Free-Space and Fiber-Integrated Measurement-Device-Independent Quantum Key Distribution under High Background Noise

Yu-Huai Li,[1,2,3] Shuang-Lin Li,[1,2,3] Xiao-Long Hu,[4] Cong Jiang,[4] Zong-Wen Yu,[4,5] Wei Li,[1,2,3] Wei-Yue Liu,[1,2,3] Sheng-Kai Liao,[1,2,3] Ji-Gang Ren,[1,2,3] Hao Li,[6] Lixing You,[6] Zhen Wang,[6] Juan Yin,[1,2,3] Feihu Xu,[1,2,3] Qiang Zhang,[1,2,3] Xiang-Bin Wang,[2,4] Yuan Cao,[1,2,3,*] Cheng-Zhi Peng,[1,2,3,†] and Jian-Wei Pan[1,2,3,‡]

[1]*Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences,*
University of Science and Technology of China, Hefei 230026, China
[2]*Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics,*
University of Science and Technology of China, Shanghai 201315, China
[3]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*
[4]*State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University,*
Beijing, 100084, People's Republic of China
[5]*Data Communication Science and Technology Research Institute, Beijing 100191, China*
[6]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology,*
Chinese Academy of Sciences, Shanghai 200050, People's Republic of China

(Received 10 March 2023; accepted 17 August 2023; published 6 September 2023)

Measurement-device-independent quantum key distribution (MDI QKD) provides immunity against all attacks targeting measurement devices. It is essential to implement MDI QKD in the future global-scale quantum communication network. Toward this goal, we demonstrate a robust MDI QKD fully covering daytime, overcoming the high background noise that prevents BB84 protocol even when using a perfect single-photon source. Based on this, we establish a hybrid quantum communication network that integrates free-space and fiber channels through Hong-Ou-Mandle (HOM) interference. Additionally, we investigate the feasibility of implementing HOM interference with moving satellites. Our results serve as a significant cornerstone for future integrated space-ground quantum communication networks that incorporate measurement-device-independent security.

DOI: 10.1103/PhysRevLett.131.100802

Quantum key distribution (QKD) in principle offers information-theoretical security for private communication [1,2]. However, due to device imperfections in realistic setups, there exist attacks in practical QKD [3]: specifically, the photon number splitting (PNS) attack on an imperfect single-photon source [4,5] and various types of attacks on measurement devices [6–9]. The decoy-state method [10,11] addresses the PNS attack issue with standard weak coherent pulses generated by attenuated laser pulses and has become a standard technique in current QKD experiments [12]. Measure-device-independent QKD (MDI QKD) [13,14] enhances the security of QKD against any detector imperfections. By combining the decoy-state method, MDI QKD can perfectly solve all possible attacks on measurement devices and the PNS attack on an imperfect source in a realistic QKD system.

In recent years, the successful operation of the Micius quantum science satellite [15–20], along with other efforts targeting nanosatellite-based long-distance quantum communication [21–24] and fiber-based backbone connecting metropolises [25], demonstrate the practical feasibility of a future global quantum network. With MDI QKD recently implemented in free space for the first time [26], extending its use in future global-scale quantum communication network is essential for enhancing the security of QKD in practice. Simultaneously, achieving robust, all-day functioning capabilities is fundamental for a large-scale quantum communication network encompassing numerous satellites across different time zones worldwide [27,28]. A flexible interface that links free space and fiber is also necessary for practical quantum communication between space and ground. Owing to the high velocity between satellites and the ground, the feasibility of independent photons interference between moving objects in MDI QKD must be thoroughly investigated.

