IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 5, 2020, accepted October 16, 2020, date of publication October 22, 2020, date of current version November 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3032992

One to Many QKD Network System Using Polarization-Wavelength Division Multiplexing

MIN KI WOO[1], BYUNG KWON PARK[2,3], YONG-SU KIM[2,3], YOUNG-WOOK CHO[2], HOJOONG JUNG[2], HYANG-TAG LIM[2], SANGIN KIM[1], SUNG MOON[2], AND SANG-WOOK HAN[2,3]

[1]Department of Electrical and Computer Engineering, Ajou University, Suwon 16499, South Korea
[2]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, South Korea
[3]Division of Nano and Information Technology, KIST 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 Korea Institute of Science and Technology under Grant 2E30620; in part by the National Research Foundation of Korea under Grant 2019 M3E4A107866011, Grant 2019M3E4A1079777, and Grant 2019R1A2C2 006381; in part by the Institute for Information and Communications Technology Promotion under Grant 2020-0-00947 and Grant 2020-0-00972.

ABSTRACT The quantum key distribution (QKD) research, which is drawing attention as the next secure communication, is actively expanding from point to point system to network architecture. In QKD network system, it is important to increase the number of users who can securely communicate. Up to date, a wavelength division multiplexing (WDM) architecture has successfully expanded the number of channels without significant system loss, but there is a limitation of increasing channels considering the range of telecommunication wavelength and crosstalk noise, etc. In this article, we propose a polarizing division method that increases user channels independently of wavelengths. The proposed architecture can increase the number of wavelength multiplexed channels by a multiple of the polarization number. We identify the issues in the QKD network system that may occur when using polarization and wavelengths simultaneously, then provide solutions and optimize the system operation accordingly. Finally, we describe a field test result of a one to many QKD network system that shows successful key exchange with 3% QBER.

INDEX TERMS Quantum cryptography, quantum key distribution network, polarization division multiplexing.

I. INTRODUCTION

The development of quantum computer research has recently shown significant development and poses a major threat to modern cryptographic technology based on mathematical complexity [1]–[4]. It has been reported that the RSA method, the most widely used cryptographic technology, can be hacked using Shor's algorithm [5], [6]. As a result, many researchers are focusing on cryptographic research that can survive the era of quantum computers. This research can be divided into two major types. The first is post quantum cryptography (PQC) research that secures safety based on complex mathematical problems that cannot be solved with currently known quantum algorithms. Although PQC has the advantage of being able to operate in the current classical computing environment, there is a limit to its ability to ensure safety against upcoming novel quantum algorithms. Conversely, QKD, the second type of study, has the great advantage of theoretically enabling secure cryptographic communication because it is based on physical law, rather than mathematical complexity [7], [8].

QKD is the first application to be commercialized among quantum technology [9], [10]. However, due to several major technological issues, it has not yet been prevalent technology. Examples include issues of distance restriction [11], [12], miniaturization for low cost [13], stable system operation [14], standardization [15], and quantum hacking [16], [17]. Especially, research on QKD networks, which enable quantum cryptography communication among multiple users, is also an important subject and has been underway for a long time [18]–[20].

The associate editor coordinating the review of this manuscript and approving it for publication was Bijoy chand Chand Chatterjee.

Unlike classical optical networks, QKD networks should be configured under optically transparent conditions. The loss of network components, which may not be problematic in classical networks, has a significant effect on quantum signal transmission because they use extremely weak signals, under single photon level. In addition, noise such as crosstalk becomes a more serious problem when implementing QKD networks than when implementing classical networks. Nevertheless, efforts have been made to implement quantum cryptographic networks. These have evolved from point to point communications to one to many communications and eventually to many to many communications, using underlying models from classical communications networks, where many prior studies had already been conducted [18]–[21]. Initially, beam splitter (BS) based passive optical QKD network (PON) methods used in classical telecommunication networks were proposed [20]. The problem with these methods is that the channel attenuation rate continues to increase as the number of channels increases from several to dozens, thereby lowering the quantum signal transmission rate significantly. This decreases the generation of keys and the signal to noise ratio.

To complement this, a network using wavelength division multiplexing (WDM), which divides channels by wavelength, has been presented [21]. The WDM method has a constant attenuation rate of the device despite the increase in the number of channels, unlike the BS method. WDM was found suitable for loss sensitive quantum cryptographic networks because the number of channels provided by a single arrayed waveguide grating (AWG) element can increase the channel without any additional loss. Additionally, Shields Group's study suggested that a QKD network can be implemented with only a pair of single photodetectors (SPDs) by additionally using time division multiplexing (TDM) methods, enabling efficient, economical system implementation [22].

The WDM method, using AWG, can successfully implement a one to many QKD network, but it has limitations when extending the number of channels above a certain level considering the number of channels of commercially available low cost AWG device and crosstalk noise. In applications such as data center, where it is important to increase the number of users who can securely communicate with one server, it is necessary to introduce an additional division method.

