Journal of Technology and Social Science (JTSS)

A Simulation of Multi-Layers Quantum Key Distribution with Enhancing Ability for Against PNS Attacks

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]<phichai.yo@rmuti.ac.th>

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

Abstract. This paper presents the simulation results of a modified quantum key distribution (QKD) protocol with an enhancing ability for against the photon number splitting (PNS) attack. By performing the proposed protocol with specified parameters as k = 1024 bits, correspond to y = 10 bits, and repeating rounds n = 10, the probability that eavesdropper can obtain the shared secret key will remain as only 3.94×10^{-31}. Furthermore, by dint of the enhancing ability to against the PNS strategy, the multi-layers QKD application can be realized and consequently possible to achieve a higher useful bits rate. The performance of key distribution has been demonstrated by the relationship of the useful bits rate as a function of the optical link distance between the two parties, referred to Alice and Bob. The QKD system parameters are specified as the light pulses rate of 1 GHz and 10 GHz and the photon number of $\mu = 1$. The optical link attenuations of 2.0, 0.35, and 0.25 dB/km. The detector efficiencies of 50%, 20%, and 10%, with the dark count probabilities of 10^{-7}, 10^{-5}, and 10^{-5}. Each is for the light pulses of 800, 1300, and 1550 nm, respectively. From the simulation results, the useful bits rate in each optical wavelength of approximately 24.2 kbit/s, 111.8 kbit/s, and 12.1 kbit/s can be achieved for the distances of 20 km, 80 km, and 120 km, respectively. Besides 97.0 kBit/s with 1550 nm at 120 km for 8-layers system. The potential of using such the proposed protocol with a multi-layers QKD system is performed and discussed.

1. Introduction

At present, communications can take place in many forms to get their message across, anywhere, anytime. Provide us a fast and easy way to communicate with the others, which play a vital role in our daily lives, especially optical communication. It has been found widespread adoption in many kinds of systems since it is one of the most promising platforms that can meet the requirements, such as large bandwidth capacity, speed, and offers a good property for information security. In addition, privacy has become increasingly important from a communication perspective. A secure conversation between two parties should be private. This generally means only the two of them should be able to understand the content. Consequently, they must have a secure method to share their secret information. Although exchanging information can be secured by encryption algorithms [1, 2], however, due to the computing performance improvement of a modern supercomputer, and the advent of a powerful quantum computer besides in the near future, the private information that was encrypted by traditional methods may no longer be secure.

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 quantum state using single photon that eavesdropper, called Eve, does not know. She cannot theoretically get information on the photon without introducing errors in the correlation between Alice and Bob according to the principle of Heisenberg's uncertainty. If Eve makes measurements for the quantum states, she will reveal her presence. Thus, Alice and Bob will terminate

the communication. However, security of this protocol can be technically compromised by a new attack strategy, known as photon number splitting (PNS) attack [4-6]. In PNS, as shown in Fig. 1, Eve splits off a few extra photons (or a single photon) from each photons pulse without disturbing the rest and allows it pass to Bob. She can measure her photons afterward and obtain information on the key without introducing errors. It is impossible that Alice and Bob can detect the unauthorized access by this attacking strategy. In fact, 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 photons for her PNS strategy. Nevertheless, in practice, photon sources are not always perfectly emit a single photon pulse and usually attenuated to contain a very small number of photons [7]. Therefore, most of the photon pulses are empty and result in a low useful bits rate.

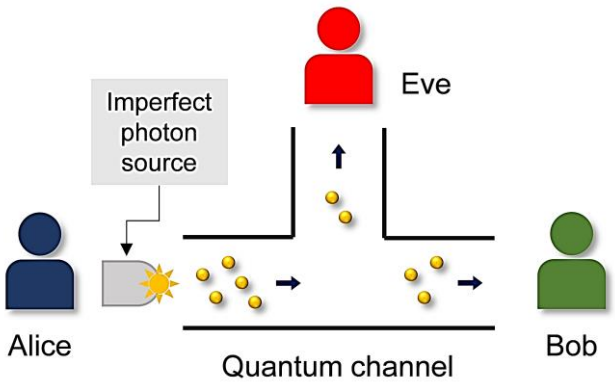


Fig. 1. Photon Number Splitting strategy.

