

# Free-space quantum network with trusted relay

Wei-Yue Liu,<sup>1</sup> Hai-Lin Yong,<sup>1</sup> Zhu Cao,<sup>2</sup> Ji-Gang Ren,<sup>1</sup> Xiongfeng Ma,<sup>2</sup> Cheng-Zhi Peng,<sup>1</sup> and Jian-Wei Pan<sup>1</sup>

<sup>1</sup>*Shanghai Branch, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, China*

<sup>2</sup>*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*

Nowadays, information security plays an increasingly important role in global communication. Quantum cryptography [1, 2], particularly quantum key distribution (QKD), offers means to expand a secure key between two distant parties, whose security is stemmed from the fundamental laws of quantum mechanics [3–5]. In practice, QKD experiments have been demonstrated over long-distance optical links through both free space [6] and fiber [7–9]. In the past decade, commercial QKD products have appeared in the market [11]. The next step toward real-life application of QKD is to build up a quantum network. However, due to the fragility of quantum signals, the transmission distance of current QKD implementations is limited to the order of hundreds of kilometers. The key reason is that the transmittance of quantum signal decays exponentially with the transmission distance.

For a global quantum network, it is natural to employ a satellite as a moving trusted relay and ground stations around the world as user nodes, as shown in Fig. 1. Currently, there are a few challenges even for a faithful feasibility test of this task. Firstly, the test should be performed at various locations with different atmosphere environment to simulate various ground stations. Secondly, for postprocessing, the test must take into account of the limited computational power in the relay and minimize classical communication between the relay and user nodes.

We demonstrate a free-space quantum network by es-

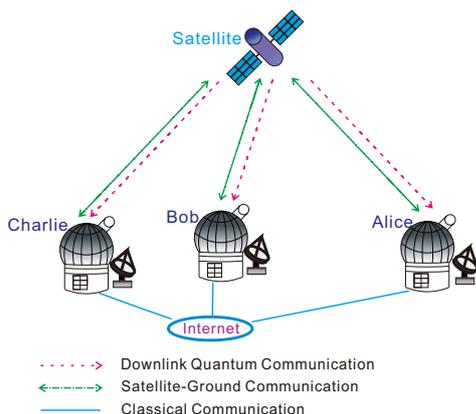


FIG. 1: A schematic diagram for the global quantum network with a satellite. The satellite, as a trusted relay, circles around the earth and communicates with each user when the corresponding optical link is available.

ablishing three QKD links in Qinghai and one in Kunshan. We use a moving transmitter (S) as a trusted relay. Two experiment locations, Qinghai and Kunshan, are 2040 km far apart and have very distinct atmosphere environment. We implemented four user (receiver) nodes, noted as Alice, Bob, Charlie and David. We test the feasibility of quantum network by performing QKD at a few different locations, viewing S at different place to be the same relay.

Each QKD link consists of a transmitter and a receiver. The transmitter is composed of a 200-mm-diameter tailored telescope with an automatic precise acquisition-tracking-pointing (ATP) system and a 100 MHz quantum source implementing decoy-state method, along with auxiliary electronics including functions of control, synchronization, data acquisition, random number generation, and classical communication. The transmitter we designed is highly integrated and robust, which can be put in moving objects such as trucks and satellites.

The receiver consists of a 300-mm-diameter telescope with an ATP system similar to the one in the transmitter, quantum measurement module with four Geiger mode avalanche photodiodes (APDs), and auxiliary electronics. The receiver can be modified from a widely-used laser-ranging telescope system, by replacing its detection part with our quantum measurement modules. Note that in the real ground-satellite QKD, a larger (for instance, 1-meter-diameter) telescope will be used to increase the collecting efficiency.

The length of the first free-space optical link, S-Alice, is 10 km. The transmitter S is put on a vehicle, driving in the Bird Island Natural Reserve in Qinghai. The user node Alice is settled in an office building. The quantum link length varies when the vehicles moves, with which we test our ATP system and synchronization system. Meanwhile, the relative motion between S and Alice will result in a changing reference frame for quantum signals, for which we apply a polarization auto-compensation module. We design the transmitter system so that it can function under various distinct environments, such as low temperature and vibration.

In the second QKD link, S-Bob, the transmitter S is put in a hanging basket on a crane, while the receiver Bob is set in the Bird Island Hotel in Qinghai. The optical length in between is 15 km. In this case, the transmitter swings in the wind. Under such condition, we manage to control the tracking precision below  $6 \mu\text{rad}$  by our ATP system.