In this Letter, we have conducted a thorough examination of the aforementioned aspects in free-space and fiber hybrid channels toward a global-scale quantum network. (i) We accomplish a robust free-space MDI QKD in daylight. To overcome the bright background light, one may reduce the actual background noise in practice or improve the noise tolerance theoretically. Efforts have been made to reduce the actual background noise by spatial, spectral, and temporal filtering [27,28]. For MDI QKD, it is worth noting that, due to the twofold coincidence nature, the tolerance of background noise is greatly increased, making the scheme suitable for daylight applications. We experimentally verified this on a 7.7-km free-space channel by performing MDI QKD fully covering daytime, from 8 a.m. to 5 p.m. Notably, our system using weak coherent sources operates under background noise levels exceeding the limit of the BB84 protocol with a perfect single-photon source [29]. (ii) Building upon this, we establish a hybrid quantum communication network with two free-space channels (7.7 and 1.4 km, respectively) and a 75-km fiber channel. Utilizing single-mode-fiber coupling based on adaptive optics (AO), we achieve Hong-Ou-Mandel (HOM) interference between photons from free-space and fiber channels, serving as the interface and outcome of MDI QKD. (iii) Moreover, we conduct a feasibility study of HOM interference with a moving satellite, and our experimental results indicate that high interference quality can be implemented using state-of-the-art technology.

Our daylight free-space MDI QKD is conducted over the 7.7-km urban atmosphere and 75-km fiber coil between Alice and Bob, as shown in Fig. 1. Generally speaking, the background noise during daytime is more than 5 magnitudes higher than that at full moon midnight under the same meteorological and geographical conditions [27,38]. Consequently, spectral filtering is a critical aspect for free-space QKD in the daytime. However, a narrow band filter typically incurs additional loss in signal photons and necessitates a much higher accuracy of frequency calibration between the source and filters. Particularly for MDI QKD, since a twofold coincidence measurement is required between photons from two different channels, the additional filtering loss is doubled. Interestingly, the requirement for twofold coincidence measurement allows MDI QKD to tolerate considerably high background noise, thereby enabling the relaxation of filtering bandwidth. In our experiment, after filtering by a dense wavelength division multiplexer (DWDM) with a bandwidth of 0.8 nm, the background noise is reduced to an acceptable level, and the extra loss of signal became negligibly small.

Furthermore, atmospheric turbulence on a sunny day is considerably more severe than that at night. This turbulence distorts the spatial mode of the laser beam, significantly impairing the quality of HOM interference in MDI QKD. We address this issue through the use of AO and a postselection method. We employ an additional 1570-nm laser transmitted through the same atmospheric channel as the signal and detected by a high-speed photodiode for each

