PTL-40810-2024

Multiuser Differential-Phase-Shift Quantum Key Distribution System on a Ring Network

Kyo Inoue and Toshimori Honjo

***Abstract*—Quantum key distribution (QKD) has been studied, which is basically a point-to-point system. Therefore, when constructing a QKD network in which any pair of multiple users shares a secret key, full-mesh connections equipping each user with a transmitter and a receiver must be installed. This study presents a QKD system based on the differential-phase-shift QKD protocol, which accommodates multiusers on one transmission line. The proposed system uses a ring network connecting multiple nodes, in which one node is equipped with a transmitter and a receiver and the other nodes are with phase-modulation circuits. The system performance is evaluated and the results indicate that a 100-km ring network can support up to seven nodes.**

***Index Terms*—quantum key distribution, multiple users, ring network.**

I. INTRODUCTION

QUANTUM key distribution (QKD), which securely provides a secret key for ciphering/deciphering a message to two distant parties based on quantum mechanics, has been studied [1], along with some field experiments regarding QKD networks connecting several nodes [2–4]. In those networks, each pair of nodes is linked one-to-one via a dedicated fiber line because quantum signals cannot be manipulated during transmission. Therefore, a QKD network, in which any pair of users can share a secret key, needs full-mesh connections, resulting in a high implementation cost.

To mitigate this issue, QKD networks that connect multiple users via optical switching systems have been presented [5–9]. The use of optical switches reduces the number of connection links. For example, in a star-topology network in which multiusers are connected to one switching node, the number of links to accommodate N users is N, whereas it is $N(N-1)/2$ in a full-mesh network. However, N links are still necessary, and each user must has a quantum transmitter and receiver.

A QKD system connecting multiple users with one transmission line was also proposed [10, 11]. In this system, any pair of users on one line could create a secret key using the BB84-based quantum secret sharing (QSS) protocol. However, single-photons were sent from the transmitter to the receiver through multiusers, and thus the raw-key creation rate was low even between closely located users. Besides, polarization control was required at each user [11].

Therefore, this study presents a QKD system based on the differential-phase-shift (DPS) QKD [12-14] or DPS-QSS protocol [15], which supports multiple users with one ring network, mitigating the issues associated with the abovementioned QKD systems. A central node sends a coherent pulse train to a ring line in one direction. The intermediate nodes on the ring line phase-modulate the transmitted pulses by 0 or π, which are then received and measured by the central node. Using this setup, any pair of nodes on the ring line can share a secret key.

Although the network topology is similar to that of the BB84-QSS based system [10, 11], a higher key-creation rate can be expected because the distance traveled by the quantum signal is shorter for an identical system length. In addition, polarization control at each node is not necessary.

The key distribution performance is evaluated after describing the system setup and operation. The results indicate that a 100 km ring network can accommodate up to seven nodes.

II. SETUP AND OPERATION

The setup of the proposed multiuser QKD system is illustrated in Fig. 1. A central node (C-node), which includes a transmitter and a receiver, and multiple intermediate nodes (I-nodes) are connected to a ring-like transmission line. The transmitter sends a coherent pulse train to the ring line in one direction, and the receiver measures the pulses after one round of travel through the ring, using a delay interferometer and photon detectors.

Each I-node is equipped with a phase modulation unit, an optical variable attenuator, and apparatuses that monitor the optical power sent to the next I-node. The phase modulation unit is composed of two polarization-beam-splitters (PBSs) and two phase-modulators connected via polarization-maintaining fibers, such that the incident light is divided into two orthogonal polarization components at the first PBS, each component passes through the phase modulator with the matched polarization state, and is polarization-multiplexed at the second PBS. The two components are recombined in orthogonal polarization states at the second PBS; thus the relative phase between the two components does not matter in multiplexing. In this setup, phase modulation is stably imposed on the transmitted light irrespective of the incident polarization state [16]. The variable attenuator and power monitoring system are equipped to adjust the pulse intensity sent to the next node, as described later. This power monitoring system also counters Trojan horse attacks.

This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE.

