Research on Plug-and-Play Twin-Field Quantum Key Distribution

Chang Hoon Park
[1]*Center for Quantum Information*
Korea Institute of Science and Technology
Seoul, South Korea
[2]*Department of Electrical and Computer Engineering*
Ajou University
Suwon, South Korea
originalpch@kist.re.kr

Min Ki Woo
Department of Electrical and Computer Engineering
Ajou University
Suwon, South Korea
namdo6sung@hanmail.net

Byung Kwon Park
Center for Quantum Information
Korea Institute of Science and Technology
Seoul, South Korea
bkpark@kist.re.kr

Yong-Su Kim
Center for Quantum Information
Korea Institute of Science and Technology
Seoul, South Korea
yong-su.kim@kist.re.kr

Sangin Kim
Department of Electrical and Computer Engineering
Ajou University
Suwon, South Korea
sangin@ajou.ac.kr

Sang-Wook Han
Center for Quantum Information
Korea Institute of Science and Technology
Seoul, South Korea
swhan@kist.re.kr

***Abstract*—In this paper, we have proposed a plug-and-play twin-field quantum key distribution scheme that has passive mode-matching characteristics of quantum signals and can be operated stably. Also, we have experimentally demonstrated the implementation feasibility of our proposed scheme.**

***Index Terms*—plug-and-play, quantum key distribution, twin-field**

I. Introduction

Quantum key distribution (QKD) is a way for two distant parties to distribute common keys with security based on the law of quantum physics [1]. However, its communication distance is limited by optical channel losses, because quantum signal, extremely attenuated light, cannot be amplified or cloned. Also, the key generation rates of typical QKDs scale linearly with channel transmission [2], [3]. Actually, we have already known attractive methods for breaking the distance limitation such as quantum repeater [4] and quantum memory [5], but it is impractical to implement them with current technologies. So, nobody succeeded in breaking the limitation by applying them to QKDs, before a new QKD protocol, twin-field quantudm key distribution (TF-QKD) was proposed by M. Lucamarini [9]. With the ideal TF-QKD, by using 1st interference, the secure key rate scale can be improved to the square root of the channel transmittance same as the single-repeater QKD. Therefore, the ideal TF-QKD can be implemented at a long distance almost twice as long as traditional QKDs. Many QKD research groups have made efforts to realize it in the real world. But, only a few research groups could implement it [10]–[15], because it is difficult to construct mode-matching systems which are essential for the 1st interference of two different lasers.

In this paper, we have proposed a plug-and-play (P&P) TF-QKD scheme, that can be implemented and operated stably. In our scheme, Alice and Bob can use a single laser as their light sources and minimize the mode-matching systems by applying P&P architecture, that has a property of the round-trip of optical pulses [6]–[8]. Although there are already researches on the P&P TF-QKD, they were a limited verification at a short distance [15] or only a theoretical suggestion [16]. On the other hand, we not only implemented 1st interference of Alice and Bob in the 50 km quantum channel but also obtained a high visibility of average 98 %, which is enough to demonstrate the implementation feasibility of the proposed architecture. And we discovered a new issue of P&P TF-QKD scheme that was not mentioned in the previous two articles [15], [16]. See Sec. III for more details about this issue.

II. Proposed architecture

The first proposed TF-QKD scheme [9] is similar to Fig. 1. Alice and Bob can share secure keys according to the interference results of their weak-coherent-pulses (WCPs) in the third party, Charlie. To realize the interference of two independently-generated WCPs, high speed and precision control systems are required for making the WCPs identical in optical modes such as wavelength, phase, polarization, and timing.

This work was supported in part by National Research Foundation of Korea (2019R1A2C2006381) and in part by Institute for Information and Communications Technology Promotion (2020-0-00947, 2020-0-00972).

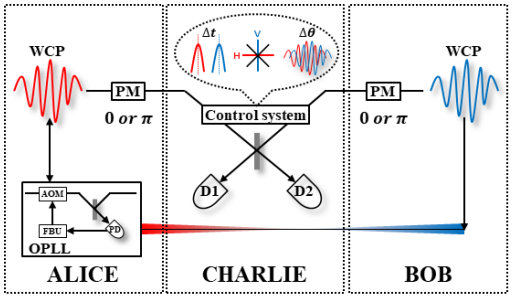

Fig. 1. Twin-field quantum key distribution.

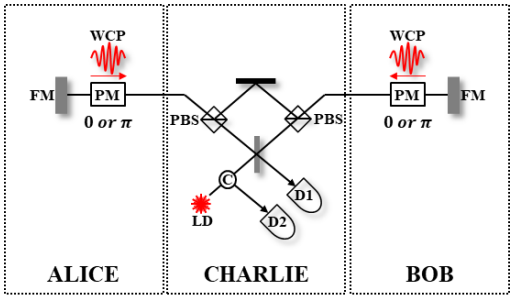

Fig. 2. Plug-and-play twin-field quantum key distribution.

