A Privacy Enhancement Algorithm Against Photon Number Splitting Attack for BB84 Protocol

Phichai Youplao[1, a]

[1]Electrical Engineering Department, Faculty of Industry and Technology, Rajamangala University of Technology Isan Sakon Nakhon Campus, 199 Village No. 3, Phungkon, Sakon Nakhon, Thailand

[a]<phichai3112@yahoo.com>

Keywords: QKD, BB84 protocol, PNS attack, quantum computer, information security.

Abstract. This paper demonstrates the novel adaptation algorithm together with the BB84 protocol aim to against the photon number splitting attack in quantum key distribution (QKD) protocol. The proposed protocol be able to restrict the ability that eavesdropper, referred to Eve, can choose the basis correctly for photon polarization measurement. Hence, the privacy of communicating between two parties, referred to Alice and Bob, can be increased. By performing QKD as the proposed protocol with specified parameter as k = 1024 bits, correspond to y = 10 bits, and n = 10 rounds repeating, the probability that eavesdropper be able to accomplish the shared secret key remains as only 3.94×10^{-31}.

1. Introduction

Nowadays, communications play an important role in our daily lives that they provide us an easy and fast way to communicate securely with the others, anywhere, anytime. Especially, an optical communication is expected to be a promising platform for modern communication systems due to it can meet the demand for data capacity, speed, and also offers a good property for security. However, due to the performance increasing of a modern computer, besides an establishment of a powerful quantum computer in the near future, the confidential information encrypted by present methods may not be secure anymore [1, 2]. Hence, the quantum key distribution (QKD), which has an ability to secure the information perfectly against any unauthorized access from the eavesdropper, is proposed and received intensive attention. This secure key distribution scheme between two parties, referred to Alice and Bob, could be a solution for information security technology in the future.

Charles Bennett and Gilles Brassard published the first protocol for quantum key distribution in 1984 (called BB84) [3], of which the concept based on the Heisenberg's uncertainty principle. It is still one of the most prominent protocols. The basic idea is that Alice can send Bob a random secret key of which the bits are encoded by photon polarizations. Eavesdropper, called Eve, cannot measure these photons and resend them to Bob without disturbing its polarization state, guaranteed by the Heisenberg's uncertainty principle, and thus will reveal her presence.

Although exchanging a secret key between the two parties can be secured by dint of the principle of QKD. However, there is a point at issue that the protocol is still susceptible to a new attack is known as the photon number splitting (PNS) attack [4, 5]. In PNS, Eve splits off a few number of photons (or a single photon) from each key bit transmission so that she can measure her photons without disturbing the rest photons that she allows it pass to Bob. It is impossible that Alice and Bob can detect the unauthorized access in this attacking strategy.

In this paper, it will focus on the additional workflow steps collaborating with the BB84 protocol to restrict the ability that the eavesdropper is able to recognize the key bit positions for photon measurements. This proposed method can enhance the privacy and security of the QKD protocol, which is the most important and essential properties of modern communication systems.

2. The Proposed Algorithm

The main structure of the QKD protocol is still based on the BB84. However, during the sifting raw key process, the additional workflow steps are set for rearranging the sending bit positions, aim to against the PNS attack. The algorithm to perform the bit rearrangement is as follows:

[S1] Starting from both Alice and Bob must have a shared secret key string of x bits. They form a new bits string, called reference key; RFK, by picked up the first y bits < x bits from the shared secret key, where 2^y = k bits (a Raw key of k bits). For example, if k = 1024 bits, the RFK will be a string of y = 10 bits. Then go to the next step.

[S2] Before starting the sifting raw key process, both Alice and Bob transforms each their time slot number into a binary string as y bits, called original position key; OPK, which is used to refer to as a position of each sending bit. For example as y = 10 bits, the time slot '1' is transformed to be '0000000001', the time slot '582' is transformed to be '1001000110', etc. Alice and Bob recording all the OPK and going to the next step.

[S3] Alice and Bob form a new one of bits string, called new position key; NPK, by performing XOR between the RFK and each OPK. Then, each NPK is defined to be a newly rearranged position for each the sending bit. For example, the RFK '0010100111' XOR with the OPK '1001000110' will get the NPK '1011100001', which corresponds to the sending bits at the position of '582' is relocated at the new position of '737'.
Whereas, if the XOR resulting as only "0" for the NPK, it will be defined as relocating a bit at this OPK position to the new at 'k' position.
In order to restrict the ability that the eavesdropper is able to recognize the key bit positions for photon measurements, they start all over again several times with the new both RFK and OPK. As n rounds repeating, the new RFK of each round is referred to the next adjacent bits string ranges from $(n\text{-}1)y\text{+}1$ to ny of the shared secret key in S1. For the new OPK, it is defined by the NPK obtained from the previous round. Complete the n rounds repeating then go to the next step.