K. Inoue is with Osaka University, Suita, 565-0871 Japan (e-mail: kyo@comm.eng.osaka-u.ac.jp).

T. Honjo is with NTT Corporation, Atsugi, 243-0198 Japan (e-mail: toshimori.honjo@ntt.com).

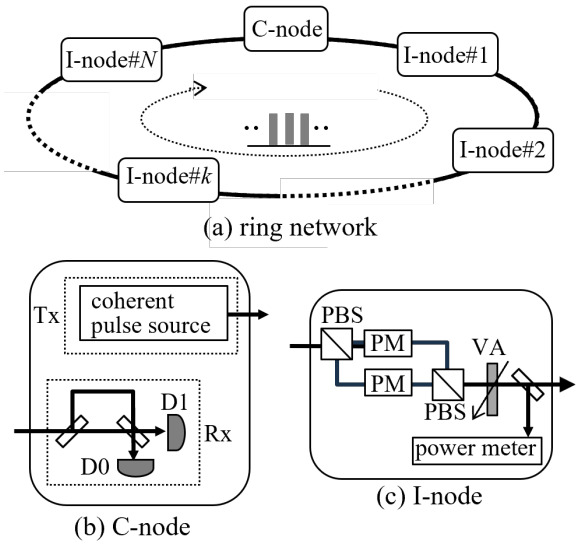

Fig. 1. The proposed QKD system: (a) network configuration, (b) setup of C-node, and (c) setup of I-node. C-node and I-nodes denote the central node and intermediate nodes, respectively. Tx: transmitter, Rx: receiver, D: single-photon detector, PM: phase modulator, PBS: polarization beam splitter, and VA: variable attenuator.

This setup enables two arbitrary nodes on the ring line to share a secret key using the following procedure. First, the two nodes intending to share a secret key announce their intension. Subsequently, the key-creation process begins, which depends on whether the key-sharing nodes include the C-node or not.

When two I-nodes, e.g., I-node#*i* and I-node#*j* ($i < j$), are to share a secret key, the key bits are created as follows.

(i) The C-node sends an unmodulated coherent pulse train of moderate intensity (e.g., 1 mW) to the ring line.

(ii) I-node#*i* adjusts its variable attenuator such that the mean photon number sent to the next node is small (e.g., 0.2/pulse). The variable attenuators of the other I-nodes are set to 0 dB.

(iii) I-nodes#*i* and #*j* phase-modulate the transmitted pulses by 0 or π, while the other I-nodes do nothing.

(iv) The C-node receives the pulse train and detects photons at the delay interferometer output while recording the detection time and clicking detector.

(v) After signal transmission, the C-node provides information regarding the photon detection time slots and detectors to I-nodes#*i* and #*j*.

(vi) Based on the C-node's information and the relative phase imposed onto the pulses having clicked the C-node's detectors, nodes#*i* and #*j* create raw-key bits as follows. First, they create bits "0" or "1" if their relative phases imposed onto the pulses are 0 or π, respectively. Subsequently, when detector 1 clicks, I-node#*j* flips its bit values.

The bit values created as above are identical between I-nodes#*i* and #*j*, which form a raw key. Here, the key bits shared between I-nodes#*i* and *j* are unknown to the C-node and the other I-nodes, who can be untrusted by the key-sharing nodes. If malicious nodes perform something to obtain the key bits, bit mismatch occurs between the key-sharing nodes or the power level varies at I-node#*j*, from which malicious nodes are noticed.

The procedure for the C-node and I-node#*i* to create key bits is as follows. The first four steps, that is, steps (i)-(iv), are the same as above, except that I-node#*i* alone performs phase modulation; however steps (v) and (vi) are different.

(v) The C-node informs I-node#*i* about the photon detection slot.

(vi) The C-node creates bits "0" or "1" if detector 0 or 1 clicks. I-node#*i* creates bits "0" or "1" if the relative phase imposed on the pulses clicking the C-node's detectors is 0 or π. The bit values created as above are identical between the C-node and I-node#*i*, and unknown to the other I-nodes. Then, the two nodes obtain a raw key.

Using the above protocol, any pair of nodes on the ring line can share a secret key. In the proposed system, only the C-node is equipped with a quantum receiver; each I-node is equipped with only a phase-modulation unit. Thus, there is no need for a set of a transmitter and a receiver at each I-node, resulting in a cost-effective multiuser QKD system.

Although the transmitter and receiver are accommodated in the central node in a ring line in the proposed system, assuming applications to metropolitan areas where ring-topology fiber networks are installed, they can be located at each end of a one-way straight line, respectively, through which multiple I-nodes are connected, as in [10, 11]. In such bus-topology networks, the transmitter is equipped also with a phase modulator and an attenuator, and then a secret key can be shared also between the transmitter and receiver nodes.

When compared to a conventional QKD network similar to the present one [10, 11], which is based on BB84-based QSS and connects multiple users on one transmission line, our proposal differs in term of the distance through which the quantum signal is transmitted. While single-photons are sent from the transmitter to the receiver in the conventional system, weak coherent pulses are transmitted from one of the I-nodes to the C-node in the proposed system. Subsequently, the number of photons arriving at the receiver will be higher in the proposed system, resulting in a higher key creation rate, particularly when the last I-node and C-node are key-sharing nodes.

