Featured in Physics

Experimental Mode-Pairing Measurement-Device-Independent Quantum Key Distribution without Global Phase Locking

Hao-Tao Zhu,[1,2,3] Yizhi Huang,[4] Hui Liu,[1,2,3] Pei Zeng,[1,2,3] Mi Zou,[1,2,3] Yunqi Dai,[5] Shibiao Tang,[5] Hao Li,[6] Lixing You,[6] Zhen Wang,[6] Yu-Ao Chen,[1,2,3] Xiongfeng Ma,[4,*] Teng-Yun Chen,[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]*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Hefei National Laboratory, University of Science and Technology of China, Hefei, Anhui 230088, China*

[4]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[5]*QuantumCTek Corporation Limited, Hefei, Anhui 230088, China*

[6]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

(Received 16 June 2022; accepted 15 November 2022; published 17 January 2023)

In the past two decades, quantum key distribution networks based on telecom fibers have been implemented on metropolitan and intercity scales. One of the bottlenecks lies in the exponential decay of the key rate with respect to the transmission distance. Recently proposed schemes mainly focus on achieving longer distances by creating a long-arm single-photon interferometer over two communication parties. Despite their advantageous performance over long communication distances, the requirement of phase locking between two remote lasers is technically challenging. By adopting the recently proposed mode-pairing idea, we realize high-performance quantum key distribution without global phase locking. Using two independent off-the-shelf lasers, we show a quadratic key-rate improvement over the conventional measurement-device-independent schemes in the regime of metropolitan and intercity distances. For longer distances, we also boost the key rate performance by 3 orders of magnitude via 304 km commercial fiber and 407 km ultralow-loss fiber. We expect this ready-to-implement high-performance scheme to be widely used in future intercity quantum communication networks.

DOI: 10.1103/PhysRevLett.130.030801

Quantum key distribution (QKD) [1,2], as a building block of quantum networks, allows remote communication parties to establish a secure key based on the laws of quantum physics [3,4]. Currently, many QKD networks of various sizes have been implemented worldwide, such as metropolitan [5–8] and intercity scales [9]. For a metropolitan network, the loss budget between two nodes is around 10 dB [8]. Usually, the network users are connected to trusted nodes as service providers. For an intercity network, the single-link loss is typically 20 dB. Often, we need to set up trusted relays outside of cities [9]. In practice, when one of the trusted nodes is compromised, the network security can be severely damaged [10]. Also, it is difficult and expensive to ensure the security of relay nodes outside cities. Moreover, due to the complicated construction of single-photon detectors, imperfect detection devices would introduce security loopholes [11,12].

To close the detection loopholes and reduce the number and cost of trusted nodes, Lo *et al.* proposed measurement-device-independent quantum key distribution (MDI QKD) [13]. In a generic MDI QKD setup, as shown in Fig. 1, the two communication parties, Alice and Bob, emit encoded laser pulses to a detection site, owned by an untrusted party, Charlie. Charlie employs an interferometer as a quantum relay to correlate the received quantum signals. Charlie announces interference measurement results, based on which Alice and Bob can extract secure key bits. The security of MDI QKD requires no assumption on how Charlie performs measurement and announcement, making it naturally immune to all the detection attacks. Meanwhile, MDI QKD helps reduce the number of trusted nodes and makes quantum communication networks more implementable.

To pursue a practical usage of MDI QKD in metropolitan and intercity quantum networks, we need to consider two main issues: improving the key rate and reducing the experiment requirement. In the conventional MDI QKD schemes, Alice and Bob encode information into two optical modes, such as two adjacent pulses [14]. This type of encoding, namely two-mode encoding, is relatively simple to implement since it does not require additional devices and modulation. However, the performance of two-mode encoding schemes is limited by the overall channel transmittance η since it requires coincidence detection at

 © 2023 American Physical Society

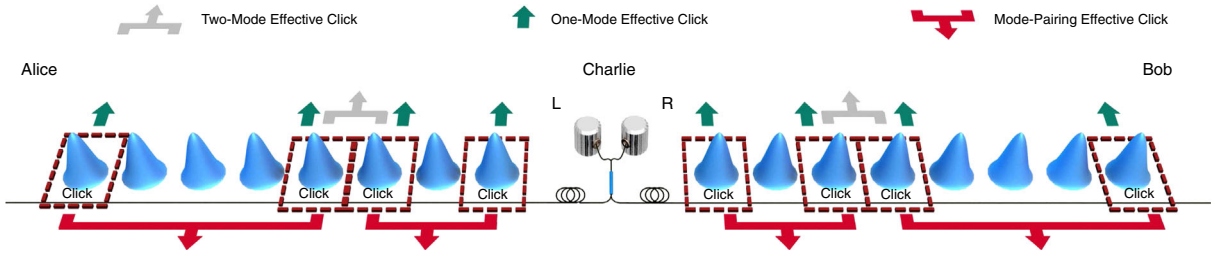

FIG. 1. Comparison of different MDI QKD schemes. In conventional MDI QKD schemes using two-mode encoding, key information is encoded into two predetermined pulses. Only when Charlie detects both pulses can Alice and Bob learn the encoded information, denoted as gray arrows. In twin-field QKD schemes using one-mode encoding, key information is encoded into one pulse, which is easily disturbed in the channel. When Charlie announces a click on a pulse, denoted as a green arrow, Alice and Bob can derive a key bit. In mode-pairing MDI QKD, Alice and Bob encode information into one pulse to get rid of the coincident detection requirement and pair the clicked pulses based on detection results. They can distill one key bit from any two paired successful detections, denoted as red arrows, which is robust against channel disturbance.

