Fully Connected Entanglement-based Quantum Communication Network without Trusted Node

Xu Liu[1], Rong Xue[1], Yidong Huang[1,2], and Wei Zhang[1,2,*]
[1]*Beijing National Research Center for Information Science and Technology (BNRist), Frontier Science Center for Quantum Information, Beijing Innovation Center for Future Chips, Electronic Engineering Department, Tsinghua University, Beijing 100084, China*
[2]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
** zwei@tsinghua.edu.cn*

Abstract: We proposed a fully connected quantum communication network architecture based on multi-user entanglement distribution by space multiplexing and wavelength multiplexing technologies. A fully connected QKD network with 40 users was demonstrated experimentally.

1. Introduction

Quantum key distribution (QKD) has been developed owing to the theoretically proven security of quantum mechanics, which may become the key technique in future information security [1,2]. However, most studies and implementations are limited to two or several parties. Moreover, an assisted trusted node is typically required for most of large user-scale quantum communication networks [3-6]. A type of fully connected quantum communication network [7,8] can form a mesh topology between the end users without a trusted node, which is efficient and with high security. However, how to experimentally build a large-scale fully connected QKD network remains challenging. In this work, we proposed and experimentally demonstrated a 40-user fully connected entanglement-based QKD network without a trusted node, which was supported by a broadband energy-time entangled photon pair source, in which each user can simultaneously generate secure keys with every other user via QKD. To the best of our knowledge, this is the largest experimentally demonstrated fully connected quantum communication network supported by a single quantum light source.

2. Network Architecture

The network is supported by a quantum light source, which providing broadband entangled photon pairs which strong frequency correlation. The quantum light source can be realized by spontaneous parametric down conversion (SPDC) or spontaneous four wave mixing (SFWM). Based on the property of frequency correlation, the generated photon pairs can be divided into many entanglement resources by wavelength de-multiplexing. Each of them includes photon pairs of two correlated wavelength channels. The network architecture is shown in Fig. 1.

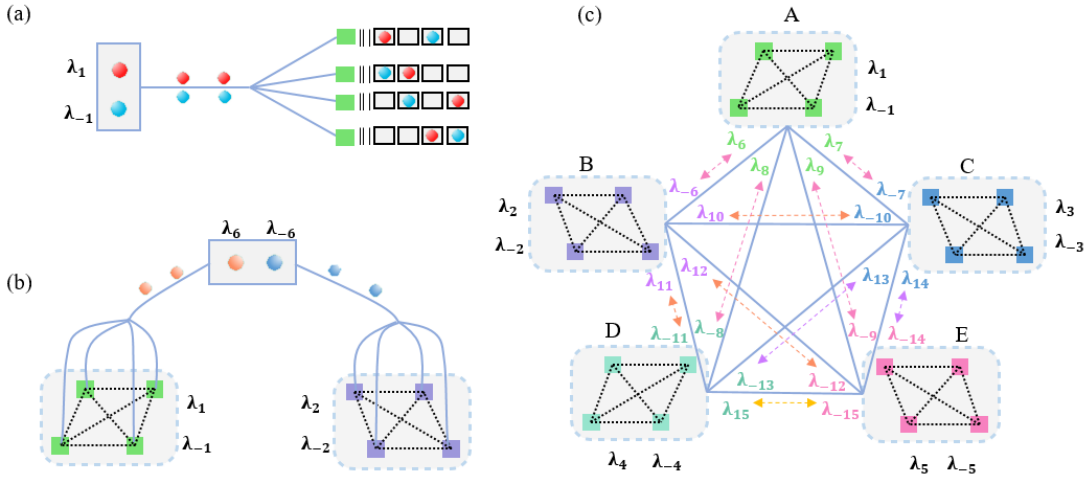

Fig. 1. The sketch of the network architecture depicting distribution of photon pairs of entanglement resources with different correlated wavelength channel pairs to users. Subscripts with opposite numbers represent wavelength channels corresponding to a specific entanglement resource. (a) Sketch of first layer, which forms a fully connected subnet; (b) Sketch of second layer, which shows the connections between the different subnets; (c) The constructed fully connected network with five subnets.

