Proceedings of International Conference
on Mechanical, Electrical and Medical Intelligent System 2017

A Simulation of Quantum Key Distribution Protocol with Enhancing Ability to Against PNS Attack

Phichai Youplao[1, a] and Sukhum Julajaturasiraratn[1,b]

[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]<phichai.yo@rmuti.ac.th>, [b]<sukhum.ju@rmuti.ac.th>

Keywords: quantum cryptography, QKD protocol, PNS attack, information security.

Abstract. This paper presents a modified quantum key distribution (QKD) protocol with an enhancing ability to restrict the probability that eavesdropper can recognize key bits information for her photon number splitting (PNS) strategy. The simulation results are demonstrated by the relationship between the secret key rates as a function of the transmission distance between the two parties. The system parameters are specified by; the pulse rate of 1 GHz, the photon number of $\mu = 1$, the attenuations of 2, 0.35, and 0.25 dB/km, the detector efficiencies of 50%, 20%, and 10%, and the dark count probabilities of 10^{-7}, 10^{-5}, and 10^{-5}, for the light pulses of 800, 1300, and 1550 nm, respectively. From the simulation results, the secret key rate in each wavelength of approximately 24.2, 111.8, and 46.6 kbit/s can be achieved for the distances of 20, 80, and 100 km, respectively.

1. Introduction

At present, optical communication systems have been found widespread adoption in many kinds of applications since it is one of the most important platforms to meet requirements of large bandwidth and offers a good security. Generally, a secure conversation between two parties should be private, means only two of them be able to understand, thus, firstly they must have a secure method to share their secret information. Although exchanging information can be secured by encryption algorithms [1, 2], however, if the advent of a powerful quantum computer can be realized, the information that was encoded by traditional methods may not be secured anymore.

Quantum key distribution is a physically secure method for distributing a secret key between two parties, traditionally named Alice and Bob. The first QKD protocol was published in 1984 by Charles Bennett and Gilles Brassard (called BB84) [3]. In this protocol, Alice and Bob wish to agree on a secret key that no eavesdropper can obtain any significant information. The basic idea is that Alice sends Bob each bit of a random secret key which was encoded by a quantum state of a photon that eavesdropper, called Eve, does not know. She cannot get information on the key without introducing errors in the correlations between Alice and Bob, according to the principle of Heisenberg's uncertainty. Thus, she will reveal her presence to Alice and Bob, and then they will terminate the communication. However, in technical, security of this protocol can be compromised by a new attack strategy known as photon number splitting (PNS) attack, by which Eve can get all the information [4-6]. Hence, to prevent the PNS attack, each photon pulse is expected to contain only a single photon so that Eve is impossible to split off any photon for her PNS strategy. Nevertheless, in practice, photon sources are not always perfectly emit a single photon, and as a result, most of the photon pulses are empty thus results in a low bit rate.

In this paper, the modified protocol with some additional workflow steps, which are well described by [7], aims to improve the privacy of QKD protocol besides enhancing its secret key rate is proposed. The implementation system of such the proposed protocol and its advantage properties are performed and discussed.

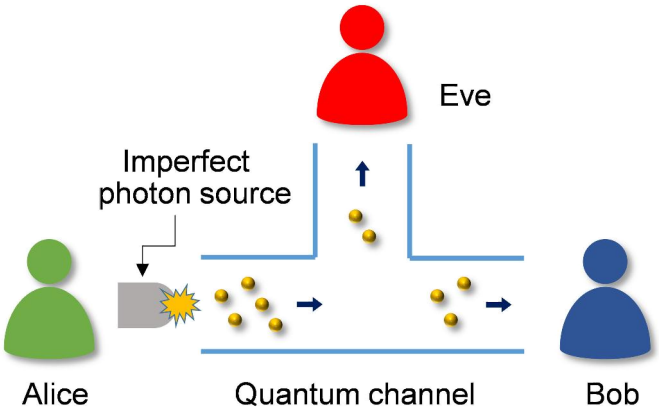

Fig. 1. Diagram of Photon Number Splitting attack: PNS attack.

2. The Proposed Protocol

The main structure of the proposed protocol still based on the BB84. However, some additional workflow steps during the sifting raw key process are established aim to against the PNS attack. The work procedure of the modified protocol is as follows:

[S1] Alice makes a bit encryption by randomly selecting one of the polarization angles of 0°, 90°, 45°, or 135°, to encode a photon pulse (containing with single photon or a few of photons) at the considered time slot i (i = 1, 2,..., k). Alice sends this encrypted photon pulse to Bob via a quantum channel.
If a third party, Eve, tries to eavesdrop, she must be the one who has an ability to 'read' the information in the quantum channel. Eve may access the bits information by using two kinds of the main strategy, intercept/resend or photon number splitting.