two optical modes. Another type of MDI QKD, twin-field QKD [15], can achieve a quadratic improvement in the key rate. We refer to this as one-mode encoding. In one-mode encoding schemes, Alice and Bob encode information into a single optical pulse, and then Charlie performs a single-photon interference to correlate pulses from two users. This type of encoding, however, necessitates a more challenging experiment implementation because it is more sensitive to environmental noises, especially phase fluctuations of lasers and phase drifts in optical channels. To suppress noises, existing experiments apply advanced global phase-locking techniques [16–21] to stabilize the phase references between two remote parties, which remains challenging and impractical for large-scale applications.

From the comparison of the existing MDI QKD schemes above, there seems to be a trade-off between high performance and simple implementation. Surprisingly, a recent MDI QKD proposal, mode-pairing quantum key distribution (MP QKD) [22], employs a hybrid encoding method to offer both high performance and simple implementation. See also Ref. [23] for a similar idea without a rigorous security proof. Different types of MDI QKD schemes are illustrated in Fig. 1. In MP QKD, Alice and Bob encode key information in a single optical pulse. After Charlie's announcement, they *pair* all the detected locations and generate raw key bits among each pair. The core observation of MP QKD is that the two optical modes used to encode the relative information can be determined after Charlie's announcement. At the encoding and detecting stage, Alice and Bob only consider a single mode and do not require coincidence detection in predetermined locations. At the postprocessing stage, they generate the raw key bits from two pulses and avoid the global phase-locking requirement. Therefore, the users can achieve a quadratic improvement in key rate with simple hardware implementation.

By adopting two off-the-shelf lasers, we realize this high-performance MDI QKD without global phase locking. To this end, we adjust the original MP QKD protocol [22] and introduce phase reference estimation techniques to deal with the frequency fluctuation of two independent lasers. The results show that our implementation can achieve a quadratic key-rate improvement over the conventional MDI QKD schemes.

We now briefly introduce the MP QKD scheme and leave a complete description in Supplemental Material [24]. In each round, Alice generates a laser pulse of coherent state $|\sqrt{\mu^a}e^{i\phi^a}\rangle$ with modulated intensity μ^a randomly chosen from $\{0,\nu,\mu\}$ and modulated phase randomly chosen from $\{0,(2\pi/D),(4\pi/D),\ldots,[2\pi(D-1)/D]\}$. In this Letter, we pick up $D=16$ and $0<\nu<\mu<1$. Similarly, Bob generates a coherent state $|\sqrt{\mu^b}e^{i\phi^b}\rangle$. They then emit the two coherent laser pulses to Charlie, who performs the interference using a balanced beam splitter and two single-photon detectors L and R. Charlie then announces the detection results of each pulse. After repeating the above procedure for many rounds, Alice and Bob postselect all the rounds with successful detection that either L or R clicks. They "pair" these rounds and determine the basis and key values on each pair based on the relative intensity and phase information. Afterward, they perform basis sifting, key mapping, and data post-processing similar to the two-mode MDI QKD schemes.

The final key length of the MP scheme is given by

$$K = M_{11}^{Z}[1-h(e_{11}^{Z,ph})] - fM_{\mu\mu}h(E_{\mu\mu}), \tag{1}$$

where $h(x)=-x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy function and f is the error correction efficiency. The single-photon component of the Z-basis pairs, M_{11}^{Z}, and the corresponding phase error rate, $e_{11}^{Z,ph}$, can be estimated by the decoy-state method [25–27]. The number of pairs used to distill final key bits, $M_{\mu\mu}$, and the bit error rate, $E_{\mu\mu}$, can be directly obtained from the experiment. For simplicity, here we only use the Z-basis pairs with intensities (μ,μ) for key generation. The key rate is defined

