Open-Source electronics for quantum key distribution

M.Mariola[1], A. Mirza[1] and F. Petruccione[1,2]

[1]University of KwaZulu-Natal, Westville Campus, Durban, South Africa,
[2]National Institute for Theoretical Physics, South Africa .

E-mail: mmspazio@libero.it

Abstract. Quantum cryptography is a coding system that allows us to exchange a secret key without the risk of eavesdropping. The cryptographic key is composed by a series of quantum states of single photons. Each quantum state is known now as quantum bit or qubit. Quantum cryptography exploits the Heisenberg's uncertainty principle, whereby after a measurement, the quantum state is necessarily changed from the original state. In order for the key exchange to takes place it is necessary that the transmitter and receiver are linked with a quantum channel. This link may be realized by fiber optics or free space. In free space the quantum state is represented as polarization. In free space the photon beam is subject to wandering, scintillation and attenuations by the atmospheric turbulence. In this article the design of a possible electronics system able to compensate for the atmospheric effects on the photon beam using open-source electronics is presented. These systems are useful in order to build prototypes and at low cost products.

1. Introduction

Cryptography is a way to secure the messages against the eavesdropper. The message is encrypted by a private key shared between the transmitter and receiver. The protocol currently used in modern communication is the RSA protocol [1]. This protocol is at best computationally secure. In the RSA protocol the private key is contained in a public key sent through the public channel. However, Shor's algorithm is the efficient way to calculate the private key given a quantum computer [2]. This is because one is able to calculate the private key in polynomial time and in that case the private key is not safe. Quantum cryptography permits one to share a private key while ensuring there is no eavesdropping in between the transmitter and receiver. By convention the transmitter is referred to as ALICE and the receiver is referred to as BOB, the eavesdropper is named EVE.

Quantum cryptography exploits the Heisenberg's uncertainty principle where the bits of the key are composed by the quantum states of single photons. If ALICE sends the single photon to BOB and EVE measures the quantum state of the photon, BOB will measure a different value from ALICE with a finite probability due to the Heisenberg's uncertainty principle. ALICE and BOB use a subset of the distributed photons to verify the validity of the photons sent. If the statistical outcome of the comparison illustrated a large variation ALICE and BOB know that there is an eavesdropper in the middle of the channel. The first protocol was invented by Bennet and Brassard in 1984 and this protocol is known as BB84 protocol [3]. In free space the quantum state is the polarization of the photon. The protocol uses two non-orthogonal polarization bases as shown in Table 1. ALICE randomly chooses the bases and sends the photons to BOB and BOB randomly chooses a basis to measure each photon. Through the public channel ALICE

Table 1. The polarization bases of the BB84 protocol.

BASE	0	1
+	↑	→
×	↗	↖

broadcasts to BOB the basis used to transmit each photon. ALICE and BOB also share the time stamp for the bits of the key. Since ALICE and BOB do not use a common basis all the time they exclude the bits where the bases chosen were not the same. Once this sifting procedure is complete, ALICE and BOB use a subset of the key to check if the measurement outcomes are coherent. If the error rate is above a security threshold it implies that EVE was between ALICE and BOB. ALICE will only send the encrypted message to BOB if she is sure that EVE has not eavesdropped on the key distribution process. The protocol is summarized in Table 2. Other

Table 2. ALICE sends each bit of the key using different polarization bases. BOB chooses randomly the bases to receive the bit from ALICE. The final key is composed by the bits sent and received with the same basis.

BOB	1	2	3	4	5	6	7	8	9
+	1		1	0			1		
×		0			0	1		0	0
ALICE									
+		0	1	0	0		1	1	
×	1					1			0
FINAL KEY			1	0		1	1		0

protocols such as B92 [4] exist for quantum key distribution(QKD). In free space the photon beam does not change in polarization however due to the turbulent atmospheric effects, the beam is subject to wandering and scintillations. If Alice occupies the stationary point and Bob is mounted on a vehicle it is necessary to design a tracking system and a system to collimate the polarizer of Alice and Bob. In this paper an electronic open-source solution is presented. Open-source electronics permits the build of low cost systems for prototyping and commercial systems.

