IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 20, 2018, accepted September 20, 2018, date of publication October 5, 2018, date of current version October 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2874028

Practical Plug-and-Play Measurement-Device-Independent Quantum Key Distribution With Polarization Division Multiplexing

CHANG HOON PARK[1,2], MIN KI WOO[2], BYUNG KWON PARK[1,3], MIN SOO LEE[1], YONG-SU KIM[1,3], YOUNG-WOOK CHO[1], SANGIN KIM[2], SANG-WOOK HAN[1], AND SUNG MOON[1]

[1]Center for Quantum Information, Korea Institute of Science and Technology, Seoul 02792, South Korea
[2]Department of Electrical and Computer Engineering, Ajou University, Suwon 16499, South Korea
[3]Division of Nano & Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul 02792, South Korea

Corresponding author: Sang-Wook Han (swhan@kist.re.kr)

This work was supported in part by the ICT Research and Development Programs of MSIP/IITP under Grant B0101-16-1355 and in part by the KIST Research Program under Grant 2E27231.

ABSTRACT We have implemented a practical plug-and-play measurement-device-independent quantum key distribution (MDI QKD) system with polarization division multiplexing (PDM). MDI QKD is known as a secure protocol that can inherently prevent detection loopholes. Significant efforts have been made toward implementing MDI QKD systems. Recently, a plug-and-play architecture has been proposed for implementing the MDI QKD system, and its feasibility has been experimentally verified in both free space and fiber channel. However, in order to apply it to the real world, it is necessary to develop a more practical architecture including multiplexing methods and self-compensation techniques. In this paper, we have proposed and implemented a practical plug-and-play MDI QKD architecture that can be implemented regardless of whether the quantum channel lengths of Alice and Bob are symmetric or asymmetric using PDM and can be operated even under ambient-temperature-changing environments through an optical path-length self-compensation technique. Experimentally, we have achieved 6.25×10^{-6} bits per pulse as the key rate and the quantum bit error rates under 3% on 25-km quantum channels.

INDEX TERMS Quantum cryptography, measurement-device-independent, plug-and-play, polarization division multiplexing, optical path-length self-compensation.

I. INTRODUCTION

Quantum key distribution (QKD) [1], [2] theoretically guarantees unconditional security by the laws of quantum physics [3]–[5]. However, when implemented as a system, it is exposed to various quantum hacking methods [6]–[16] because of the imperfect characteristics [17], [18] of real devices. To overcome security risks generated by the gap between actual and ideal devices, three methods are usually mentioned. The first method involved the development of a device-independent QKD (DI QKD) [19]–[22]. DI QKD is a QKD protocol that ensures security regardless of device characteristics. Nevertheless, DI QKD is impractical thus far because it requires the loophole-free Bell test, which is technically very difficult to implement. Secondly, there are security patch methods [23]–[27]. They guarantee security against well-known hacking methods; however, they may be exposed to potential risks of unidentified attacks. The last one is a measurement-device-independent QKD (MDI QKD) [28]–[30]. The security of MDI QKD is guaranteed independently of the characteristics of measuring devices. Most quantum hacking methods are primarily targeted at the measuring devices. Therefore, the security of QKD can be greatly improved by applying MDI QKD. In the MDI QKD protocol, Alice and Bob send the modulated single photons—independently prepared at each user—to a third party (Charlie) for Bell state measurement (BSM) and then generate the secret keys according to Charlie's measurement results and their own modulation information. Since BSM measures only the correlation between two photons, for extracting the secret keys it is necessary to know their own encoding

