

NEWS & VIEWS

Open Access

More trust in networks, more secure keys

Guan-Jie Fan-Yuan^{1,2,3} and Shuang Wang^{1,2,3,4}✉

Abstract

A novel continuous-variable quantum passive optical network is proposed in which a user can increase their key rate by trusting other users. This is because the keys, which would be discarded to remove correlations with untrusted users, can be retained when the users are trusted. It provides a new perspective for enhancing network performance.

Quantum key distribution (QKD)¹, as a quantum communication technology that provides point-to-point information-theoretic secure key sharing, must consider how to extend its native point-to-point system into a network architecture that supports fully connected, all-time communication for large-scale applications. Networking requires addressing three key issues in sequence: connectivity, stability, and high throughput. To establish connections, one approach is an active optical network using, for example, optical switches^{2–4}, which connect different pairs of users based on control signals. The other approach is a passive optical network (PON), which connects a group of users through components like splitters^{5,6} and demultiplexers^{7,8}. Heterogeneous integration is more flexible and mature⁹. Some methods, for example, self-stabilizing encoding¹⁰, active compensation¹¹ and passive matching¹², can achieve high stability in the presence of environmental disturbance.

On this basis, increasing the key rate is necessary to support more services. The most direct approach is to increase the repetition rate, enhance the fidelity of quantum state encoding and decoding, and improve detector performance. These methods essentially enhance the fundamental performance of point-to-point systems, but things become more complex within a network. The passive network with one transmitter and multiple receivers, an architecture suitable for access networks, allows quantum states from the same sender to be

measured by multiple receivers, which may lead to correlations between the keys of the users. For security, each user must compress their keys, thereby removing this correlation. For discrete-variable QKD, this can be naturally satisfied when extracting single-photon information, as a single photon can only collapse onto one user's detector, thus avoiding any correlations. For continuous-variable QKD (CV-QKD), it is necessary to address this during the privacy amplification process.

Imagine a scenario where a user claims to have removed the correlation between their key and the other user's key. If their claim is accepted, then the other user would no longer need to remove the portion of their key that is correlated with this user, as the correlation is mutual. In a recent paper published in *Light: Science & Applications*, Hajomer et al. from the Technical University of Denmark and Filip et al. from the Palacky University have proposed a CV-QKD PON to increase secure keys by trusting other users¹³. In this protocol, the transmitter (referred to as the provider) sequentially conducts key distillation with each receiver (referred to as the user). The first user chooses to distrust all other users in the network. The second user, however, chooses to trust the first user, and so on, allowing each subsequent user to trust users who have already completed distillation (see Fig. 1). They demonstrated the advantage of this protocol in an eight-user network experiment. Considering the finite-size effect, the network's total key rate reaches 1 Mbps with an average distance of 11 km. In comparison, the key rate for an untrusted protocol is 0.4 Mbps.

This work finds a new key-rate mine: trust. Based on reliable identity authentication, this scheme is very useful for scenarios of group interaction such as meetings. Moreover, it further clarified the relationship between

Correspondence: Shuang Wang (wshuang@ustc.edu.cn)

¹CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, China

²Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, 230026 Hefei, China

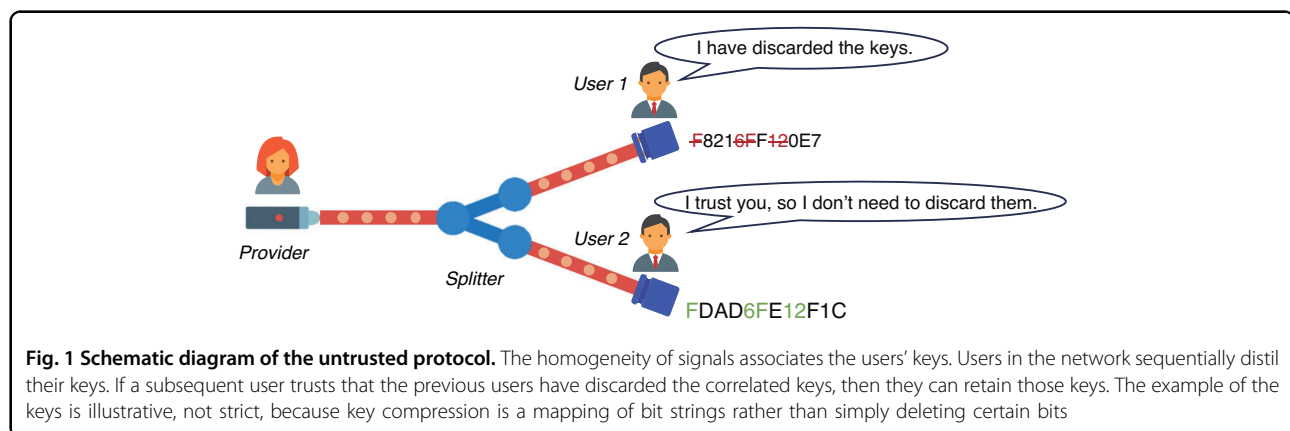
Full list of author information is available at the end of the article

© The Author(s) 2025



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.





security and performance, providing additional references for standardization and application. This encourages us to reassess the role of network trustworthiness in quantum networks, rather than merely striving for minimal assumptions, especially in the context of practicality. Following this, future research may find additional points for increasing key rates and clarify the trade-offs in different application scenarios.

Author details

¹CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, China. ²Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, 230026 Hefei, China. ³CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, China. ⁴Hefei National Laboratory, University of Science and Technology of China, 230088 Hefei, China

Conflict of interest

The authors declare no competing interests.

Published online: 02 January 2025

References

- Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing* 175–179 (IEEE, 1984).
- Chen, Y. A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
- Wang, C. et al. Experimental symmetric private information retrieval with measurement-device-independent quantum network. *Light Sci. Appl.* **11**, 268 (2022).
- Wang, S. et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22**, 21739–21756 (2014).
- Fröhlich, B. et al. A quantum access network. *Nature* **501**, 69–72 (2013).
- Huang, Y. D. et al. Realizing a downstream-access network using continuous-variable quantum key distribution. *Phys. Rev. Appl.* **16**, 064051 (2021).
- Chen, W. et al. Field experiment on a “star type” metropolitan quantum key distribution network. *IEEE Photonics Technol. Lett.* **21**, 575–577 (2009).
- Wang, S. et al. Field test of wavelength-saving quantum key distribution network. *Opt. Lett.* **35**, 2454–2456 (2010).
- Martin, V. et al. MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Inf.* **10**, 80 (2024).
- Wang, S. et al. Practical gigahertz quantum key distribution robust against channel disturbance. *Opt. Lett.* **43**, 2030–2033 (2018).
- Li, W. et al. High-rate quantum key distribution exceeding 110 Mb s⁻¹. *Nat. Photonics* **17**, 416–421 (2023).
- Fan-Yuan, G. J. et al. Robust and adaptable quantum key distribution network without trusted nodes. *Optica* **9**, 812–823 (2022).
- Hajomer, A. A. E. et al. Continuous-variable quantum passive optical network. *Light Sci. Appl.* **13**, 291 (2024).