In order to improve the performance of QKD, the author has previously introduced a technical method for privacy enhancement together with BB84 based protocol [8, 9]. Of which the concept is to restrict the probability that Eve can identify compatible choices in basic usage for her PNS strategy. In this paper, the implementation system of such the proposed protocol and its advantage properties for multi-layers QKD system are performed and discussed.

2. The Proposed QKD Protocol

The main structure of the proposed protocol still based on the BB84, except some additional workflow steps for against the PNS attack during the sifting raw key process. The work procedure of the proposed protocol is as follows:

[S1] Alice makes a bit encoding by randomly select one of the polarization angles of 0°, 90°, 45°, or 135°, for a photon pulse (containing a single photon or a few) at the considered time slot i (i = 1, 2,..., k). Alice sends this encrypted photon pulse to Bob via a quantum channel.
If there is a third party, Eve, tries to eavesdrop on the communication, she must have an ability to 'read' the information in the quantum channel.
Eve performs attack on the system to obtain the bits information by using two kinds of the main strategy, intercept/resend and photon number splitting attack.

[S2] Then, Alice concurrently records the information of her choices in S1, which are the encoding basis usage (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 basis choice either rectilinear or diagonal to measure the photon pulse that he received during the considered time slot i. He records his information, the chosen basis, the interpreted bit string ("0" or "1"), and the considered time slot i. This information will be used later for discussion procedure, then go to next step.

[S4] Checking the time slot number i (the size of sending bits). If 'i' is less than a 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 additional workflow steps for rearranging the sending bit positions. The algorithm to perform the bit rearrangement is as follows:

[S5.1] Firstly, 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 picking 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 sub-step.

[S5.2] Both Alice and Bob transform each of their time slot numbers into a binary string of y bits, called original position key (OPK), which refer to an original position of each sending bit. For example, if y = 10 bits, the time slot '1' will be transformed to a binary string of '0000000001', the time slot '658' will be transformed to '1010010010', etc. Alice and Bob record all the OPK and going to the next sub-step.

[S5.3] Alice and Bob then form a new set 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 new rearranged position for each sending bit. For example, the RFK '0010100111' XOR with the OPK '1010010010' will get the NPK '1000110101', corresponds to the sending bit at the original position '658' has been relocated at the new position '565'. If the XOR results in the NPK as all bit is "0", it will assign a bit at this OPK to relocate at the 'k' position (the NPK for this OPK is 'k').

To reduce the probability that Eve can identify the rearranged bit positions, they repeat all from S5.1 several times with both the new RFK and OPK. As n rounds repeating, the new RFK in each round refer to the next adjacent bits string ranges from [n-1]y+1 to ny < x bits of the shared secret key in S5.1. For the new OPK, it will be used the NPK of the previous round instead. Complete n rounds repeating then go to the next sub-step.

[S5.4] Finally, they both will get the last set of secret NPK that refer to the new position of each sending bit.

Then, going to the next step.

[S6] The sifting raw key process. Without sorting by the time slot number (from i to k), but sorting by one of the different 'k!' formats that only both Alice and Bob were randomly approved, detailed as in S5. Alice and Bob make discussions 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 basis usage (Sifted key). Then, they randomly pick up a key string of m bits from the Sifted key (m bits < Sifted key) and going to the next step.

[S7] Alice and Bob inspect some errors to evaluate an eavesdropper. They compare their m bits to calculate bit error rate (e_r). If the bit error rate is higher than a maximum bit error rate ($e_r > e_{r,max} \cong 16\%$ [10]), they will suspend the communication and restart all over again. If not, going to the next step.