Another advantage of the proposed system is its polarization-independent operation. The polarization state of light propagating through fibers varies randomly in practice; thus polarization control is required when conventional polarization-sensitive phase-modulators are used on transmission lines, as in [11]. To mitigate this issue, a polarization diversity scheme is employed in the proposed system, which can be applied to cascaded I-nodes, unlike a polarization-insensitive scheme of scrambling the polarization state [17]. The feasibility of this modulation scheme was demonstrated in [16], where the measurement basis was actively selected in a BB84 or DQPS QKD experiment.

III. SYSTEM PERFORMANCE

The key-creation performance of the proposed system is evaluated in this section, considering eavesdropping. Against the present system, eavesdropping will be performed as illustrated in Fig. 2, where I-node#*i* and I-node#*j* are the key-

sharing nodes. Because the signals before I-node#*i* and after I-node#*j* provide no key-bit information, an eavesdropper (Eve) attacks the signal at the I-node#*i* output. Eve performs some operation on the signal, which is then sent to I-node#*j* through a lossless line, bypassing the I-nodes located between I-nodes#*i* and #*j*, to compensate for the photon-number reduction resulting from the eavesdropping operation. Eve also injects dummy light into the I-nodes that monitor the transmitted light power.

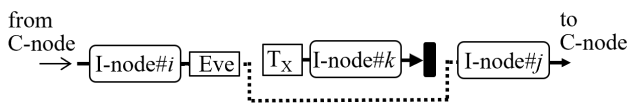

Fig. 2. Eavesdropping against the proposed QKD network in which I-node#*i* and I-node#*j* are the key-sharing nodes. Tx: light source.

For evaluating the QKD performance of the proposed system, we assume a general individual attack [18], which is typically assumed against DPS-QKD [19, 20]. The final key-creation rate R of a point-to-point DPS-QKD system suffering from the general individual attack is given by [18]

$$R = R_{\mathrm{r}}\left[\{1-2\mu(1-T)\}\log_2[1-e^2-\frac{(1-6e)^2}{2}]-H(e)\right], \quad (1)$$

where R_{r} is the raw-key rate, μ is the mean photon number per pulse sent from the transmitter, T is the transmittivity from the transmitter to the receiver, e is the bit error rate at the receiver, and $H(e) = -e\log_2 e - (1-e)\log_2(1-e)$ represents the information leakage probability through ideal error correction.

In our ring network in which I-node#*i* and I-node#*j* are the key-sharing nodes, the raw-key rate R_{r} is expressed as $R_{\mathrm{r}} = \eta\mu T_{i\to\mathrm{C}}$, where η is the C-node's detection efficiency, μ is the mean photon number per pulse at the I-node#*i* output, and $T_{i\to\mathrm{C}}$ is the transmittivity from I-node#*i* to the C-node. The C-node's bit error rate in the normal condition, e, can be expressed as

$$e = \frac{2d}{\eta\mu T_{i\to\mathrm{C}} + 2d} + e_{\mathrm{MZ}}, \quad (2)$$

where d is the dark count rate of the detectors and e_{MZ} is the bit error rate caused by imperfect interference. The transmittivity T in Eq. (1) represents the transmittivity between the transmitter and receiver in a point-to-point QKD system. The corresponding parameter in the proposed system is the transmittivity from I-node#*i* to the C-node, $T_{i\to\mathrm{C}}$.

To evaluate the key-creation rate, the transmittivity from I-node#*i* to the C-node, $T_{i\to\mathrm{C}}$, should be given, which depends on the network condition. We assume that N I-nodes are located at equal intervals along a ring transmission line of length L. In such a network, the transmittivity $T_{i\to\mathrm{C}}$ is expressed as

$$T_{i\to\mathrm{C}} = 10^{-\alpha(N-i+1)L_0} \times T_{\mathrm{B}}^{(N-i)}, \quad (3)$$

where α is the fiber attenuation coefficient, $L_0 = L/(N+1)$ is the distance between the neighboring nodes, and T_{B} is the transmittivity of the I-node.

Using the above equations, we calculate the secret key creation rate in ring networks with lengths of 100 and 50 km. The parameter values assumed are as follows: dark count rate $d = 10^{-7}$, detection efficiency $\eta = 0.25$ [21], fiber attenuation = 0.2 dB/km, interference error rate $e_{\mathrm{MZ}} = 0.01$ [22], and node transmittivity $T_{\mathrm{B}} = 0.5$. The results are shown in Fig. 3, where the highest and lowest rates are plotted as open and closed circles, respectively. The highest key rates are obtained by I-node#*N* and the C-node and the lowest key rates are obtained by I-node#1 and the C-node.

