Scalable Multi-user Twin Field Quantum Key Distribution Network

Xiaoqing Zhong[1], Wenyuan Wang[2], Reem Mandil[1], Hoi-Kwong Lo[1,2], Li Qian[1]

1. University of Toronto, Toronto, On. Canada
2. University of Hong Kong, Hong Kong, China

Abstract

Twin-field quantum key distribution (TFQKD) systems have shown great promise for implementing practical long-distance secure quantum communication. In this work, we demonstrate a proof-of-principle Sagnac-interferometer-based TFQKD network, where three user pairs sharing the same measurement station can perform pair-wise TFQKD through time multiplexing, with channel losses up to 58 dB, and channel loss asymmetry up to 15 dB.

I. Introduction

- TFQKD[1] has shown great promise for implementing practical long-distance secure quantum communication due to its measurement-device-independent (MDI) nature and its ability to outperform the fundamental rate-loss limit[2,3] of conventional point-to-point QKD systems. One of the natural applications is to build a TFQKD network.
- The advantages of such a network over existing QKD networks are twofold: 1) the MDI feature of TFQKD removes the security dependence on the central relay, making the network more secure; 2) by allowing users to perform TF-QKD, the network can provide higher key rate and larger communication range without requiring trusted central replays or quantum repeaters.

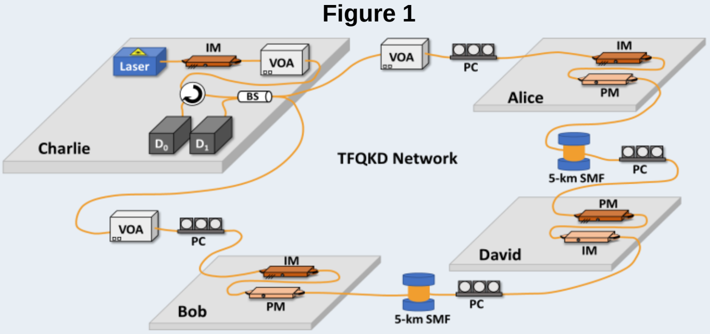
II. Methodology

- Most demonstrated TFQKD systems[4,5,6] interfering quantum signals from two remotely phase-locked laser sources are in essence giant Mach-Zehnder interferometers (MZIs), which require the same path length for the two arms to stabilize the system, and thus are inherently unsuitable for a network setting.
- On the other hand, TFQKD systems using Sagnac Interferometers[7,8], which have the inherent phase stability, have high tolerance for channel asymmetry, and are therefore eminently suitable for implementing a TFQKD network. In this work[9], we demonstrate a ring-shape TFQKD network based on the configuration of a Sagnac interferometer.

III. Experimental set-up

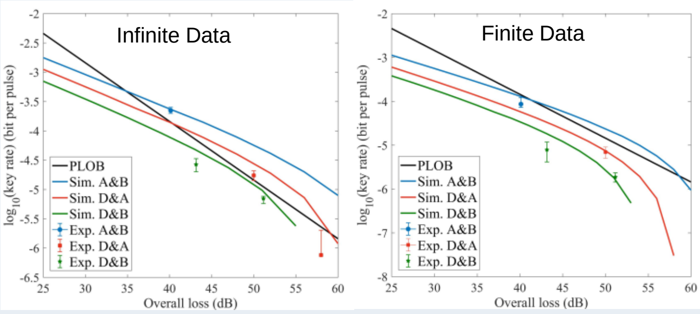
- As shown in Fig.1, in this network, three users, Alice, Bob and David, can perform pair-wise TFQKD with the assistance of an untrusted central relay, Charlie. Alice and Bob have symmetric optical losses to Charlie and use the “CAL19” protocol[10] to generate secure keys. While the channel loss asymmetry between Alice and David is 10 dB, and between Bob and David is 15 dB. These two pairs use the asymmetric version of “CAL19” protocol[11] when generating keys.
- One laser and a pair of single photon detectors are located on Charlie’s station. This setting not only removes lasers from the users’ stations and thus removes the need of phase-locking, but also reduces the cost and complexity of the network.
- To run this network, Charlie sends weak coherent pulses into the fiber loop. The users encode their information into the pulses that are in their designated time slots and forward the modulated pulses back to Charlie for measurement.

Figure 1



IV. Experimental Result

Figure 2



- In the infinite-data case, the key rates for both pairs with symmetric channel loss and 10 dB Channel loss asymmetry can beat the repeaterless rate-loss limit.
- In the finite-date case, the maximum key rate for the pair with 10 dB channel asymmetry and 58.0 dB overall loss is 3.3×10^{-8} bit per pulse, while the key rate for the pair with 15 dB channel asymmetry and 51.16 dB overall loss is as high as 7.6×10^{-6} bit per pulse.
- Our experiment has demonstrated the advantages and feasibility of TFQKD networks, an important step in advancing quantum communication technologies.

V. References

1. Lucamarini, M., Yuan, Z. L., Dynes, J. F., and Shields, A. J., *Nature*, 557(7705), 400 (2018).
2. Takeoka, M., Guha, S., and Wilde, M. M., *Nature Communications*, 5, 5235 (2014).
3. Pirandola, S., Laurenza, R., Ottaviani, C.,et al.. *Nature Communications*, 8, 15043 (2017).
4. Minder, M., et al.. *Nature Photonics*, 1 (2019).
5. Liu, Y., et al., *Physical Review Letters*, 123(10), 100505 (2019).
6. Wang, S., et al., *Physical Review X*, 9(2), 021046 (2019).
7. Zhong, X., Hu, J., Curty, M., Qian, L., Lo H.K.. *Physical Review Letters*, 123(10), 100506 (2019)
8. Zhong, X., Wang, W., Qian, L., and Lo, H.K.. *npj Quantum Information*, 7(1), 1-6 (2021).
9. Zhong, X., Wang, W., Mandil, R., Lo, H.K., and Qian, L.. arXiv:2106.07768 (2021).
10. Curty, M., Azuma, K., and Lo, H.K.. *npj Quantum Information*, 5(1), 1-6 (2019).
11. Wang, W., and Lo, H.K.. *New Journal of Physics*, 22(1), 013020 (2020).

UNIVERSITY OF TORONTO

QCRYPT 2021

Funding sources: NSERC, MITACS, CFI, ORF, Royal Bank of Canada, Huawei Technology Canada, CRCEF, the University of Hong Kong start-up grant.