Polarization alignment system 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 (KZN), Durban, South Africa.

E-mail: mmspazio7610@gmail.com

Abstract. To share a secret message between a sender and a receiver it is necessary to encrypt the message using a particular key and related algorithm. Generally a public key has an associated private key. The private key is computationally secure unless the eavesdropper has a quantum computer. In quantum cryptography the transmitter and receiver share a private key used to encrypt and decrypt the message. In one implementation of quantum cryptography the bits of the key are sent as series of polarized single photons. If an eavesdropper is present in the channel, the receiver receives a different bits of the key, because after the measurements by the eavesdropper, by the Heisenberg's Uncertainty Principle, the quantum state of the single photons may change. Since the value of the single bit depends on the polarization states, the polarization basis of the transmitter and receiver must be aligned. In this paper various solutions for automatic alignment control of the polarization basis are shown.

1. Introduction

The RSA protocol is a method to share a secret key between the transmitter, conventionally called Alice, and the receiver conventionally called Bob [1]. This numerical method is still computationally secure due to the calculation time in order to extract the private key contained in the public key. In 1997 Shor showed that quantum computers are able to factorize the public key in polynomial time [2] and hence the RSA protocol can be violated. The protocol above is known as an asymmetric key system. 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, conventionally called Eve, during the transmission of the key. The idea exploits the Heisenberg's Uncertainty Principle.

Quantum key distribution was proposed in 1984 and the first protocol is known as BB84 [3]. Alice sends to Bob a private key as a series of single polarized photons. The protocol uses two nonorthogonal basis, and the polarization state of the single photons represents the value of the bit of the private key. The basis are tilted 45 degrees. Alice, for each single photon, randomly chooses the polarization base and the value of the quantum bit. Bob randomly choose 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 0. The second base, indicated with the symbol $\times$ is tilted by 45 degrees with respect to 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,

Table 1. Alice sends to Bob the key using different basis. The bits are choosen when the basis of Alice and Bob are the same.

Alice	Base	+	+	×	+	×	×	+
	Quantum bit	→	↑	↖	↑	↗	↗	↑
	bit of the key sent	0	1	1	1	0	0	1
Bob	Base	+	×	×	×	×	×	+
	Quantum bit	→	↑	↖	↑	↗	↗	↑
	bit of the key received	0	1	1	N	0	1	1
	Final key	0		1		0	1	1

Alice transmits via a public channel to Bob the basis used, and the final key is composed by the bits transmitted and received with the same basis. The process of the key exchange is represented in Table 1.

If the basis chosen are the same and the polarization base of the transmitter and the receiver are not aligned some, errors may still occur as indicated by the red bit 1 shown on the table 1. With the presence of a misalignment Alice and Bob may register the presence of Eve in the channel. In order to remove the errors the process called distillation is necessary. Bob should know the timing of the photon transmission and the basis must be aligned. The timing can be obtained by radio or optical synchronization [4]. The commercial systems for quantum cryptography use fiber optics as optical channel and can be used only when Alice and Bob are stationary. Quantum cryptography in free space permits to share a secret message between two stationary points or when Alice and Bob are two non stationary points.

2. Polarization alignment system using one laser beacon and one polarizer

In order to align the polarization basis of the transmitter and receiver, the system uses a vertically polarized laser beacon [5] and one polarizer. The wavelength of the laser beacon and the wavelength of the single photons are different. The polarization direction of the laser beacon is aligned with the polarization basis used by Bob for the quantum transmission. The polarizer is mounted on Alice's side, and the direction of polarization is aligned with the polarization basis of Alice for the quantum transmission. The system is shown in figure 1. Bob sends the polarised laser beacon to Alice, and Alice receives the signals affected by scintillation and wandering due to atmospheric turbulence. The turbulence effects on the polarization of the laser beacon can be neglected [6]. When a polarized laser beacon with the intensity I'_0 crosses a polariser, in output the intensity follows the Malus' law:

$$I_1 = I'_0 \cos^2(\theta), \tag{1}$$

where I'_0 is the intensity of the spot at the input of the polarizer and I_1 is the intensity of the spot at the output. θ is the angle between the direction of polarization of the laser and the direction of the polarization of the polarizer. When $\theta = 0$ It follows $I_1 = I'_0$. Since the intensity changes with the time, due the atmospheric turbulence, it is not possible to know in advance the value of I'_0. As shown in figure 1, the value of I_1 can be obtained if the misalignment correspond to an angle θ_1 and exist an ambiguity of rotation between θ and θ_1. In order to find the correct direction, the polarizer can be rotated until the maximum value of the intensity is measured. The Algorithm is shown in figure 2. The tracking system of Alice measures the intensity I_1 stored