In this article, we propose a new structure that can support dramatically more channels by introducing new division method that can branch out regardless of wavelength. The number of channels can be expanded to multiples of existing wavelength numbers by taking advantage of polarizing characteristics that can branch light signals regardless of the wavelength. The new QKD network architecture using polarization division multiplexing (PDM) is presented. Its problems are analyzed and experimentally investigated to solve problems arising from the proposed architecture.

Chapter 2 describes the proposed QKD network system structure. Chapter 3 presents experimental results using the implemented system in the actual environment. Chapter 4 summarizes our work.

II. QUANTUM KEY DISTRIBUTION NETWORK SYSTEM

In implementing the one to many QKD network, we use PDM-WDM to expand the channel number. Additionally, TDM is used in parallel, requiring only one pair of SPDs, which is an advantage, as SPDs are difficult to control and expensive to use in QKD systems. Thus, the overall network structure is PDM-WDM-TDM. The basic architecture of the server and user systems follows a plug and play (PnP) structure [23]. The PnP structure has many advantages when implementing QKD networks. At first, many user systems can be implemented relatively cheaply and operated easily. And PnP operation is also reliable enough, in principle, to be adopted by many commercial systems. Furthermore, with PnP, complex controls that use weak light signals can be implemented efficiently within a single server. The proposed PDM-WDM-TDM QKD network system is shown in Fig. 1.

A. PLUG AND PLAY QKD NETWORK SYSTEM ARCHITECTURE

The PnP QKD system transmits a strong signal from the server (Bob), attenuates the signal to the level of a single photon at the client (Alice), then encodes and retransmits it, after which, Bob decodes and detects the signal. This method is structured to reciprocate a Mach–Zehnder interferometer inside Bob. Therefore, unlike CV-QKD or one-way structures [24] that require phase matching and phase stabilization over time by constructing Mach–Zehnder interferometers for both Alice and Bob, there is no need for a separate operation to stabilize the interferometer.

And, in a typical single mode fiber (SMF) channel, the reciprocating signal structure cancels the random variation in the signal's polarizing characteristics. In other words, the polarization change during transmission via optical fiber is automatically compensated because the pulse passes though the same channel twice in reverse order in PnP QKD. In these conditions, the Faraday mirror (FM) implemented in Alice orthogonally reflects the polarization of the incoming signal. Using this characteristic, the signal arriving at Bob can be made orthogonal to the transmission from the initial Bob. Thus, it is possible to control the beam path through a polarization beam splitter (PBS). A PBS is a passive element, rather than an active element needing complicated systems for interference path control in Bob. This enables the PDM to be implemented with only passive elements. When a PBS used for interference path control is used as a 2 × 2, transmission through different paths is possible depending on the initial polarization, which completes the PDM without an active element. In the proposed configuration, PBS can be also suitable for use as a quantum cryptographic network system for applications in which system loss has a significant effect on performance because it has less loss than general BS and WDM undergo when increasing the number of channels.

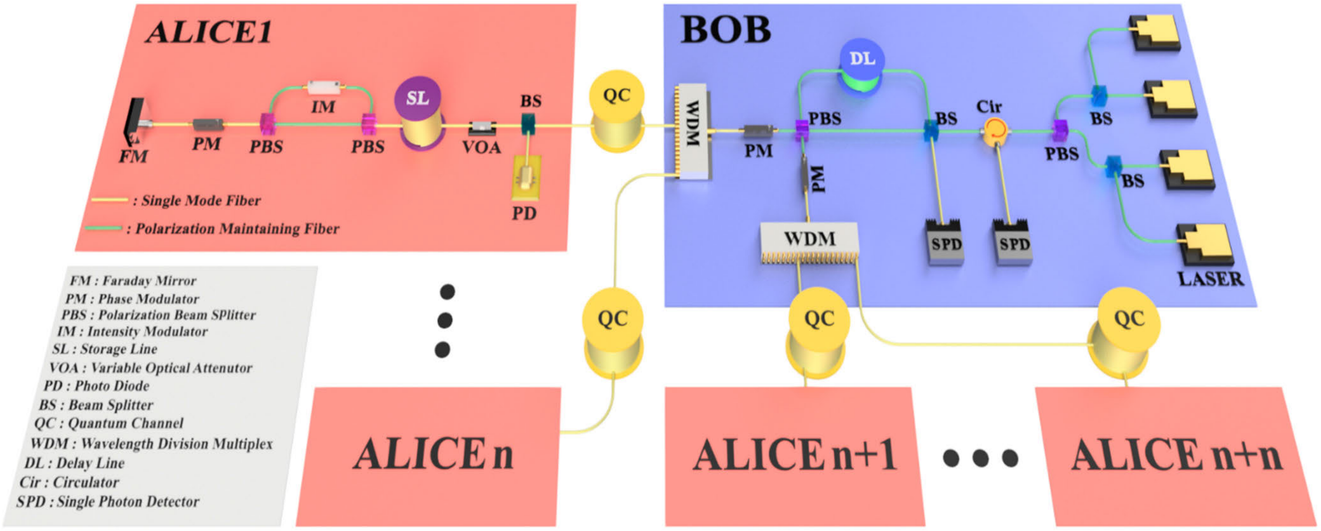

FIGURE 1. One to many PDM-WDM-TDM QKD network system architecture.