The required control systems for TF-QKD consist of:

- *Phase-locking* to maintain the relative phase between the WCPs (of Alice and Bob),
- *Timing control* to compensate for the different arrival times of the WCPs,
- *Frequency-locking* to match the wavelengths of two independently-operated lasers,
- *Polarization control* to compensate for polarization drifts from the birefringence effects of the optical channels.

While these four control systems have already been used successfully and frequently in typical QKD systems, it is much more difficult to operate them between two lasers hundreds of kilometers away. Additionally, various TF-QKD protocols were developed to improve practicality, but high technologies for mode-locking systems are still required. For this reason, there are only four studies [11]–[14] that have successfully implemented TF-QKD systems in quantum channels longer than 100 km, and only Chinese research groups have succeeded.

To solve this practicality issue, we have proposed P&P TF-QKD as shown in Fig. 2. By applying the P&P architecture, our scheme has the following advantages. First, because both of the WCPs of Alice and Bob are generated from a single laser in Charlie, the wavelengths of the WCPs are fundamentally identical. Therefore, we do not have to implement the frequency-locking system. Second, the polarization control system is also not required since the polarization drift in the quantum channel is automatically compensated through the round-trip of the WCP using a faraday rotator mirror (FM) which reflects the lights with a 90-degree rotated polarization state. Last, because all WCPs go through the same optical path, the phase drifts and arrival times of them are also same. So, we do not need to implement the phase-locking and timing control systems. As such, by eliminating all of the complex control systems and passively applying mode-matchings, our scheme can greatly improve the practicality of TF-QKD.

The optical pulse flow is described as follows. At first in Charlie, Laser produces horizontally-polarized strong-coherent-pulses (SCPs), and SCPs are divided at a beam splitter (BS) with a splitting ratio of 5:5. They are also horizontally polarized, so go through the transmitting port of the polarization beam splitter (PBS) and are delivered to Alice and Bob via each quantum channel. SCPs transmitted to Alice (Bob) are reflected and vertically polarized by the FM and return to Charlie via the same quantum channel again. Alice (Bob) does not make any modulation for the reflected SCPs. Therefore, we do not have to consider how to prevent the information leakages from the SPCs. The vertically-polarized and returned SCPs are reflected by both PBSs and transmitted to Bob (Alice) via another quantum channel on the opposite side. Next, they are reflected and horizontally polarized by the FM, and then return to Charlie. At this turn, Bob (Alice) modulates the phases of SCPs according to randomly generated basis and encoding bits using a phase modulator (PM). And, Bob (Alice) also applies decoy-state and attenuates the SCPs to WCPs using an intensity modulator (IM) and variable attenuator (VOA), which are not shown in the Figure. Finally, the two returned WCPs of Alice and Bob, which are horizontally polarized, go through the transmitting ports of the PBSs and interfere on the BS. The result of the interference is measured as a constructive (D1) and destructive (D2) interference according to the relative phase between the two WCPs.

III. Experiment and Result

The most important thing for implementing TF-QKD is to realize the phase interference of the two WCPs of Alice and Bob. In this paper, we have verified our proposed scheme by measuring the visibility of the interference in a totally 50 km quantum channel which consists of two 25 km quantum channels. Initially, to check the passive mode-matching characteristics, the experimental setup was implemented without any control systems mentioned in Sec II. However, unlike the description in the former section, the implemented setup did not guarantee the same phase drifts between two WCPs of Alice and Bob. Through the unstable counts representing the interference result as shown in Fig. 3, we can know that the relative phase is not fixed due to the different phase drifts in each quantum channel. As described in the previous section, the two WCPs of Alice and Bob go through the same path in different directions, so ideally they should have the same phase drift from the quantum channel. By the way, the longer the quantum channel length becomes, the greater the time difference when the two WCPs go through the same point is. That is the reason why the two WCPs have different phase drifts. It is assumed that the two WCPs could have the same phase drift with a much shorter quantum channel length.

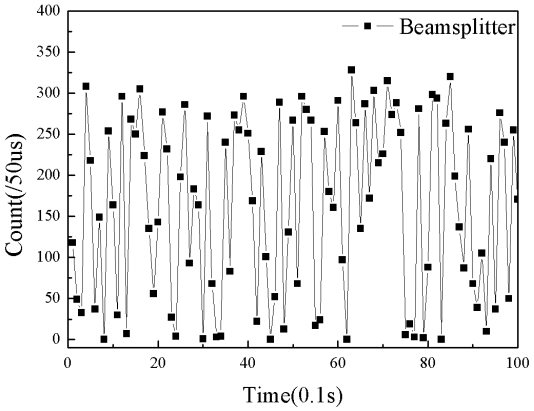

Fig. 3. Unstable count rates due to different phase drifts.

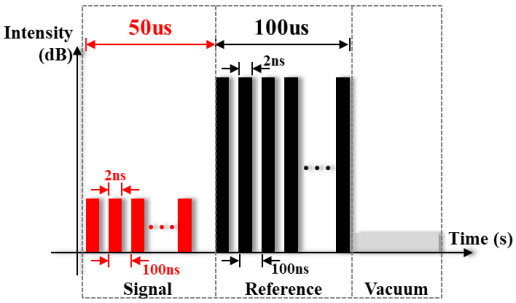

Fig. 4. Pulse train sequence.

