Satellite-to-Ground Entanglement-Based Quantum Key Distribution

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Ji-Gang Ren,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Ming Li,[3] Yong-Mei Huang,[4] Lei Deng,[5] Li Li,[1,2] Qiang Zhang,[1,2] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2] Jian-Yu Wang,[2,3] and Jian-Wei Pan[1,2]

[1]*National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China*

[4]*The Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China*

[5]*Shanghai Engineering Center for Microsatellites, Shanghai 201203, China*

(Received 12 September 2017; published 13 November 2017)

We report on entanglement-based quantum key distribution between a low-Earth-orbit satellite equipped with a space borne entangled-photon source and a ground observatory. One of the entangled photons is measured locally at the satellite, and the other one is sent via a down link to the receiver in the Delingha ground station. The link attenuation is measured to vary from 29 dB at 530 km to 36 dB at 1000 km. We observe that the two-photon entanglement survives after being distributed between the satellite and the ground, with a measured state fidelity of ≥ 0.86. We then perform the entanglement-based quantum key distribution protocol and obtain an average final key rate of 3.5 bits/s at the distance range of 530–1000 km.

DOI: 10.1103/PhysRevLett.119.200501

Quantum entangled particles shared between distant locations have a central role in the fundamental test of quantum mechanics [1], and serve as important resources in quantum information technologies such as quantum key distribution (QKD) [2–4] and quantum teleportation [5,6]. QKD allows two distant parties to generate a common, random string of secret bits: an information-theoretically secure solution to the secret key exchange problem [7,8], where the security is protected by the laws of quantum physics instead of the mathematical complexity in classical public-key cryptography.

There are mainly two types of QKD protocols for practical implementations. One is by preparing and measuring single-photon states, such as the original proposal by Bennett and Brassard in 1984 (BB84) [2]. Because of the lack of high-performance single-photon sources, weak coherent pulses under the decoy-state BB84 protocol [9,10] is widely used, which is immune to photon-number-splitting attack. The decoy-state QKD has been implemented over a few hundred kilometers [11,12], and very recently from a low-Earth-orbit satellite to a ground station in China [13,14].

The other type of QKD is entanglement based, as proposed by Ekert in 1991 (E91) [3] and Bennett, Brassard, and Mermin in 1992 (BBM92) [4]. In these entanglement-based protocols, the entangled photon source could even be in the hands of an adversary while it is still possible to generate a secret key between two parties. Compared to the coherent-state QKD, it has been shown that practically the entanglement-based QKD can tolerate higher channel loss, is more robust to environmental fluctuations, and can simplify the analysis of the cryptographic key [15]. However, in the previous entanglement-based QKD [16,17], the photon loss in the optical fibers or terrestrial free space, which scaled exponentially as a function of channel length, limited a distance on the order of 100 km [18].

This Letter reports entanglement-based QKD between a low-Earth-orbit satellite (Micius) and a ground station in Delingha, China [see Fig. 1(a) for an overview of the experimental setup]. Compared to optical fibers or terrestrial free-space channels, the satellite-to-ground connection has, in principle, greatly reduced channel loss because the effective thickness of the atmosphere is only about 10 km and most of the propagation path of the photons is in empty space [16,19]. By developing precise time synchronization, dynamical polarization compensation, high-bandwidth acquiring, pointing and tracking (APT) techniques, we are able to optimize the satellite-to-ground link efficiency and obtain a cryptographic key rate of 3.5 bits/s.

As shown in Fig. 1, a compact space borne entangled photon source is equipped in the satellite as a payload with a size of 430 mm × 355 mm × 150 mm. By pumping a periodically poled $KTiOPO_4$ crystal inside a Sagnac interferometer in both the clockwise and anticlockwise direction simultaneously with a continuous-wave laser at a wavelength of ~405 nm, polarization-entangled photon pairs are produced via spontaneous parametric