[S2] Whereupon, Alice concurrently records the information of her choices in S1, which are the encoded basis (either rectilinear basis; [0°, 90°] or diagonal basis; [45°, 135°]), the polarization angle, the bit value "0" or "1", and the time slot number i. Then go to next step.

[S3] Bob randomly chooses his used basis either rectilinear basis or diagonal basis to measure the photon pulse that he received during the considered time slot i. He thereupon records the information of his measurement, his chosen one basis, the interpreted bit string ("0" or "1"), and the time slot number i. This information will be used later for discussing with Alice, then go to next step.

[S4] Checking the size of transmission key bits (the time slot number i). If 'i' is less than the specified k bits, then going to repeat on S1 with the next time slot 'i+1'. In contrast, if it reaches to the specified k bits, then going to the next step.

[S5] Starting the sifting raw key process. Without sorting by the time slot number from I to k, but with the sorting form, which is a form of all the different k! forms that only both Alice and Bob were approved, detailed as in [7]. Alice and Bob make a discussion for their basis choice and some measured information by announcing in a public channel. Alice reads Bob's measurement and confirms to him the position that he made compatible choices of bases used (Sifted key). Afterward, they randomly picked up a key string of m bits from the Sifted key (m bits < Sifted key) and going to the next step.

[S6] Alice and Bob estimate errors to detect an eavesdropper. They compare their m bits string to calculate its bit error rate (e_r). If the bit error rate is higher than a maximum bit error rate ($e_r > e_{r,max} = 16\%$ [8]), they will suspend the communication and restart all over again. If not, going to the next step.

[S7] Now, both Alice and Bob will have a shared key, called raw key. This key is not a final shared secret key since Alice and Bob's version might have some different bits. They eliminate the *m* bits from the raw key and then go to the next step.

[S8] Correcting errors in the rest key bits and improving its privacy by minimizing the number of bits that the eavesdropper may know, both Alice and Bob perform the error correction and privacy amplification process to their raw key [9].

[S9] Finally, they both will get the same string of bits, which is the shared secret key.

[S10] Ending the process.

3. QKD System based on Polarization Encoding

The polarization coding QKD protocol typically employs a system as shown in figure 3 to operate the keys distribution. The system consists of laser diodes, LD1 - LD4, each employed as a photon pulse source for each polarization state of 0°, 90°, 135°, and 45°, respectively. The polarized photon pulse propagates along its route through the beam splitters, BS, and will be finally attenuated by a photon density filter, F, for restricting the number of photons in each photon pulse to be a few as possible. Thereafter, Alice sends each the polarized photon pulse to Bob via a quantum channel such as a fiber optic link.

Indeed, to prevent the PNS attack, each photon pulse is expected to consist of one photon so that the eavesdropper cannot split off the photon pulse without revealing her presence. However, it is difficult to construct an on-demand light source which can perfectly emit a light pulse that contains only a single photon [10-12]. Therefore, the photon number, μ, the probability that a light pulse has photons (or a single photon) is usually small, that means most of the pulses are empty and consequently obtain a low corrected secret bits rate (number of remaining bits). In contrast, due to the probability that eavesdropper can recognize the key bit positions for her photon measurements has been restricted by using the proposed protocol, each the photon pulse will be allowed to contain with few photons so that the photon number can be raised to $\mu = 1$. Thus, it can be possible to achieve a higher useful bit rate.

As the polarization of the photon pulses that arrived at Bob might be deviated by random imperfections and asymmetries in the fiber optic link, then a wave plate, WP, is employed to compensate the polarized angle of each the arrived pulse. After which, the pulse has been split by a beam splitter, and then each one propagates along its route through a polarizing beam splitter, PBS, each at the rectilinear and diagonal basis part, respectively. Finally, the photon pulse incidents on a photodiode, PD, each represents the bit value either "0" or "1".