[S4] Finally, they both get the last secret NPK that referred to the position of each sending bit.

[S5] Ending the process.

3. Typical System for QKD Protocol

Figure 3 shows a typical system for the proposed polarization coding QKD protocol [6]. In operation, laser diodes, LD1 – LD4, are employed as a photon source for each polarization state as 0°, 90°, 45°, or 135°. The polarized photon pulse is propagated through the beam splitter, BS, and direction to a photon density filter, F, for photon number attenuation. This photon number must be restricted to a few as much as possible (a single photon is desired) so that it will be difficult for the eavesdropper to split any excess photons from the light pulse. Then, Alice sends Bob the polarized photon pulse via the quantum channel such as a fiber optic link.

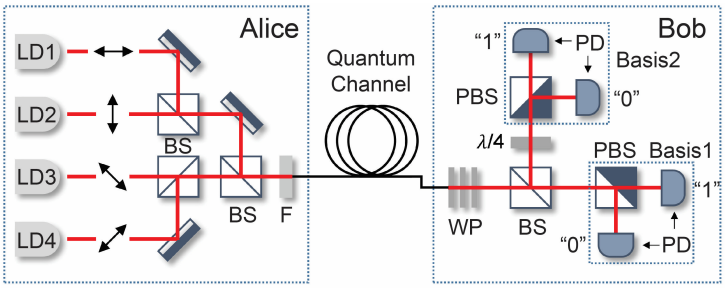

Fig. 3. Typical system for polarization coding quantum cryptography.

As the polarized angle of a photon pulse that arrived at Bob, the single end of the fiber link, might be deviated due to polarization mode dispersion, the arrived photon pulse will be compensated using a wave plate, WP. After which, the photon pulse is split by a beam splitter and propagates through the polarizing beam splitter, PBS. Finally, the photon pulse incidents on a photodiode, PD, each represented the bit value either "0" or "1".

4. Discussions

As the performing of bit position rearrangement is starting from both Alice and Bob must have a shared secret key, required for assigning the RFK, therefore, in the first phase, the QKD must be performed by the original BB84 protocol with a photon number of $\mu \leq 1$ to achieve the first RFK string. Thereafter, the first shared secret key obtained by the BB84 is used to setup the new RFK for performing the next round of key distribution using the proposed protocol.

For the PNS attack, Eve has no choice, she just only choosing the basis randomly to measure her photons, which has a correct probability of 50%. Furthermore, she has no idea about each the sending bit position, she randomly rearranges her bit position with a correct probability of $1/(2^y)^n$. So, if specifying the parameter as k = 1024 bits, correspond to y = 10 bits and n = 10 rounds repeating, the probability that Eve be able to accomplish the correct information is remaining as only $[1/2]\times[1/(2^{10\times10})] = 3.94\times10^{-31}$.

5. Conclusion

This paper proposes the additional algorithm that can be performed together with the BB84 quantum key distribution protocol aim to increase the privacy of the key distribution. The primary concept is to restrict the opportunity that eavesdropper can be identifying the sending bit position correctly for her photon measurements in the case of photon number splitting attack. By using the proposed protocol, with the specified parameter of k = 1024 bits, y = 10 bits and n = 10 rounds, the probability of eavesdropper be able to obtain the shared secret key is remain as only 3.94×10^{-31}. This proposed strategy can be useful to enhance the privacy of the QKD protocol, which is an essential property of communications.

References

[1] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", ***SIAM Journal of Computing***, Vol. 26, pp. 1484-1509, 1997.

[2] D. Bruss, G. Erdelyti, T. Meyer, T. Riege and J. Rothe, "Quantum Cryptography: A Survey" ***ACM Computing Surveys***, Vol. 39(2), Article 6, pp. 1-27, 2007.

[3] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", ***International Conference on Computers, Systems & Signal Processing,*** (Bangalore, India,) December 1984.

[4] G. Brassard, N. Lutkenhaus, T. Mor and B. Sanders, "Security against individual attacks for realistic quantum key distribution", ***Physical Review A,*** Vol. 61, pp. 052304(1)-052304(10), 2000.

[5] G. Brassard, N. Lutkenhaus, T. Mor and B. C. Sanders, "Limitations on Practical Quantum Cryptography", ***Physical Review Letters,*** Vol. 85(6), pp. 1330-1333, 2000.

[6] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography", ***Reviews of Modern Physics,*** Vol. 74, pp. 146-195, 2002.