B. SERVER (BOB)

Unlike the one-way structure, the PnP architecture server system (Bob) has both a laser system that generates a light signal and an SPD system that detects a quantum signal. The laser system consists of a set of vertical and horizontal polarization laser modules to implement the PDM. Each laser module set consists of a laser with N/2 different wavelengths in the C band, for the WDM. After combining lasers with different wavelengths through the BS, two laser module sets with different polarizations are combined into PBS. This part uses a polarization maintaining fiber (PMF) because the polarization must be kept constant. Each laser is independently controlled regardless of the other's signals using precision timing pulse signals implemented using the FPGA. Therefore, it is possible to adjust the arrival time variation due to operation condition such as different wavelengths or environmental temperature [25].

The SPD system is composed of a pair of avalanche photodiodes (APD) and a control unit for APD control. APD is an expensive device, requiring complicated control of temperature, bias, gate, and other parameters, making it difficult to use. To minimize the requirements, the QKD network was constructed with only two APDs by measuring incoming signals with time separation using TDM. One of the APDs is connected to one of the output ports of the BS, where interference occurs in Bob's optical system. The other is connected to the output port of the circulator connected to the other output port of the BS. At this time, the BS-APD path and BS-C-APD path are made as close in length as possible. If the length of the APDs' reach paths are different, the time difference between each signal reaching the APD will also change, depending on the wavelength and polarizing changes. The change in the arrival time of the signal at the APD may degrade the efficiency of the APD detection set at the maximum at a specific time, degrading system performance. The SPD system, like the laser system, is controlled by a precision timing pulse signal implemented using Bob's FPGA. This enables efficient control by controlling both the generation and detection of signals through one of Bob's master clocks.

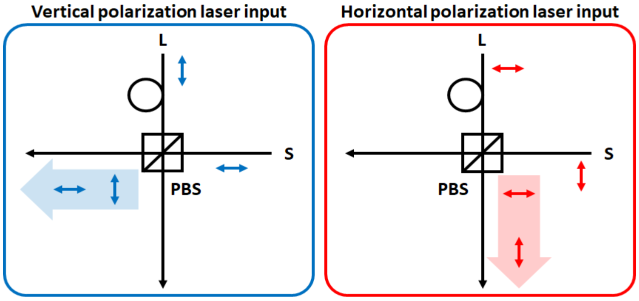
Vertical polarization laser input
L
S
PBS
Horizontal polarization laser input
L
S
PBS

FIGURE 2. Propagation of the polarization light according to the Initial.

The optical system uses a time bin encoding method that implements a Mach-Zehnder interferometer. As mentioned above, this interferometer is configured to enable PDM using 2 × 2 PBS. Of the superposition signals from the beam splitter (BS), the signal input to the PBS through the delay line (D. L) is called Long (L), and the signal directly input to the PBS is called short (S). The signal coming to the S path is orthogonally changed. The signal transmitted from the vertical laser set is split at the BS into the S and L paths. The signal coming from the L path is directly in PBS, while the signal coming from the S path is horizontally changed and input to PBS. As shown in Fig. 2, both superposition signals go to one output port (V) of PBS. The signals transmitted from the horizontal laser, set in the same manner, are sent to the other output port (H).

The optical system's phase modulator (PM) is located after the PBS, not within the Mach-Zehnder interferometer. Typical PMs based on LiNbO3, used in most practical implementations, operate normally only in a specific polarization. When using PDM in the system, both vertical and horizontal polarization signals are input to each Mach–Zehnder interferometer path. If the PM is installed inside the interferometer, the PM may not operate correctly due to polarization changes. For this reason, two PMs are installed outside the Mach-Zehnder interferometer, as shown in Fig. 1. In addition, the fiber that connects each element of this path to maintain polarization uses PMF. SMF, commonly used elsewhere, is unsuitable in this role, as it is difficult to maintain polarization during changes in the external environment. Finally, the AWG device is connected to the back of the PM to implement the PDM-WDM network. This path is composed of a typical SMF because even if the AWG element is newly connected, causing polarization changes, it will not affect the PDM, due to the characteristics of PnP.