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

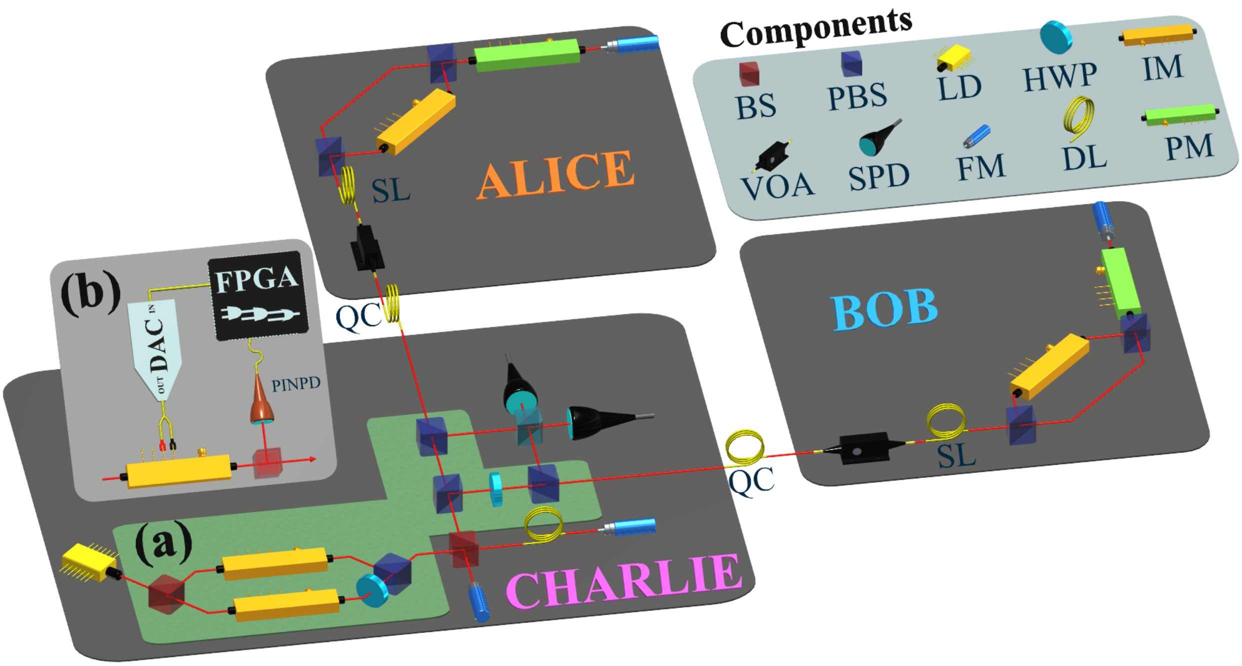

FIGURE 1. Experimental setup of the plug-and-play measurement-device-independent quantum key distribution. The green area (a) is for the PDM and light gray area (b) is for the intensity modulator feedback system. On each user side (Alice and Bob), two PBSs are added to reduce the polarization-dependent loss of IM. LD: laser diode (1550 nm); PBS: polarization beam splitter; IM: intensity modulator; BS: beam splitter; FM: Faraday mirror; DL: delay line; SPD: single photon detector; QC: quantum channel (25 km); VOA: variable optical attenuator; PM: phase modulator; SL: storage line (15 km); PINPD: p-i-n photodiode; DAC: digital-to-analog converter; FPGA: field programmable gate array; HWP: half wave plate.

information of Alice or Bob. Thus, although all BSM results are eavesdropped, nobody except Alice and Bob, who know their own encoding information, can extract the secret keys (as described in [28]–[30]). Therefore, the security of MDI QKD can be guaranteed independent of the measuring devices. However, to realize BSM, active controls for polarization, wavelength, and photon arrival timing are essentially required to maintain the indistinguishability of two photons that make the system become more complex and impractical [29]–[32]. Therefore, as a solution for improving the practicability, a plug-and-play architecture [33], [34], which is favorable for mode matching, has been proposed.

In the plug-and-play architecture, the optical pulses of Alice and Bob are generated by a single laser and pass through the same interferometer. Therefore, wavelengths and phase reference frames of Alice and Bob are automatically matched. Besides, polarization drift due to the birefringence effects of the optical fiber can be naturally compensated through the round trip of the optical signals using a Faraday mirror (FM). Consequently, no active controls except the timing control are required, and this makes the system simple.

