Implementation of Plug & Play Quantum Key Distribution Protocol

Byungkyu Ahn*, Jinyoung Ha, Youngjin Seo, Jun Heo
School of electrical engineering
Korea University
Seoul, Korea
{bk440*, ksuwer, cherishiz, junheo}@korea.ac.kr

Jeonghwan Shin, Kyungwoon Lee
Institution of Convergence Technology
KT
Seoul, Korea
{jhsh77, kyungwoon.Lee}@gmail.com

Abstract**—** This paper represents an experimental implementation of the "Two way Plug & play" quantum key distribution (QKD) protocol, which uses weak coherent pulses at a single photon level to transfer key information from Alice to Bob via the quantum channel. In this experiment, we applied the 25km optical fiber channel and the results show a quantum bit error rate (QBER) of about 3%.

Keywords— Quantum key distribution, Single photon detection, Plug & Play protocol.

I. INTRODUCTION

The asymmetric public key cryptography system, which is currently used in communication systems including internet, is a cryptography protocol that is based on computational complexity [1], that is, adopts difficult mathematical problems like prime factorization algorithm as public key. However, the recent dramatic development of quantum computer has revealed that the conventional cryptography is decipherable and thus cannot ensure security [2].

Thus, the quantum key distribution (QKD) technology, which applies principles of quantum mechanics, comes into greater prominence as an alternative that could attain perfect encryption against wiretapping attack. The QKD technology was first introduced in 1984 by Bennet and Brassard [3]. The BB84 protocol proposed by them distributed keys by using four polarization states of a single photon forming two bases. Since then, a lot of studies [4-9] on QKD have been performed. Depending on types of channel implementing methods, the wired QKD uses optical fiber as channel, while the wireless QKD transmits and receives the encryption keys through atmosphere.

In this work, among wired QKD protocols, we present a practical process of implementing the plug & play QKD protocol that uses a Faraday mirror for auto compensation for polarization changes or channel vibration, which occur due to optical fiber distributing quantum keys, without separate components. The experiment using a single photon detector and 25 km quantum channel showed a quantum bit error rate (QBER) of 3% and 100 bps key rate when the mean photon number of 0.1 was employed.

II. PLUG & PLAY QKD PROTOCOL

A. Plug & Play QKD protocol

This QKD technique is a phase coding cryptography system [4-6] developed by A. Muller of Geneva University. Fig. 1 illustrates the configuration of the Plug & Play quantum cryptography system, and it is operated as follows.

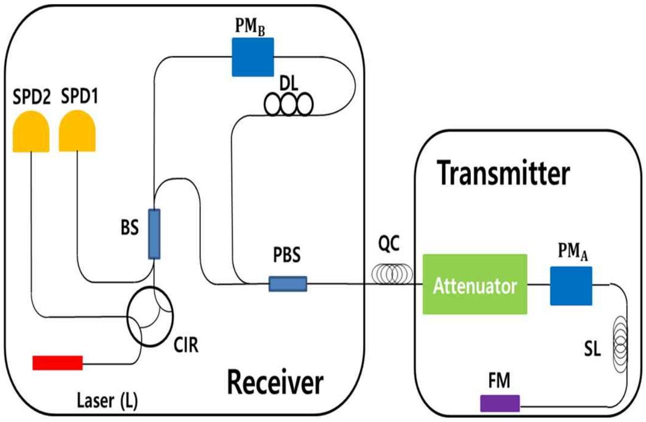

Fig. 1. Block diagram of the Plug & Play QKD system (BS : Beam Splitter, DL : Delay Line , PBS : Polarization Beam Splitter, CIR : Circulator, PM_B : Phase Modulator in receiver, SPD : Single Photon Detector, FM : Faraday Mirror, PM_A : Phase Modulator in transmitter, SL : Storage Line)

1) A strong laser pulse with 1550 nm wavelength is generated from the receiver and is divided 50:50 by a beam splitter (BS).

2) Two split pulses pass a shorter path and a longer one including PM_B and DL, respectively.

3) After passing through each path, they come out of the output of the receiver after pulses pass PBS. The output pulses after passing through the PBS have polarization components perpendicular to each other.

978-1-5386-4646-5/18/$31.00 ©2018 IEEE

4) The output pulses of the receiver pass through a 25 km optical fiber channel. The pulses have the transmission loss of about 0.2dB/km.

5) After passing through the channel, the pulses are transferred to a tranmitter and are reduced to a single photon level by an attenuator. Then, the pulses are changed to polarization components, which are perpendicular to the incident polarization, by a Farraday mirror (FM), and come back to the receiver.