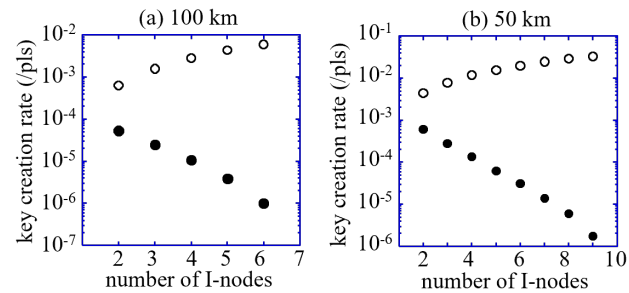

Fig. 3. Key-creation rates in systems with ring lengths of (a) 100 km and (b) 50 km. Open and closed circles indicate the calculation results for the best and worst cases, respectively. The parameter values assumed are the dark count rate: $d = 10^{-7}$, detection efficiency: $\eta = 0.25$, fiber attenuation: 0.2 dB/km, interference error rate: $e_{\mathrm{MZ}} = 0.01$, and node transmittivity: $T_{\mathrm{B}} = 0.5$. The mean photon number sent from I-node#*i* is optimized to obtain the highest key-creation rate under each system condition.

Figure 3 shows that the lowest key-rate decreases as the number of I-nodes increases, because the transmission loss between I-node#1 and the C-node increases. Noting that the number of I-nodes N is plotted along the horizontal axis in the figure and the C-node can also be a key-sharing node, Fig. 3 indicates that any pair of nodes up to seven and ten (including the C-node) can share a secret key in the 100 km and 50 km networks, respectively. In contrast, the highest key rate obtained between I-node#*N* and the C-node increases with the number of I-nodes, because the distance between them decreases for a fixed ring length. Such a high key-creation rate cannot be achieved in the conventional QKD system that accommodates multiple users on one transmission line [11]. The other pairs of key-sharing nodes achieve key rates between the highest and lowest ones.

We also evaluate the system performance in another scenario, that is, when the distance between neighboring I-nodes is fixed. As the number of I-nodes increases, the total ring length increases. The calculation results for the lowest key-creation rate as a function of the number of I-nodes are presented in Fig. 4. The results indicate that a 10 km span can accommodate up to eight nodes.

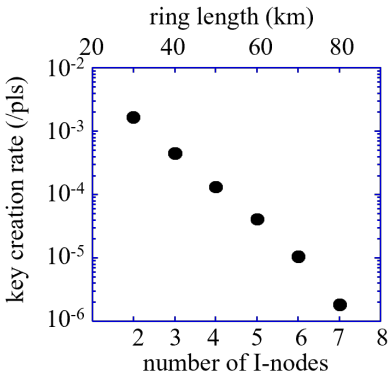

Fig. 4. Key-creation rate under the condition that the distance between adjacent I-nodes is 10 km. The lowest key rate is plotted and the corresponding total ring length is labeled in the upper horizontal axis. The parameter values assumed are the same as those in Fig. 3.

In this study, we evaluated the key creation rate at which a secret key was securely created under the condition that the general individual attack presented in [18] was conducted. Unfortunately, the system performance against other general attacks cannot be evaluated, because the security analysis for general eavesdropping against a long weak coherent pulse train that conveys a number of bit information in it has been unknown.

IV. SUMMARY

This paper presented a DPS-QKD system that supported multiple users in one ring network. One transmitter/receiver node launched an unmodulated coherent pulse train onto the ring transmission line in one direction and received the pulses after one round of travel through the ring. One or two intermediate nodes on the ring line that shares a secret key, {0, π}-phase-modulated the transmitted pulses.

The proposed system enabled any pair of nodes on the ring network to share a secret key with a simple setup. The system performance was also evaluated assuming the general individual attack, and the results indicated that a 100 or 50 km ring network could accommodate up to seven or ten nodes, respectively.

REFERENCES

[1] S. Pirandola et al., "Advances in quantum cryptography," Adv. Opt. Photon., vol. 12, no. 4. 2020, pp. 1012–1236, doi:10.1364/AOP.361502.

[2] M. Peev, et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys., vol. 11, Jul. 2009, Art. no. 075001, doi:10.1088/1367-2630/11/7/075001.

[3] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express, vol. 19, no. 11, May 2011, pp. 10387–10409, doi:10.1364/OE.19.010387.