The plug-and-play MDI QKD has already been experimentally verified in both free space and fiber channel [35]–[37]. Among the reported studies, Tang's work is noticeable because it reports the first plug-and-play MDI QKD implemented in the optical fiber. However, due to its unique technique—called the passive timing calibration method—it requires several additional components, including laser diodes, and it can only operate when the quantum channel lengths of Alice and Bob are asymmetric. In Tang's paper, Charlie cannot choose the transmission path since the optical pulses are divided by a simple beam splitter (BS). So, the time division multiplexing should be used to distinguish signals. It means that their setup cannot be implemented in symmetric quantum channels.

In this study, we have implemented a more practical plug-and-play MDI QKD system. Polarization division multiplexing (PDM) technique has been applied to overcome the above issue. Since the optical pulse trains are distinguished according to the polarization like as horizontal-Alice, vertical-Bob and generated at independent timing by using the PDM, our setup can be implemented regardless of whether the quantum channel lengths of Alice and Bob are symmetric or asymmetric. Further, a compact optical path-length self-compensation system has been applied to avoid the problem of change in photon arrival timing due to ambient temperature changes. In the following section, we will describe the proposed system architecture and the experimental results.

II. PROPOSED ARCHITECTURE

The proposed scheme of the plug-and-play MDI QKD is shown in Fig. 1. The overall signal flow is as follows. First, because of the plug-and-play architecture, only a single laser is used for the light source of Alice and Bob. The light is modulated into optical pulse trains with a pulse width of 3 ns (FWHM) at a repetition rate of 1 MHz by two of Charlie's intensity modulators (IMs). Although we used low repetition rate 1MHz for feasibility test, our proposed setup also can be operated at a faster rate. For the higher speed operation, we need to consider not only the repetition rate of Charlie's IMs but also the time-bin size of Michelson interferometer and path lengths between IM to FM in each of Alice and Bob. Each optical pulse of the trains is separated into two time-bins (early time-bin and late time-bin) with a time delay of 100 ns via a Michelson interferometer. Subsequently, the trains are split by a second polarization beam splitter (PBS) according to the polarization states. Since the optical pulse trains of Alice and Bob are distinguished and generated at independent times by using this PDM technique, our scheme can be operated regardless of whether the quantum channel lengths of Alice and Bob are symmetric or asymmetric. The horizontally (vertically) polarized optical pulse train is transmitted to Alice (Bob) through a 25 km quantum channel and encoded using the time-bin phase encoding [29,] [30], [38]. The Z basis can be encoded by selecting either an early or late time-bin using an IM, whereas the X basis encoding can be done by modulating the relative phase of time-bins to 0 or π using a phase modulator (PM). The encoded light is reflected by an FM, attenuated by a variable optical attenuator (VOA), and then returned to Charlie. The correlation of the returned photon pairs of Alice and Bob are measured using BSM, which is implemented with a BS and two single photon detectors (SPDs) with a quantum efficiency of 10%, a gate width of 3 ns, a dead time of 1 μs, and a dark count rate of 4×10^{-6} counts per gate pulse. Additionally, SPDs are also used for the optical path-length self-compensation system, which can compensate for the variation of the effective fiber length due to ambient temperature changes [31], [39].

If the result of BSM is $|\Psi^-\rangle$ which is defined as $1/\sqrt{2}(|10> -|01>)$, Charlie announces the result via the classical channel. Experimentally, it means that the photons of Alice and Bob are detected at two alternative time-bins (i.e., one of the detectors has an event at the early (late) time-bin and the other detector has an event at the late (early) time-bin). After Charlie's announcement, Alice and Bob can generate secret keys through the basis exchange and post-selection with each own encoding information.

III. EXPERIMENTAL SETUP AND RESULTS

A. POLARIZATION DIVISION MULTIPLEXING

The proposed setup can be operated independently of whether the quantum channel lengths of Alice and Bob are symmetric or asymmetric through the PDM technique. To apply this technique, we implemented a setup shown in Fig. 1 (a) and used only polarization maintaining fiber (PMF) coupled devices for implementing Charlie. The signal flow is as follows. At first, the vertically polarized light is divided into two individual paths by the first BS, and the IM on each path generates the optical pulse trains of Alice and Bob. Then, the optical pulse trains, which are orthogonally polarized with respect to each other because of the first half wave plate (HWP), are combined by the first PBS and pass through the same path and interferometer. Finally, they are split into Alice and Bob by the second PBS according to the polarization states. By using this PDM method, optical pulse trains of Alice and Bob are distinguished according to the polarization and generated at independent timings by two of Charlie's IMs; therefore, the proposed QKD scheme can be operated regardless of whether Alice and Bob have symmetric or asymmetric quantum channels.