2. Propagation of electromagnetic beam in atmosphere

Recent studies show the feasibility of quantum cryptography for long distances [5]. The synchronization between ALICE and BOB is necessary to ensure correct time stamping and gating by ALICE and BOB respectively. For the BB84 protocol it is necessary that BOB knows how many bits ALICE has sent. In free space a tracking and synchronization system is also required. The tracking system is composed of a coarse and fine alignment system. For coarse alignment, it is possible to exploit the radio channels used to transmit the encrypted message [6]. The coarse alignment is necessary when the relative positions of ALICE and BOB are not known. Fine alignment and synchronization between ALICE and BOB can be implemented through a laser beacon. The laser beacon unfortunately is also affected by wandering, scintillations and spread due to atmospheric turbulence. It is therefore necessary to know the characteristic of the channel and build a system able to follow the centroid of the laser beacon.

2.1. 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 [7]

$$n_1(\vec{r},t) = n_1[\vec{r} - \vec{V}(\vec{r})t], \tag{1}$$

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

$$n(\vec{r},t) = 1 + n_1(\vec{r},t). \tag{2}$$

To design the tracking system it is necessary to consider the beam wandering and reciprocal movements between ALICE and BOB. The tracking system is required to align the polarizers of ALICE and BOB. The effects of the turbulence on the polarization of the beam is negligible [7]. 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. If the turbulent effect is small compared to the diameter of the laser beam, the beam is not deflected significantly, while if the turbulent effect is larger than the diameter of the laser beam, the beam is significantly deflected. According to Equation (1), the refractive index changes with time. If we compare pictures in different temporal steps it is possible observe the change in position of the laser spot. The single spots are inside a circle with average radius ρ_l as shows in the Figure 1. When the

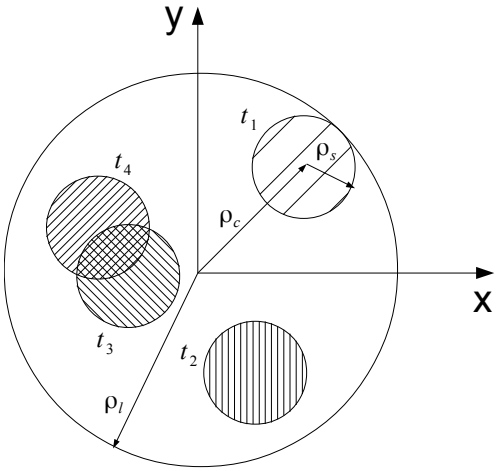

Figure 1. With time, the position of the laser spot changes. ρ_s is the spot of the laser, ρ_l is the average radius contained the single spots and ρ_c is the position of single spot at time t [7].

turbulence is greater the laser does not wander significantly hence multiple spots are received that are contained in circular area of radius ρ_l. The weighted average point of the spatial positioning of the laser beam is defined as the centroid. The tracking system must be able to follow the wandering of the centroid with respect to the inertial frame reference.

3. Open-Source electronics used for tracking systems

For the experiment and prototyping, open-source electronics is used. Analog signals from the sensor are captured by the micro-controller, ARDUINO UNO, which then provides a command to the actuators to move the mechanics of the tracking systems. The ARDUINO UNO micro-controller has six analog inputs, thirteen digital lines of input and output and is

easily programmable in C [8]. Arduino can be controlled through the USB port of a personal computer. This permits the use ARDUINO UNO in conjuction with RASPBERRY PI. RASPBERRY PI is an ARM based computer, the size of a credit card, and the operating system is linux [9]. The peculiarity of ARDUINO UNO and RASPBERRY PI is that they can be exploited to build an integrated system for prototyping a system at low-cost for quantum cryptography.

4. Tracking system

In this section the tracking system is described. The tracking system is used to compensate for the beam wandering and the relative movements between ALICE and BOB. The system aligns the polarizers of Alice and Bob.