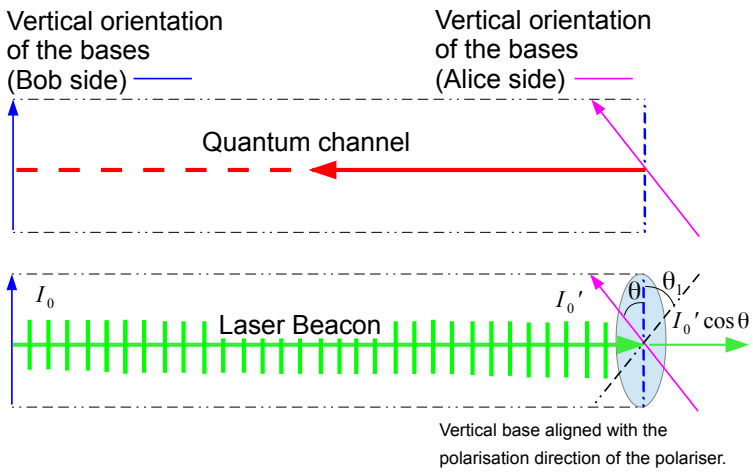

Figure 1. The blue dashed line and the green lines, correspond to the vertical direction of the laser beacon and the violet arrow correspond to the direction of the vertical polarization base of Alice. The vertical polarization direction of Alice is orientated in the same direction of the polariser of the alignment system. The black dashed line represents the ambiguity between the real angle of misalignment θ and the specular angle θ_1. When the laser crosses the polarizer the intensity in output follows the equation (1) from which is possible calculate the angle of misalignment without information of the verse of rotation (θ or θ_1).

in the the variable *a1*. The system randomly chooses the direction of rotation, for example clockwise, and the power drive mechanically turns the basis (polarizer of the tracking system and the bases of the quantum channel). Alice measures the intensity of the laser beacon and store this value in the variable *a2*. If *a2* is smaller than *a1*, Alice changes the verse of rotation to anticlockwise. If the condition is true the direction of rotation does not change from clockwise. This kind of system can not work properly when the atmospheric turbulence is strong. The basis can not be stable in one direction but an oscillation around the vertical position occurs. Increasing the sensitivity of the detectors the amplitude of the oscillations decrease and the system can be considered aligned also if a small oscillations are present. The experimental setup is shown in the figure 3. The side where the fixed polarizer is mounted represent the position of Bob. The fixed polarizer is used in order to create a polarized laser beacon. Initially the polarizers are not aligned and the shaft starts to rotate by the micro-controller command. For the experiment a stepper motor was used. The stepper motor is used in order to control the speed and the amplitude of rotation. At each step the micro-controller measures the intensity of the signal outcome from the rotating polarizer and decides the direction of rotation using the algorithm in figure 2. The system shown on the bottom can be modified as shown in figure 4, in order to calculate the angle θ. A beam splitter divides the signal in direction of the detector D1 and detector D2. The signal measured from the detector D1 can be used to calculate the initial intensity I_0, and by the inverse of equation (1) it is possible calculate the angle θ. Since the ambiguity of the direction of rotation is still present, it is possible to follow the algorithm in figure 2. Instead of using the intensity, the test can be done on the angle θ. The angle θ can be calculated by the inverse of equation (1). The last configuration is the best way if the alignment system works in strong turbulent environment because the power I_0' received is known by the measurement in D1 after previous corrections.

