prettyprint('\theta (rad)'),"fontsize",4)
    subplot(2,2,3)
    plot(0,0)
    stringa='picture'+string(count_frame)+'.jpg'
    xs2jpg(figure(0),stringa, 1)
    count_frame=count_frame+1;
end
    clf()
    subplot(2,2,1)
    a=get("current_axes");
    param3d1(x_coord,y_coord,z_coord)
    param3d1(x_sat,y_sat,z_sat)
    plot3d2(X,Y,Z,flag=[12,4,4]);
    a.thickness = 0;
    a.rotation_angles=[90,0,0];
    a.background=-2;
    subplot(2,2,2)
    plot(musat,lambdasat,mut,lambdat)
    xlabel(prettyprint('\mu'),"fontsize",4);
    ylabel(prettyprint('\lambda'),"fontsize",4)
    subplot(2,2,4)
    plot(-25*%pi/180,0.56,3.14,0.56,mutton,theta1);
    xlabel(prettyprint('\mu'),"fontsize",5)
    ylabel(prettyprint('\theta'),"fontsize",5)
    subplot(2,2,3)
    plot(0,0)
    xs2jpg(figure(0),'foo_2.jpg', 1)
```

A.3 Python code to read the GPS areal Bluetooth

```
#from distutils.core import setup
#import py2exe
#setup(console=["gps.py"])
import serial
somma1=0.0
somma2=0.0
somma3=0.0
somma4=0.0
counter1=0.0
ser = serial.Serial("com5", 9600, 8, "N", 2, timeout=1)
c=ser.readline()
ser.flush()
f=open('dati_gps.dat','w')
messaggio="Coordinates N/S"+" "+"Coordinates E/W"+"\n\n"
f.write(messaggio)
for counter in range(1,60):
    c=ser.readline()
    if c[1:6]=="GPGGA":
        counter1=counter1+1.0
        a=c.split(',')
        stringa=a[2]+" "+a[4]+"\n"
        print (c)
        print(stringa)
        e=float(a[2])
        f=float(a[4])
        g=float(a[9])
        h=float(a[11])
        somma1=somma1+(int(e)/100+(float(e)-int(e)/100*100)/60)
        somma2=somma2+(int(f)/100+(float(f)-int(f)/100*100)/60)
        somma3=somma3+g
        somma4=somma4+h
print "Latitude"
print(somma1/counter1)
print "Longitude"
print(somma2/counter1)
print "Altitude above mean see level"
print(somma3/counter1)
print "Height of geoide above WGS84 ellipsoide"
print(somma4/counter1)
ser.close()
```

A.4 Microcontroller C code for the polarization bases alignment using one polariser

```
int counter,counter1,minus,valore;
boolean vero=true;
boolean conta_mezzi=false;
void setup(){
  analogReference(DEFAULT);
  pinMode(12,OUTPUT);
  pinMode(11,OUTPUT);
  // Comunicazione seriale
  Serial.begin(9600);
}
int verso=0;
int hold_var,hold_var1,change=0;
void loop(){
  digitalWrite(12,vero);
  while(change==0){
    for (counter=1;counter<11;counter++){
      hold_var=hold_var+analogRead(0);
      delay(10);
    }
    hold_var=hold_var/10;
    digitalWrite(11,1);
    delay(10);
    digitalWrite(11,0);
    delay(1);
    for (counter=1;counter<11;counter++){
      hold_var1=hold_var1+analogRead(0);
      delay(10);
    }
    hold_var1=hold_var1/10;

    if (hold_var >hold_var1){
      vero=!(vero);
      change=0;
      digitalWrite(12,vero);
    }
    Serial.println(hold_var);
  }
}
```

A.5 C code for the tracking system plug and play

