Type: Research paper
Section: Quantum and Non-Linear Optics

Free Space Decoy-state Quantum Key Distribution Implementation

Distribución Cuántica de Claves en Aire con Estados Señuelo

A. G. Magnoni[1,2], I. H. López Grande[1,2], M. A. Larotonda[1,2]

1. Departamento de Física, Facultad de Ciencias Exactas y Naturales - Universidad de Buenos Aires

2. Departamento de Investigaciones en Láseres y Aplicaciones (CITEDEF) - UNIDEF - CONICET

(*) E-mail: magnoni.agustina@gmail.com

Received: 02/12/2016 Accepted: 18/05/2017
DOI: 10.7149/OPA.50.2.49045

ABSTRACT:

In this work we introduce a complete Quantum Key Distribution device that implements a decoy-state protocol [1]. Qubits are coded in the polarization state of weak optical pulses, produced by infrared LEDs [2]. The link between Transmission (Alice) and Reception (Bob) stages is open air, which is the preferred channel to eventually through low-orbit satellites establish quantum communications. Both terminals are placed on different rooms, separated by approximately 8 meters. In order to compensate misalignments produced by small mechanic displacements or atmospheric thermal gradients, the system implements a closed-loop for automatic alignment based on a counter-propagating laser, a servo-actuated mirror and a CMOS image sensor. The apparatus runs in an autonomous way, and in the above described conditions it is able to generate raw cryptographic key at a rate of 185 bits/s, with a QBER of 6.15%.

Key words: Quantum Key Distribution; Open Air Communications; Decoy State

RESUMEN:

En este trabajo se presenta un sistema completo de Distribución Cuántica de Claves criptográficas, utilizando un protocolo con estados señuelo [1]. Los qubits se codifican en el estado de polarización de pulsos ópticos atenuados, producidos por LEDs infrarrojos [2]. La propagación de los mismos entre las estaciones que buscan compartir una clave se realiza en aire, que es la implementación más prometedora para cubrir grandes distancias (vía satélites de baja órbita). Las terminales de emisión y recepción se encuentran en plataformas independientes y están separadas 8 metros, siendo este sistema el primero a nivel local en ser ensayado a distancias que exceden las de la mesa óptica.

Para compensar eventuales desalineaciones por gradientes térmicos en atmósfera y pequeñas variaciones mecánicas, el sistema cuenta con un método de corrección de la puntería, basado en un haz contrapropagante, un sensor de imagen CMOS y un espejo con actuadores remotos. El aparato en su conjunto funciona de forma autónoma, y en las condiciones descriptas es capaz de generar clave criptográfica cruda a una tasa de 185 bits/s, con un error de 6,15%.

Palabras clave: Distribución Cuántica de Claves; comunicaciones por propagación en Aire; Estados Señuelo

REFERENCES AND LINKS / REFERENCIAS Y ENLACES

[1] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91**, 057901 (2003). https://doi.org/10.1103/PhysRevLett.91.057901

[2] I.H. López Grande, C.T. Schmiegelow, M.A. Larotonda, Papers in Physics, **8**, 080002 (2016). https://doi.org/10.4279/pip.080002

[3] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,* **175**, 8 (1984).

[4] W. K. Wooters, W. H. Zurek, "A single quanta cannot be cloned," **299**, Nature, 802-803 (1982). https://doi.org/10.1038/299802a0

[5] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell Syst. Tech. J, **28**, (IV), 656-715 (1949). https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[6] N. Gisin et al., "Quantum Cryptography," Rev. Mod. Phys, **74**, (I), 42-43 (2002). https://doi.org/10.1103/revmodphys.74.145

[7] G. Nogues et al., "Seeing a single photon without destroying it," Nature, **400**, pp. 239–242, (1999). https://doi.org/10.1038/22275

[8] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," Phys. Rev. Lett., **94**, (230503) (2005). https://doi.org/10.1103/physrevlett.94.230503

[9] H.-K Lo et al., "Decoy State Quantum Key Distribution," Phys. Rev. Lett., **94**, (230504) (2005). https://doi.org/10.1142/9789812701633_0013