C. CLIENTS (ALICES)

Alice, the client, uses implementation like that used in the general PnP QKD system [23]. In addition, we have applied a structure that uses a decoy protocol. The decoy protocol is technologies to ensure the security of QKD and can be implemented by varying the intensity of quantum signals and decoy signals. Commercially produced intensity modulators (IM), which are used to produce decoy signals, are mainly made of LiNbO3 materials. As in the PM described above, the IM also has polarization dependency. The polarization reaching Alice along the quantum channel (QC) has randomness according to the channel state. There is a way to install a polarization controller in Alice, but this is very inefficient. Therefore, we implemented an additional interferometer inside Alice [26] to make the IM work properly. As shown in Fig. 3, two PBSs, and the existing FM, were combined to complete the interferometer. The IM is located between the two PBSs, and the added interferometer path uses the PMF to maintain polarization. The path through the IM always passes only vertical polarization, so the IM can operate properly. The PM and FM are connected to each other as closely as possible, and the signal is configured for phase modulation over two times [27]. With the proposed structure, even if random polarization reaches Alice, phase and intensity can be controlled stably.

III. EXPERIMENTS

We implemented the proposed PDM-WDM-TDM QKD network system and then connected the Alices to each channel to conduct an experiment. Several issues may arise when operating the implemented network system, such as the difference in fiber transmission speeds and changes in the characteristics of photoelectric devices. This occurs because the polarization and wavelength are different for each channel of the PDM-WDM.

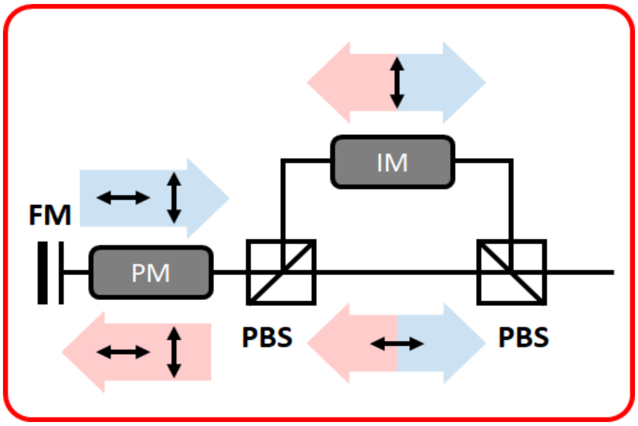

FIGURE 3. Alice interferometer scheme for decoy protocol. To passively compensate polarization drift, we use two PBS and intensity modulator. The red and blue arrows indicate the input and output from the FM.

First, the change in arrival time in the storage line (SL) as a function of the change in wavelength and polarization was measured. In the PnP QKD system, part of the signal is detected by the PD and used as a synchronization signal. The photoelectric elements to be controlled by this synchronization signal are connected after the SL. To control the photoelectric device, it is important to measure the time it takes for the signal to pass through the SL. Theoretically, the time taken for the optical signal to pass through the fiber can be calculated using the refractive index value. The light velocity in a material with refractive index n is v = c/n.

When the length of the material is L, the transmission time of the optical signal is $t = L/v$, or alternatively $t = Ln/c$. Thus, the transmission time can be determined from the n value. However, the fiber is subject to dispersion; n varies as a function of wavelength. When 1550 nm wavelength light passes through, the fiber has an approximate index of 1.444, but the index is slightly different for the 32 wavelengths in the C band. We allocated Ch1 ~ Ch32 to ITU channel 57 ~ 22 (1532.11 ~ 1559.44 nm) except 53, 48, 35, 30 [28]. We used those wavelengths for WDM, which indexes are slightly different from that. At short distances, this difference is not noticeable, but it presents problems in a 50 km SL. The measured value of the transmission time of the optical signal passing through an actual SL is shown in Fig. 4. One can see that there is an arrival time difference of approximately 20 ns between 1532.11 nm (Ch1, ITU57) and 1559.44 nm (Ch32, ITU22). This result shows that an error may occur when operating a fixed delay time as one value for Alice's control of each photoelectric element. Therefore, each channel must be operated according to the appropriate delay time.

In contrast, variations in index due to polarization are expected to be minimal, since the SL is composed of SMF, which theoretically has no characteristic changes due to polarization. Since the core is not a perfect circle, there may be changes in characteristics due to polarization, but because of experiments using signals from 33 to 64 channels, it was confirmed that the difference in arrival time due to polarization is negligible.

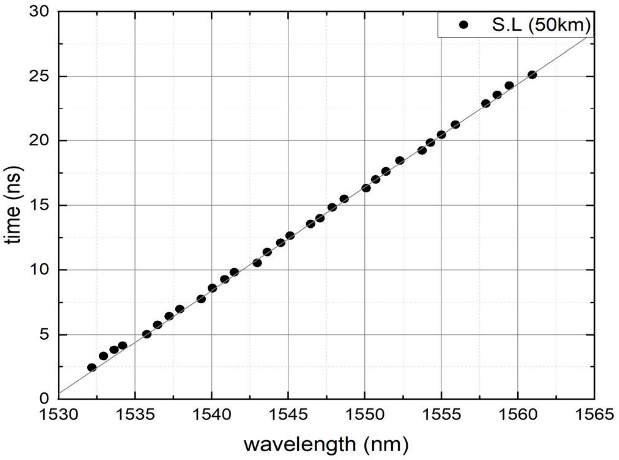

FIGURE 4. The time for the quantum signal to pass through the storage line. (offset : 235170 ns).