```
/////////////////////////////////////////////////////////////////
// TRACKING PROGRAM
/////////////////////////////////////////////////////////////////
// THE MICRO-CONTROLLER IS MOUNTED IN THE TRANSMITTER SIDE.
// THE REFERENCE STATION AND THE RECEIVER STATION SEND THEM
//         COORDINATES  TO THE TRANSMITTER.   //
// THE SYSTEM USES THE PROTOCOLS IERS: SEMI-MAJOR AXES OF THE
//         ELLIPSOID a=6378136 m            //
//         SEMI-MINOR AXES OF THE ELLIPSOID b=6356751.302 m
/////////////////////////////////////////////////////////////////
  #include <LiquidCrystal.h>
// initialize the library with the numbers of the interface pins
LiquidCrystal lcd(12, 11, 5, 4, 3, 2);
void setup(){
   // Serial transmission
   // include the library code:
// set up the LCD's number of columns and rows:
  lcd.begin(16, 2);
  // Print a message to the LCD.
  lcd.print("hello, world!");
}
// variable used in order to calculate the execution time
unsigned long time;
// Angular constast used for conversion degree to radiant
const float trasf=0.0174533;
// vector for plane angle measure
double v1[3]={0,0,0};
double v2[3]={0,0,0};
// Vector Rrf initialization
double vrf[3]={0,0,0};
// Vector RTX initialization
double vtx[3]={0,0,0};
// Vector RRX initialization
```

```
double vrx[3]={0,0,0};
// Initialization of the vector given by the difference vrx-vtx
double vtxrx[3]={0,0,0};
// Initialization of the vector given by the difference vrf-vtx
double vtxrf[3]={0,0,0};
// Initialization of the global variable, angle of rotation
//  and verse
//   calculated by the procedure
double angrot=0;
// Definition of the angle around the vector vtxrf
double avtxrf,angz;
// Definition of the variable used for the serial
//   transmisison of the float number
char appstr[12];

// DEFINITION OF THE ELLIPSOID VALUES
// ( The dimensions are normalized whit respect to the
//  semi-major axes a
float a=6378137;
float b=6356752.3142;
// Eccentricity
float e2=0.006694;
// GLOBAL VARIABLE USED IN THE PROCEDURE
// By passage of variable the results produced by the subroutine
//  are stored in the variable of
//        the interest.
double v_result[3]={0,0,0};
// Definition of the variable for the angle calculation
float angle;
// Verse of rotation
int verse,avtxrfverse;
//////////////////////////////////////////////////////////////////////////
//  COORDINATES OF THE REFERENCE STATION, RECEIVER AND
//  TRANSMITTER    ////
//////////////////////////////////////////////////////////////////////////
```

```
//  Latitude reference station
float lrf=-29.0551500;
//  Longitude of the reference station
float mrf=27.2399583;
//  Altitude of the reference station
float hrf=0;

float lrx=-29.0002667;
float mrx=27.3096083;
float hrx=0;

float ltx=-29.0600694;
float mtx=27.2450667;
float htx=0;
// MAIN PROGRAM
void loop(){
  a=a;
  b=b;
  time=micros();
  // Chartesian coordinates of the reference station
  coordinates(e2, lrf, mrf, hrf);
  vrf[0]=v_result[0];
  vrf[1]=v_result[1];
  vrf[2]=v_result[2];

  // Chartesian coordinates of the transmitter
  coordinates(e2, ltx, mtx, htx);
  vtx[0]=v_result[0];
  vtx[1]=v_result[1];
  vtx[2]=v_result[2];

  // Chartesian coordinates of the receiver
  coordinates(e2, lrx, mrx, hrx);
  vrx[0]=v_result[0];
  vrx[1]=v_result[1];
  vrx[2]=v_result[2];

  // Vector transmitter-reference station
  difference(vrf, vtx);
  vtxrf[0]=v_result[0];
  vtxrf[1]=v_result[1];
  vtxrf[2]=v_result[2];

  // Vector transmitter-receiver
  difference(vrx, vtx);
  vtxrx[0]=v_result[0];
  vtxrx[1]=v_result[1];
  vtxrx[2]=v_result[2];

  // Angle theta of rotation by the subroutine vectors. Contains
//  the verse of rotation
  vectorial(vtxrf,vtxrx,ltx);
  v1[0]=vtxrf[0]/1000;
  v1[1]=vtxrf[1]/1000;
  v1[2]=vtxrf[2]/1000;
  v2[0]=vtxrx[0]/1000;
  v2[1]=vtxrx[1]/1000;
  v2[2]=vtxrx[2]/1000;
  scalar(v1,v2);
  angrot=angle;
  avtxrfverse=verse;
  // Calculation of the angle rotation around the vector vtxrf
  vectorial(vtx,vrf,0);
  v1[0]=v_result[0];
  v1[1]=v_result[1];
  v1[2]=v_result[2];
  vectorial(vtxrf,vtxrx,0);
  v2[0]=v_result[0];
  v2[1]=v_result[1];
  v2[2]=v_result[2];
  if ((v1[2]<0 && v2[2]>0)||(v1[2]>0 && v2[2]<0)){
    vectorial(vtxrx,vtxrf,0);
    v2[0]=v_result[0];
    v2[1]=v_result[1];
    v2[2]=v_result[2];
  }
  scalar(v1,v2);
  avtxrfverse=angle;
  if (v_result[2]<0){
    verse=1;
  }
  else{
    verse=-1;
  }
  angz=90-angle/trasf;