[10] I. Marcikic et al., "Distribution of time-bin entangled qubits over 50 km of optical fiber," Phys. Rev. Lett., **93**, (180502), (2004). https://doi.org/10.1103/physrevlett.93.180502

[11] N. Gisin et al., "Quantum Cryptography," Rev. Mod. Phys, **74**, (I), 30 (2002). https://doi.org/10.1103/revmodphys.74.145

[12] N. Gisin et al., "Operational system for quantum cryptography," Elect. Lett., **31**, 232–234, (1995). https://doi.org/10.1049/el:19950153

[13] R. J. Hughes et al., "Free-space quantum key distribution in daylight," J. Mod. Opt, **47**, (2-3), 549–562, (2000). https://doi.org/10.1080/09500340008244059

[14] A. G. Magnoni, "Distribución Cuántica de Claves en aire con estados señuelo," tesis de licenciatura Ciencias Física, FCEN-UBA (2016).

[15] J. F. Dynes et al., "Unconditionally secure one-wat Quantum Key Distribution using decoy states," Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies, QML3, OSA (2007).

1. Introduction

Quantum Key Distribution (QKD) is one of the first technological applications of Quantum Mechanics that has been implemented. It was first proposed by Bennett and Brassard (BB84) in [3], as a method for achieving a secure secret key between two parties (usually called Alice and Bob) that want to establish a secret communication. This protocol guarantees perfect security of the key by relying on Quantum principles such as the Quantum Non Cloning Theorem [4], instead of relying on assumptions on the technological capacity of a potential eavesdropper. In particular -theoretically- the combination of QKD and the cryptographic protocol *one time pad* is inconditionally secure [5].

Nevertheless, the practical implementation of a protocol raises some security concerns. The most important one is the necessity to use a perfect single photon source for the generation of qubits. Such a source is not technologically available in present day, so it is usually replaced by coherent states in the form of heavily attenuated light sources. These states have a photon number value that obeys the Poisson statistics, so there is always a probability of emitting multi-photon pulses. This brings up a security breach, giving a potential eavesdropper (Eve) the possibility of performing a *photon number splitting* (PNS) attack [6]. In this attack, Eve measures the photon number of each pulse in a non destructively manner, and in case of a multi-photon event, she keeps one photon and resends the others to Bob. By doing this she can obtain a great amount of information about the key. Such kind of attacks have no effect on the Quantum Bit Error Rate (QBER) of the key, because of the performance of Quantum Non Demolition measurements on the qubits exchanged by Alice and Bob. Even though this type of measurements are far from being implemented nowadays, it is a real possibility in near future [7]. In 2003, Hwang proposed a way of overcoming this security issue [1], introducing a modification on the protocol. Such a decoy state protocol uses two sources to prepare two different states: the signal ones, used to generate key in a BB84 way, and the decoy ones, only incorporated to bring security. These two sources must have a different mean photon number (μ and ν respectively), so

that they suffer an asymmetric loss in case of a PNS attack. Accordingly, by monitoring the transmittance of each state (Q_μ and Q_ν) the security of the key can be guaranteed [8,9].

Finally, even though the resulting key of a protocol has errors (experimental or due to an eavesdropper) it is still possible to obtain a perfectly secure key from it by applying classical post processing algorithms, such as error correction and privacy amplification. However, these algorithms only work when the error in the raw key is less than 14.6%, which is the maximum bearable amount of error that can be accepted.

Quantum Key Distribution can be implemented either on open air and on optical fibers. For intermediate distance communications (~100 km) fibers are the preferred propagation medium, because of the extremely low attenuation in the telecommunications window (~1550 nm). Also, fibers allow for communication between two distant locations without a line of sight. Protocols with propagation in fiber tend to have qubit codifications in other degrees of freedom than polarization, because of the birefringence effects they exhibit [10].

On the other hand, free space implementations of QKD present the most promising option for finally accomplishing communications all around the globe, by establishing links between the Earth and Low Earth Orbiting Satellites (LEOS) [11]. Also, free space communications offer some comparative advantages compared to optical fibers: first, birefringence effects that could alter the polarization state of the photons are not present. Second, the atmosphere has a high transmission window in wavelengths of ~770 nm where the most efficient photon counting detectors can be found [12,13].