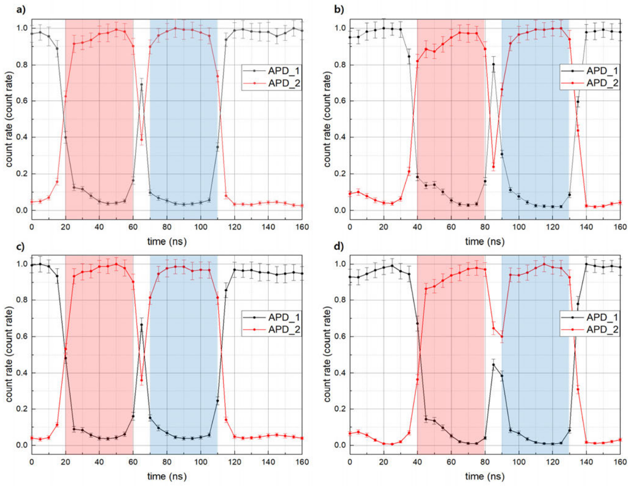

FIGURE 5. Normalized count rate versus timing delay of the Alice PM modulation. The red area indicates that interference result of the S-signal and the blue area indicates that interference result of the L-signal. a) ch1, 1532.11 nm, V-polarization, b) ch32, 1559.44 nm, V-polarization, c) ch33, 1532.11 nm, H-polarization, d) ch64, 1559.44 nm, H-polarization.

Second, we conducted an experiment to determine the exact operating time and voltage of the Alice PM. The interference result represented by the count of APD_1, APD_2, was checked while changing the time at which a constant voltage was driven in Alice PM. The applied voltage was 2.5 V, the time duration was approximately 40 ns, and the channels used were Ch1 and Ch32, which have the largest wavelength difference. Ch33 and Ch64 were also used to test the results relative to the polarization. The results are shown in Fig. 5.

The experiment was conducted just after the signal passed out from SL. The Alice PM in Ch1 operates normally in the delay interval from 20 ns to 60 ns for signal S, and 70 ns to 110 ns for signal L. Thus, the S and L signals of the time bin signal are modulated to the PM. The PM in Ch32 operates normally in the delay interval from 40 ns to 80 ns and 90 ns to 130 ns, and there is a difference of 20 ns from Ch1. These results show that if the control time of the Alice PM is fixed with a delay of 80 ns, the signal can be normally encoded in Ch1, but the signal is not encoded in Ch32. In this case, even if everything except the control time is set normally, an error may occur during QKD operation. In contrast, the Alice PM modulation section on Ch33 is 20–60 ns and 70–110 ns, which is the same as the result of Channel 1. Additionally, the 64th channel has a modulation section of 40–80 ns and 90–130 ns, which is the same as Channel 32. This result indicates that the change in polarization, as shown in Fig. 4, does not affect the control time, and that the control time needs to be adjusted according to the wavelength.

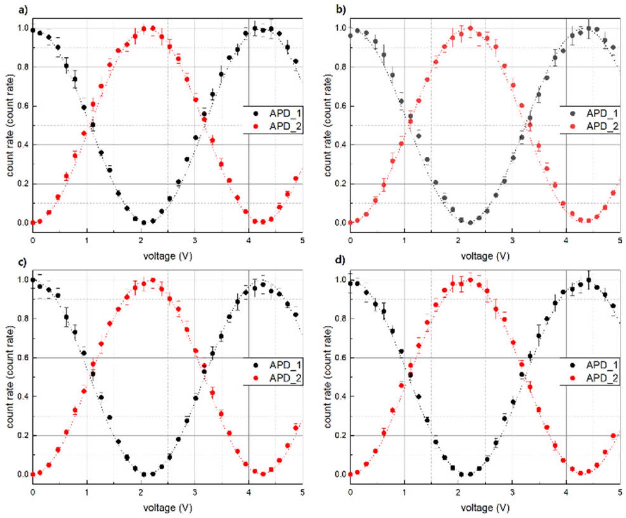

FIGURE 6. Interference results according to voltage of the Alice PM modulation. a) ch1, 1532.11 nm, V-polarization, b) ch32, 1559.44 nm, V-polarization, c) ch33, 1532.11 nm, H-polarization, d) ch64, 1559.44 nm, H-polarization.