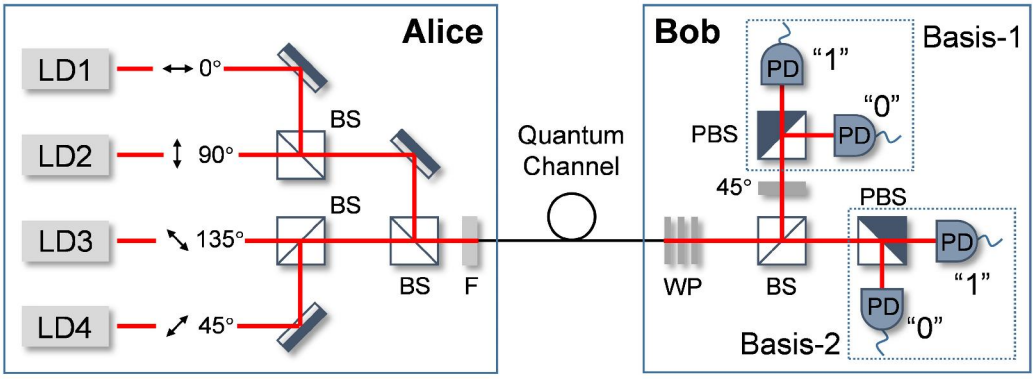

Fig. 2. A typical system for BB84 QKD system based on polarization encoding, where LD is a laser diode, BS is a beam splitter, F is light pulse filter, WP is wave plate, PBS is a polarizing beam splitter, and PD is photon detector.

4. Simulation Results

In practice, the exchanged key rate that transmitted through between the two parties, referred to Alice and Bob, depends on the limitations due to imperfect tools and equipment used. However, in principle, the useful bit rate, R_{net}, can be calculated as the sifted key rate, R_{sift}, multiplied by the difference between the probability of Bob's Shannon information, p_{Bob}, and the probability of Eve's maximal Shannon information, $p_{Eve(max)}$, which can be expressed as:

$$R_{net} = R_{sift}[p_{Bob} - p_{Eve(max)}] \tag{1}$$

The sifted key rate, R_{sift}, corresponds to the event that Alice and Bob made compatible choices of bases used for encoding and measuring the photon pulse. Hence, the sifted rate is a half of the raw key rate, R_{raw}, which is the product of the emitted light pulse rate, f_{pulse}, the photon number, μ, the detection efficiency of the detector, η, and the probability of a photon pulse arrives at Bob's analyzer (a function of the quantum channel attenuation), p_{link}, which can be expressed as:

$$R_{sift} = \frac{1}{2}R_{raw} = \frac{1}{2}f_{pulse}\mu\eta p_{link} \tag{2}$$

The probabilities of Bob's Shannon information and Eve's maximal Shannon information are expressed as p_{Bob}= 1 - $h(e)$, and $p_{Eve(max)} \cong 2.9e$, respectively, where e is the quantum bit error rate ($QBER$) of the QKD system [8], and $h(e) = -elog_2(e)-(1-e)log_2(1-e)$ [13].

The quantum bit error rate is defined as a ratio of the wrong bits, which are usually a few, to all the received bits, can be expressed as:

$$QBER = \frac{Number\ of\ wrong\ bits}{(Number\ of\ right\ bits)+(Number\ of\ wrong\ bits)} = \frac{R_{error}}{R_{sift}+R_{error}} \approx \frac{R_{error}}{R_{sift}} \tag{3}$$

The wrong bits error rate, R_{error}, can be considered separately as three different contributions. The first is due to the probability that a photon pulse propagates to a wrong detector since its polarization deviated, p_{opt}. This error rate, R_{opt}, is given by the sifted key rate multiplied by p_{opt}. However, typically in polarization-based systems, the probability p_{opt} is approximately of 1%, which can be neglected. The second bits error rate, R_{det}, is due to the detector's dark counts, given by the product of f_{pulse}, the probability of registering a dark count during a considered time window, p_{dark}, number of detectors, n, and the two constant values of 1/2. Which are related to the 50% probability that the dark count happens when Alice and Bob made incompatible choices of bases and 50% probability that the photon incidents on the correct detector. The third bits error rate, R_{acc}, is due to uncorrelated photons from imperfect photon sources, which appears only in systems based on entangled photons and can be paid no attention to this polarization-based system. Then, the $QBER$ can be expressed as:

$$QBER \cong QBER_{det} = \frac{R_{det}}{R_{sift}} = \frac{np_{dark}}{2\mu\eta p_{link}} \tag{4}$$

Figure 3 shows the relationship between the useful bit rate, R_{net}, which can be transmitted through between Alice and Bob, as a function of the transmission distance. The results are obtained by equation (1) to (4). The system parameters are specified as follows: the light pulse rate of 1 GHz, the photon number of $\mu = 1$, the optical link attenuations of 2, 0.35, and 0.25 dB/km, the detector efficiencies of 50%, 20%, and 10%, the dark count probabilities of 10^{-7}, 10^{-5}, and 10^{-5}, for the light pulses of 800, 1300, and 1550 nm, respectively.