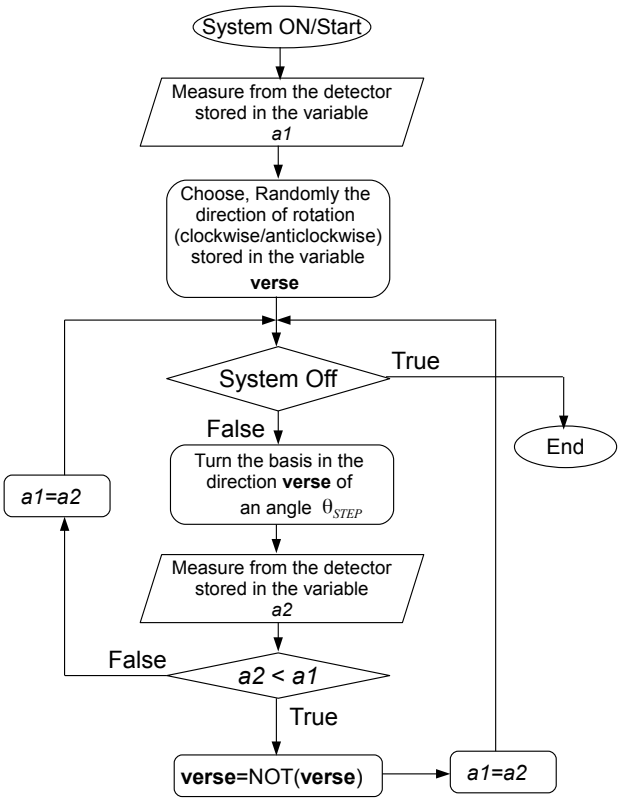

Figure 2. The flowchart shows the algorithm used to find the direction of the vertical polarization.

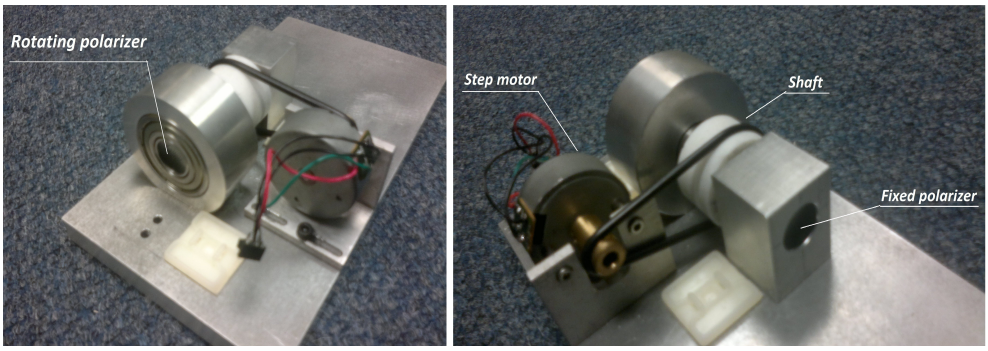

Figure 3. The experimental setup moves the rotating polarizer mounted on the shaft. The laser is incident on the fixed polarizer to create a reference signal. The signal is acquired from the detector fixed to the rotating polarizer. The micro-controller acquires from the detector the signal, and rotates the shaft until the polarizers are aligned.

3. Polarization alignment system using a polarizer beam splitter

The previous system is able to work when Alice and Bob are located at two fixed points. A recent patented system uses a polarising beam splitter as shown in figure 5 and is able to work in non-stationary conditions [7]. If the polarization of the beam is not aligned with the basis of Alice, the detector 1 receives a power $I_1(\theta) = I_0' \cos^2\theta$, where θ is the angle of misalignment. The detector 2 receives a power $I_2(\theta) = I_0' \sin^2\theta$. Theoretically we obtain the following curve in

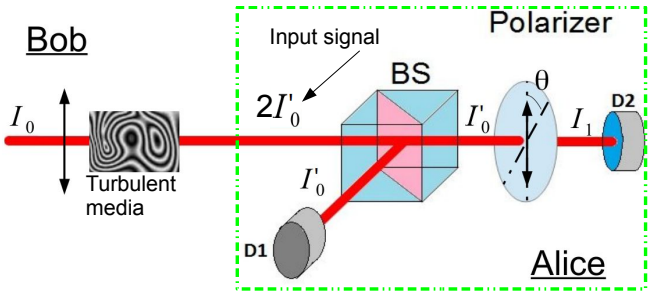

Figure 4. The beam is split at the beam splitter (BS), the value of I_0 can be determined from the value measured in detector D1. The angle can be calculated by the equation $\theta = \arccos\sqrt{\frac{I_1}{I'_0}}$.