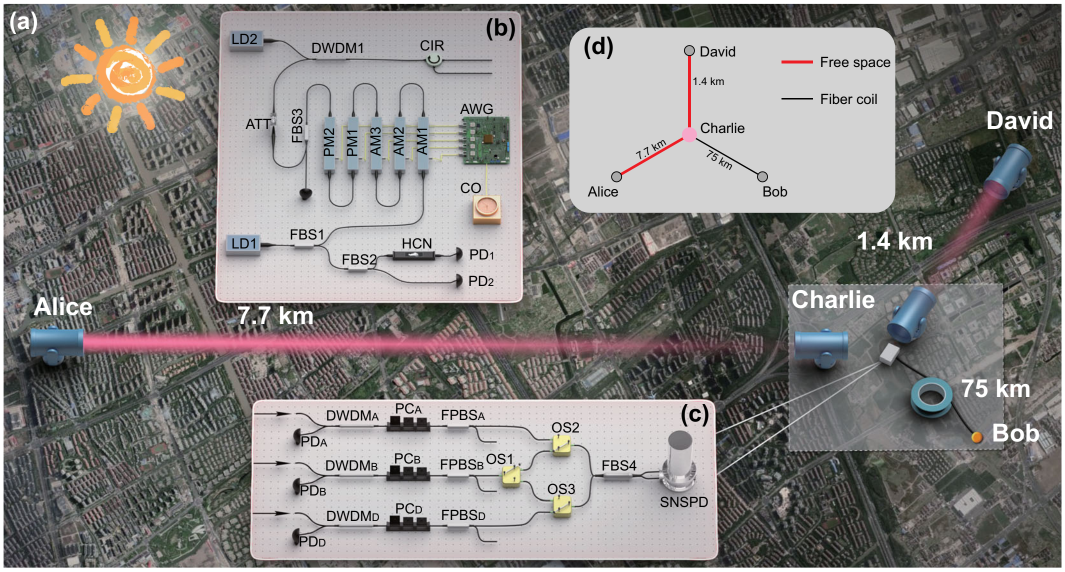

FIG. 1. Setup of free-space and fiber-integrated MDI QKD. (a) Top view of the experimental layout in the Pudong area, Shanghai. The distances of the two free-space channels are 7.7 and 1.4 km, respectively. Signal pulses are sent by 280-mm-diameter telescopes and received by 400-mm-diameter telescopes. Both the transmitters and the receivers are equipped with a tracking system to ensure an optimized efficiency. A 75-km-long fiber coil connects the measurement terminal to the third encoding terminal. (b) A detailed diagram of the encoding terminals. A portion of the signal laser is transmitted through a hydrogen cyanide (HCN) gas absorption cell for optical frequency calibration. The remaining portion is modulated using amplitude modulators (AMs) and phase modulators (PMs) to construct pulse pairs, decoy-state, time-bin encoding, phase encoding, and phase randomization. The modulation pattern's timing sequence is generated using a homemade arbitrary waveform generator (AWG), with its clock locked to an ultrastable crystal oscillator (CO). (c) After filtering by dense wavelength division multiplexers (DWDMs), the incoming signal photons enter an optical switch (OS) network-based router. Two beams are selected for interference measurement using superconducting nanowire single-photon detectors (SNSPDs) with a detection efficiency of approximately 70% and dark counts below 30 cps. The detection output is recorded with a time-to-digital converter, whose clock is also locked to an ultrastable CO. (d) The topology of the setup. LD, laser diode; PD, photodiode; FBS, fiber beam splitter; FPBS, fiber polarizing beam splitter; PC, polarization controller; CIR, circulator; ATT, attenuation.

channel to probe the instantaneous channel efficiency. This serves as the reference for both AO and the postselection method. AO can be classified as conventional AO with aberration measurement [39] and optimized AO without aberration measurement [40]. The latter is more suitable for the long-distance horizontal free-space channel since strong turbulence can cause intensity scintillations and phase discontinuity, leading to errors in aberration measurement. Utilizing the measured intensity as input and a deformable mirror as output, we operate a modal version of the stochastic parallel gradient descent (M-SPDG) algorithm-based optimized AO system [40] to compensate for the first 12 orders of Zernike aberration. It effectively corrects the primary part of the atmospheric turbulence, with frequencies in the tens of hertz range, as well as the static aberration of the 400-mm-diameter receiver telescope. The AO enhances single-mode-fiber coupling efficiency and suppresses intensity fluctuations in most scenarios during the day, at a distance of 7.7 km, which is comparable to the effective thickness of the atmosphere [12]. Furthermore, we postselect twofold clicking events in time windows where the ratio of probe lights intensities is sufficiently close to an expected value. At a certain moment, we denote the efficiency of the two channels as $\eta_1(t)$ and $\eta_2(t)$, respectively. The efficiency of a free-space channel is estimated by the measured intensity of the corresponding probe light, which varies dramatically with time. The efficiency of a fiber channel is stable and measured beforehand. The ratio of two channel efficiencies $r_\eta(t) = \eta_1(t)/\eta_2(t)$ serves as a reliable indication for postselection of signals. A ratio that deviates from the expected value suggests an intensity mismatch of signal pulses. Consequently, we only select signal pulses at moments that satisfy $(1/r_t) > [r_\eta(t)/r_e] > r_t$, where r_e represents the expected value and r_t denotes the threshold. Owing to the measurement-device-independent nature of the protocol, r_t and r_e can be determined afterward, optimizing key generation based on a specific atmospheric condition. In our Letter, we choose r_t values between 0.34 and 0.58. We employ the Fried parameter r_0 [30], or Fried's coherence length, to describe the strength of atmospheric turbulence, with smaller r_0 values indicating stronger turbulence. Notably, under extremely strong turbulence conditions, such as during sunny noon, the intensity fluctuation cannot be effectively suppressed by AO; thus, the postselection method plays a more significant role. As shown in Fig. 2, a positive final key rate can still be generated with a small r_0 of ~1.8 cm (at 810 nm), equivalent to ~4.5% of the receiving diameter.

A detailed diagram of the encoding terminals is illustrated in Fig. 1(b). To implement the decoy-state MDI QKD [31,41–43], the four-intensity protocol was employed [32,33]. A continuous-wave (cw) distributed feedback (DFB) laser diode with a wavelength of 1550 nm and a linewidth of 10 MHz is utilized in each encoding terminal.