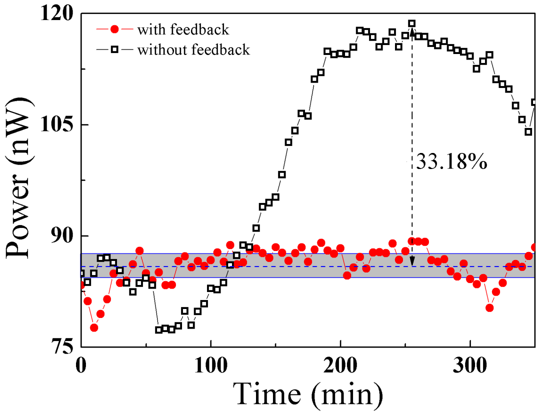

FIGURE 2. Variation of the IM output power. The light gray area indicates the target optical power when the count of the output optical pulse of the IM equals that of its input electrical pulse.

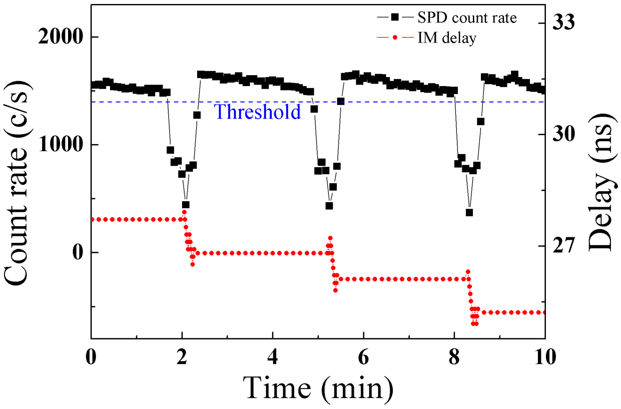

FIGURE 3. Variation of the SPD count rate in an environment where the quantum channel (25 km) of Alice is enclosed in a heating cabinet. While the optimal driving delay of the IM varies over 2 ns for 10 min, the SPD count rate is recovered three times over the threshold value (1400 c/s) by the optical path-length self-compensation system.

By the way, we had to solve an intrinsic problem of the IM used for this multiplexing technique. Depending on the operating condition, the output power of the IM varies slightly even under a constant DC control voltage [40], [41]. Therefore, we applied the IM feedback system to compensate this DC drift. The feedback system tracks the DC voltage at which the output power is maintained in the region of the target power (the light gray region of Fig. 2) in response to the operating condition changes. As shown in Fig. 1 (b), the feedback system was implemented using a field programmable gate