[S8] Now both Alice and Bob will have a shared key, called raw key. This key is not a final shared secret key since each of them version might have some different bits. They eliminate the m bits from the raw key and then go to the next step.

[S9] Correcting errors in the rest key bits and improving its privacy by minimizing the number of bits that Eve may know, both Alice and Bob perform the error correction and privacy amplification process to their raw key [11].

[S10] Finally, they both will get the same string of bits, which is the shared secret key.

[S11] Ending the process.

3. Polarization Encoding based QKD System

The polarization coding QKD protocol typically employs a system as shown in Fig. 2 to perform the keys distribution. The system consists of laser diodes, LD1 - LD4, each employed as a photon source for each polarization state of 0°, 90°, 135°, and 45°, respectively. The encoded photon pulse then propagates along its route through the beam splitters (BS) and will be attenuated by a photon density filter (F) to restrict the number of photons as less as possible for each pulse. Then, Alice sends each the encoded photon pulse to Bob via a quantum channel such as a fiber optic link.

Each photon pulse is expected to consist of a single photon indeed so that there are no extra photons for Eve (to prevent the PNS attack) and thus she cannot split off any photons without introducing detectable errors. However, it is difficult to complete an on-demand photon source that can perfectly emit light pulse with a single photon [12-14]. Then, the photon number (μ), the probability that a light pulse has photons (or a single photon), is usually small. Most of the pulses are empty and consequently obtain a low useful bits rate. In contrast, due to the probability that eavesdropper can identify the bit positions for her PNS strategy has been restricted by using the proposed protocol, each the light pulse is allowed to consist of a few photons so that the photon number can rise to $\mu = 1$. Therefore, the QKD performing can be possible to achieve with a higher useful bits rate.

The polarization of photon pulses that arrived at Bob might deviate due to random imperfections and asymmetries in the fiber optic link. Thus, a wave plate (WP) is employed to compensate the polarized angle for each pulse. Thereupon, the pulse has been split into two coincident pulsed by a beam splitter. Each one propagates along its route through a polarizing beam splitter (PBS), each at the rectilinear and diagonal basis part, respectively. Finally, each the photon pulse is incident on a photodiode (PD), each represents the bit value either "0" or "1".

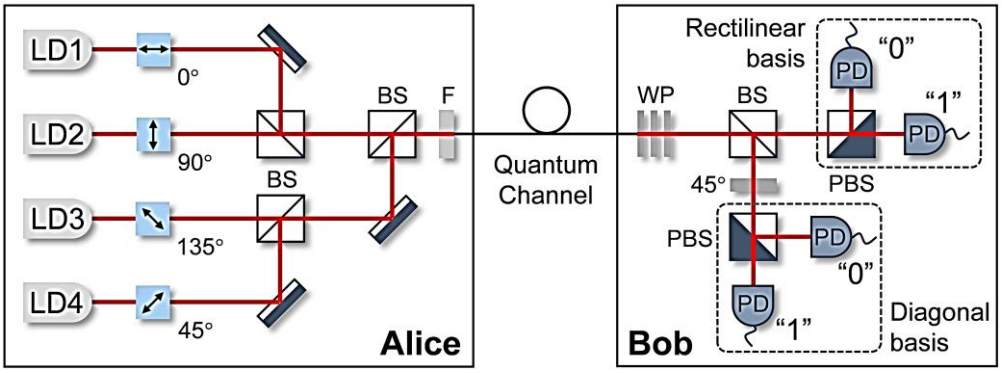


Fig. 2. A typical system for BB84 QKD system based on polarization encoding, where LD is a laser diode, BS is a beam splitter, F is light pulse filter, WP is wave plate, PBS is a polarizing beam splitter, and PD is photon detector.