Here we report a successful practical implementation of a BB84 Quantum Key Distribution protocol between two stations with free space propagation. The stations are completely independent and distant, and the protocol counts with the addition of decoy states in order to guarantee the security of the key from PNS attacks.

2. Experimental Implementation

The decoy state QKD implementation developed in this work includes an emission and a reception stage mounted on two platforms separated by approximately 8 m. Therefore, it was necessary to design an actively-controlled alignment system in orden to maintain the original conditions of the experiment through time. A diagram of the complete experimental setup is presented in figure 1. Both Alice and Bob included an optical arrangement for state preparation and measurement, respectively (figure 2). Alice's setup consists in a polarization beam splitter that transmits the horizontal component and reflects the vertical one. It has four inputs, each one for one of the four quantum states relevant to the protocol: $|H\rangle, |V\rangle, |D\rangle, |A\rangle$.The characterization of this output is presented in figure 3, via Quantum State Tomography measurements to obtain the density matrix of each output state.

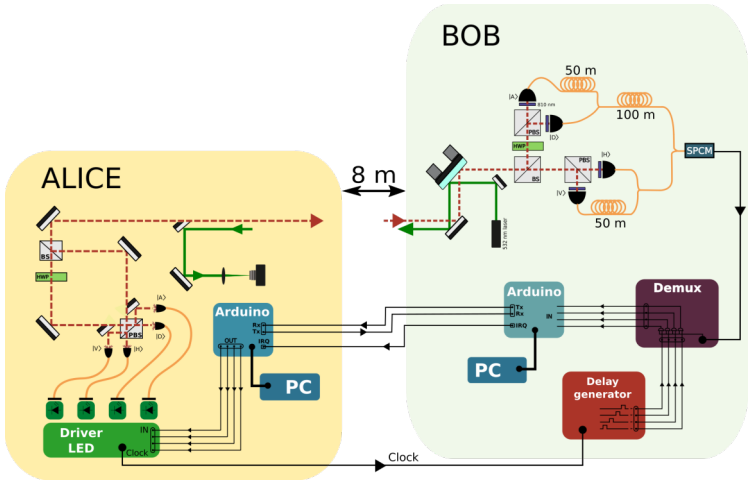

Fig 1: Diagram of the complete experimental setup. Alice and Bob consist of two independent platforms separated by approximately 8 m. The QKD implementation and the active pointing stabilization system are designed to run in parallel.

At Bob's side (figure2), the optical arrangement is in charge of the detection in either one of the two basis of interest: the computational $\{|H\rangle, |V\rangle\}$ and the diagonal $\{|D\rangle, |A\rangle\}$ bases. The incoming qubits from Alice

encounter a beam splitter that introduces the randomness in the choice of detection basis. These device has four exits that are temporally multiplexed with four fiber patchcords of different length in order to use only one photon counter. The light distribution at the four exits was also characterized, obtaining only a 6% of potential errors due to imperfections either on the optical elements or in the alignment.

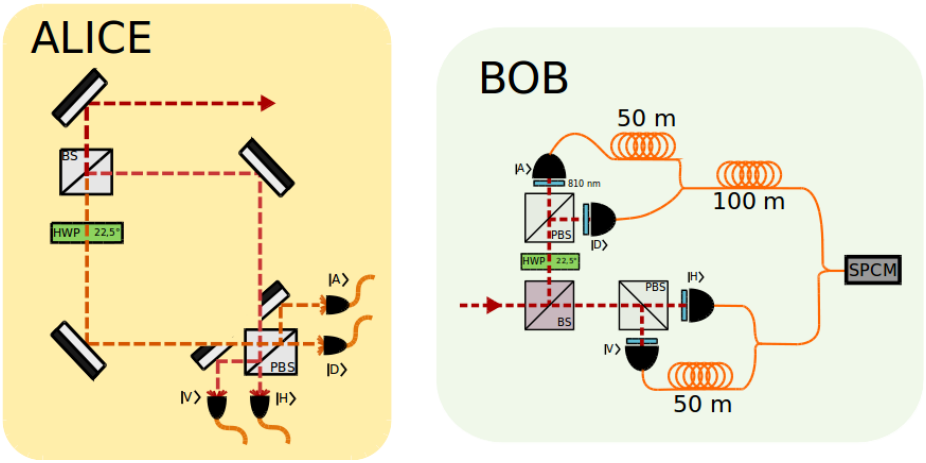

Fig 2: Optical setups included in the two stations of the device. At Alice's side the state preparation takes place, whereas the detection on either the computational or diagonal basis occurs at Bob's side. In order to use only one detector, a temporal multiplexing optical system is incorporated.