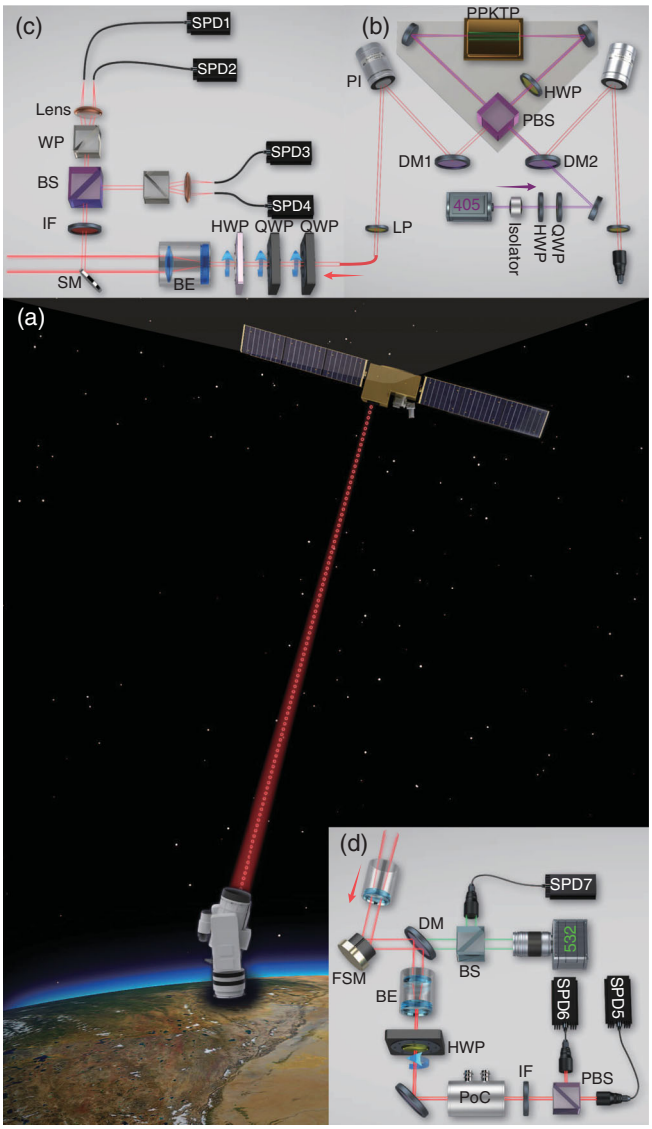

FIG. 1. Illustration of the experimental setup. (a) Overview of the satellite-to-ground entanglement-based quantum key distribution. (b) The measurement module in the satellite. About 1% of the idler photons are reflected by the sampling mirror (SM) to be measured in the satellite. (c) Schematic of the space borne entangled photon source. (d) The measurement module in the ground station. Beam splitter (BS); polarization beam splitter (PBS); beam expander (BE); Wollaston prism (WP); interference filter (IF); half-wave plate (HWP); quarter-wave plate (QWP); dichroic mirror (DM); fast-steering mirror (FSM); piezo steering mirror (PI); periodically poled $KTiOPO_4$ (PPKTP).

down-conversion [20] close to the form of $|\Psi\rangle_{12} = (|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2)/\sqrt{2}$, where $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization states, respectively, and the subscript 1 and 2 denote the two output spatial modes. The entangled photon pairs are then collected by two single-mode fibers (SMFs). Under a pump power of 30 mW, 5.9×10^6 entangled photon pairs per second are coupled into the SMFs. This source survived from rocket acceleration and is tested to be robust against various vibration, temperature, and electromagnetic conditions in space (see Ref. [21] for more details).

For entanglement-based QKD, one of the entangled pair, the photon 1, is measured in the satellite, whereas the other one, the photon 2, is sent to the ground station through a telescope. Because of the storage space limit of the random-access memory on the satellite, the optical path of photon 1 is sampled for only 1% using a mirror edge, which is then detected inside the satellite. The detection module consists of a beam splitter, two Wollaston prisms, and four single-photon detectors for measuring the polarization of the photons in the bases of $|H\rangle$, $|V\rangle$, and $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, $|-\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$.

Photon 2 is guided through a single-mode fiber to a transmitter, which consists of a telescope with a diameter of 300 mm, a polarization compensation module, and an APT system. The receiving ground station is located at Delingha ($37°22'44.43''N$, $97°43'37.01''E$; altitude 3153 m), Qinghai province, China. The ground telescope has a diameter of 1.2 m and a field view of 65 μrad. All the optical elements such as mirrors in the telescope are coated to maintain the photon polarization.

As the entangled photons travel from the satellite through the atmosphere to the ground station with a physical separation of 500–1000 km, several effects contribute to channel loss, including beam diffraction, pointing error, atmospheric turbulence, and absorption. To optimize the down-link efficiency, we design a transmitting telescope with narrow divergence, and develop a high-bandwidth and high-precision APT system to optimize the link efficiency. We develop cascaded multistage APT systems both in the satellite transmitter and the ground receiver. For the transmitter and receiver, the APT systems achieved a tracking accuracy of ~2 and ~0.4 μrad, respectively. More details of the APT system were reported in Refs. [13,21].