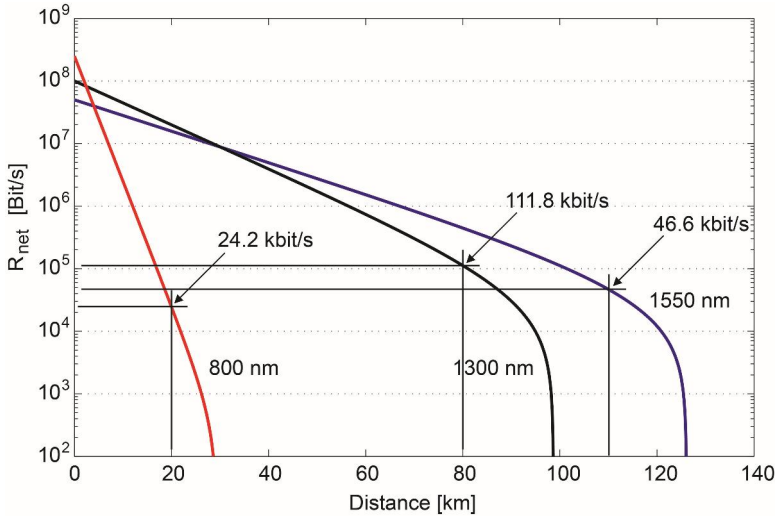

Fig. 3. Simulation results of the useful bit rates as a function of the transmission distance.

5. Conclusion

This paper proposes the modified quantum key distribution protocol with the enhancing ability to against PNS attack, by restricting the probability that eavesdropper can recognize the key bit positions for her photon measurements. In contrast with the traditional method that most of the photon pulses are empty and result in the low secret key rate. The advantage of such the proposed protocol is that it allows the photon source to emit a light pulse with a few containing photons so that the photon number can rise to $\mu = 1$, which cause possible to obtain the higher secret key rate. As a result, the proposed protocol is valuable for improving the privacy of QKD protocol besides enhancing its secret key rate. These properties are essential for modern optical communication systems.

References

[1] J. Cai, X. Shen and M. Lei, "Optical asymmetric cryptography based on amplitude reconstruction of elliptically polarized light", ***Optics Communications***, Vol. 403, pp. 211-216, 2017.

[2] K. Hariss, H. Noura and A.E. Samhat, "Fully Enhanced Homomorphic Encryption algorithm of MORE approach for real world applications", ***Journal of Information Security and Applications***, Vol. 34, No. 2, pp. 233-242, 2017.

[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] A.Niederberger, V. Scarani and N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography", ***Physical Review A***, Vol. 71, No. 4, pp. 052304(1)-052304(10), 2000.

[7] P. Youplao, "A Privacy Enhancement Algorithm Against Photon Number Splitting Attack for BB84 Protocol" ***Proc. ICTSS 2017*** (Kiryu, Japan) May 2017.

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

[9] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and John Smolin, "Experimental Quantum Cryptography", ***Journal of Cryptology***, Vol. 5, No. 3, pp. 1-28, 1992.

[10] S. Yu, Y.T. Wang, J.S. Tang, Y. Yu, G.W. Zha, H.Q. Ni, Z.C. Niu, Y.J. Han, C.F. Li and G.C. Guo, "Tunable-correlation phenomenon of single photons emitted from a self-assembled quantum dot", ***Physica E***, Vol. 86, pp. 042316, 2005.

[11] H. Kobayashi, H. Kumano, M. Endo, M. Jo, I. Suemune, H. Sasakura, S. Adachi and S. Muto, "Highly circular-polarized single photon generation from a single quantum dot at zero magnetic field", ***Microelectronics Journal***, Vol. 39, No. 3-4, pp. 327-330, 2008.

[12] M. Bertolotti, F. Bovino and C. Sibilia, "Chapter One - Quantum State Engineering: Generation of Single and Pairs of Photons", ***Progress in Optics***, Vol. 60, pp. 1-117, 2015.

[13] C.E. Shannon, "A Mathematical Theory of Communication", ***Bell System Technical Journal***, Vol. 27, No. 4, pp. 623–666, 1948.