Four infrared LEDs were used as light sources, one for each state, powered by two different electrical pulses in order to emit signal and decoy states [14]. The mean photon number obtained on each type of state were $\mu = 0.64$ and $\nu = 0.48$, with a ratio of ~0.76. It is worth to note that these sources have a high probability of emitting multi-photon pulses, but the inclusion of the decoy states solves this problem. The infrared LEDs were coupled to multimode optical fibers in order to improve the spatial profile and collimation, and were then placed at the four entries of Alice's optical arrangement. The ratio of decoy-to-signal states included in the protocol to reveal a potential photon number splitting attack was 12.5%.

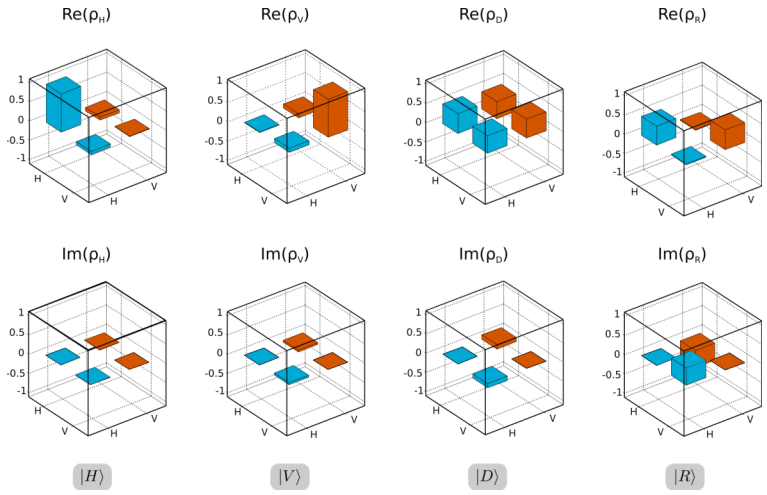

Fig 3: Density matrices obtained by Quatum State Tomography that fully characterize the states prepared at the emission stage.

On Bob's side, an electronic demultiplexing system is used to re-obtain four different paths. This system is triggered by a clock signal sent by Alice. Two Arduino micro-controllers are used to control the experiment and to synchronize the different steps of the protocol.

Finally, the setup includes an active alignment control (figure 4) in order to maintain the original pointing conditions of the experiment despite small misalignments produced by mechanical displacements or atmospheric thermal gradients. This system utilizes a counter-propagating additional beam, parallel to the quantum channel, represented by a green laser (532 nm).

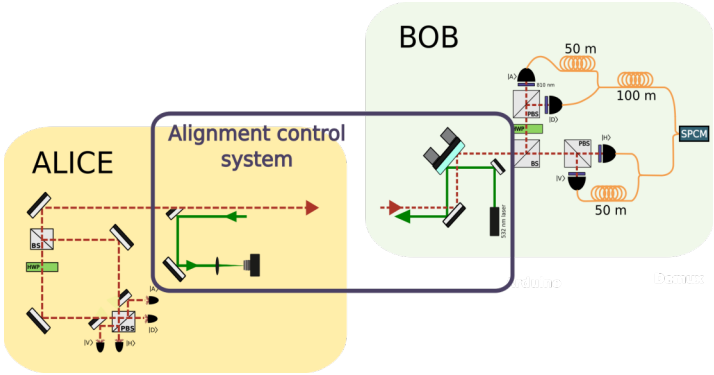

Fig 4: An experimental diagram of the active system for alignment control that was developed for the device. It comprises an additional control beam, parallel to the quantum channel that is monitored constantly with a CMOS image sensor.