A Pockels cell (POC) and a PBS are combined for analyzing the polarization of the entangled photons in the $|H\rangle/|V\rangle$ or $|+\rangle/|-\rangle$ bases randomly, as shown in Fig. 1(d). The optical axis of the POC is aligned at $\pi/8$. The POC does not change the polarization of photons when no external voltage is applied. In this case, the PBS performs a measurement in the $|H\rangle/|V\rangle$ basis. When applying a half-wave voltage of ~600 V, the POC becomes equivalent to a half-wave plate, where the measurement on the $|+\rangle/|-\rangle$ basis is performed. The high-voltage modulation pulses are controlled by a quantum random number generator with a frequency of 5 kHz. After being transmitted or reflected by the PBS, the photons are collected by two multimode fibers with the core diameter of 320 μm and detected by two single photon detectors (SPDs), respectively. The output signal of the detectors is sent to a time-to-diginal converter (TDC) that records the arrival time of the photons.

For coincidence measurements of the remotely distributed entangled photon pairs, time synchronization between the satellite and the ground station is essential to reduce the background noise. The beacon laser (532 nm) in the satellite is a passive Q-switched pulse laser with a repetition rate of 10 kHz and a pulse width of 0.8 ns. Before being sent from the satellite, the beacon laser was sampled and detected by a PIN photodiode and recorded by the TDC in the satellite. When the beacon laser arrives at the ground station, it is divided into two parts by a BS. One beam is sent to the camera for the APT system. The other one is detected by an SPD and the arrival times are recorded by the TDC for the synchronization system. The satellite-based and ground-based TDCs are synchronized by the GPS signal. The synchronization accuracy is verified by analyzing coincidence distribution of entangled photon pairs in the time domain, which is close to a Gaussian distribution with $\sigma = 0.7$ ns. We set a narrow coincidence time gate of 2 ns to reduce the accident coincident events.

In the experiment it is crucial to preserve the photon's polarization, which is used to encode the information. The polarization rotation and phase shift induced by both the optical elements and the motion of the satellite relative to the ground are calibrated and dynamically compensated. For calibration, we use lasers with the same wavelength as the entangled photons prepared in the probe state $|H\rangle$ and $|+\rangle$. On the satellite, the single-mode fiber which connects the entangled photon source and the transmitter causes a random unitary transformation on the photon polarization, which is corrected by two quarter-wave plates and a half-wave plate. On the ground station, an additional half-wave plate is used to compensate the relative motion between the transmitter and the receiver, where the correction angle offsets are calculated in advance. As shown in Fig. 2(a), the polarization visibilities of the four tested states $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$ are 97.9%, 97.1%, 97.7%, and 96.5%, respectively.

The satellite is operated on a sun-synchronized orbit at an altitude of 500 km and circles the Earth every 94 min. Each night starting at around 1:30 AM, the satellite comes into view of the ground station with a duration of ~400 s. When the satellite rises from the northern horizon line of the ground station, the telescopes in the satellite and the ground station become visible and start to track each other [13]. Depending on different altitude angles, the satellite-to-ground distance varies from 530 km (at the highest altitude angle of 70.6°, when the satellite passes through the ground station above the top) to 1600 km (at an altitude angle of 11.6°). We use the two-photon source to calibrate the channel attenuation as a function of the distance during one orbit of the satellite passing through the Delingha station, which varies from 29 dB at 530 km to 44 dB at 1600 km, as shown in Fig. 2(b).

To verify whether the two photons distributed between the satellite and the ground are still entangled, we analyze