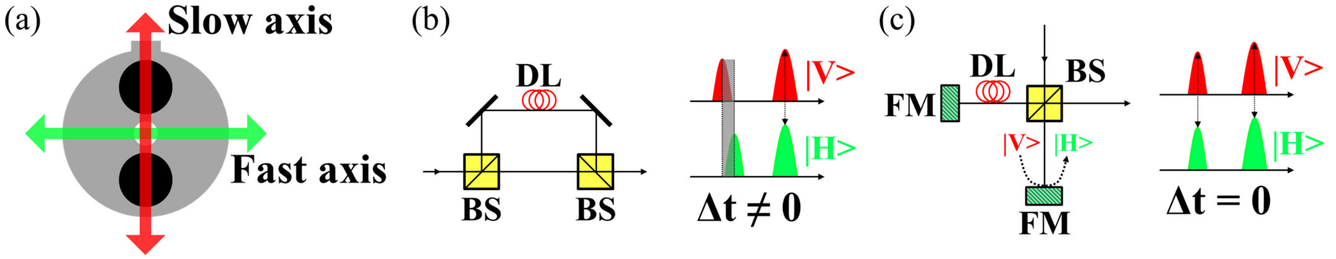

FIGURE 4. (a) is a cross section of the Panda PMF. The transmission speed is determined by the polarization (i.e., the horizontally polarized light is transmitted at a speed greater than that of the vertically polarized light). (b), (c) are setups of Mach-Zehnder and Michelson interferometers. In the Michelson interferometer, the difference of the transmission speed according to the transmission axis in the PMF is automatically compensated by FMs that reflect the input light to orthogonally rotated output light. Therefore, the phase reference frames of Alice and Bob are naturally identical regardless of the polarization states of the optical pulse signals. Whereas, since the MZI does not have such a compensation function, the optical pulses of Alice and Bob have non-identical phase reference frames in the MZI. BS: beam splitter; DL: delay line; FM: Faraday mirror.

array (FPGA), p-i-n photodiode (PIN PD), digital-to-analog converter (DAC), and BS. The FPGA counts the electrical output signals of the PIN PD, which detects optical output signals of the IM. If the measured count per train is not equal to the pulse number of a train, the FPGA changes the DC control voltage until they are equal. To verify this feedback system, we measured the variation of the IM output power for approximately 9 hours. As shown in Fig. 2, the feedback system stably maintains the output power of the IM, whereas the output power without the feedback varies greatly up to 30% error.

B. OPTICAL PATH-LENGTH SELF-COMPENSATION SYSTEM

To implement a fiber-based QKD, it is essential to compensate for the variation in the effective fiber length caused by temperature changes. By this effective length variation, the photon arrival time is changed up to approximately 18 ns in one day for a 25 km quantum channel [39]. Therefore, even if the gate pulse timing of the SPD is set to cover the photon arrival time in the initial stage, it cannot be maintained for a long time. To avoid this timing problem, we applied the optical path-length self-compensation system.

In this system, when the measured single photon count rate is lower than a threshold value, the driving timings of Charlie's IMs which generates optical pulse trains for Alice and Bob are automatically adjusted, so that the count rate is over the threshold value again. By repeating this process, the QKD system can cope with temperature changes.

To confirm whether this self-compensation system can be operated appropriately in response to the rapid change in the effective fiber length, we measured the SPD count rate in an environment where the 25 km quantum channel of Alice was enclosed in a heating cabinet. The temperature of the heating cabinet was rapidly changed from 30 °C to 60 °C. Since the effective optical fiber length becomes longer with the increase in ambient temperature, the gate timing cannot cover the photon arrival timing. In other words, photons arrive after SPD gate timings. Consequently, the SPD count rate falls below the threshold value as shown in Fig. 3, but it is recovered again by the self-compensation system. In this case, because the photon arrival timing is delayed by an increase in the effective length, count recovery is achieved by reducing the time delay of the driving pulses for Charlie's IMs. By checking the results of this experiment, we can see that the self-compensation system works properly.

C. MICHELSON INTERFEROMETER

Since Charlie consists of only the PMF-coupled devices due to implementation of the PDM, we used the Michelson interferometer instead of Mach-Zehnder interferometer (MZI) in order to generate the time-bin phase basis. Specifically, the speed of light in a PMF is determined by the polarization (see Fig. 4 (a)). Therefore, Even though two optical pulses of Alice and Bob, which are orthogonally polarized with respect to each other, can pass through the same interferometer, they have non-identical phase reference frames in the MZI that cannot compensate for the difference in transmission speed, as shown in Fig. 4 (b). This leads to further error in the X basis. Whereas, in a Michelson interferometer (Fig. 4 (c)), since the polarization of the output light is orthogonal to the input light by FMs, the difference in transmission speed according to polarization can be automatically compensated. Therefore, the phase reference frames of Alice and Bob are naturally identical, even though Alice and Bob have different transmission axes according to the polarization states. Consequently, the variation of $|\Psi^{-}\rangle$ that leads to the X basis error can be solved as shown in Fig. 5. The $|\Psi^{-}\rangle$ count rate of the Michelson interferometer is maintained stably, unlike the one for the MZI.

