Influence of the motion of aerospace systems on the polarization angle of qubits for free space QKD

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 allows private key exchange between the transmitter system, called Alice, and receiver system, called Bob. The key must be sent as a sequence of single photons and must be appropriately polarized. A photon sent with a horizontal base polarization must be received with the same base polarization. The polarization of the photon in free space, especially for satellite communication does not change enough to be a problem in our system. However, the change of directions of an aerospace system does require the system to be able to compensate for the relative rotations between Alice and Bob. In the case of satellite communications, the tracking angle can be deduced from the orbital parameter. For an atmospheric vehicle, a particular system to hold the contact between the transmitter and receiver is required. This proceeding shows some possible solution for a robust solution for a robust compensation.

1. Introduction

From the oldest to the newest cryptography systems, the fundamental security is related in terms of the key exchange used to decrypt and encrypt the message. The keys can be of public or private domain and when it comes to quantum cryptography it refers to the exchange of private keys, where the key for coding and encoding is the same. Using this kind of system, the receiver and the transmitter must be sure that the key is not interceptable from an eventual eavesdropper, that from this moment we'll call Eve. The quantum cryptography is guaranteed by the no-cloning theorem [2] such that the key is received without any interception from Eve and it is possible to send the encrypted message by using the public channel. The key will be formed by bit sequence called quantum bit (qubit) which is obtained by a reading of the quantum state of the corpuscle. As known for this kind of communication, qubits are sent as a sequence of photons [3]. Briefly, the qubit will be sent and received by using two non-orthogonal bases (vertical and horizontal). Alice and Bob separately and randomly decide which polarizing base they use to receive or transmit the photon. If Alice uses a different base from that of Bob which he used to receive the qubit, this would result in the loss of one bit of the key but they know that in that time interval Bob received one qubit. When the transmission is complete, Alice and Bob will compare some received qubits with the same base used (that will be removed from the key). If there are important statistic differences, this means that Eve was present in the channel and it is not possible to send the message. From this brief discussion Alice and Bob must be synchronized, be spatially aligned [4] and with polarizers of the receiver and transmitter collimated.

2. Tracking system

It was shown that it's possible to obtain a quantum cryptography system in free space between two stationary points on the ground [5]. In aerospace systems, it is not possible to have two stationary units because the relative position of the transmitter and receiver change continuously with time. The communication systems must guarantee the optical link between Alice and Bob. This can be achieved by the GPS system or a system that uses the radio or laser signals.

2.1. GPS system

By using a GPS, Alice and Bob, knowing their positions and altitude, can send their location's data one after each other. Alice and Bob knowing their relative positions in space are able to align and send the key. One of the advantages of this system is that the same GPS signal can be used to synchronize the qubit transmission. This system is not independent from the other systems and it is possible to have Doppler problem [4] in some case.

2.2. Radio signal system

The system proposed to use a radio signal to send the encrypted message [4], synchronizes the qubit and for tracking as shown in Figure 1. The system resolves the Doppler effect and the system is completely autonomous. The radio signal is however transmitted from aerospace system which means an increase of the power budget on board of aerospace vehicle.

2.3. Laser tracking system

The system uses a laser with a different wavelength to the laser used for qubit exchange. This tracking laser signal is sent from Alice and received at Bob. In the system shown in the Figure 1, the laser signal will be detected at sensor 1 and sensor 2. As the same signal is received with varying phases by the sensors, it is possible to extract a voltage signal from the phase comparator circuit which is used to control the orientation of an aerospace vehicle. Bob must send another radio or laser signal to control the tracking of Alice. 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 collimation of the polarizer.

2.4. Tracking scheme

Using the system suggested in §2.3, suppose Alice is the satellite system that is not aligned with the Earth station, Bob. Photosensor 1 detects the signal at a varying time with respect photosensor 2. The signal in the channel 1 (CH1) has a different phase with respect to the signal detected in channel 2 (CH2). The phase difference provides the voltage difference which is able to drive the control tracking system. An example is shown in Figure 1. By using a pulsed laser beam as tracking signal, if the satellite is not aligned with the ground station, a phase difference will exist. In this proceeding, the phase sensor is shown like a XOR port. From the measured phase difference in output of the logical port, we have an impulse sequence through a filter which is converted to a voltage difference that is able to control the tracking. In this particular scheme, the filter can be a low-pass filter. The phase difference received between channel 1 and channel 2 is:

$$\Delta\phi = \frac{2\pi}{\lambda}(\lambda - d\sin(\alpha)), \tag{1}$$

where, $\Delta\phi$ is the phase difference between the received signal and λ is the wavelength of the signal. The precision of tracking depends on the frequency, the distance d and the reactivity of the electronic circuits at high frequency.