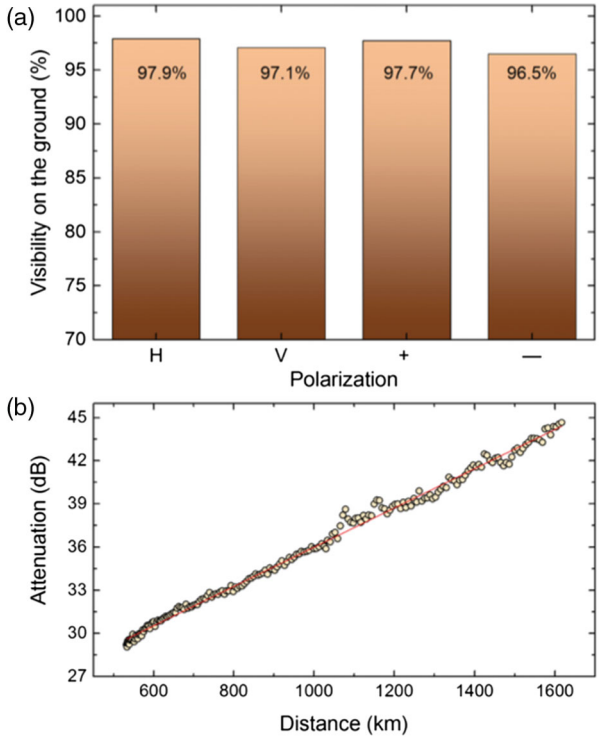

FIG. 2. The characterization of the satellite-to-ground optical link. (a) The polarization visibilities using the calibration lasers in four specific states. (b) The attenuation of the down-link channel with different distances between the satellite and the ground. These diagrams show that the overall polarization visibilities and efficiency are sufficient to implement the satellite-to-ground QKD.

their polarization in the bases of $|H\rangle/|V\rangle$ and $|+\rangle/|-\rangle$. The received photons are analyzed by a half-wave plate, a POC, and a polarizing beam splitter, then coupled into a multi-mode fiber and detected by single-photon detectors with dark count rates below 100 Hz. Figures 3(a) and 3(b) shows

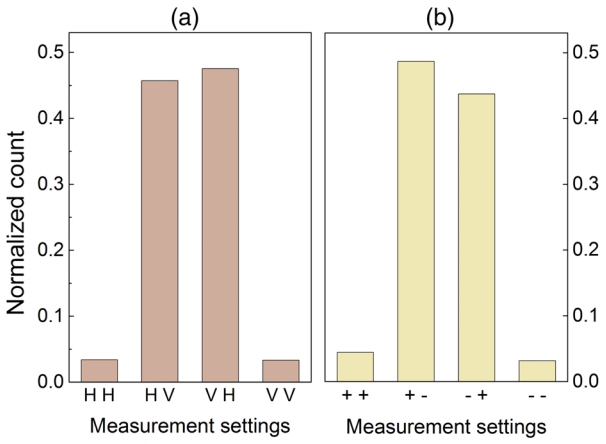

FIG. 3. Measurement of the entangled photons after traveling the down-link channel. (a) Normalized two-photon coincidence counts in the $|H\rangle/|V\rangle$ basis. (b) Normalized two-photon coincidence counts in the $|+\rangle/|-\rangle$ basis.

the data for the normalized two-photon coincidence counts without subtracting background noise in the $|H\rangle/|V\rangle$ and $|+\rangle/|-\rangle$ bases, respectively, obtained during 240 s passage. It is shown that the $|H\rangle_1|V\rangle_2$ and $|V\rangle_1|H\rangle_2$ population dominates in the $|H\rangle/|V\rangle$ bases, with a contrast of 13.9:1. Further, Fig. 3(b) shows the measured $|+\rangle_1|-\rangle_2$ and $|-\rangle_1|+\rangle_2$ counts dominate over $|+\rangle_1|+\rangle_2$ and $|-\rangle_1|-\rangle_2$, with a contrast of 12.2:1. From these measurements, we can estimate the state fidelity—defined as the overlap of the experimentally obtained state density matrix with the ideal —of the two photons: $F \geq 0.86 \pm 0.02$, confirming the two-qubit entanglement [21].

During the satellite's one passage, we use 40 sec (depending on the different location, the satellite-to-ground distance is 500–1000 km) for generating the quantum cryptographic key. Summarizing the data from six orbits, we obtain 9080 coincidence events. Discarding the events chosen at different bases, we obtain 4434 bits of sifted key with an overall quantum bit error rate (QBER) of 7.1%, as shown in Fig. 4(b). The QBER in the $|H\rangle/|V\rangle$ bases and the $|+\rangle/|-\rangle$ bases are 6.7% and 7.6%, respectively. We estimate that 5.4% of the QBER was caused by the accident coincident events and the rest was due to the imperfections of our setup.