  lcd.setCursor(0, 1);
  // print the number of seconds since reset:
  lcd.print(dtostrf(angrot/trasf,9,6,appstr));
}
// Vectorial product between vec1 and vec2 in order to find
//  the vector v_result and
// vers of rotation
void vectorial(double vec1[],double vec2[],double lr){
  v_result[0]=vec1[1]*vec2[2]-vec1[2]*vec2[1];
  v_result[1]=vec1[2]*vec2[0]-vec1[0]*vec2[2];
  v_result[2]=vec1[0]*vec2[1]-vec1[1]*vec2[0];
  angle=sqrt(pow(vec1[0],2)+pow(vec1[1],2)+pow(vec1[2],2));
  angle=angle*sqrt(pow(vec2[0],2)+pow(vec2[1],2)+pow(vec2[2],2));
  angle=asin(sqrt(pow(v_result[0],2)+pow(v_result[1],2)...
      +pow(v_result[2],2))/angle);
  if (((v_result[2]>0) && (lr<0)) || ((v_result[2]<0) && (lr>0))){
    verse=1;
  }
  else{
    verse=-1;
  }
  return;
}
void scalar(double v1[],double v2[]){
  angle=acos((v1[0]*v2[0]+v1[1]*v2[1]+v1[2]*v2[2])/...
 (sqrt(v1[0]*v1[0]+ v1[1]*v1[1]+v1[2]*v1[2])* ...
 sqrt(v2[0]*v2[0]+ v2[1]*v2[1]+v2[2]*v2[2])));
}
// Subroutine for chartesia coordinates
void coordinates(float ee2, float lambda, float mu, float h){
  // Variable uses for the calculatio of the curvature
// of the first vertical
  float cx;
  // Conversion from angle in DDDMM.MMMMM format in radiant
  lambda=lambda*trasf;
  mu=mu*trasf;
  // Calculation of the coordinates of the vecxtor position
  cx=(a/sqrt(1-e2*pow(sin(lambda),2)));
  v_result[0]=(cx+h)*cos(lambda)*cos(mu);
  v_result[1]=(cx+h)*cos(lambda)*sin(mu);
  v_result[2]=(cx*(1-e2)+h)*sin(lambda);
}
// Subrutine for the difference of the vectors
void difference(double vettore1[], double vettore2[]){
  v_result[0]=vettore1[0]-vettore2[0];
  v_result[1]=vettore1[1]-vettore2[1];
  v_result[2]=vettore1[2]-vettore2[2];
}
```

Bibliography

[1] E. Salvador, “Appunti di crittografia, complementi al modulo 3 del laboratorio, una introduzione all’ algebra moderna,” Universitá degli studi di Torino, Tech. Rep., December 2007. [Online]. Available: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.fogazzaro.it%2FISA%2F5AT%2FCrittografia.pdf&ei=01XKVIfAFcWqUe_TgpAI&usg=AFQjCNG6VEIAwQ0Nud6n4xOJSuK7RE6PMg&sig2=cERVCE3NGfj7rKFT-NV6SA

[2] D. Bacco, “Comunicazione quantistica finalizzata alla realizzazione di chiavi in spazio libero,” Master’s thesis, Universitá degli Studi di Padova, 2011.

[3] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[4] “How to plot the distribution of a cyphertext.” [Online]. Available: http://crypto.stackexchange.com/questions/3854/how-to-plot-the-distribution-of-a-ciphertext

[5] A. Nunzi, F. Genevois, and F. Russo, “I cifrari perfetti,” Universitá Degli Studi Roma Tre, Tech. Rep., 2005. [Online]. Available: http://www.dia.uniroma3.it/~dispense/merola/critto/tesine/perfettislides.pdf

[6] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 2010.

[7] G. Acquaviva, “Clonazione di stati quantistici,” Ph.D. dissertation, Università Cattolica del Sacro Cuore, Brescia, 2006.

[8] S. Weigert, “No-cloning theorem,” in *Compendium of Quantum Physics*, D. Greenberger, K. Hentschel, and F. Weinert, Eds. Springer Berlin Heidelberg, 2009, pp. 404–405. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-70626-7_124

[9] C. H. Bennett, G. Brassard *et al.*, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, no. 0. New York, 1984.

[10] G. Ribordy, “Key distillation-part i,” IDQ Winter School, Switzerland, Tech. Rep., 2014.

[11] M. Mariola, A. Mirza and F. Petruccione, Quantum cryptography for satellite communication, in Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, edited by I. Basson and A.E. Botha (University of South Africa, Pretoria, 2011), pp. 403 - 408. ISBN: 978-1-86888-688-3. Available online at http://events.saip.org.za.