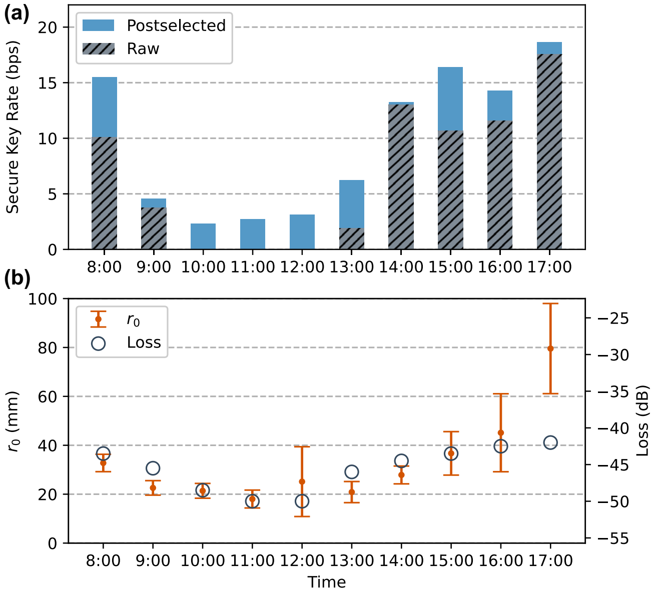

FIG. 2. Results of MDI QKD at each hour of daytime. (a) The estimated secure key rate for different times during the full day, without considering statistic fluctuation. All collected data are grouped in units of one hour. Higher secure key rates are obtained using the postselection method (blue bars). By summing up all the achieved data from 8:00 to 17:00, 35 629 bits of the final key were distilled in 20 786 s, taking statistical fluctuations into account. (b) The mean atmospheric turbulence parameter r_0 (see text) and the loss for each hour. The single-mode-fiber coupling efficiency makes a prominent contribution to channel loss under strong atmospheric turbulence, i.e., small r_0. Consequently, the values of r_0 and loss at different times are highly correlated during the daytime. As atmospheric turbulence subsides at dusk, reflected as large r_0, the correlation weakens.

The background noise associated with 1550-nm light is only 3% of the background noise by 800-nm light [27]. A portion of the signal laser is transmitted through a hydrogen cyanide gas cell for optical frequency calibration. The remaining portion is modulated using amplitude modulators (AMs) and phase modulators to create pulse pairs, decoy-state, time-bin encoding, phase encoding, and phase randomization with a pulse pair repetition rate of 250 MHz and a pulse duration of 1 ns. Time-phase encoding is used in the experiment. In the Z basis, the key bit is encoded by eliminating the later pulse or the earlier pulse, while in the X basis, the key bit is encoded into the linear superposition state with relative phases of 0 or π between the two pulses. Pulse pairs are directly modulated by AMs on the cw laser, rather than passing single pulses through an unbiased Mach-Zehnder interferometer (MZI). Given that the pulse separation of 2 ns is significantly shorter than the laser's coherence time of 100 ns, the relative phase between the two pulses is stable. The timing sequence of the modulation pattern is generated using a homemade arbitrary waveform generator, with its clock locked to an ultrastable crystal oscillator to ensure a low-frequency drift. The residual differences in clock frequency are measured and compensated by evaluating the pulse arrival times at Charlie's terminal, ultimately achieving a time synchronization accuracy of 32 ps [26], which ensures high indistinguishability in the time domain. The encoded signal is sent along with an additional 1570-nm probe laser of approximately 10-mW emitting power.