4.1. Tracking system with PSD

The laser beacon is received by a telescope and the spot is concentrated on the position sensitive device (PSD) [10]. 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, as a function of the current values for each terminal. Using this current signature we are able to determine the position of the centroid as shows in the Figure 2. The automatic tracking control can be

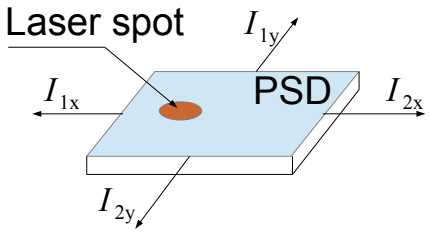

Figure 2. The laser is received by a PSD. When the laser spot changes from the central position the values of the current I_{1x}, I_{2x}, I_{1y} and I_{2y} change.

implemented using the open-source micro-controller ARDUINO UNO. The signal from the PSD is amplified and successively elaborated by the micro-controller. Micro-controller provides the measurement of the movement of the spot and at the same time it can control the power system able to move the mechanics for the tracking.

4.2. Tracking system using a camera

In the previous subsection the tracking system uses a PSD sensor to follow the spot. In the previous case the system is completely autonomous and it is not necessary to use a computer but it is not accurate. It is also possible to follow the laser spot using a camera. The spot of the laser is visualized with a camera, the position of the centroid can be computed and consequently the command can be sent to the electromechanical system of the tracking unit. The computer receives the images as a matrix of numbers. The dimension of the matrix depends on the number of pixels on the sensor of the camera. The color of the single pixel is represented by a number. When the 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 by SCILAB [11] and the result is shown in the Figure 3. The same algorithm proposed in SCILAB can be rewritten in phyton to be used in RASPBERRY PI. RASPBERRY PI and ARDUINO UNO permit one to have an integrable and autonomous system.

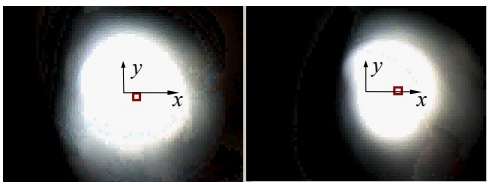

Figure 3. The red square follows the movement of the spot with respect the center of the camera indicated by the axes x, y. The same coordinates used to follow the centroid with the red square can be used to move the mechanics of the tracking system.

4.3. Polarization tracking systems

The effects of the turbulence on the polarization of the laser beam can be neglected since atmospheric turbulence does not effect polarization of the beam. If ALICE and BOB are two non stationary systems the relative position and the geometrical collimation of the polarizers will continuously change. BOB transmits a polarized laser beacon to ALICE who follows the polarization of the laser beacons using a sensor system. The system comprises of two polarizers where the polarization direction is tilted by 90 degrees as shown in the Figure 4. The reference