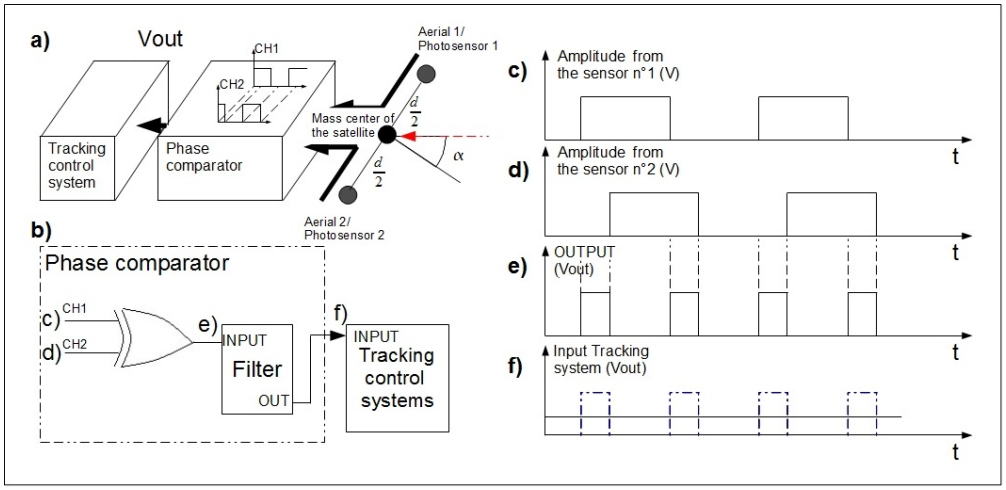

Figure 1. The figure shows the scheme for tracking between Alice and Bob.

3. Quantum cryptography for satellite communication

The tracking scheme shown in the Figure 1 can be used for any kind of aerospace systems. Once the systems are accurately tracked, it is necessary to adjust the angle of the polarizers of the receiver and the transmitter. The polarization of the photon does not change drastically [6]. By considering Alice as a satellite, and the horizontal base of the polarizer parallel at the orbital plane, it is possible to know the polarization received on 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 degree between the Greenwich and the Aries constellation. These conditions are at the initial time when the satellite crosses over the descendent node. The ground trace is calculated by considering the rotation motion of the Earth. The ground trace is given by the formulas:

$$\sin(\lambda) = \sin(\phi)\sin(\beta), \tag{2}$$

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 surface. The longitude, μ, is given by,

$$\mu = \mu_\Omega + \omega_E \Delta t - \arcsin\frac{\cos(\phi)}{\cos(\lambda)}, \tag{3}$$

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 2 the polarizer's angle θ is calculated from the nodes line until 1 rad. The angle θ, represents the angle between the line of horizontal base of the polarizer (parallel to the orbital plane) and the equatorial plane. The simulation considers the equatorial plane as the reference plane. On the ground trace the additional phase per period is due to the rotation of the Earth.

4. Aerosystem to Aerosystem links

A link between two aerosystems is realizable without a complicated orientation control system of the aerosystem because it is possible to exploit the aerodynamics forces. The synchronism by the laser is particularly easy if two vehicles fly at the same altitude and are sufficiency close since this will prevent the multipath [4]. In the previous section, it is possible to calculate the polarizer's angles during the orbit evolution, but in this case the change in relative position

