A chip-based quantum access network without trusted relays

Feihu Xu
School of Physical Science, University of Science and Technology of China, Hefei 230026, People's Republic of China
Author e-mail address: feihuxu@ustc.edu.cn

Abstract: I will report our recent efforts towards the construction of a chip-based quantum access network using the measurement-device-independent protocols. This includes the recent experiments on Si chip-based QKD, high-rate QKD, twin-field QKD and all-photonic quantum repeater.

The field of quantum key distribution (QKD) has witnessed and supplied evolutionary contributions to the next generation of secure communication networks [1]. Nonetheless, nearly all existing QKD networks rely on a trustful relay, which is a critical security drawback. The invention of measurement-device-independent QKD (MDI-QKD) resolves this challenge, enabling secure QKD with an *untrusted* relay [2]. The recent extension to an efficient version, namely twin-field QKD [3], can overcome the repeaterless key-rate bound. The previous implementations of MDI-QKD and TF-QKD proved the well-functioning and great potential for a practical QKD network [4]. However, all these implementations use bulky equipment and point-to-point protocols, which limited the scalability and complexity for network infrastructure. The future developments of MDI-QKD are widely believed to be low-cost, scalable and high rate for practical applications.

Chip-based QKD provides a great opportunity for quantum network with small size, low cost, high stability, high reliability and the potential for mass production [1]. It has received a lot of attention from the science and technology community to realize QKD protocols (such as BB84) based on different fabrication technologies. The combination of photonic chips and MDI-QKD protocols enables a remarkably new quantum access structure with an *untrusted* relay [5]. In such a structure, each user only needs a compact transmitter chip, whereas the untrusted relay holds the expensive and bulky measurement system which are shared by all users. Importantly, this network can by-pass the challenging technique for intergrading single-photon detectors on chip, since the users do not need to do the quantum detection. Moreover, this network is compatible with general quantum communication protocols such as all-photonic quantum repeater [6], blind quantum computing [7] and so forth. Therefore, chip-based MDI-QKD enables a promising solution for low-cost, scalable, secure quantum network without trusted relays.

I will report our recent efforts towards the chip-based quantum access network. First, we experimentally demonstrate a 1.25 GHz silicon photonic *chip-based MDI-QKD* system [8]. The photonic chip transmitters integrate all the encoding components for a standard QKD source, where the two-stage modulation for polarization states enables a low error rate of 0.35%. Second, we report a *high-rate* QKD system that can generate secret key rate of 115.8 Mb/s over a 10-km standard fiber under the composable security against general attacks [9]. We adopt the integrated chip modulator to realize the fast and stable modulations, the performance of which is optimized to produce an ultra-low error rate. More importantly, we introduce the advanced implementation of multi-pixel superconducting nanowire single-photon detector (SNSPD) to quantum communication. Finally, the recent results in all-photonic quantum repeater [10], large-scale quantum network [11] and device-independent QKD [12,13] will also be briefly discussed.

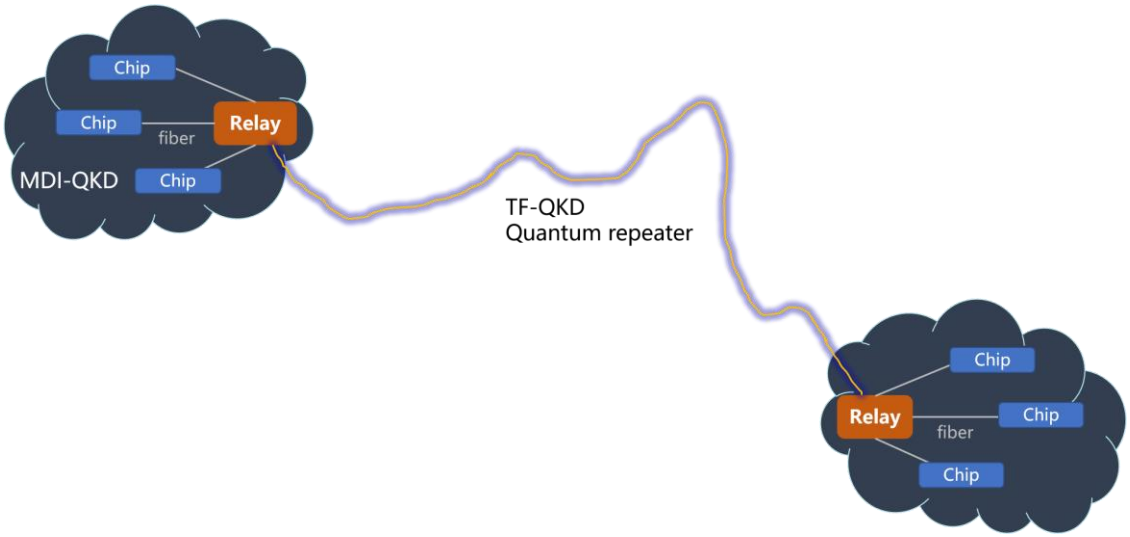

Figure 1: an illustration of chip-based quantum network based on MDI-QKD and TF-QKD protocols

References

[1] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. Rev. Mod. Phys. 92, 025002 (2020).

[2] Lo, H.-K. Curty, M. Qi. B. Measurement-Device-Independent Quantum Key Distribution. Phys. Rev. Lett. 108, 130503 (2012).

[3] Lucamarini, M. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature 557, 400 (2018).

[4] Zhang, Q., Xu, F., Chen, Y. A., Peng, C. Z., & Pan, J. W. Large scale quantum key distribution: challenges and solutions. Optics express, 26, 24260 (2018).

[5] Xu, F. et al. Discrete and continuous variables for measurement-device-independent quantum cryptography. Nat. Photon. 9, 772 (2015).

[6] Azuma, K., Tamaki, K., & Lo, H. K. All-photonic quantum repeaters. Nature communications, 6, 1-7 (2015).

[7] Jiang, Y.-F. et al. Remote blind state preparation with weak coherent pulses in the field. Physical Review Letters 123, 100503 (2019).

[8] Wei, K. et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys. Rev. X 10, 031030 (2020).

[9] Li, W. et al., High-rate quantum key distribution. Submitted (2022)

[10] Li, Z.-D. et al. Experimental quantum repeater without quantum memory. Nature photonics 13, 644 (2019).

[11] Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214 (2021).

[12] Xu, F. et al. Device-Independent Quantum Key Distribution with Random Postselection. Phys. Rev. Lett. 128, 110506 (2022).

[13] Liu, W.-Z. et al. Toward a photonic demonstration of device-independent quantum key distribution. Physical Review Letters 129, 050502 (2022).