6) While the pulses come back from the transmitter to the receiver, when the second pulse passes through PM_A , encryption keys are transferred by randomly applying phase shifts of 0 or π and $\pi/2$ or $3\pi/2$.

7) Single photons coming back to the receiver passes through a different path from that of 2) to reach BS simultaneously, thereby causing mutual interference. The measurement basis is obtained by applying the phase shift of 0 or $\pi/2$ to the first pulse entering PM_B in the longer channel.

8) Interfered signals are detected by a single photon detector.

B. Post processing protocols

Since a sifted key received from the single photon detector in the above process usually has a bit error of about 3~7% due to the imperfect channel and transceiver system, a post processing process is essential which includes the information reconciliation for error corrections and the privacy amplification for removing information leaked during quantum communication or error correction.

For the process of information reconciliation [10], error bits have been conventionally corrected by the cascade method, which splits key blocks of the receiver and transmitter and uses a binary search based on the parity calculation of split blocks, or the winnow method based on the syndrome of hamming code. Recently, the Low-density parity-check (LDPC) code or the Polar code are also applied which show higher error correction capability.

In the privacy amplification, a Toeplitz matrix is multiplied by a reconciled key to remove any leaked information, thereby obtaining a final secret key.

III. Implementation of Plug & play QKD system

Fig. 2 shows the two-way Plug & Play QKD protocol implemented in this study. When the system is actually implemented, we can generates digital pulses of 10000 bits at a time.

The generated pulses are converted to electric signals by PXI-6542 digital waveform device, which is shown on the right side of Fig. 3. Then, strong laser pulses with 1MHz frequency are generated from the 1550 nm laser source illustrated on the left side of Fig. 3.

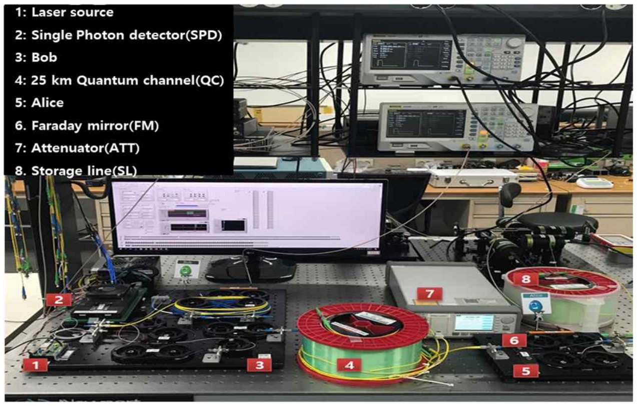

Fig. 2. Real Configuration of the Plug & Play QKD system

Fig. 3. Figure of digital wave device (right) / Laser source (left)

Laser pulses transmit a secret key as the procedure described in Section II. In this procedure, a single photon level is obtained by the following three steps.

1) Calculate the energy of single photon whose wavelength is 1550nm:

$$E = hf = h * \frac{c}{\lambda} = 1.28 * 10^{-19} J \qquad (1)$$

(E: energy of single photon h: plank constant=$6.626 * 10^{-34} J \cdot s$ *, f: frequency, c: the speed of light=* $3.0 * 10^{8} m/s$ *,* λ *: wavelength of light=*$1550nm$*)*

2) Because we are using 0.1 photon level of 1MHz pulse, the power of the pulse can be shown as

$$P = 0.1 * E * 1 * 10^{6}/s = 1.28 * 10^{-14} J/s \qquad (2)$$

$$= 1.28 * 10^{-14} W = 1.28 * 10^{-11} mW$$

$$= -108.92 dBm$$

3) A single photon is generated by using an attenuator to decrease the difference between the value of (2) and the subtraction of the loss of the entire system from the power of laser.

In addition, if the values of phase modulations, which are applied to $\mathrm{PM_A}$ and $\mathrm{PM_B}$, are θ_A and θ_B respectively, the state of a single photon arriving at the single photon detector of the receiver can be expressed as follows.

$$\frac{1}{2}\left(e^{i\theta_A} + e^{i\theta_B}\right) SP\,D_1,\ \frac{1}{2} i\left(e^{i\theta_A} - e^{i\theta_B}\right) SP\,D_2 \qquad (3)$$

Accordingly, the measurements results of the detector 1 and 2, which are obtained according to θ_A and θ_B, can be presented as in Table I. If the measurements at $SP\ D_1$ and $SP\ D_2$ are matched to classical bits 0 and 1 respectively, the values of key can be obtained.