In practice, the exchanged bits rate that transmitted through between 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 multiply the sifted key rate (R_{sift}) by the difference between Bob's Shannon information probability (p_{Bob}) and Eve's maximal Shannon information probability ($p_{Eve,max}$), which can be expressed as:

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

The sifted key rate corresponds to the frequency that Alice and Bob made compatible choices of basis usage for encoding and measuring the photon pulses. Thus, the probability to achieve the sifted key is 50% of the raw key. In addition, the raw key rate (R_{raw}) 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 arrived at Bob's analyzer (p_{link}). Therefore, the sifted key rate can be expressed as:

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

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 [10], and $h(e) = -elog_2(e)-(1-e)log_2(1-e)$ [15]. The $QBER$ is defined as a ratio of the wrong bits, which are usually a few, to all the received bits, can be expressed as:

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

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 was deviated (p_{opt}). This error rate (R_{opt}) is given by the product of the sifted key rate and p_{opt}. However, typically in polarization-based systems, p_{opt} is approximately of 1% and 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 make incompatible choices of basis and 50% probability that the photon is incident 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:

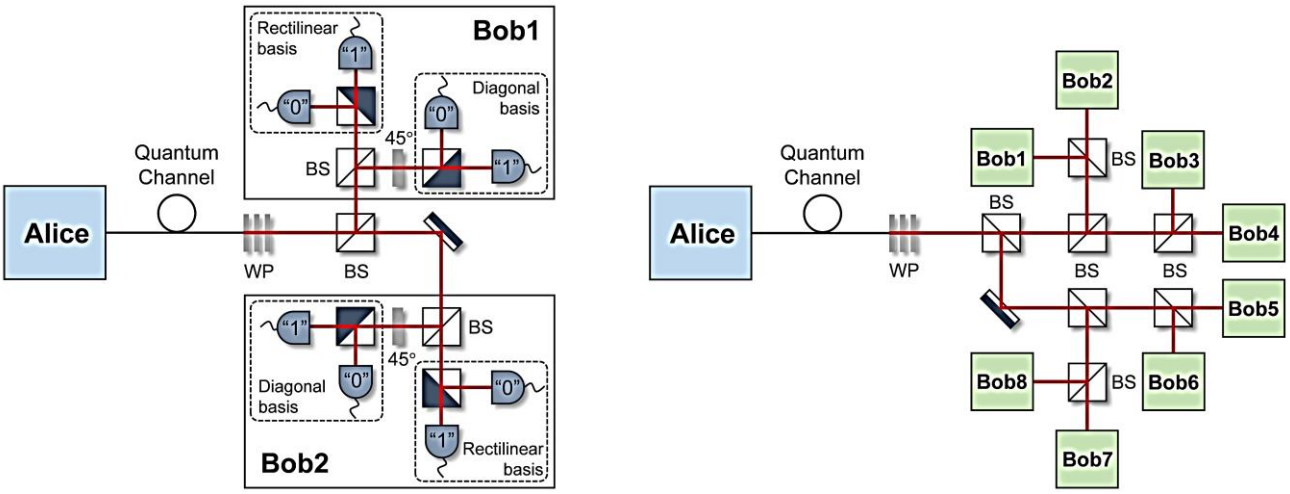
$$QBER \cong QBER_{det} = \frac{R_{det}}{R_{sift}} = \frac{np_{dark}}{2\mu\eta p_{link}} \quad (4)$$

4. Performing Multi-layers QKD and Simulation Results

A modified system for multi-layers QKD aims to increase the efficiency of the key distribution is shown in Fig. 3. The system has been set up by the same configuration as in Fig. 2, except that the Bob part will be added more to correspond with the number of photons in each emitted light pulse. These Bob parts operate independently of each other but relate to the same reference time slot.