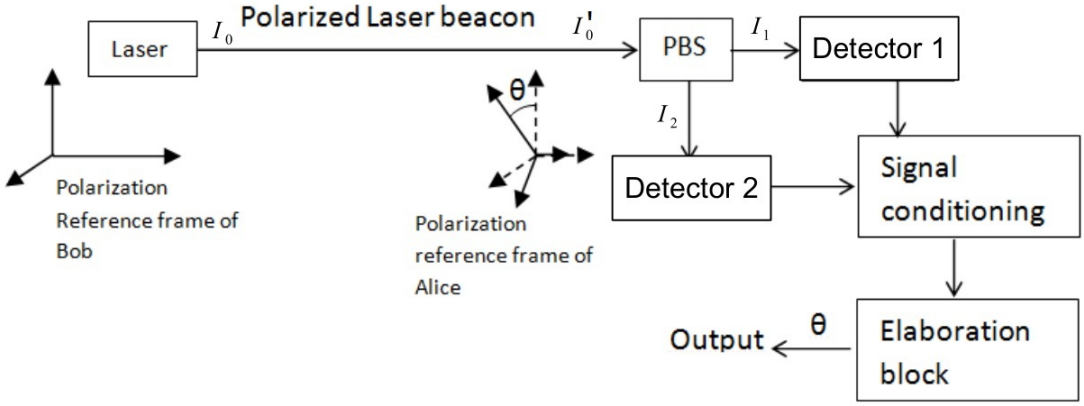

Figure 5. Patent pending application no. 2014/03405

function of the angle θ.

In order to align the system, the laser beacon is sent with a polarization of 45 degrees with respect to the vertical polarization. Alice receives the laser beacon and by the measurement of I_1 and I_2 is able to know the angle. The system is aligned when $I_1 = I_2$. It is possible to

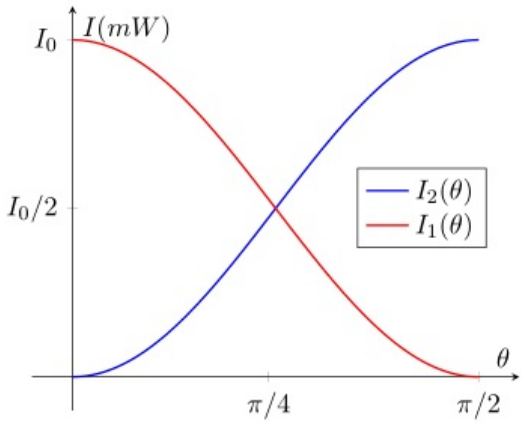

Figure 6. I_1 and I_2 from figure 5. The measurements of both channels make it possible to calculate the angle θ.

calculate the angle without ambiguity. Comparing the signals it is possible to know in which direction the systems should be rotated. This systems can work using a programmable logic unit or using the analog controls.

4. Conclusion

In this work a polarizer tracking system for quantum key distribution was proposed. The system proposed in the second section can be used when Alice and Bob are located at stationary points. This first system requires more effort with respect to the system proposed in the third section, because it continuously rotates the polarization basis around the exact alignment position. The system proposed in the third section works when Alice and Bob are located at stationary or non-stationary points. This is because this system calculates the "instantaneously" angle θ and the direction of rotation. The first system proposed was tested using a programmable logic unit (Atmega328P programmed by Arduino software). The third proposed system was tested with the micro-controller and with an analog electronic circuit. It was experimentally observed that the alignment system developed is relatively accurate for the purpose of free space QKD.

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] Bonavoglia P 2014 Il cifrario rsa URL `http://www.crittologia.eu/critto/rsa/rsa.html`
[2] Shor P W 1997 *SIAM journal on computing* **26** 1484–1509
[3] Bennett C H, Brassard G *et al.* 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (New York)
[4] Mariola M, Abdul M and Francesco P 2011 vol ISBN:978-1-86888688-3 pp.403-408 (South African Institute of Physics)
[5] Mariola M, Abdul M and Francesco P 2012 (South African Institute of Physics)
[6] Fante R L 1979 *Proceedings of IEEE* vol 63 pp 1669–1692
[7] Mariola M, Mirza A and Petruccione F 2014 System and method for determining angles between apparatuses, devices or systems