The two beams share a motorized mirror that is controlled remotely. The control laser is monitored on a CMOS image sensor of 1280x960 pixels. Any misalignment between the two platforms is seen as a change in the position of the laser spot on the CMOS array sensor. Therefore, by rotating the motorized mirror in such a way to restore the original position, the alignment condition is corrected. This control system operates simultaneously with the QKD set up.

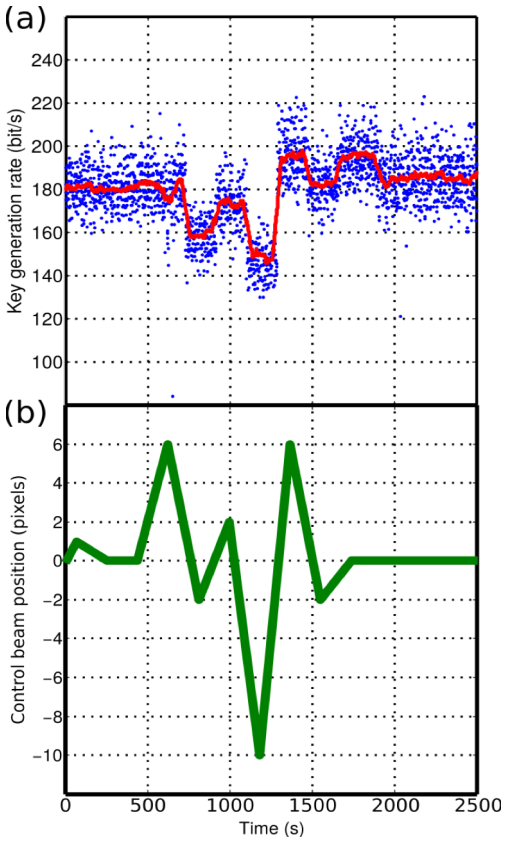

Fig 5:. Performance of the device under induced mechanical perturbations. Figure (a) corresponds to the key generation rate as a function of time. The red line shows the mean value of the measurement. Figure (b) corresponds to the position of the control beam in the CMOS array sensor as a function of time.

The results of the complete experiment show a key generation rate of approximately 185 bit/s with an QBER of 6.15%. This error value allows the generation of perfectly secure key by the use of post processing algorithms. A very simple error correction algorithm was applied, reducing the QBER to 0.4% with the cost of reducing also the key generation rate to a value of 40 bit/s. Regardless, more effective algorithms can be employed to reduce the error in the key with minor effect in the generation rate. Also the transmittances of

the two states were monitored obtaining an average value of 0.72. This value differs from to the original ratio of 0.76 less than a 17% [15]. The alignment control system functioned in parallel to the QKD setup all through the experiment. Intentional misalignments between the two platforms were performed as the key generation rate was monitored in real time. The results are shown in figure 5. It can be seen that when a misalignment takes place, the value of the key generation rate is modified. Then, when the system restores the alignment condition, the original value of the key generation rate is also restored. This shows that the two systems can work simultaneously, and the alignment correction system is capable of maintaining the original conditions of the experiment in real time. The "overshoot" on the key rate generation that occurred after the correction at 1300 s is due to a small mismatch between the initial alignment of the two beams (i.e. during the experiment the control beam alignment was optimized while the quantum channel alignment was slightly off the optimum condition).

This experiment is a first step to develop a QKD implementation between two independent and distant stations separated by a few meters. This set up can be later on adapted to study cases in which one platform moves slowly away from the other, in order to advance towards earth-satellite communications.

3. Conclusions

In this work we present a practical implementation of a Quantum Key Distribution device with decoy states, incorporated in order to guarantee the security of the protocol from photon number splitting attacks. This device distributes key between two independent locations separated by approximately 8 m, with an alignment control active system, in order to maintain the original conditions of the experiment. The apparatus generates key at a rate of 185 bit/s, with a QBER of 6.15%, that allows the obtaining of perfectly secure key by post processing algorithms.

Acknowledgements

This work was presented in the IX Conference RIAO/OPTILAS, 2016.