A total sifted key of 1 295 684 was obtained in 20 786 s after postselection, from which 35 629 bits of the final key were distilled using the double-scanning method [34]. The error rates on the Z-Z and X-X bases are 0.69% and 32.7%, respectively. As the experiment was performed before the double-scanning method was proposed, experimental parameters were set according to the single-scanning method. The key rate would be even higher with the optimization of the double-scanning method. For each one-hour interval, the channel efficiency and the final key rate are estimated, along with r_0 values, as shown in Fig. 2(b). Particularly, the strongest atmospheric turbulence and the largest background noise typically occur at noon. To demonstrate the high background noise tolerance of our system, we replace the DWDM with a bandwidth of 0.8 nm with an interference filter featuring a bandwidth of 3 nm at noon. When disregarding statistical fluctuation, a final secure key rate of 9.33 bps (bits per second) was obtained, under an observed background noise of 12.9 kcps (kilo counts per second) on a sunny day with the solar altitude angle of around 50°. It is interesting to note that the BB84 protocol with a perfect single-photon source has the highest secure key rate among all prepare-and-measurement schemes of qubit-encoded QKD under the same condition and can be considered as a benchmark for evaluating other QKD schemes. As shown in the Supplemental Material [29], the BB84 protocol with a perfect single-photon source fails to work under such a high noise level as in this Letter.

We express that all MDI QKD network demonstrations were implemented in optical fibers before our current work. Prior art MDI QKD network have been limited to fiber channel only. However, in order to achieve the ultimate goal of integrating a space-to-ground global quantum communication network, a hybrid and scalable network comprising both fiber and free-space channels is essential. Here, trade-offs are made on the selection of wavelength to satisfy the requirement of both types of channels. To facilitate long-distance transmission in fiber channels, we need to use telecom wavelengths. However, as this wavelength is much longer than visible light, additional diffraction loss is introduced in free-space channels. Moreover, prior works have relied on additional fiber channels to share time and frequency standard [44,45], which constrained the network scalability. In our experiment, the frequency and temporal domain of each user node are locked independently. In addition, pulse pairs for the encoding are generated through external modulation of a cw laser rather than constructing an asymmetric MZI. These improvements render the stability of our system unaffected by the number of users, providing a distinct advantage in scalability for our MDI QKD network system. All three encoding terminals concurrently transmit signal pulses to the measurement terminal through distinct channels. Three optical switches are utilized to direct two of these signals for interference measurement. The routing of optical switches in the measurement terminal undergoes alterations in several-minute intervals to display the capability to arbitrarily select encoding nodes. The detailed parameters for the setup are presented in the Supplemental Material [29]. The corresponding final key rates are 4.325 bps (Alice-Bob), 1.506 bps (Alice-David), and 3.261 bps (Bob-David), respectively, estimated using the double-scanning method. As no data were collected under extreme conditions during noon time, the final key rate is slightly higher than the above full-day demonstration.

We further demonstrate the feasibility of performing MDI QKD with a satellite. Because of the rapid movement of satellites, the arrival time of signal pulses varies on the order of milliseconds, while frequency variations lie within the range of several gigahertz [29,46]. The variation in both degrees of freedom significantly disrupts the indistinguishability of arrival pulses and should be compensated to achieve high-quality HOM interference. Fortunately, the precise values of distances and frequency shifts can be predicted in advance or in real time. Notably, with the assistance of laser ranging [47], satellite orbit determination can achieve a precision of approximately 1 cm (corresponding to an arrival time precision of $\delta T = 33$ ps) and 1 cm/s (corresponding to a frequency shift precision of $\delta f = 6.5$ kHz). The relationship $\delta T \delta f = 2.2 \times 10^{-6} \ll 1/4\pi$ indicates that high visibility HOM interference can be achieved with appropriate compensation for frequency and time [48]. Doppler frequency shift compensation can be effectively implemented by adjusting the temperature of the laser cavity or introducing an additional electro-optic modulator (EOM) or acoustic-optic modulator (AOM) [49]. Employing a field-programmable gate array and high-speed digital-to-analog converter, the emitting time of optical pulses can be fine-tuned to the order of several picoseconds, ensuring indistinguishable arrival times in variable channels.

A proof-of-principle experiment is performed to demonstrate the feasibility of compensating for Doppler frequency shifts. The DFB laser has a frequency-temperature coefficient of approximately 12.5 GHz/K. This implies that by adjusting the temperature of the laser cavity by 0.6 K, the frequency of the laser can be tuned by 7.5 GHz. We perform HOM interference between two independently temperature-controlled DFB lasers to demonstrate frequency shift compensation, as shown in Fig. 3. A Doppler frequency shift covering 6.87 GHz over 500 s is calculated based on Micius' orbit, and can be considered close to the worst-case scenario. The temperature of the

