Contemporary Engineering Sciences, Vol. 4, 2011, no. 8, 363 - 370

Statistical Analysis of Common Qubits between Alice and Bob in BB84 Protocol

B. Ouchao[1] and E. H. El Kinani[2]

[1] Informatics Department, Moulay Ismaïl University
Faculty of Sciences and Technics
Box 509 Errachidia, Morocco

[2] G.A.A, Mathematical Department, Moulay Ismaïl University
Faculty of Sciences and Technics
Box 509 Errachidia, Morocco
elkinani_67@yahoo.com

Abstract

In this paper a statistical analysis of common qubits(photon) transmitted by Alice and received by Bob in the same basis using BB84 protocol with and without the presence of eavesdroppers are studied. The simulation used here is based on java language for transmission of the polarized photon between Alice and Bob via quantum channel (BB84 Protocol coding in Java).

Keywords: BB84 protocol; qubits; quantum cryptography, simulation

1 Introduction

Nowadays, sine the emergence of the e-commerce including electronic funds transfer, Internet marketing, electronics data interchange(EDI), the secure communication becomes a big task in wired and wireless networks. The communication between both user and system administrator using the public channel to exchange data are enough to the intruders who wish to get the information about the exchanging data. The genius of quantum cryptography is that is solves the problem of key distribution.

Quantum key distribution (QKD)[1] is a technique explanting the fundamental laws of quantum mechanics to obtains secret key with provable security. Hence, quantum cryptography is different from the classical cryptographic system in that it relies more in physics, rather than in mathematics. The fundamental of quantum cryptography lies on the foundations on the quantum

mechanics precisely the Heinsenberg uncertainty principle and non-cloning theorem. Actually, there are many QKD protocol which have been developing such BB84 protocol [2], B 92 protocol [3], EPR protocol [4] and others,...

The most widely used one today is BB84 protocol, which is the first (QKD) protocol, invented by Charles Bennet and Gilles Brassard. In this work, a statistical analysis of common qubits(photon) transmitted by Alice and received by Bob in the same basis in BB84 protocol is studied. We first examine the case without the presence of an eavesdropper, Eve (without attack). Then, we will analyze the case with the presence of an (and two) eavesdroppers, Eves. The simulation used here is based on BB84 Protocol coding in Java language for quantum transmission of the polarize photons between Alice and Bob [7].

2 Description of BB84 Protocol

In this section we have recalled the description the BB84 protocol for more details see e.g [2, 5, 6]. Then, BB84 quantum coding scheme was the first proposed quantum encoding introduced and elaborated by Charles Bennett and Gilles Brassard in 1984. Hence, the protocol is called BB84, and it uses the four-orthogonal polarization sate of the photon ($0°, 45°, 90°$ and $135°(-45°)$) that will polarize each photon that will be transmitted. Alice and Bob have to communicate with two channels, quantum channel (quantum transmission for example optic fiber) and public channel (classical channel for example phone or internet) to share a secret key. The BB84 can be described as follows :

(i) Fist step (via quantum channel).

1- Alice will be send N quantum objects such as polarize photons which are measured as a random sting of bits 0 or 1 to Bob using quantum channel (if Bob chooses the same basis as Alice he can for sure identify the polarization of the photon).

2- After all the photons are transmitted, for each photon (bits) Bob randomly chooses rectilinear or diagonal bases to measure it. Bob makes measurements on received photons, by randomly choosing a basis on his known (with equal probability for each bit). Hence, Bob may choose a different basis than the one in which Alice originally encoded it. These incorrect measurements are taken care of in the next stage of the protocol.

(ii) Second step (via Public channel).

The purpose of this stage is to identify and eliminate those qubit positions where Alice and Bob used different bases.

1- They both will establish a communication via a public channel and Bob tells Alice which basis he used for each position (note that no information about the actual values of qubit is exchanged) .

2- Alice transmits back which measurements are done in compatible bases.

3- Alice and Bob throw away photons measured in compatible bases, decoding remaining photons to 0 and 1 that makes the raw key.