Some resources are used to support subnets as Fig. 1(a). In this figure, photons in a specific entanglement resource are distributed to many users by a passive N-port beam splitter. The photons in a pair would be distributed to any users randomly, hence, any two users in the subnet would be connected by photon pairs, which could be discriminated by post-selection after they are detected. The coincidence events between the two users could be used to realize entanglement based QKD. Hence, each subnet has a fully connected mesh topology supported by a specific entanglement resource. Other entanglement resources are used to connect these subnets as shown by Fig. 1(b). In the figure, the two photons of a photon pair in a specific entanglement resource are sent to two subnets, respectively. Then, they distributed to any users in their corresponding subnet randomly. By this way, any user in one subnet would be connected with any users in the other subnet by photon pairs. The coincidence events between them also can be selected and used to realize QKD. By this way, a large QKD network can be used by the ways shown in Fig. 1(a) and (b). Figure 1 (c) shows an example. In the figure, 5 entanglement resources are used to support five subnets, and then 10 entanglement resources are used to connect these subnets. The whole network has a fully connected mesh topology, i.e., any two users are connected by photon pairs and their coincidence events could be used to realize QKD.

3. The experiment

Based on the network architecture, the experimental system of the 40-user fully connected quantum communication network without a trusted node is shown in Fig. 2. In the experiments, broadband energy-time entangled photon pairs were generated by spontaneous four-wave mixing (SFWM) under continuous wave pumping in a silicon waveguide. Fifteen entanglement resources were extracted from the quantum light source, which corresponded to correlated wavelength channel pairs of C35/C45, C34/C46, …, C21/C59, as shown in Fig. 2(b). The first five entanglement resources (represented in green) were used to support the connection of users in the five subnets. Each subnet has 8 users. The remaining 10 entanglement resources (represented in orange) were used to connect users between the subnets. Subsequently, these wavelength channels were multiplexed by commercial dense wavelength division multiplexing components, as illustrated in Fig. 1(c), and then sent to the passive beam splitters.

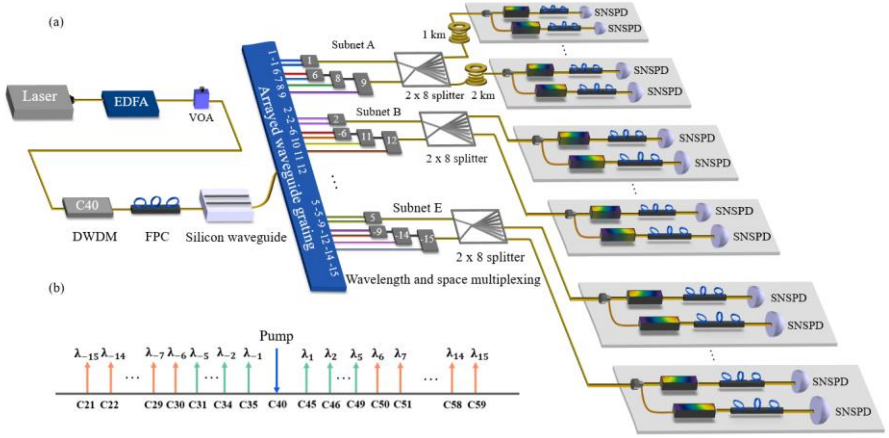

Fig.2 (a) Experimental system of 40-user fully connected quantum communication network; (b) The pump and generated entanglement resources. Subscripts of wavelengths with opposite numbers correspond to a correlated wavelength channel pair for a specific entanglement resource.