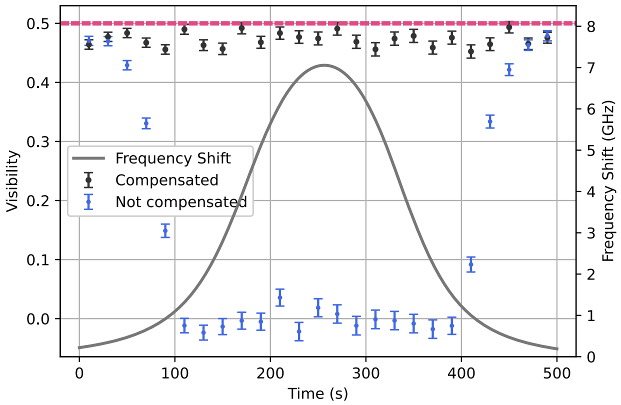

FIG. 3. Compensation of Doppler frequency shift by controlling the temperature of laser diodes. The gray curve represents the expected Doppler frequency shift between arrival photons calculated based on the orbit of Micius. One of the lasers is temperature modulated to simulate this frequency shift. In the absence of compensation, the visibility of HOM interference diminishes due to a substantial frequency difference (blue). By modulating the temperature of the other laser, the frequency shift is compensated in real time, and the visibility is maintained up to the limit of 0.5 (black).

first laser is modulated according to the frequency shift curve, thus simulating the Doppler frequency shift between the arrival photons associated with a moving satellite. As the temperature of the second laser remains unchanged, the visibility of HOM interference rapidly decreases to 0. To compensate, the temperature of the second laser is also modulated according to the expected frequency shift. In this case, an average visibility of 0.472 is achieved, which is near the visibility limit of 0.5 when using coherent light.

In conclusion, we have successfully demonstrated, for the first time, a free-space MDI QKD in full daytime and a hybrid MDI QKD network comprising both free-space and fiber channels. To further enhance the key rate for a practical system in the future, several improvements can be developed, including increasing the pulse repetition rate, optimizing AO technology to augment the average channel efficiency and suppress fluctuation, and dynamically adjusting the QKD parameters. The robustness of our system against background noise indicates promising potential for practical application in the future. Alongside the study of interference from moving objects, there is substantial feasibility for an integrated space-ground quantum communication network with MDI QKD, or even twin-field QKD [50].

We acknowledge insightful discussions with Bo Li and Na Li. This work was supported by the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300100), the National Key R&D Program of China (Grants No. 2020YFA0309803 and No. 2020YFC2200103), the National Natural Science Foundation of China (Grants No. 11904358, No. 12174374, and No. 12274398), the Chinese Academy of Sciences (CAS), Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), the Natural Science Foundation of Shanghai (Grant No. 20ZR1473700), the Shanghai Rising-Star Program (Grant No. 21QA1409600), and Anhui Initiative in Quantum Information Technologies. Y. Cao and Y.-H. Li were supported by the Youth Innovation Promotion Association of CAS (under Grants No. 2018492 and No. 2023475).

Y.-H. L. and S.-L. L. contributed equally to this work.

[*] yuancao@ustc.edu.cn
[†] pcz@ustc.edu.cn
[‡] pan@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[4] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[5] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A **61**, 052304 (2000).

[6] F. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12**, 113026 (2010).

[7] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[10] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[11] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[12] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, Micius quantum experiments in space, Rev. Mod. Phys. **94**, 035001 (2022).

[13] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[14] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[15] S.-K. Liao *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).

[16] S.-K. Liao *et al.*, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120**, 030501 (2018).

[17] J. Yin *et al.*, Satellite-based entanglement distribution over 1200 kilometers, Science **356**, 1140 (2017).

[18] J. Yin *et al.*, Entanglement-based secure quantum cryptography over 1,120 kilometres, Nature (London) **582**, 501 (2020).

[19] J. Yin *et al.*, Satellite-to-Ground Entanglement-Based Quantum Key Distribution, Phys. Rev. Lett. **119**, 200501 (2017).

[20] J.-G. Ren *et al.*, Ground-to-satellite quantum teleportation, Nature (London) **549**, 70 (2017).