Based on the results of the previous experiments, the Alice PM was tested to measure its operating voltage. The interference result measured by changing the driving voltage of the Alice PM from 0 V to 5 V is shown in Fig. 6. As a result of interference, it was confirmed that the Vpi value of the Alice PM is 2.12 V at Ch1 and 2.16 V at Ch32 and that the Vpi value varies depending on the wavelength. The Alice PM is composed of characteristics that operate irrespective of polarization, so the Vpi values are 2.12 V at Ch33 and 2.16 V at Ch64, the same as at Ch1 and Ch32, respectively. This means that the Vpi value of the Alice PM is unrelated to polarization, but it changes with the wavelength. If the Vpi value is fixed at 2.12 V, the optimum value for Ch1, only 98.15% of the required Vpi value will be applied at Ch32. As shown in Table 1, assuming that Bob PM performs bipolar modulation normally, keys are generated at {Alice(0), Bob(0)}, {Alice(π), Bob(0)}, {Alice($\pi/2$), Bob($\pi/2$)}, {Alice($\pi/2$), Bob($\pi/2$)} where phase modulation error rates of 0, 1.85%, 0.9% and 2.8% were measured respectively. These phase errors are directly related to the quantum signal errors, so it is necessary to find and use the appropriate Vpi for each channel.

TABLE 1. Interferometer results for Ch32 when using Ch1's Vpi

	0	π/2	π	3π/2
0(Bob)	0 π	0.491 π	0.9815 π	1.472 π
π/2(Bob)	-0.5 π	-0.009 π	0.4815 π	0.972 π

a) Sifted key is generated when Alice and Bob choose identical basis {Alice(0), Bob(0)}, {Alice(π), Bob(0)}, {Alice(π/2), Bob(π/2)}, and {Alice(3π/2), Bob(π/2)}.

Third, we tested the operating characteristics of the Bob PM under differing polarizations and wavelengths. Bob implements TDM by setting the time division based on the time when quantum key signals from each channel reach the SPD. The time bins for each channel are allocated for having the same time internal, and therefore the time to reach the Bob PM may be different because the transmission time from the Bob PM to the SPD may be different. Bob consists of PMFs, which can cause transmission time differences depending on polarization. However, the distance difference between the SPD and Bob PM is not very large, no more than several tens of meters. Thus, the difference in arrival time caused by polarization or wavelength can be neglected. Therefore, only the characteristics of the Bob PM were measured, based on the change in the driving signal. The interference result measured by changing the driving voltage of Bob PM from 0 V to 3.6 V at the correct time for each channel is shown in Fig. 7. Vpi was found to be 3.4 V at Ch1 and 3.46 V at Ch32. As with the Alice PM, Bob PM also has a wavelength dependent driving voltage. Ch33 and Ch64 were driven at 3.62 V and 3.68 V, respectively, results different from those of Ch1 and Ch32. This result is not due to the difference in polarization, but because the two PMs have different Vpi values. If the Bob PM is also fixed and used as the Vpi value for a specific channel, as in Alice's result, an error value of up to 2% occurs. In the case of the Bob PM, there is an additional difficulty in changing the phase of various wavelengths coming from multiple channels with one device. Ideally, a different PM driving voltage should be applied for each wavelength, but this is impractical to implement. In the BB84 protocol, the modulation of the Bob PM uses only 0 and pi/2. When using a fixed driving voltage, 0 modulation does not cause an error, but pi/2 modulation generates an error value depending on the wavelength. This error can be compensated by controlling the Alice PM. When the error rate of pi/2 modulation in Bob PM is δ, the Alice PM modulation value is not 0, pi/2, pi, 3pi/2, but 0, pi/2 $\times\,\delta$ pi, pi$+$(pi/2 $\times\,\delta$). This can be compensated by modulating by pi/2 $\times\,\delta$ in the Bob PM.

Finally, we implemented a 1 × 4 PDM-WDM-PDM QKD network connecting four Alices considering previous experimental results. The experiment was conducted based on the widely used BB84 protocol. We also used the decoy protocol. The average photon numbers of the key and decoy signals were 0.6, 0.1 and vacuum level, respectively. The detection efficiency of a single photon detector was 15%. The channels used for the experiment were Ch1, Ch32, Ch33 and Ch64. This network system was installed and tested on commercial metropolitan networks in Seoul, Korea. The channels were 5.8 km, 9.9 km, 2.9 km, and 7.7 km long, respectively. The channel loss values were 1.29 dB, 2.23 dB, 1.14 dB, and 1.63 dB, respectively. The attenuation rate was greater than the theoretical value of 0.2dB/km found by experimenting on an actual commercial network. Based on the previous results, the PDM-WDM-TDM QKD network was conducted through appropriate control based on wavelength and polarization. This experiment was conducted for 24 hours and the results are shown in Figure 8. In the test, the sifted key rate is updated once a minute. The QBER represents the error rate of comparing randomly sampled data among the sifted keys of Alice and Bob generated for 1 minute. The QBER is be simply calculated as (the number of error keys) / {(the number of correct keys) + (the number of error keys)}. One point in Figure 8 corresponds to the average rate of the sifted key