In the calculation of the final secure key length, we employ the postprocessing method proposed in Ref. [15], without taking account the finite-key size effect. After performing the error correction [22] and privacy amplification [23], the final secure key length is given by $NR \geq n_{\mathrm{sift}}[1 - f(\delta_b)H_2(\delta_b) - H_2(\delta_p)]$, where NR is the final secure key length, n_{sift} is the sifted key length, the item of $f(\delta_b)H_2(\delta_b)$ represents the secure-key cost of error correction, the item of $H_2(\delta_p)$ represents the secure-key cost of privacy amplification, $\delta_b(\delta_p)$ is the bit (phase) error rate, $f(x)$ is the error correction efficiency as a function of the error rate, normally $f(x) \geq 1$ with $f(x) = 1$ at the Shannon limit, and $H_2(x)$ is the binary entropy function: $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

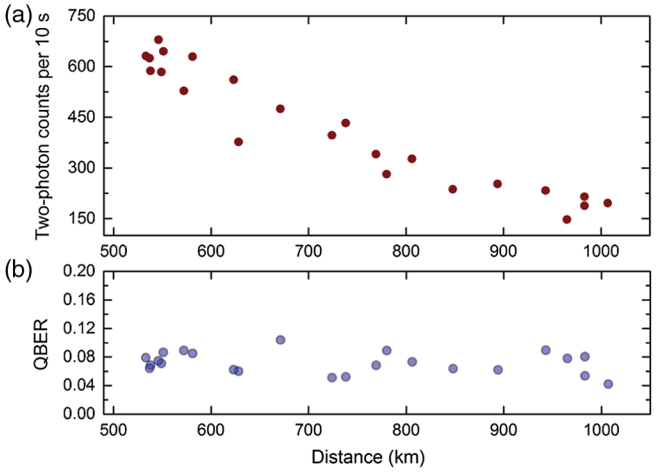

FIG. 4. Performance of the satellite-to-ground entanglement-based QKD during one orbit. The typical distance from the satellite to the ground station varies from 530 to 1000 km. (a) The coincident counts with different distances between the satellite and the ground. (b) The overall QBER with different distances between the satellite and the ground.

Because of the symmetry of the $|+\rangle/|-\rangle$ and $|H\rangle/|V\rangle$ bases measurement, δ_b and δ_p are given by $\delta_b = \delta_p = E_\lambda$, where E_λ is the overall QBER. The error correction efficiency is evaluated by considering the low-density parity-check codes and progressive edge-growth algorithm [24]. Here, we set $f(x) = 1.2$. Finally, we obtain 831 bits of final secure key. This corresponds to an average key distribution rate of 3.5 bits/s, which is ~1.5 times higher than the previous experiment using terrestrial free-space channel with a distance of 144 km [17].

We note that in this current work the triggering efficiency in the satellite is set to be 1% due to the storage limit. This can be straightforwardly improved, which can readily increase the average final key rate to ~350 bits/s. Compared to directly transmitting one of the entangled photons over a distance over 500–1600 km using commercially best-performance optical fibers (with a loss of 0.16 dB/km), we estimate that the effective link efficiency of the satellite-based method is on average 4–5 orders of magnitude higher. The next step is to extend our current work to the bidirectional distribution of entanglement [21] and generate secure keys between two remote locations on Earth without replying on any trustful relay.

We thank colleagues at the National Space Science Center, China Xi'an Satellite Control Center, National Astronomical Observatories, Purple Mountain Observatory, and Qinghai Station for their management and coordination. We thank G.-B. Li, S.-L. Li, Z. Wang, and W.-W. Ye for their long-term observation assistance. This work was supported by the Strategic Priority Research Program on Space Science of the Chinese Academy of Sciences and by the National Natural Science Foundation of China.

J. Y. and Y. C. contributed equally to this work.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), p. 175.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[6] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).
[7] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[9] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[10] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[11] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007); D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007); T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).
[12] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).
[13] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu *et al.*, Nature (London) **549**, 43 (2017).
[14] S.-K. Liao, J. Lin, J.-G. Ren, W.-Y. Liu, J. Qiang, J. Yin, Y. Li, Q. Shen, L. Zhang, X.-F. Liang, H.-L. Yong, F.-Z. Li, Y.-Y. Yin, Y. Cao, W.-Q. Cai *et al.*, Chin. Phys. Lett. **34**, 090302 (2017).
[15] X. Ma, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
[16] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, Phys. Rev. Lett. **94**, 150501 (2005).
[17] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik *et al.*, Nat. Phys. **3**, 481 (2007).
[18] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[19] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82 (2002).
[20] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, Opt. Express **15**, 15377 (2007).
[21] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li *et al.*, Science **356**, 1140 (2017).
[22] G. Brassard and L. Salvail, *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology. Lofthus, Norway* (Springer-Verlag, New York, 1994), p. 410.
[23] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[24] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, IEEE Trans. Inf. Theory **51**, 386 (2005).