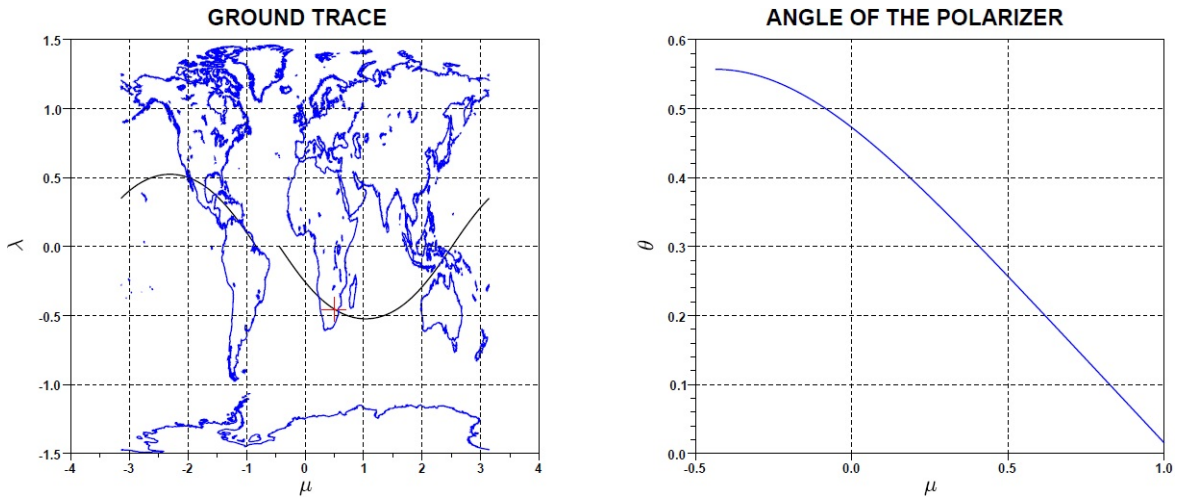

Figure 2. Angle of polarizer θ in function of the longitude μ. It is possible to observe from the first chart the simulation which considers the satellite that crosses the geographical position of Johannesburg.

between Alice and Bob is random and it is impossible to predict the orientation of the polarizers of Alice and Bob during the flight. To resolve this problem, the communications systems must have the appropriate polarization compensation controls.

5. Satellite to satellite

As the satellite orbit is predictable, it is possible to know the relative position of the satellites. In the satellite to satellite link, the direction of the link and the position of the polarizers are either known or it possible by the use of an appropriate systems of tracking and collimation.

6. Possible solutions

Other experiments show the possibility of using a beam laser reference which is able to hold a correct polarization angle between Alice and Bob [7]. A possible circuit for this is shown in Figure 3. Bob has two optical receivers, one for the quantum channel and another for the polarization control. The intensity of the polarized light I_0 through the Polaroid foil at an angle of θ from polarization axis has a final intensity according to the formula [8]:

$$I(\theta) = I_0 \cos^2(\theta). \tag{4}$$

The hypothetical scheme is shown in Figure 3. Suppose that Bob receives a beam laser reference with an angle α between $\frac{\pi}{4}$ and $\frac{\pi}{2}$, the intensities received at P1 and P2 (see Figure 3) are respectively:

$$I_{P1} = \cos^2(\alpha) \tag{5}$$

$$I_{P2} = \cos^2(\frac{\pi}{4} + \alpha). \tag{6}$$

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 polarizer until the difference is zero. This system is generic, but necessary observations must be made by considering the limit it uses. If the wavelength of the laser beam is much different from the wavelength of the photon, the aerosystems must have the same altitude and are limited to be close to each other. As shown in Figure 4, Alice sends the quantum key to Bob 1 and the laser beam and photon

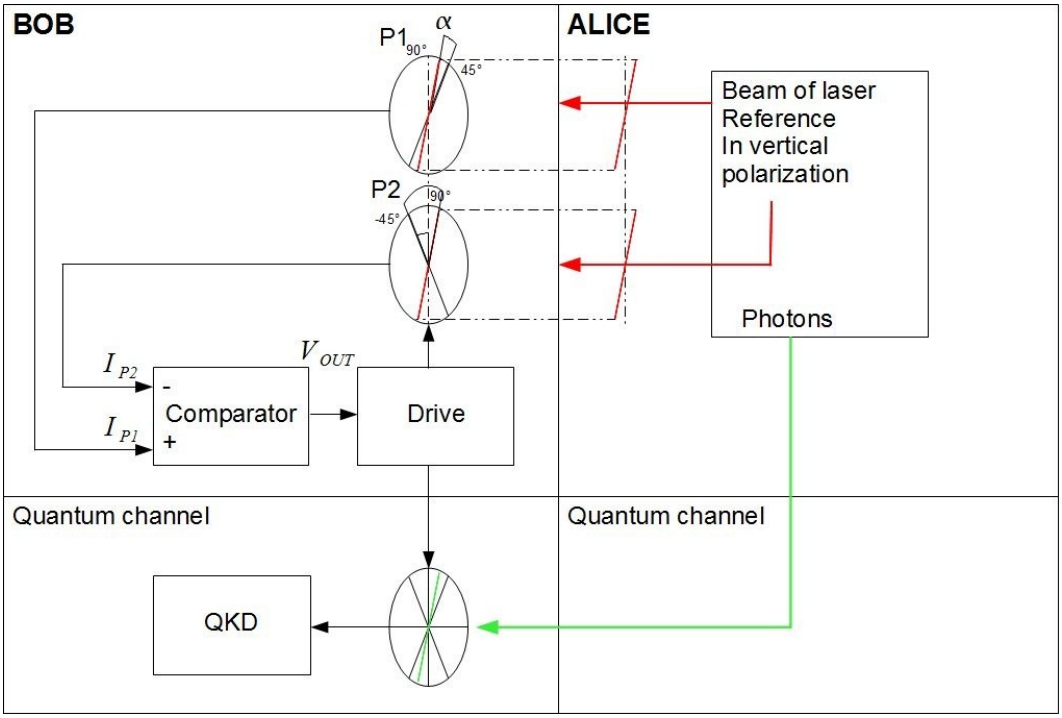

Figure 3. Scheme of the circuit to track the polarization angle of Alice and Bob.