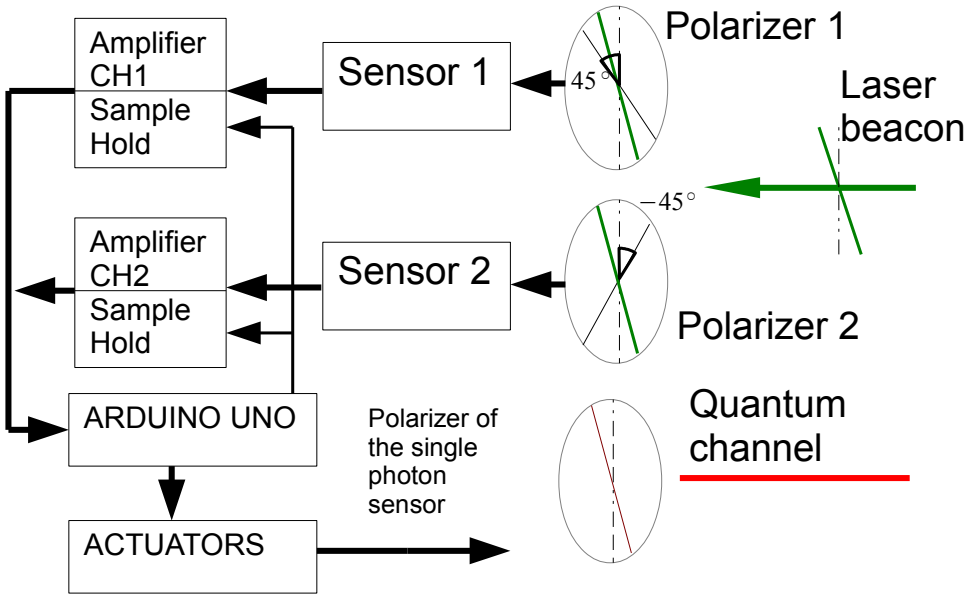

Figure 4. The figure shows the optical and electronic scheme to track the polarization of the laser beacon. If the laser beacon is received at a different angle with respect to the vertical, indicated by the dash line, the signals from polarizer 1 and polarizer 2 are different. By this difference the tracking system turns the optics until the signals from polarizer 1 and polarizer 2 are the same.

frame of the polarizers of ALICE are aligned with the vertical polarization of the incident laser beacon. If BOB is not aligned with the vertical polarization of the laser beacon, sensor 1 will measure a different value from sensor 2. The signals from the sensors are amplified and by ARDUINO UNO the analogical signals from the sensors are converted to digital signals and these are numerically compared. If the signal from the sensor 1 is higher than the signal from the sensor 2, as shows in the Figure 4, the system mechanically turns the instrument using the actuators in an anticlockwise direction. When the QKD units are correctly orientated, the

signal from sensor 1 and sensor 2 are identical and the tracking system locks this position of the polarizers. The state of polarization of the qubit is tilted with respect to the tracking polarizers of 45 and -45 degrees respectively.

5. Conclusion

The paper shows that in free space QKD it is necessary to have automatic control tracking system able to follow the relative movement of ALICE and BOB and to be able to align their orientation and hence, polarization. For a stationary unit, the turbulence affects the laser beam through wandering and spread. The prototyping of the tracking system can be made by open source electronics. The micro-controller and micro-computer mentioned in this paper permit one to build prototypes and low cost systems. The circuit of the ARDUINO UNO and RASPBERRY PI can be modified for our purposes with the advantage that it is possible to use the open-source software such as python for video processing and hardware control. Currently experiments are being undertaken in the laboratory but in the future this system will be tested for long distance QKD and for transmission between two non stationary points. The success of the experiment will encourage quantum cryptography for commercial users.

6. Acknowledgments

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. M. Mariola would like to thank Professor Paolo Villoresi for a very useful research visit at the University of Padova.

reference

[1] [online] Dalla crittografia classica alla crittografia quantistica; http://www.philos.unifi.it/upload/sub/Seminari /Filosofia-Fisica/crittografia.pdf
[2] P. Shor, Polynomial-time algorithms for prime factorization and discrete log- arithms on a quantum computer, SIAM J.SCI.STATIST.COMPUT., vol. **26**, p. 1484, 1997.
[3] Bennett C and Brassard G 1984 *Quantum cryptography: public key distribution and coin tossing* Proc of IEEE International conference on computer systems and signal processing 175-179
[4] Bennet C 1992 Quantum cryptography using two nonorthogonal states *Phys. Rev. Lett.* **68** 3121-31247
[5] Ursin R et al.3 June 2007 *Entanglement-based quantum communication over 144 km* Nature physics **3** 481-486
[6] Mariola M Mirza F Petruccione 2011 *Quantum cryptography for satellite communications* Proc. South African Institute of Physics ISBN:978-1-86888-688-3 pp.403-408
[7] Ronald L. Fante 1979 *Electromagnetic beam propagation in turbulent media* proc. of IEEE, Vol. 63, NO.12 1669-1692
[8] [online] http://www.arduino.cc/
[9] [online] http://www.raspberrypi.org/
[10] [online] http://en.wikipedia.org/wiki/Position_sensitive_device
[11] [online] http://sivp.sourceforge.net/