[21] A. Villar, A. Lohrmann, X. Bai, T. Vergoossen, R. Bedington, C. Perumangatt, H. Y. Lim, T. Islam, A. Reezwana, Z. Tang, R. Chandrasekara, S. Sachidananda, K. Durak, C. F. Wildfeuer, D. Griffin, D. K. L. Oi, and A. Ling, Entanglement demonstration on board a nano-satellite, Optica **7**, 734 (2020).

[22] Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, L. Sha, G. C. Hiang, D. K. L. Oi, and A. Ling, Generation and Analysis of Correlated Pairs of Photons Aboard a Nano-satellite, Phys. Rev. Appl. **5**, 054022 (2016).

[23] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nat. Photonics **11**, 502 (2017).

[24] S. K. Joshi *et al.*, Space QUEST mission proposal: Experimentally testing decoherence due to gravity, New J. Phys. **20**, 063016 (2018).

[25] Y.-A. Chen *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature (London) **589**, 214 (2021).

[26] Y. Cao *et al.*, Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **125**, 260503 (2020).

[27] S.-K. Liao *et al.*, Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, Nat. Photonics **11**, 509 (2017).

[28] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics, npj Quantum Inf. **7**, 93 (2021).

[29] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.100802 for details on four-intensity protocol, the limit of the BB84 protocol, turbulence measurement, parameters for free-space and fiber MDI-QKD network, and configurations for network with satellite, which includes Refs. [30–37].

[30] D. L. Fried, Optical resolution through a randomly inhomogeneous medium for very long and very short exposures, J. Opt. Soc. Am. **56**, 1372 (1966).

[31] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method, Phys. Rev. A **91**, 032318 (2015).

[32] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A **93**, 042324 (2016).

[33] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel, Sci. Rep. **8**, 17634 (2018).

[34] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Higher key rate of measurement-device-independent quantum key distribution through joint data processing, Phys. Rev. A **103**, 012402 (2021).

[35] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[36] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[37] D. L. Fried, Differential angle of arrival: Theory, evaluation, and measurement feasibility, Radio Sci. **10**, 71 (1975).

[38] E.-L. Miao, Z-F. Han, S.-S. Gong, T. Zhang, D-S. Diao, and G.-C. Guo, Background noise of satellite-to-ground quantum key distribution, New J. Phys. **7**, 215 (2005).

[39] M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, K. E. Stoltenberg, J. F. Morris, M. Bareian, M. A. Harris, D. W. Oesch, M. D. Oliker, M. B. Flanagan, B. T. Kay, J. D. Schiller, and R. N. Lanning, Adaptive-Optics-Enabled Quantum Communication: A Technique for Daytime Space-to-Earth Links, Phys. Rev. Appl. **16**, 014067 (2021).

[40] K.-X. Yang, M. Abulizi, Y.-H. Li, B.-Y. Zhang, S.-L. Li, W.-Y. Liu, J. Yin, Y. Cao, J.-G. Ren, and C.-Z. Peng, Single-mode fiber coupling with a M-SPGD algorithm for long-range quantum communications, Opt. Express **28**, 36600 (2020).

[41] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A **87**, 012320 (2013).

[42] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).

[43] F. Xu, H. Xu, and H.-K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052333 (2014).

[44] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network, Phys. Rev. X **6**, 011024 (2016).

[45] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution over 200 km, Phys. Rev. Lett. **113**, 190501 (2014).

[46] X. Wang, C. Dong, S. Zhao, Y. Liu, X. Liu, and H. Zhu, Feasibility of space-based measurement-device-independent quantum key distribution, New J. Phys. **23**, 045001 (2021).

[47] M. R. Pearlman, C. E. Noll, E. C. Pavlis, F. G. Lemoine, L. Combrink, J. J. Degnan, G. Kirchner, and U. Schreiber, The ILRS: Approaching 20 years and planning for the future, J. Geod. **93**, 2161 (2019).

[48] P. Pfeifer and J. Fröhlich, Generalized time-energy uncertainty relations and bounds on lifetimes of resonances, Rev. Mod. Phys. **67**, 759 (1995).

[49] X.-B. Wang, C.-X. Yang, and Y.-B. Liu, On-demand entanglement source with polarization-dependent frequency shift, Appl. Phys. Lett. **96**, 201103 (2010).

[50] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and S. A. J., Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).