have different wavelengths. By dividing the atmosphere into layers, where the state atmosphere parameters remains constant, the communication is possible without any problems. If Alice sends the message to Bob 2, the laser beam and the photons cross different atmospherics layers and follow different paths due to refractive indexes. It is possible to enhance the solution, if the value of wavelength of the laser beam is near to the wavelength of the photons, but this will lead to noise which is received by Bob. In this case the laser beam must be off when Alice sends the photons or the laser beam must be spatially far from the path of photons. This kind of system can be used for ground to aerospace vehicle links as well.

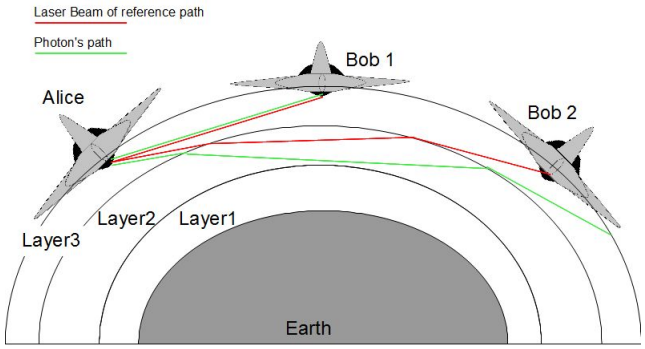

Figure 4. Consider the link between Alice and Bob. If the link propagates through a single layer of the atmosphere, minimal diffraction occurs, hence the green laser and the red laser (Single photon) have the similar paths as illustrated with Bob 1. The link to Bob 2 propagates through various layers of the atmosphere and due to chromatic dispersion the lasers follow different paths.

7. Conclusion

The QKD for satellite communications can be made possible from the knowledge of the orbital parameters. It is also possible to use the radio signal or laser signal to provide the synchronization between the earth station and the satellite or between two generic aerospace systems. If the system uses the laser beam to collimate the polarizer, the same signal can be used for tracking and synchronizing Alice and Bob for any kind of link. By considering Alice as satellite, this offers an advantage for not complicating the orientation control system and also makes it possible to improve the key generation rate [9]. For QKD, the proposed method of using the radio signal to synchronize Alice and Bob and the laser beam reference to control the polarization during the flight of Alice and Bob is seen to be the most elegant solution. This is seen from the fact that if the power budget for satellite is high it is necessary to use the simulation proposed in §3, but in our case it is not necessary to use it. This further shows the efficiency of our system.

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.

References

[1] Salvador E 2007 *Appunti di crittografia complementi al modulo 3 del laboratorio una introduzione all'algebra moderna* (Torino: Universita' degli studi di Torino)

[2] Bonzio S Galeazzi S 2011 *Dalla crittografia classica alla crittografia quantistica* (Firenze: Unifi)

[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] Mariola M Mirza A Petruccione F 2011 *Quantum cryptography for satellite communication* Proc of SAIP 403-408

[5] Ursin R Tiefenbacher F Schmitt-Manderbach T Weier H Scheild T Lindenthal M Blauensteiner B Jennewein T Perdigues T Trojek P Ömer B Fürst M Meyenburg M Rarity J Sodnik Z Barbieri C Weinfurter H Zeilinger A 2007 Entaglement-based quantum communication over 144 km *Nature physics* **3** 481-486

[6] Bonato C Aspelmeyer Jennewein T Pernechele C Villoresi P Zeilinger A 2006 Influence of satellite motion on polarization qubits in a Space-Harth quantum communication link *Optics express* **14** 10058-10059

[7] Toyoshima M Takenaka H Shoji Y Takayama Y Takeoka M Fujiwara M Sasaki Polarization-basis tracking scheme in satellite quantum key distribution International Journal of Optics **2011** 5-6

[8] Di Pierro A *Quantum Computing* http://oldweb.ct.infn.it/ terrasi/LezioniQC-05.pdf

[9] Bonato C Tomaello A, Da Deppo V, Naletto G, Villoresi P *Feasibility of satellite quantum key distribution* Department of Information Engineering, University of Padova CNR-INFM LUXOR, New Journal of Physics **20 2009**