[12] “Bb84 and ekert91 protocols.” [Online]. Available: http://www.quantiki.org/wiki/BB84_and_Ekert91_protocols

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.74.145

[14] L. Matthieu, “Assembling of a qkd system,” IDQ Winter School, Switzerland, Tech. Rep., 2014.

[15] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, “Fast and user-friendly quantum key distribution,” *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 517–531, 2000. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/09500340008244057

[16] R. L. Fante, “Electromagnetic beam propagation in turbulent media,” in *IEEE Proceedings*, vol. 63, 1975, pp. 1669–1692.

[17] T. Morio, T. Hideki, S. Yozo, T. Yoshihisa, K. Yoshisada, and K. Hiroo, “Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space,” *Opt. Express*, vol. 17, no. 25, pp.

22 333–22 340, Dec 2009. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-17-25-22333

[18] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.

[19] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, "Free space quantum key distribution: Towards a real life application," *Fortschritte der Physik*, vol. 54, no. 8-10, pp. 840–845, 2006. [Online]. Available: http://dx.doi.org/10.1002/prop.200610322

[20] J. G. Rarity, P. R. Tapster, and P. M. Gorman, "Secure free-space key exchange to 1.9km and beyond," *Journal of Modern Optics*, vol. 48, no. 13, pp. 1887–1901, 2001. [Online]. Available: http://dx.doi.org/10.1080/09500340108240895

[21] Morio Toyoshima, Hideki Takenaka, Yozo Shoji, et al., "Polarization-Basis Tracking Scheme in Satellite Quantum Key Distribution," International Journal of Optics, vol. 2011, Article ID 254154, 8 pages, 2011. doi:10.1155/2011/254154.

[22] W.-L. Saw, H. H. Refai, and J. J. Sluss, Jr., "Free space optical alignment system using gps," vol. 5712, 2005, pp. 101–109. [Online]. Available: http://dx.doi.org/10.1117/12.591226

[23] A. Shrestha and M. Brechtelsbauer, "Transportable optical ground station for high-speed free-space laser communication," *Proc. SPIE*, vol. 8517, pp. 851 706–851 706–9, 2012. [Online]. Available: http://dx.doi.org/10.1117/12.928966

[24] A. Bernardi, *Lezioni del corso di sistemi di comunicazioni satellitari*. Roma: Edizioni ingegneria 2000, 2000, vol. 1.

[25] "Itu-r p.453-8." [Online]. Available: http://www.catr.cn/radar/itur/201007/P020100714503680970889.pdf

[26] "Itu-r p.835-3." [Online]. Available: http://www.catr.cn/radar/itur/201007/P020100714463265537648.pdf

[27] "ionos.ingv.it - /roma/." [Online]. Available: http://ionos.ingv.it/Roma

[28] M. H. De Canck, *Ionosphere Properties and Behaviors*, June 2006. [Online]. Available: http://www.antennex.com/prop/prop0606/prop0606.pdf

[29] T. Pratt, C. W. Bostian, and J. E. Allnutt, *Satellite communications*. John Wiley & Sons, 2003, ch. 12.11.

[30] D. Grosso, "Introduzione al physical computing e arduino," Universitá di Genova, Tech. Rep., July 2014. [Online]. Available: http://www.fisica.unige.it/~grosso/scuola-estiva-fisica-2013/appunti/arduino%20e%20robotica%20in%20laboratorio,%20PLS2013%20-%2000%20introduzione%20al%20physical%20computing%20e%20arduino.pdf

[31] P. Nikolaos, "Egm2008 - wgs 84 version," April 2013. [Online]. Available: http://earth-info.nga.mil/GandG/wgs84/gravitymod/egm2008/egm08_wgs84.html

[32] "Learjet 85." [Online]. Available: businessaircraft.bombardier.com/en/aircraft/learjet/learjet85.html