In each user, the photons were separated into two paths by a beam splitter. A normal dispersion component was placed in one path and an anomalous dispersion component was placed in the other path. Then, the photons were detected by two NbN superconducting nanowire single-photon detectors (SNSPDs). By these user setups, the symmetric dispersive optics QKD (DO-QKD) [9] was performed between any two users. The symmetric DO-QKD was modified from the conventional DO-QKD scheme [10,11] to fully adapt to the entanglement distribution network based on passive beam splitters. High-dimensional encoding based on the time of recorded single photon detection events can be used in symmetric DO-QKD to improve the utilization of coincidence events by multi-bit key generation per coincidence. The QKD performance measured between different users are shown in Fig. 3. The measured secure key rates between any two users in subnet A is shown in Fig. 3(a), in which the results of all the 28 QKD links are shown. The average secure key rate of QKD links in subnet A is ~51 bps. Figure 3 (b) shows the typical results of QKD between users in difference subnets. It can be seen that and the average secure key rate of QKD between different subnets was ~22 bps.

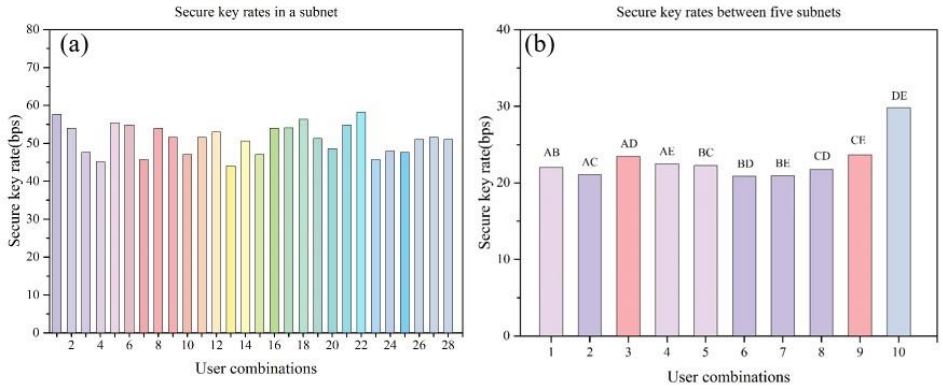

Fig. 3 Performances of symmetric DO-QKD in the network. (a) Measured secure key rates between any two users in subnet A; (b) Measured secure key rates between users in different subnets.

4. Conclusion

We demonstrated a 40-user fully connected entanglement based QKD network without a trusted node. The user numbers and performance of QKDs could be further improved by improving the bandwidth and brightness of the quantum light source. This network architecture provides a simple way to realize large quantum communication networks without trusted nodes.

Acknowledgments

This work was supported by the National Key R&D Program of China (2017YFA0303704, 2018YFB2200400), National Natural Science Foundation of China (NSFC) (61875101, 91750206, 61575102), Beijing National Science Foundation (BNSF) (Z180012), Beijing Academy of Quantum Information Sciences (Y18G26), and the Tsinghua University Initiative Scientific Research Program.

References

[1] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett.67, 661–663 (1991).
[2] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. 85, 441–444 (2000).
[3] Chen, T.-Y, Liang H., Liu Y., et al. "Field test of a practical secure communication network with decoy-state quantum cryptography," Opt. Express 17, 6540-6549 (2009).
[4] Peev, M. et al. "The SECOQC quantum key distribution network in Vienna," New J. Phys. 11, 075001 (2009).
[5] T.-Y. Chen, J. Wang, H. Liang, et al., "Metropolitan all-pass and intercity quantum communication network," Opt. Express 18, 27217–27225 (2010).
[6] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," New J. Phys. 13, 063039 (2011)
[7] Wengerowsky, S., Joshi, S. K., Steinlechner, et al. "An entanglement-based wavelength-multiplexed quantum communication network," Nature 564, 225-228 (2018).
[8] Joshi, S. K, et al., "A trusted node–free eight-user metropolitan quantum communication network," Sci. Adv. 6: eaba0959 (2020).
[9] X. Liu, X. Yao, R. Xue, et al. "An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution," APL Photonics 5, 076104 (2020).
[10] Lee, Catherine, Bunandar, Darius, Zhang, Zheshen, et al., "Large-alphabet encoding for higher-rate quantum key distribution," Opt. Express 27, 17539 (2019).
[11] Mower, Jacob, Zhang, Zheshen, Desjardins, Pierre, et al., "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A 87, 062322 (2013).