[4] D. Huang, P. Haung, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," Opt. Lett., vol. 41, no. 15, Aug. 2016, pp. 3511–3514, doi:10.1364/OL.41.003511.

[5] P. Toliver et al., "Experimental investigation of quantum key distribution through transparent optical switch elements," IEEE Photon. Technol. Lett., vol. 15, no. 11, Nov. 2003, pp. 1669–1671, doi:10.1109/LPT.2003.818687.

[6] T. Honjo, K. Inoue, A. Sahara, E. Yamazaki, and H. Takesue, "Quantum key distribution experiment through a PLC matrix switch," Opt. Commun., vol. 263, Dec. 2006, pp. 120–123, doi:10.1016.j.optcom.2006.01.018.

[7] L. Ma, A. Mink, H. Xu, O. Slattery, and X. Tang, "Experimental demonstration of an active quantum key distribution network with over Gbps clock synchronization," IEEE Commun. Lett., vol. 11, no. 12, Dec. 2007, pp. 1019–1021, doi:10.1109/LCOMM.2007.071477.

[8] T. E. Chapuran, et al., "Optical networking for quantum key distribution and quantum communications," New J. Phys., vol. 11, Oct. 2009, Art. no. 105001, doi:10.1088/1367-2630/11/10/105001.

[9] O. Alia, R. Stange, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dynamic DV-QKD networking in trusted-node-free software-defined optical networks," J. Lightw. Technol., vol. 40, no. 17, Sep. 2022, pp. 5816–5824, doi:10.1109/JLT.2022.3183962.

[10] M. Doosti, L. Hanouz, A. Marin, E. Kashefi, and M. Kaplan, "Establishing shared secret keys on quantum line networks: protocol and security," arXiv:2304.01881, Apr. 2023, doi:10.48550/arXiv.2304.01881.

[11] M. Sena, G. Harder, R. Döring, R. Braun, M. Ritter, M. Kaplan, and M. Geitz, "Experimental validation of DV-QKD-based Qline architecture for metropolitan network on Berlin openQKD testbed," in *ECOC*, Glasgow, Scotland, 2023, paper M.A.4.2.

[12] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A, vol. 68, no. 2, Aug. 2003, Art. no. 022317, doi:10.1103/PhysRevA.68.022317.

[13] S. Wang, Z. Yin, W. Chen, D. He, X. Song, H. Li, L. Zhang, Z.Zhou, G. Guo, and Z. Han, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," Nat. Photon., vol. 9, pp. 832–836, Dec. 2015, doi:10.1038/NPHOTON.2015.209.

[14] Z. Yin, S. Wang, W. Chen, Y. Han, R. Wang, G. Guo, and Z. Han, "Improved security bound for the round-robin-differential-phase-shoft quantum key distribution," Nat. Commun., vol. 9, 2018, Art. no. 457, doi:10.1038/s41467-017-02211-x.

[15] K. Inoue, T. Ohashi, T. Kukita, K. Watanabe, S. Hayashi, T. Honjo, and H. Takesue, "Differential-phase-shift quantum secret sharing," Opt. Express, vol. 16, no. 20, Sep. 2008, pp. 15469–15476, doi:10.1364/OE.16.015469.

[16] M. Alhussein, K. Inoue, and T. Honjo, "BB84 and DQPS-QKD experiments using one polarization-insensitive measurement setup with a countermeasure against detector blinding and control attacks," in *CLEO*, San Jose, CA, USA, 2019, paper JTu2A.28.

[17] G. Fan-Yuan, F. Lu, S. Wang, Z. Yin, D. He, W. Chen, Zhou, Z. Wang, J. Teng, G. Guo, and Z. Han, "Robust and adaptable quantum key distribution network without trusted nodes," Optica, vol. 9, no. 7, pp. 812–823, Jul. 2022, doi/10.1364/OPTCA.458937.

[18] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys. Rev. A, vol. 73, no. 1, Jan. 2006, Art. no. 012344, doi:10.1103/PhysRevA.73.012344.

[19] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nat. Photon., vol. 1, June 2007, pp. 343–348, doi:10.1038/nphoton.2007.75.

[20] H. Shibata, T. Honjo, and K. Shimizu, "Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors," Opt. Lett., vol. 39, no. 17, Sep. 2014, pp. 5078–5081, doi:10.1364/OL.39.005078.

[21] ID Quantique, https://www.idquantique.com/quantum-sensing/products/id230/.

[22] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution with a planar light-wave circuit Mach-Zehnder interferometer," Opt. Lett., vol. 29, no. 23, Dec. 2004, pp. 2797–2799, doi/10.1364/OL.29.002797.