Official journal of the CIOMP 2047-7538
www.nature.com/lsa

NEWS & VIEWS Open Access

# Symmetric private information retrieval supported by quantum-secure key-exchange network

Shuang Wang[1,2,3]✉

**Abstract**
Quantum key distribution provides a provably secure way for private key distribution, which enables the practical implementation of information retrieval that preserves both the user privacy and database security.

Based on the fast-growing communication and networking techniques, retrieving information from a database is now a ubiquitous service that has a broad application prospect. For example, using a search engine to find out nearby restaurants, watching a movie on a streaming platform, etc. However, this task becomes nontrivial when there are privacy concerns, i.e., the user does not want to reveal his/her selection to either the data center or a third party, at the same time the data center does not want to reveal more information about the database other than the requested entry.

In 2000, Gertner and his colleagues proposed symmetric private information retrieval (SPIR) protocol that provides security guarantees to both the user and the database[1]. However, its practical implementation turns out to be experimentally demanding, requiring private random strings shared among parties. This is technically cumbersome with classical key distribution schemes based on computational complexity, and may not be suitable for applications requiring long-term security.

Quantum key distribution (QKD), whose security is based on the laws of quantum mechanics, is able to provide secret key distribution among distant parties with information-theoretic security. Since the first QKD protocol proposed by Bennet and Brassard in 1984, the field of QKD has developed extensively in both theory and experiment. With commercially available components and well-developed implementation techniques, QKD is now the most mature subfield of quantum cryptography[2,3]. Commercial QKD systems are also currently available on the market from several companies. Compared to its classical counterpart, the security of keys from QKD is independent of future advances in either hardware or algorithm, which is preferable for information retrieving tasks with data requiring long-term security.

Now, writing in this issue of *Light: Science & Applications*, Chao Wang and colleagues at the National University of Singapore report for the first time an experimental realization of SPIR supported by a measurement-device-independent (MDI) QKD network[4]. The SPIR demonstration looks at biometric security, and successfully retrieved a 582-byte fingerprint file from a database with 800 entries.

In the work presented here, the authors adopted a two-layered scheme for the system implementation, the SPIR application layer, and the MDI QKD layer (Fig. 1). The design of these two layers is based on the considerations of practicability and implementation security of the whole system. For the application layer, the authors adopted a two-database SPIR protocol[5], since information-theoretically secure SPIR with a single data center is proven to be impossible[1]. For the QKD layer, they deployed MDI QKD[6,7] with decoy states[8,9]. It has two main advantages. First, in MDI QKD, each party holds a quantum transmitter and communicates with each other via a central quantum receiver, which is operated by an

Correspondence: Shuang Wang (wshuang@ustc.edu.cn)
[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, China
[2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, China
Full list of author information is available at the end of the article

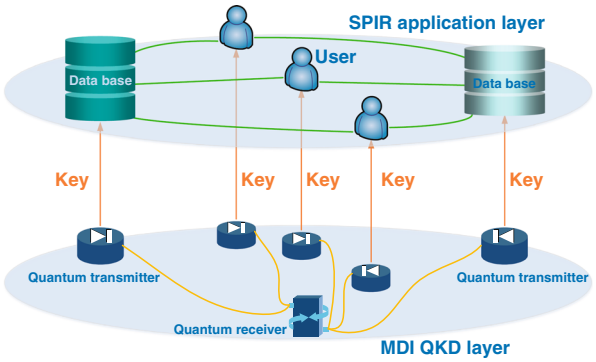


**Fig. 1 Schematic view of QKD-based SPIR.** The symmetric private information retrieval (SPIR) application is supported by a measurement-device-independent quantum key distribution (MDI QKD) network

untrusted third party. Thus, MDI QKD provides an appealing feature of immunity against any potential side-channel attacks on the quantum receiver, which is typically regarded as the most vulnerable part in practical QKD implementation. As such, each party only needs to secure their own transmitter and need not worry about the implementation of the quantum receiver. Second, MDI QKD holds a natural star topology, making it suitable for network expansion.

With the presented work, Chao Wang and co-authors set up a fiber-based MDI QKD system with a working frequency of 125 MHz. The quantum transmitter held by the user and data centers prepares time-bin phase encoding quantum states, where the information is coded on the intensities and the relative phase of the two successive temporal modes. Then, the quantum states are sent to the quantum receiver for measurement via an untrusted optical fiber channel with a length of 25 km. By carefully matching all the degree of freedoms of the incoming photonic quantum states, the authors obtained a Hong–Ou–Mandel interference visibility of 0.48 (±0.015), showing an efficient Bell-state measurement for the MDI QKD. They also measured the averaged bit error rate in the key generation basis to be 0.83%. After obtaining raw key bits, the authors performed classical post-processing, including error correction and privacy amplification, to obtain the final secure keys of $6.5 \times 10^5$ bits. Finally, with the final keys, SPIR over a fingerprint database is successfully demonstrated.

The successful realization of SPIR supported by MDI QKD demonstrates the feasibility of the proposed scheme, providing a promising approach for the practical implementation of SPIR with information-theoretic security. With the recent advances of QKD in terms of high-speed[10,11], long-distance[12–15], and network optimization[16–18], we can expect that the performance of the proposed scheme can be further promoted, pushing its practicability to a higher level. This will open the door to many applications where long-term security is critical, such as medical record retrieval, biometric authentication, and pay-per-use online contents, that would remain secure against even quantum computing based attacks.

**Author details**
[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, China. [2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, China. [3]Hefei National Laboratory, University of Science and Technology of China, 230088 Hefei, China

Published online: 14 October 2022

**References**

1. Gertner, Y. et al. Protecting data privacy in private information retrieval schemes. *J. Computer Syst. Sci.* **60**, 592–629 (2000).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
3. Xu, F. H. et al. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
4. Wang, C. et al. Experimental symmetric private information retrieval with measurement-device-independent quantum network. *Light Sci. Appl.* **11**, 268 (2022).
5. Kon, W. Y. & Lim, C. C. W. Provably secure symmetric private information retrieval with quantum cryptography. *Entropy* **23**, 54 (2021).
6. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
7. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
8. Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
9. Lo, H. K., Ma, X. F. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
10. Wang, S. et al. Practical gigahertz quantum key distribution robust against channel disturbance. *Opt. Lett.* **43**, 2030–2033 (2018).
11. Wei, K. J. et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **10**, 031030 (2020).
12. Lucamarini, M. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
13. Wang, S. et al. Beating the Fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
14. Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photonics* **15**, 530–535 (2021).
15. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
16. Fan-Yuan, G. J. et al. Measurement-device-independent quantum key distribution for nonstandalone networks. *Photonics Res.* **9**, 1881–1891 (2021).
17. Park, C. H. et al. 2×*N* twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing. *npj Quantum Inf.* **8**, 48 (2022).
18. Fan-Yuan, G. J. et al. Robust and adaptable quantum key distribution network without trusted nodes. *Optica* **9**, 812–823 (2022).