TABLE I. RESULTS OF SINGLE PHOTON DETECTION ACCORDING TO PHASE

θ_B \ θ_A	0 (+ basis, ⟷)	$\pi/2$ (x basis, ⤢)	π (+ basis, ↕)	$3\pi/2$ (x basis, ⤡)
0 (+ basis)	SPD1	Random	SPD2	Random
$\pi/2$ (x basis)	Random	SPD1	Random	SPD2

IV. EXPERIMENTAL RESULTS

Plug & Play QKD experiment is conducted over a 25 km quantum channel. The laser at 1550nm generates 125 pulses at a frequency of 1MHz at a time, repeats the same procedure of 80 times to generate 10000 pulses, and the mean photon number per pulse is experimented at 0.1 level.

A sifted key received through the single photon detector of the receiver had the average QBER of 2.8%. The QBER 2.8% refers to the average error rate of the results accumulated 100 iterations after 10000 bit key is generated and the error rate is measured every time as shown in Fig 4.

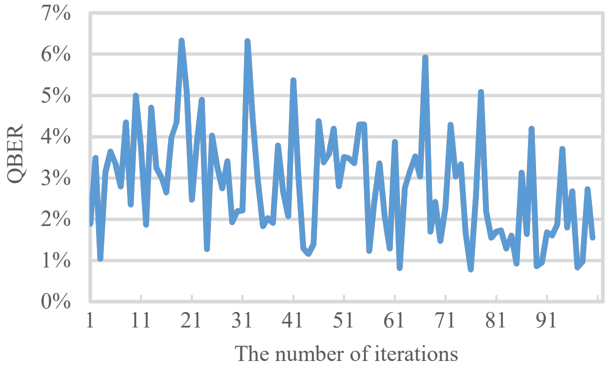

Fig. 4. Measurement result of QBER during 100 iterations (In a time, 10000 keys are generated.)

Then, we applied the cascade method for error correction. We set the minimum block size to 4 and the pass to 2 in order to minimize the complexity of error correction process. Therefore, the number of paths and block sizes defined here must be set to the minimum size that can correct all the errors contained in the sift key, so we repeatedly experimented with various values to find the optimal value.

TABLE II. THE SPECIFICATION OF THE QKD SYSTEM

Key rate	100 bps secure key @ 25km
QBER	about 3 % @ 25km
Frequency	1 MHz
Key generation protocol	Plug & Play protocol
	Cascade

Table II summarizes the QKD protocol specification implemented in this paper. The maximum allowable range of QBER that can guarantee safety in a general quantum cryptography system is about 10 to 15%. Therefore, it can be seen that the quantum cryptography implementation technique of this paper which transmits the quantum key 25 km has a QBER of about 3%, which is a stable security technique applicable as a quantum cryptography technique.

V. CONCLUSIONS

In this paper, we show the practical implementation of 2way plug & play quantum cryptography system. The laser with 1550nm wavelength band and the 2channel InGaAs Avalanche photo detectors (APDs) with 1 MHz are used to transmit and receive the key information of the QKD system. We have shown through experiments that the key transmitted over the 25 km quantum channel has a key rate of 100 bps and a QBER of about 3%.

Acknowledgment

“This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2015-0-00385) supervised by the IITP(Institute for Information & communications Technology Promotion).”

REFERENCES

[1] J.L. Massey, “An Introduction to Contemporary Cryptography,” Proc. of the IEEE, Vol.76, No.5, 1988, pp.533.

[2] P. Shor, in Proc. of the 35th Annu. Symp. on Foundations of Computer Science, edited by S. Goldwasser, IEEE Computer Society Press, Los Alamitos, California, 1994, pp.124.

[3] C.H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proc. of IEEE Int’l Conf. on Computers, Systems and Signal Proc., Bangalore, India, IEEE, New York, 1984, pp.175.

[4] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “Plug and Play Systems for Quantum Cryptography,” Appl. Phys. Lett., Vol.70, 1997, pp.793.

[5] G. Ribordy, J.D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, “Automated ‘Plug & Play’ Quantum Key Distribution,” Electron. Lett., Vol.34, 1998, pp.2116.

[6] D. Stucki, N. Gisin, O. Guinnared, G. Ribordy, and H. Zbinden, “Quantum key distribution over 67 km with a plug & play system”, New J. Phys. 4, 41.1-41.8, 2002.

[7] J.L. Massey, “An Introduction to Contemporary Cryptography,” Proc. of the IEEE, Vol.76, No.5, 1988, pp.533.

[8] C.H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States” Phys. Rev. Lett., Vol.68, 1992, pp.3121.

[9] A.K. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett., Vol.67, 1991,pp.661.

[10] J. S. Johnson , “An Analysis of Error Reconciliation Protocols for use in Quantum Key Distribution”, Ph.D. thesis, Air Force Institute of Technology, 2012.