3 Case 1. Statistical analysis without the presence of an eavesdropper, Eve

In this section, we present simulation results of the common qubits (photon) transmitted by Alice and received by Bob in the same basis without the presence of an eavesdropper as we have mentioned before. Our simulation is based on the java language for transmission of the polarize photons (qubit) between Alice and Bob. In this simulation, we suppose that the rate of measurements is perfect. This means that all transmitted photon by Alice will be intercepted by Bob. We have considered a random sting of bits 0 or 1 on the interval [10-100], which are transmitted by Alice and received by Bob using quantum channel. In the absence of Eve we remark that the number of qubits received by Bob in the same basis represents approximately half of those sent by Alice as it is illustrated in the figure 3.

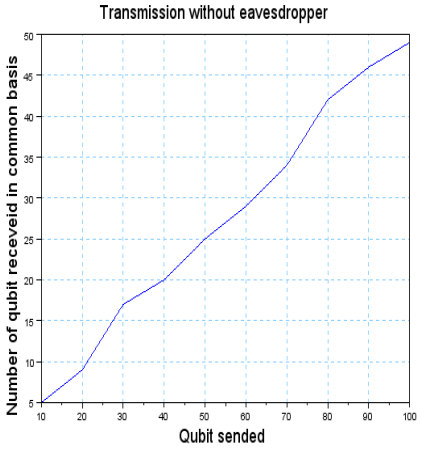

Figure 1: Illustrates the simulation results without the presence of eavesdropper

4 Case 2. Statistical analysis with the presence of the eavesdroppers

Here we present our simulation results of the common qubits (photon) transmitted by Alice and received by Bob in the same basis with the presence of an eavesdropper. As it is illustrated in figure 2, the number of the qubits received by Bob and Eve are comparable in the zone [0-50], whereas in the zone [50-80] the number of the qubits received by Bob than Alice is largely higher than those received by Eve. In the interval [80-90] the opposite phenomenon is produced, especially that the number of the received qubits by Eve is higher than those received by Bob. Henceforth, the zone where the number of qubits transmitted is between 50 qubits and 80 qubits is more protected. Then this simulation lets us to conclude that the number of sending qubits play a major role in the security of transmission.

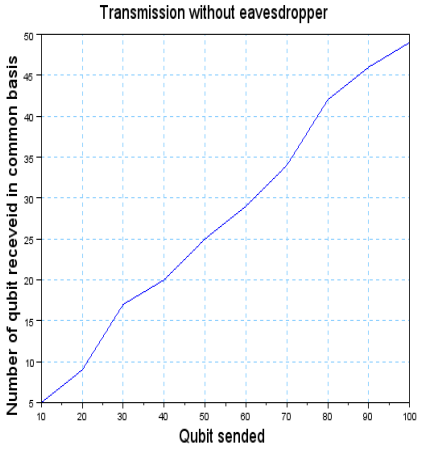

Figure 2: Simulation results with the presence of an eavesdropper

After the transmission with the classic channel, Alice and Bob compare the obtained results on one range of transmitted and received qubits on the common basis and calculate the estimated error rate (*Err.*) which is given by

$$Err. = 1 - \frac{\text{number of qubits common}}{\text{number of qubits exachanged}},$$

then if the $(Err.) \leq 0.2$, Alice and Bob may transmitted their information with securities in spite of the presence of Eve, because the number of common qubits between Alice and Bob is widely higher than those exchanged between Alice and Eve. In the case where $(Err.) > 0.2$ the transmission is not secured because of the presence of Eve as illustrated in figure.3

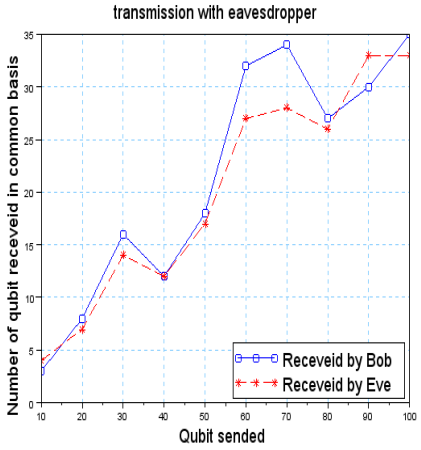

Figure 3: Estimated error rate with the presence of eavesdropper

After taking into account that the estimated error rate and the eliminating of the measures with estimated error rate is higher than 0.2, the simulation show that the number of the common qubits between Alice and Bob is higher than those exchanged between Alice and Eve as illustrated in figure 4.