Figure 4 shows the simulation results of the QKD performing as a relationship between the useful bit rate (R_{net}) as a function of the optical link distance between Alice and Bob. The results are obtained by Eq. (1) to (4) together with the proposed protocol. The system parameters are specified as follows: f_{pulse}= 1 GHz and 10 GHz with $\mu = 1$. The optical link attenuations of 2.0 dB/km, 0.35 dB/km, and 0.25 dB/km. The detector efficiencies of 50%, 20%, and 10%, with p_{dark}= 10^{-7}, 10^{-5}, and 10^{-5}. Each is for the light pulses of 800 nm, 1300 nm, and 1550 nm, respectively.

From the simulation results, when performing the proposed protocol through the multi-layers system as for a single user (8-layers for this case), the useful bit rate rise to a higher rate, such as 97.0 kBit/s at 120 km for 1550 nm light pulses. Which corresponds to 8 times higher than a single-layer QKD that obtained 12.1 kBit/s at the same place. Furthermore, each individual user, as Bob1 to Bob8, can also concurrently achieve their independent random secret keys with one time QKD performing through the 8-layers system.



(a) 2-layers system (b) 8-layers system

Fig. 3. Polarization encoding based systems as multi-layers QKD.

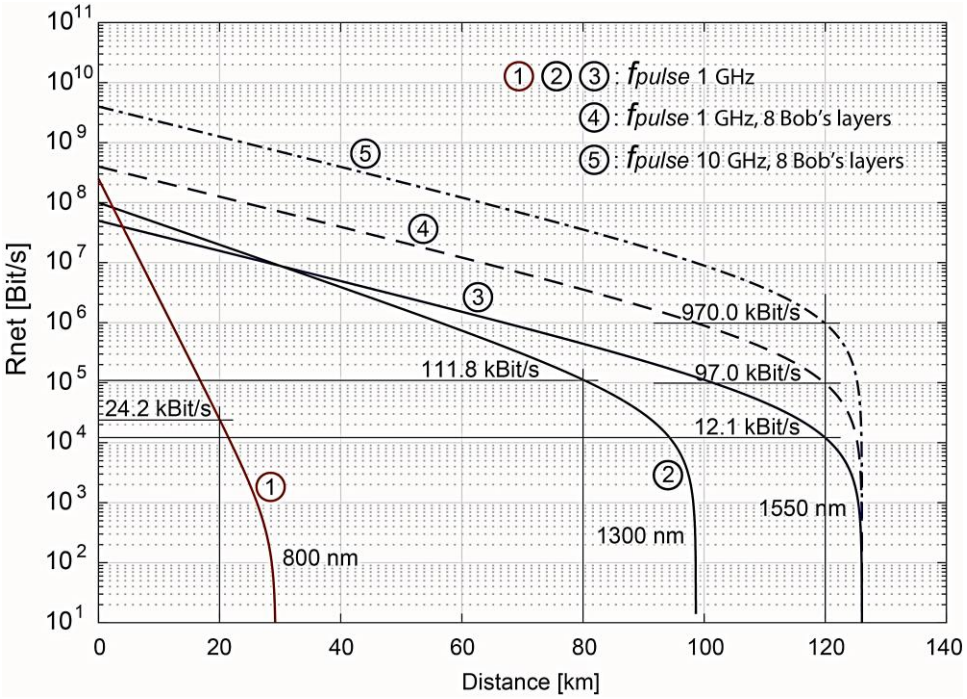


Fig. 4. Simulation results, the useful bit rates as a function of the optical link distance.

5. Discussion

Although the proposed method has a potential to improve the security and performance of QKD systems, however, there are some significant conditions must be considered to function it properly. The conditions are as follows:

[C1] *Starting the reference key:* As the algorithm for bit positions rearrangement is starting from both Alice and Bob must have a shared secret key, required for assigning the RFK. Thus, the QKD must be firstly performed by the original BB84 protocol with $\mu \leq 1$ to obtain the first shared secret key (string of x bits). Thereupon, it will be used to assign the RFK for the proposed protocol.