The third link, S-Charlie, is established across Qinghai Lake. The transmitter S is set on top of a rotating

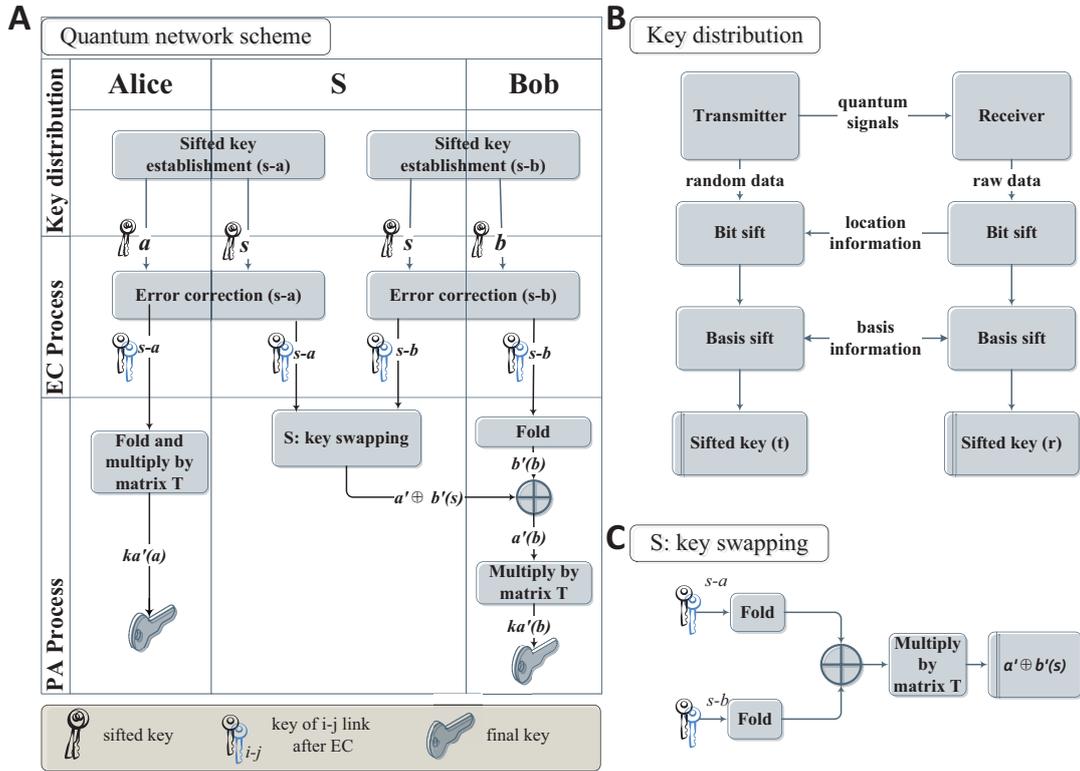


FIG. 2: (A) shows the flowchart of a quantum network with our delayed privacy amplification scheme, which is mainly composed of the following steps: quantum signal transmission and measurement, bit and basis sift, error correction, key swapping and privacy amplification. (B) Alice and Bob each establishes a sifted key with the relay  $S$  via standard QKD procedures. After obtaining raw data through quantum signal transmission, Alice and Bob discard the data for lost signals (bit sift) and the case when they use different bases (basis sift). Alice and Bob each runs error correction with  $S$  (C) The relay  $S$  divides the error-corrected key into two equal-length parts and XOR them as a new key (fold).  $S$  sends the parity string of two folded keys (one with Alice and the other with Bob) to Bob. Both Alice and Bob run the privacy amplification procedure, say, via multiplying the key by a Toeplitz matrix  $T$ .

platform in the same office building as Alice and the receiver Charlie is set at a house near Heimahe Town. The optical length is 40 km. In a typical ground-satellite optical tracking system, one needs to get ride of ambient lights from the Moon and stars. This effect can be simulated by the light reflected from the lake surface, which is substantially reduced by windowing our tracking camera. Meanwhile, in a future generation of quantum network, it is possible that one of the ground station nodes is in the ocean. The lake environment can simulate this case as well. To precisely simulate the relative movement between satellite and ground station, we rotate the transmitter platform. The ATP system is able to control and spin the telescope on the platform base to compensate the platform rotation. The rotation is performed sinusoidally with a period of 15 seconds and an amplitude of 3 degrees. Thus, the maximum rotation speed is 1.257 deg/s and the maximum angular acceleration is 0.526 deg/s<sup>2</sup>, which are greater than the parameters corresponding to movement of low Earth orbit (LEO) satellites [12].