D. QKD SYSTEM OPERATION

To confirm the performance of our setup with the above techniques, we measured the quantum bit error rates (QBERs) and SPD count rates for several hours in 25 km quantum channels without temperature controls. When the mean photon number was 0.5, we achieved the average QBERs as 2.4% (Z basis) and 28% (X basis) and the key generation rate as 6.25 × 10^{-6} bits per pulse (see Table 1 for more information). As shown in Fig. 6, QBERs and count rates were maintained stably for that time. Furthermore, from the

TABLE 1. Experimental conditions and results.

Condition	Quantum efficiency	10%	Dead time	1 µs
	Gate width	3 ns	Laser width	3 ns
	Quantum channel	25 km	Storage line	15 km
	Repetition rate	1 MHz	Wavelength	1550 nm
Result	QBER (avg.)		Key rate	
	Z basis	2.4%	6.25×10^{-6} bits per pulse	
	X basis	28%		

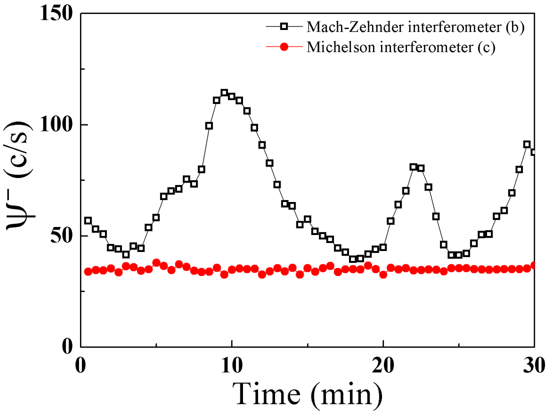

FIGURE 5. Comparison of $|\Psi^-\rangle$ count rates of two interferometers. The count rate in the Michelson interferometer is much more stable than that in the MZI. In the MZI, the count rate changes greatly according to the difference in the phase reference frames of Alice and Bob.

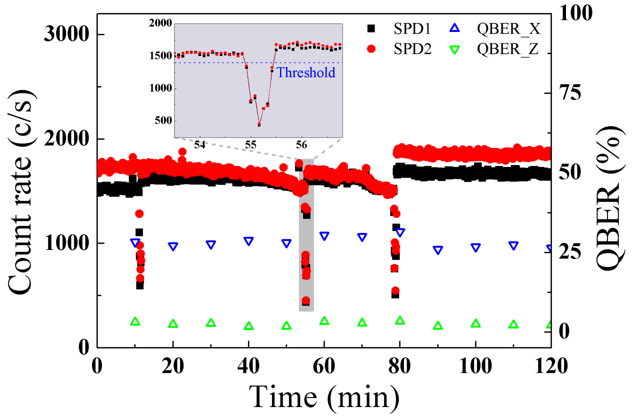

FIGURE 6. Results of validation of the performance of the QKD. The stabilities of QBERs verify the feasibility of our experimental setup. The inset shows that the optical path-length self-compensation system can maintain the count rates over the threshold value (1400 c/s). Since the quantum channels were under room temperature conditions in this experiment, the occurrence frequency of the self-compensation system was less than that in Fig. 3. QBER_Z: Z basis QBER; QBER_X: X basis QBER; SPD1: SPD1 count rate; SPD2: SPD2 count rate.

results of this experiment, we can verify that the feedback and self-compensation systems can operate properly.

IV. CONCLUSION

In this study, we have implemented a practical plug-and-play MDI QKD system. By applying the plug-and-play architecture, we could implement our setup using minimal number of active controllers. Moreover, our setup can not only be implemented independently of whether the quantum channel lengths of Alice and Bob are symmetric or asymmetric via our unique technique "PDM" but also cope with the ambient-temperature-changing environment by using the "optical path-length self-compensation" technique that is essential for a fiber-based QKD system.