[33] RFI, "Crossed polarized yagi antennas, ycp4047 series, 400-470 mhz," April 2014. [Online]. Available: http://www.rfiwireless.com.au/media/downloads/pdfs/YCP4047_Series_P-40987-6.pdf

[34] A. Kostopoulos, *Corso di telecomunicazioni*. Petrini Editore, 1999, pp. 296–297.

[35] "Raspberry pi, model a b." [Online]. Available: http://www.raspberrypi.org/new-graphic/

[36] A. Chadwick,"Baking Pi Operating Systems Development", University of Cambridge, 2012. [Online]. Available: http://www.cl.cam.ac.uk/projects/raspberrypi/tutorials/os/

[37] "Arduino." [Online]. Available: http://www.arduino.cc/

[38] W. Elliot, *AVR Programming*. Makermedia, 2014.

[39] "Arduino." [Online]. Available: http://arduino.cc/en/Main/arduinoBoardUno#

[40] "Position sensitive device." [Online]. Available: http://en.wikipedia.org/wiki/Position_sensitive_device/

[41] "Scilab image and video processing toolbox." [Online]. Available: http://sivp.sourceforge.net/

[42] S. Sgubbini, “Moti kepleriani,” Scuola di ingegneria aerospaziale, Universitá La Sapienza, Rome, Tech. Rep., 2006.

[43] M. Mariola, A. Mirza and F. Petruccione,Influence of the motion of aerospace systems on the polarization angle of qubits for free-space QKD, in Proceedings of SAIP2012: the 57th Annual Conference of the South African Institute of Physics, edited by Johan Janse van Rensburg (2014), pp. 505 - 510. ISBN: 978-1-77592-070-0. Available online at http://events.saip.org.za.

[44] A. Di Pierro, “Quantum computing,” University of Verona, Tech. Rep., 2010. [Online]. Available: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fprofs.sci.univr.it%2F~dipierro%2FInfQuant%2Farticles%2FLezioni-IQ.pdf&ei=dVTKVIzVHszlUtaggugM&usg=AFQjCNHRWawHcrAgPF34rz8yZif6LCSCfQ&sig2=vGkmkQV9FsAe06TJmKJnww

[45] M. Mariola, A. Mirza, F. Petruccione, SYSTEM AND METHOD FOR DETERMINING ANGLES BETWEEN APPARATUSES, DEVICES OR SYSTEMS, 2014, PROVISIONAL PATENT APPLICATION NO. 2014/03405, South Africa.

[46] V. D’Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, “Complete experimental toolbox for alignment-free quantum communication,” *Nature communications*, vol. 3, p. 961, 2012.

[47] E. Pannella and G. Spalierno, *Corso di Elettronica*. LORETO: Edizioni CUPIDO, 1995, vol. 2.

[48] “Acquisizione dati da fotodiodo.” [Online]. Available: http://www-3.unipv.it/lde/didattica_elettronicaII/Fotodiodo.pdf

[49] G. Biondo and E. Sacchi, *Manuale di elettronica e telecomunicazioni*, hoepli ed., 2005.

[50] “Atmel 8-bit avr microcontroller with 2/4/8k bytes in-system programmable flash,” Atmel, Microcontroller Division Applications. [Online]. Available: http://www.atmel.com/Images/doc8006.pdf

[51] “Driving an analog keyboard with the st7 adc,” ST, Microcontroller Division Applications. [Online]. Available: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDIQFjAA&url=http%3A%

2F%2Fwww.st.com%2Fweb%2Fen%2Fresource%2Ftechnical%2Fdocument%2Fapplication_note%2FCD00004024.pdf&ei=phK1VMeeEcGsUeeNgZgC&usg=AFQjCNE4oGyQdvLeWT6bxYlfZUGBjy--pg&sig2=3rQEpPVqix7Yt_cypJO3Ig

[52] "Atmel 8-bit avr microcontroller with 4/8/16/32k bytes in-system programmable flash," Atmel, Microcontroller Division Applications. [Online]. Available: www.atmel.com/images/doc8161.pdf

[53] "ngspice." [Online]. Available: http://ngspice.sourceforge.net/download.html

[54] "Lh0084/lh0084c digitally-programmable-gain instrumental amplifier." [Online]. Available: http://pdf.datasheetcatalog.com/datasheets2/43/430682_1.pdf