[C2] *Intercept/resend attack:* When Eve performs the intercept-resend attack, the probability that she incorrectly chooses the basis is 50%. If Bob measures this intercepted photon in the compatible

basis choice to Alice, he will get a random result, which has the incorrect probability of 50%. This intercepted photon then generates an error in the raw key with a probability of 50% × 50% = 25%. When Alice and Bob compare their *m* bits during the errors inspection process, the probability that they discover disagreement and identify the presence of Eve is p_{dis}=1-(3/4)^m. Therefore, to detect the eavesdropper with p_{dis}= 0.999999999, Alice and Bob need to compare *m* = 72 bits during the errors inspection.

[C3] *PNS attack:* Eve has no choice since she has no idea about each bit position. Then, she randomly rearranges her bit position and chooses the basis to measure her photons with a correct probability of $1/(2^y)^n$ and 50%, respectively. Consequently, if specifying the parameters as k = 1024 bits, corresponds to *y* = 10 bits and *n* = 10 rounds repeating, the probability that Eve can achieve correct information is remaining as only $[1/2]\times[1/(2^{10\times10})] = 3.94\times10^{-31}$.

[C4] *Faint laser pulses source:* Principally, each the encoded light pulse must be attenuated to restrict the number of photons as less as possible (to avoid the PNS). In addition, the energy of a single photon (E_{ph}) as a function of its frequency can be expressed by $E_{ph}=hv$, where h=6.62607×10^{-34} J·s is the Planck constant [16]. Then, the energy of photon in 1550 nm (193.4 THz) can be calculated as $[6.62607\times10^{-34}]\times[193.4\times10^{12}]=1.28148\times10^{-19}$ J. Suppose the light pulse is 50% duty cycle, corresponds to a pulse width of 0.5 ns and 0.05 ns for 1 GHz and 10 GHz pulse, respectively. Thus, the light power of a 1550 nm single photon pulse is $[1.28148\times10^{-19}]/[0.5\times10^{-9}] = 2.56296\times10^{-10}$ W for 1 GHz (and 2.56296×10^{-9} W for 10 GHz). Consequently, to appropriate with the 8-layers QKD, each the light pulse should be containing 8 photons. Therefore, the light pulse power (does not take into account the transmission losses) should be at least $8\times[2.56296\times10^{-10}] = 2.05037\times10^{-9}$ W for the 1 GHz, and 2.05037×10^{-8} W for the 10 GHz.

6. 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 identify the bit positions for her photon measurements. In contrast with the traditional method that most of the light pulses are empty and consequently result in a low bits rate. The advantage of such the proposed protocol is that it allows the photon source to emit the light pulses each containing a few photons so that the photon number can rise to $\mu = 1$. Moreover, the multi-layers QKD can be realized with a higher useful bits rate and consequently possible for multi-user applications by using the proposed protocol. 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", ***Proc. 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, No. 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] M. D. Eisaman, J. Fan, A. Migdall and S. V. Polyakov, "Invited review article: single-photon sources and detectors", ***Review of Scientific Instruments***, Vol. 82, pp. 071101(1)-071101(25), 2011.

[8] P. Youplao, "A privacy enhancement algorithm against photon number splitting attack for BB84 protocol", ***Proc. ICTSS 2017*** (Kiryu, Japan) May 2017.

[9] P. Youplao and S. Julajaturasiraratn, "A simulation of quantum key distribution protocol with enhancing ability to against PNS attack", ***Proc. ICMEMIS2017*** (Kiryu, Japan) November 2017.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] C.E. Shannon, "A mathematical theory of communication", ***Bell System Technical Journal***, Vol. 27, No. 4, pp. 623–666, 1948.

[16] S. Schlamminger, D. Haddad, F. Seifert, L.S. Chao, D.B. Newell, R. Liu, R.L. Steiner and J.R. Pratt, "Determination of the Planck constant using a watt balance with a superconducting magnet system at the National Institute of Standards and Technology", ***Metrologia,*** Vol. 51, No. 2, pp. S15, 2014.