We have proved the feasibility from the experimental results of 2.4% (Z basis) and 28% (X basis) as average QBERs and 6.25×10^{-6} bits per pulse as the key generation rate. Given that the theoretical QBERs are 0% for the Z basis and 25% for the X basis when a laser is used as the light source (as described in [35] and [37]), the actual QBERs of both bases are under 3%. Moreover, the functional aspect of the proposed setup is also verified by experimentally validating the functionality of our key methods.

Based on our experimental results, we believe that our practical architecture will offer even more benefits if it is implemented in a real-deployed fiber network environment.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[3] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul. 2000.

[5] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[6] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 73, p. 022320, Feb. 2006.

[7] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A, Gen. Phys.*, vol. 74, p. 022313, Aug. 2006.

[8] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 75, p. 032314, Mar. 2007.

[9] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 78, p. 042333, Oct. 2008.

[10] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. (2010). "Full-field implementation of a perfect eavesdropper on a quantum cryptography system." [Online]. Available: https://arxiv.org/abs/1011.0105

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photon.*, vol. 4, pp. 686–689, Aug. 2010.

[12] F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," *New J. Phys.*, vol. 12, p. 113026, Nov. 2010.

[13] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system," *Phys. Rev. A, Gen. Phys.*, vol. 83, p. 062331, Jun. 2011.

[14] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors," *New J. Phys.*, vol. 13, p. 073024, Jul. 2011.

[15] N. Jain *et al.*, "Device calibration impacts security of quantum key distribution," *Phys. Rev. Lett.*, vol. 107, p. 110501, Sep. 2011.

[16] J.-Z. Huang *et al.*, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Phys. Rev. A, Gen. Phys.*, vol. 87, p. 062329, Jun. 2013.

[17] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing models for optical measurements in quantum communication," *Phys. Rev. Lett.*, vol. 101, no. 1, p. 093601, 2008.

[18] T. Tsurumaru and K. Tamaki, "Security proof for quantum-key-distribution systems with threshold detectors," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 3, p. 032302, 2008.

[19] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun. 2007.

[20] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," *Phys. Rev. Lett.*, vol. 105, p. 070501, Aug. 2010.

[21] L. Masanes, S. Pironio, and A. Acín. (2010). "Secure device-independent quantum key distribution with causally independent measurement devices." [Online]. Available: https://arxiv.org/abs/1009.1567

[22] M. Curty and T. Moroder, "Heralded-qubit amplifiers for practical device-independent quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 84, p. 010304, Jul. 2011.

[23] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the blinding attack in QKD," *Nature Photon.*, vol. 4, pp. 800–801, Dec. 2010.

[24] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems," *Opt. Express*, vol. 20, no. 17, pp. 18911–18924, 2012.

[25] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 87, p. 062313, Jun. 2013.

[26] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 192–196, May 2015.

[27] M. S. Lee *et al.*, "Countermeasure against blinding attacks on low-noise detectors with a background-noise-cancellation scheme," *Phys. Rev. A, Gen. Phys.*, vol. 94, p. 062321, Dec. 2016.

[28] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar. 2012.

[29] Y. Liu *et al.*, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep. 2013.

[30] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.*, vol. 113, p. 190501, Nov. 2014.

[31] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, p. 130501, Sep. 2013.

[32] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 112, p. 190503, May 2014.

[33] A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, pp. 793–795, Aug. 1998.

[34] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New J. Phys.*, vol. 4, p. 41, Jul. 2002.

[35] Y. Choi *et al.*, "Plug-and-play measurement-device-independent quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 93, p. 032319, Mar. 2016.

[36] F. Xu, "Measurement-device-independent quantum communication with an untrusted source," *Phys. Rev. A, Gen. Phys.*, vol. 92, p. 012333, Jul. 2015.

[37] G.-Z. Tang, S.-H. Sun, F. Xu, H. Chen, C.-Y. Li, and L.-M. Liang, "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 94, p. 032326, Sep. 2016.

[38] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 86, p. 062319, Dec. 2012.

[39] B. K. Park, M. S. Lee, M. K. Woo, Y.-S. Kim, S.-W. Han, and S. Moon, "QKD system with fast active optical path length compensation," *Sci. China Phys., Mech. Astron.*, vol. 60, p. 060311, Jun. 2017.