The fourth link is demonstrated in Zhoushi, Kunshan, 2040 km away from the first three links. S-David test is held on two buildings 5 km apart, under very distinct atmosphere environment. This test is performed in the city area, while the the ones in Qinghai are operated in the rural area. The total channel loss, including collection efficiency, is 44.53 dB.. If we view the transmitter  $S$  as the moving satellite, we simulate a quantum network over a large scale geometric distance.

After the transmission and measurement of quantum signals, there may exist errors between the relay and the user, and more critically, certain amount of key information may be leaked to an eavesdropper. In order to extract a secure key from the raw data, the user needs to run data postprocessing with the relay. In a conventional QKD system, the local computation and classical communication is normally considered to be free for post-processing. However, in the case of a global quantum network, where the relay is set in a satellite, computational power could be limited and the classical commu-

nication would be expensive. On the other hand, the current realization of privacy amplification, a key component of postprocessing, requires lots of computational resource and classical communication. One key observation here is that the computational power limit is mainly on the satellite. A solution to this problem is by off-loading computation from the satellite to ground stations users, which is the key idea of the delayed privacy amplification scheme [10].

However, if we follow the original delayed privacy amplification scheme [10], our quantum network setup cannot yield any positive keys. Here we propose a new scheme to solve this problem. Before the privacy amplification, we divide the error-corrected key into two equal-length parts and XOR them as a new key, as shown in Fig. 2. In this new postprocessing scheme, the cost by the delayed privacy amplification is substantially reduced. As a consequence, we have the best of both worlds—enjoying low computation and communication requirement on the relay and yet sustaining the performance.

The attenuations for the four links we demonstrated are from 34 to 45 dB which is comparable to the typical ground-satellite optical link. We achieved a final key

size larger than  $10^4$  bits and a final key rate larger than 25 bps in every pair of the user nodes. In this trusted network, both the computational power assumed in the relay and classical communication required between the trusted relay and the nodes are reduced.

In summary, we have experimentally demonstrated a four-nodes quantum network with a moving trusted relay. Moreover, our trusted relay is resistant to various environment and turbulence caused by moving. From a fundamental point of view, it is interesting as a QKD system to be performed at a macroscopic scale. From a practical perspective, the combined techniques introduced here, including modified delayed privacy amplification, ATP technology and high-precision time synchronization, may provide a tool kit for global QKD network. Methods for further reducing communication cost includes reducing the cost of bit and basis sift and error correction and further reducing the cost of privacy amplification. Our experiment confirms that building a ground-satellite network by sending satellite into space is plausible and this can be viewed as the first step toward this blueprint.

- 
- [1] Bennett, C. H. & Brassard, G.  
In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (IEEE Press, New York, 1984).
- [2] Ekert, A. K.  
*Phys. Rev. Lett.* **67**, 661–663 (1991).
- [3] Mayers, D. In *Advances in Cryptology-Crypto '96, Lecture Notes in Computer Science*, vol. 1109, 343–357 (Springer, Berlin, 1996).
- [4] Lo, H.-K. & Chau, H. F.  
*Science* **283**, 2050 (1999).
- [5] Shor, P. W. & Preskill, J.  
*Phys. Rev. Lett.* **85**, 441 (2000).
- [6] Schmitt-Manderbach, T. *et al.*  
*Phys. Rev. Lett.* **98**, 010504 (2007).
- [7] Takesue, H. *et al.* *Nature Photonics* **1**, 343–348 (2007).
- [8] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. *New J. of Phys.* **4**, 41 (2002).
- [9] Wang, S. *et al.* *Opt. Lett.* **37**, 1008–1010 (2012).
- [10] Fung, C.-H. F., Ma, X., Chau, H. F. & Cai, Q.-y. *Phys. Rev. A* **85**, 032308 (2012).
- [11] See for example, [www.magiqtech.com](http://www.magiqtech.com); [www.idquantique.com](http://www.idquantique.com); [www.quantum-info.com](http://www.quantum-info.com).
- [12] For a satellite on a 500 km Sun-synchronous orbit, the maximum speed and acceleration is 1.14 deg/s and 0.013 deg/s<sup>2</sup>.