By this reason, we had to change the pulse sequence to estimate and compensate the phase difference between the two WCPs of Alice and Bob by using the reference parts as shown in Fig. 4.

The interference result of the signal part is measured and recorded only when the relative phase of the reference part is estimated to 0 or π. To estimate the interference visibility of our scheme, we modulate the relative phase between the signal parts of the two WCPs from 0 to 2π. And the visibility was calculated using the well-known equation below.

$$Visibility = \frac{C_{max} - C_{min}}{C_{max} + C_{min}} \quad (1)$$

where $C_{max}(C_{min})$ is the maximum (minimum) count in the experimental result.

As a result shown in Fig. 5, we have achieved the interference visibilities as 98.8 % and 97.8 % in each of the beam splitter and circulator ports. Through these high visibilities obtained from the experiment, we can know that the passive phase-locking characteristic is invalid in the long distance quantum channel, but all other modes of the two WCPs, such as frequency, timing and polarization, can be passively compensated. Also, our experimental result can verify the implementation feasibility of our scheme. And in future work for full implementation of TF-QKD, we will also solve the relative phase fluctuation issue using a practical phase-locking method that is already used frequently in TF-QKDs [12]–[14].

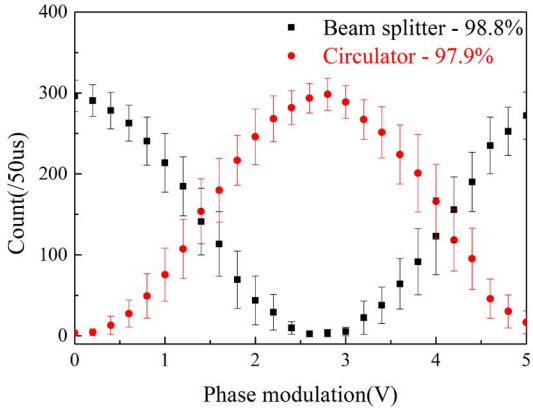

Fig. 5. Experimental result of the interference visibilities.

In the practical phase-locking method, since the relative phase between the two WCPs is compensated in the post-processing step instead of stabilizing it in real-time, we do not need to implement the high speed and precision control systems.

IV. Conclusion

In this paper, a practical P&P TF-QKD structure with passive mode-matching characteristics has been proposed and we have experimentally demonstrated the implementation feasibility by achieving the high interference visibilities, which is one of the most important thing in TF-QKD, as 98.8 % and 97.8 %. And we not only have discovered a new issue that the passive phase-locking property is invalid in the long distance quantum channel but also referred a solution to that issue. Based on our experimental results, we believe that the proposed architecture could be used as a practical method for implementing TF-QKD.

Future Work

Following this research, we are planning to implement P&P TF-QKD system proposed in this paper and expand it to a network system.

Acknowledgment

This work was supported in part by National Research Foundation of Korea (2019R1A2C2006381) and in part by Institute for Information and Communications Technology Promotion (2020-0-00947, 2020-0-00972).

References

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

[2] M. Takeoka, S. Guha and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," Nature Communications, vol. 5, pp. 5235, 2014.

[3] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nature Communications, vol. 8, pp. 15043, 2017.

[4] H. J. Briegel, W. Dür, J. I. Cirac and P. Zoller, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication," Physical Review Letters, vol. 81, pp. 5932-5935, 1998.

[5] N. Lo Piparo, M. Razavi and W. J. Munro, "Memory-assisted quantum key distribution with a single nitrogen-vacancy center," Physical Review A, vol. 96, pp. 052313, 2017.
[6] A. Muller, et al., ""Plug and play" systems for quantum cryptography," Appl. Phys. Lett., vol. 70, pp. 793-795, 1997.
[7] 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," Photonics Research, vol. 8, 2020.
[8] C. h. Park, et al., "Practical Plug-and-Play Measurement-Device-Independent Quantum Key Distribution With Polarization Division Multiplexing," IEEE Access, vol. 6, pp. 58587-58593, 2018.
[9] 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, pp. 400-403, 2018.
[10] M. Minder, et al., "Experimental quantum key distribution beyond the repeaterless secret key capacity," Nature Photonics, vol. 13, pp. 334-338, 2019.
[11] S. Wang, et al., "Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System," Physical Review X, vol. 9, pp. 2019.
[12] Y. Liu, et al., "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending," Phys Rev Lett, vol. 123, pp. 100505, 2019.
[13] J. P. Chen, et al., "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km," Phys Rev Lett, vol. 124, pp. 070501, 2020.
[14] X.-T. Fang, et al., "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," Nature Photonics, vol. 14, pp. 422-425, 2020.
[15] X. Zhong, J. Hu, M. Curty, L. Qian and H. K. Lo, "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution," Phys Rev Lett, vol. 123, pp. 100506, 2019.
[16] H. L. Yin and Y. Fu, "Measurement-Device-Independent Twin-Field Quantum Key Distribution," Sci Rep, vol. 9, pp. 3045, 2019.