[40] N. Miyazaki, K. Ooizumi, T. Hara, M. Yamada, H. Nagata, and T. Sakane, "$\mathrm{LiNbO_3}$ optical intensity modulator packaged with monitor photodiode," *IEEE Photon. Technol. Lett.*, vol. 13, no. 5, pp. 442–444, May 2001.

[41] C. R. Yang, W. Y. Hwang, H. Park, H. H. Hong, and S. G. Han, "Off-level sampling method for bias stabilisation of electro-optic Mach-Zehnder modulator," *Electron. Lett.*, vol. 35, no. 7, pp. 590–591, Apr. 1999.

CHANG HOON PARK received the B.S. degree in electrical, electronics and communication engineering from the Korea University of Technology and Education, Cheonan, South Korea, in 2016. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Ajou University, Suwon, South Korea. He is a Student Researcher with the Korea Institute of Science and Technology, Seoul, South Korea. His research interests include quantum key distribution and quantum information.

MIN KI WOO received the B.S. degree in control and instrumentation engineering from Korea University, South Korea, in 2012, and the M.S. degree in information and electronics engineering from Ajou University, Suwon, South Korea, in 2017, where he is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering.

BYUNG KWON PARK received the B.S. degree in electrical, electronics and communication engineering from the Korea University of Technology and Education, Cheonan, South Korea, in 2012. He is currently pursuing the Ph.D. degree with the Division of Nano & Information Technology, University of Science and Technology. He is a Student Researcher with the Center for Quantum Information, Korea Institute of Science and Technology, Seoul, South Korea. His research interests include quantum key distribution, quantum information, and quantum authentication.

MIN SOO LEE received the B.S. degree in electronics from Korea Polytechnic University, South Korea, in 2008, and the M.S. and Ph.D. degrees in quantum cryptography from the University of Science and Technology, South Korea, in 2017. He currently holds a post-doctoral position with the Korea Institute of Science and Technology. His current research interests include quantum key distribution system, quantum cryptography, single photon detection, and quantum network.

YONG-SU KIM received the B.S. degree in physics from Yonsei University, Seoul, South Korea, in 2006, and the M.S. and Ph.D. degrees in physics from POSTECH, Pohang, South Korea, in 2007 and 2012, respectively. He is currently a Senior Researcher with the Korea Institute of Science and Technology. His research interests include quantum optics and quantum information.

YOUNG-WOOK CHO received the B.S. and Ph.D. degrees in physics from the Pohang University of Science and Technology, Pohang, South Korea, in 2007 and 2014, respectively. He is currently a Senior Researcher with the Korea Institute of Science and Technology. His research interests include photonic quantum information and coherent light–matter interaction.

SANGIN KIM received the B.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 1992, and the M.S. and Ph.D. degrees in electrical engineering from the University of Minnesota, Minneapolis-St. Paul, MN, USA, in 1995 and 1997, respectively. He is currently a Professor with the Department of Electrical and Computer Engineering, Ajou University, Suwon, South Korea. His research interests include nanophotonics, nanolasers, guided wave optics, plasmonics, photonic integrated circuits, and quantum information.

SANG-WOOK HAN received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 1999, 2001, and 2006, respectively. From 2006 to 2009, he was with Pixelplus Corporation, South Korea. From 2009 to 2012, he was a Research Staff with the Samsung Advanced Institute of Technology, South Korea, where he engaged in researching high sensitivity CMOS imagers and photon counting X-ray detector. In 2012, he joined the Korea Institute of Science and Technology, Seoul, South Korea. His research interests are in quantum information, especially quantum key distribution system, random number generator, quantum signature, single photon detector, and quantum computing.

SUNG MOON received the B.S. and M.S. degrees in material engineering and the Ph.D. degree in semiconductor engineering from Yonsei University, Seoul, South Korea, in 1986, 1988, and 1994, respectively. He is currently the Director of the Center for Quantum Information, Korea Institute of Science and Technology, Seoul. His current research interests include quantum cryptography, integrated quantum photonics, and quantum devices.