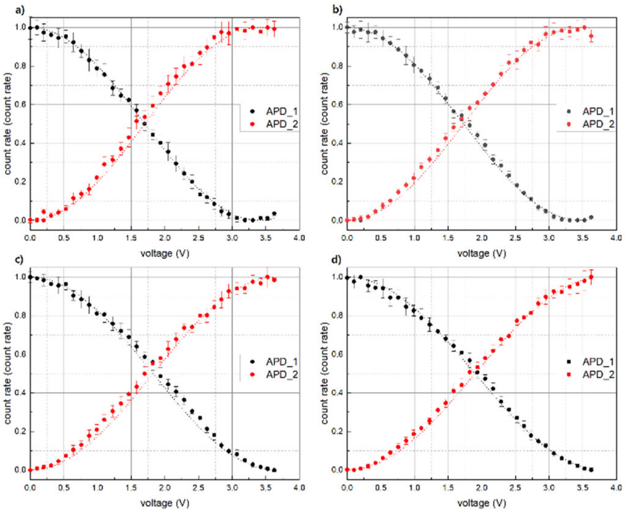

FIGURE 7. Interference result according to voltage of the Bob PM modulation. A) ch1, 1532.11 nm, V-polarization, B) ch32, 1559.44 nm, V-polarization, C) ch33, 1532.11 nm, H-polarization D) ch64, 1559.44 nm, H-polarization.

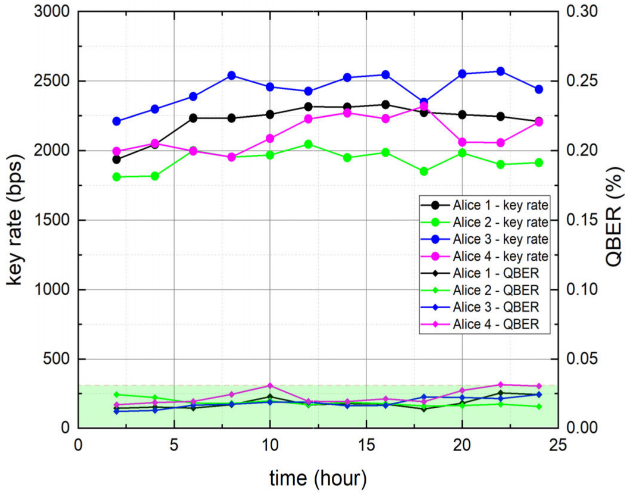

FIGURE 8. Experimental result of the QKD network system in the deployed commercial network.

and the QBER recorded over 2 hours. The average sifted key rates that are shown in upper area were 2.22kbps 1.93kbps, 2.44kbps, and 2.12kbps, respectively, and the QBERs that are shown in bottom area were maintained at less than 3% on all channels. This experimental result shows that proposed PDM-WDM-TDM QKD network architecture can reliably generate a sifted key even in a commercial network.

IV. CONCLUSION

We implemented the PDM-WDM-TDM architecture for the increasing the number of channels only using passive devices, and analyzed issues that may occur during implementation, and verified the proposed architecture experimentally. Problems with the existing WDM method were identified, including the difference in quantum signal transmission speed in the fiber and the changing characteristics of the photoelectric device. These problems were solved by introducing additional control methods. PDM has issues involving the utilization of PMF and photoelectric devices. Thus, polarization related problems involving PDM operation were solved by adjusting the path length from the Bob BS to each detector, installing the Bob PM outside the Mach-Zehnder interferometer, using a PnP type system, and using a new interferometer (Alice). The PDM implemented through these solutions can be a prevalent configuration for implementing QKD networks, as the attenuation generated by increasing channels is minimal. In addition, although there is a disadvantage from giving the PM drive voltage differently for each channel when using TDM, it was solved by adjusting Alice's X basis drive voltage.

Finally, four Alices and one Bob suitable for the proposed PDM-WDM-TDM QKD network were implemented and tested in the field. The experiment was conducted using BB84 and decoy protocol. We selected channels that can test PDM-WDM (Ch1, Ch32, Ch33, Ch64) and succeeded in exchanging cryptographic keys with an average QBER of 3%.In addition, the proposed network architecture can be applicable not only discrete variable QKD but also continuous variable QKD system. Therefore, it is expected to be widely adopted when considering the implementation of QKD network with current prevalent QKD technology.

REFERENCES

[1] [Online]. Available: https://newsroom.intel.com/news/intel-introduces-horse-ridge-enable-commercially-viable-quantum-computers/#gs.7a2x08

[2] [Online]. Available: https://www.ibm.com/quantum-computing/

[3] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[4] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[5] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, Aug. 2014, doi: 10.1038/nphoton.2014.149.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999, doi: 10.1137/s0036144598347011.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.

[8] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[9] [Online]. Available: http://www.qtec.cn/

[10] [Online]. Available: https://www.idquantique.com/

[11] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Jan. 2018, Art. no. 030501, doi: 10.1103/PhysRevLett.120.030501.