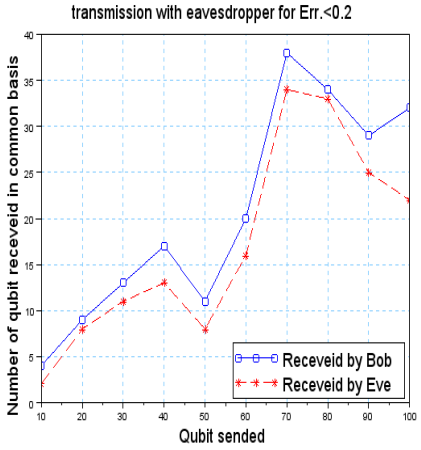

Figure 4: Simulation results with the presence of an eavesdropper taking into account estimated error rate

In the case of the presence of second eavesdropper the simulation obtained results is illustrated in figure 5. As presented on the figures the presence of the second eavesdropper reduce the number of common qubits received by Bob.

And the number of common qubits received by Eve 1 is higher than those received by Bob. This tendency is awaited for and understood because of the presence of second eavesdropper. The common qubits received Eve 1 lower than those received by Eve 2. Hence, this simulation lets us conclude that the presence of the second eavesdropper makes the transmission between Alice and Bob unsecured.

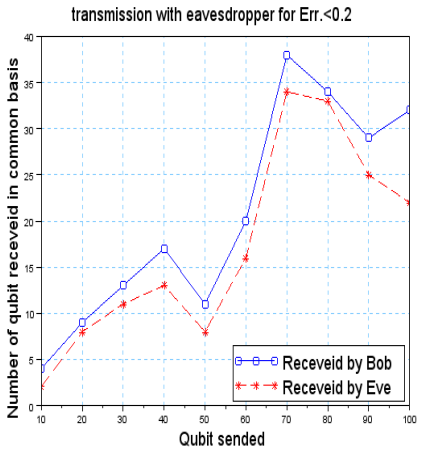

Figure 5: Simulation results with the presence of two eavesdroppers

5 Conclusion

In this paper we have studied a statistical analyze of common qubits(photon) transmitted by Alice and received by Bob in the same basis using BB84 protocol with and without the presence of eavesdroppers. In this analysis, we have assumed that the rate of measurements is perfect. thai is to say that all sent photons by Alice will be intercepted by Bob. The simulation used in this paper is based on java language for transmission of the polarized photon between Alice and Bob via quantum channel. We have seen that the introduction of the one eavesdropper reduce the number of common qubits and the transmission is only secured in the zone when the estimated error rate is lower than 0.2. While the presence of two eavesdroppers makes the transmission unsecured.

References

[1] Ch.H. Bennett, G. Brassard and A. Ekert, Quantum cryptography, Scientific Am. 267,pp. 26-33, 1992 (int. ed.).

[2] Ch.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossinh. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, IEEE, New York, pp. 175-179, 1984.

[3] C.H. Bennett, Quantum cryptography using any two nonorthogonal states, Physical Rewiew Letters, Vol.68, No.21, pp.3121-3124, 1992.

[4] Ekert, Artur K., Quantum cryptography based on Bell's theorem, Physical Rewiew Letters, Vol.67, No.6, pp.3121-3124, 1991.

[5] Bennett, Ch.H. and G. Brassard, Quantum public key distribution system, IBM Technical Disclosure Bulletin, 28, pp.3153-3163, 1985.

[6] Bennett, Ch.H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental Quantum Cryptography, J. Cryptology 5,pp. 3-28, 1992.

[7] Andrew G D Rowley, "The BB84 Protocol", in QCrypt - A Quantum Cryptography Simulation. http://www.dcs.st-and.ac.uk, June 2001.

Received: August, 2011