[12] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018, doi: 10.1038/s41586-018-0066-6.

[13] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, no. 1, p. 13984, Feb. 2017, doi: 10.1038/ncomms13984.

[14] 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, no. 6, Jun. 2017, doi: 10.1007/s11433-017-9026-8.

[15] W. Weigel and G. Lenhart, "Standardization of quantum key distribution in ETSI," *Wireless Pers. Commun.*, vol. 58, no. 1, pp. 145–157, May 2011, doi: 10.1007/s11277-011-0293-8.

[16] M. S. Lee, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S.-W. Han, and S. Moon, "Quantum hacking on a free-space quantum key distribution system without measuring quantum signals," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 36, no. 3, p. B77, Mar. 2019, doi: 10.1364/josab.36.000b77.

[17] 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, no. 10, pp. 686–689, Oct. 2010, doi: 10.1038/nphoton.2010.214.

[18] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnilall, G. Lepert, A. Sinclair, J.-P. Elbers, A. Lord, and A. Shields, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Opt. Express*, vol. 22, no. 19, pp. 23121–23128, Sep. 2014, doi: 10.1364/OE.22.023121.

[19] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," *J. Lightw. Technol.*, vol. 23, no. 1, p. 268, Jan. 2005. [Online]. Available: http://jlt.osa.org/abstract.cfm?URI=jlt-23-1-268

[20] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, no. 6611, pp. 47–49, Jan. 1997, doi: 10.1038/385047a0.

[21] G. Brassard, F. Bussieres, N. Godbout, and S. Lacroix, *Multiuser Quantum Key Distribution Using Wavelength Division Multiplexing* (Applications of Photonic Technology). Bellingham, WA, USA: SPIE, 2003.

[22] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, Sep. 2013, doi: 10.1038/nature12493.

[23] 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, no. 7, pp. 793–795, 1997, doi: 10.1063/1.118224.

[24] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Single photon interference in 10 km long optical fibre interferometer," *Electron. Lett.*, vol. 29, no. 7, p. 634, 1993, doi: 10.1049/el:19930424.

[25] B. K. Park, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S. Moon, and S.-W. Han, "User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1×N quantum key distribution network system," *Photon. Res.*, vol. 8, no. 3, p. 296, Mar. 2020, doi: 10.1364/prj.377101.

[26] C. H. Park, M. K. Woo, B. K. Park, M. S. Lee, Y.-S. Kim, Y.-W. Cho, S. Kim, S.-W. Han, and S. Moon, "Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing," *IEEE Access*, vol. 6, pp. 58587–58593, 2018, doi: 10.1109/access.2018.2874028.

[27] O. Kwon, M.-S. Lee, M. K. Woo, B. K. Park, I. Y. Kim, Y.-S. Kim, S.-W. Han, and S. Moon, "Characterization of polarization-independent phase modulation method for practical plug and play quantum cryptography," *Laser Phys.*, vol. 25, no. 12, Dec. 2015, Art. no. 125201, doi: 10.1088/1054-660x/25/12/125201.

[28] *Spectral Grids for WDM Applications: DWDM Frequency Grid*, document G. 694.1 Recommendation, International Telecommunications Union, 2012.

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, South Korea, in 2017.

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, and the Ph.D. degree from the Division of Nano and Information Technology, University of Science and Technology, Daejeon, in 2020. He is currently a Researcher with the Korea Institute of Science and Technology (KIST). His research interests include quantum key distribution, quantum information, and quantum authentication.

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 (KIST). 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 (POSTECH), Pohang, South Korea, in 2007 and 2014, respectively. He is currently a Senior Researcher with the Korea Institute of Science and Technology (KIST). His research interests include photonic quantum information and coherent light-matter interaction.

HOJOONG JUNG received the B.S. degree in physics and the M.S. degree in applied physics from Yonsei University, Seoul, South Korea, in 2008 and 2015, respectively, and the Ph.D. degree in electrical engineering from Yale University, New Haven, USA, in 2017. He is currently a Senior Researcher with the Korea Institute of Science and Technology (KIST). His research interests include quantum and nonlinear integrated nanophotonics

HYANG-TAG LIM received the B.S. and Ph.D. degrees in physics from the Pohang University of Science and Technology (POSTECH), Pohang, South Korea, in 2008 and 2015, respectively. He is currently a Senior Researcher with the Korea Institute of Science and Technology (KIST). His research interests include photonic quantum information and strong 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, 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.

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, South Korea. His current research interests include quantum cryptography, integrated quantum photonics, and quantum devices.

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 worked for the Pixelplus Corporation, Gyeonggi, South Korea, where he is working on the development of various CMOS imagers. From 2009 to 2012, he was a Research Staff with the Samsung Advanced Institute of Technology, Gyeonggi, 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 include quantum information, especially quantum key distribution systems, random number generator, quantum signature, single photon detector, and quantum computing.