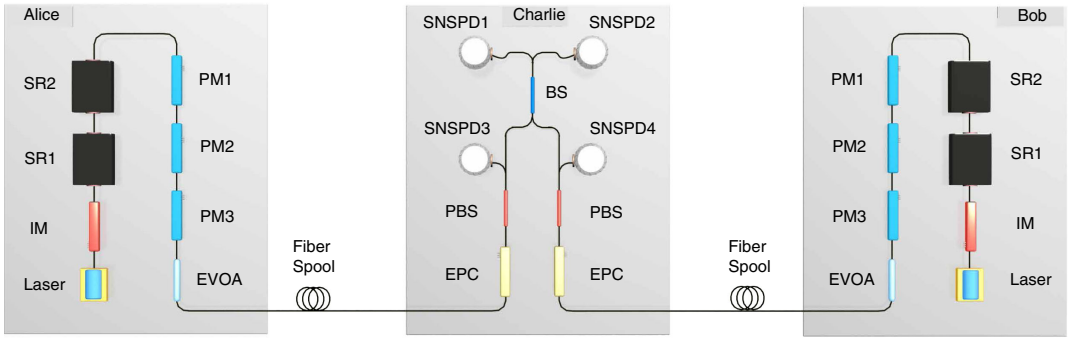

FIG. 2. Experimental setup. Alice's and Bob's setups are identical, but their encoding modulations are independent. The continuous-wave laser is chopped into discrete pulses by an intensity modulator (IM). Then these pulses are randomly modulated into one of the four intensities—strong, signal, decoy, and vacuum pulses—with the aid of two Sagnac rings (SR1, SR2). Three phase modulators (PM1, PM2, PM3) are used for phase encoding and active phase randomization. The encoded pulses are attenuated to the single-photon level by an electrical variable optical attenuator (EVOA) and transmitted to Charlie. Before interference measurements, the pulse polarisation is aligned by an electric polarization controller (EPC) and a polarization beam splitter (PBS). Finally, the signals are detected by superconducting nanowire single-photon detectors (SNSPDs). SNSPD1 and SNSPD2 are used for interference detection, and SNSPD3 and SNSPD4 are used for polarization feedback and arriving time feedback. Note that we do not carry out any phase-locking operations in the setup.

as $R = K/N_{\text{pair}}$, where N_{pair} is the number of possible pairs and equals half the total number of rounds.

When we implement MP QKD with two independent lasers, it brings new challenges. When the fiber length increases, the probability of successful detection decreases, enlarging the average pairing length. Consequently, the phase references between the pairs of the two users will drift away due to the phase fluctuation of the lasers and fibers. This leads to a high phase error rate and hence a low key rate. To compensate for the phase reference deviation, Alice and Bob need to estimate the underlying phase reference. To do this, for some rounds, they emit strong light pulses without phase modulation for the interference detection. In a 100 μs cycle, Alice and Bob use the first 25.76 μs for strong light pulses, followed by a 3.07 μs recovery region of vacuum state to avoid the cross talks, and the rest 71.17 μs for QKD pulses. After Charlie announces the measurement results, Alice and Bob can use the maximum likelihood estimation (MLE) method to estimate the $\Delta\omega(t)$ with the click results of strong light pulses. The likelihood function we use is

$$f(\Delta\omega) = \sum_{(i,j)} \ln\left\{\frac{1}{2} + (-1)^{D_i - D_j}\frac{\cos\left[\Delta\omega\tau(j-i)\right]}{4}\right\}, \quad (2)$$

where i, j denote the locations of the two paired rounds and D_i, D_j denote corresponding results. For convenience, we use 0 to represent the left detector clicks and 1 to represent the right one clicks. The time interval between two adjacent pulses is τ. The summation here is taken over all possible pairs of strong light pulses. Alice and Bob can repeat the estimation steps to get frequency differences for a period of time. They fit the estimated results to obtain $\Delta\omega(t)$ of QKD pulses using 200 periods. More details and test results are shown in Supplemental Material [24].

The experimental setup is shown in Fig. 2. Alice and Bob employ the off-the-shelf continuous-wave lasers (ORION 1550 nm Laser Module) whose linewidth is 2 kHz and center wavelength is 1550.12 nm. An intensity modulator chops the emitted light into pulses of width 400 ps at 625 MHz. Then, the key and basis information is encoded into these pulses by two Sagnac rings and three phase modulators for different intensities and phases. Afterward, pulses are attenuated to the single-photon level by an electrical variable optical attenuator and transmitted to Charlie for interference detection. More details for the setup are shown in Supplemental Material [24].

We consider the experimental settings under the scenario of metropolitan and intercity quantum networks. For a metropolitan (intercity) network, the loss budget between Alice to the measurement site is around 10 dB [8] (20 dB [9]), corresponding to 100 km (200 km) fiber from Alice to Bob when using a symmetric channel. A longer intercity communication distance of 300 to 400 km is also of practical interest. Hence, we perform the experiment via 101, 202, 304 km standard and 407 km ultralow-loss optical fibers. The main experiment parameters are listed in Table I.

After Alice and Bob compensate for the phase differences using estimated $\Delta\omega(t)$, they can use the X-basis error rate to quantify how well they have estimated the phase reference. We test the X-basis error rate and the number of pairs under different pairing lengths and communication distances. The results show there is a trade-off: a larger l results in more pairs but increases the X-basis error rate. In practice, Alice and Bob can set a proper maximum pairing length $L_{\max}$, beyond which they

TABLE I. Experimental parameters. The mean photon numbers of signal and decoy states are denoted as μ and ν, respectively. The total transmittance of a single side is η. The total pulses sent by users is N. The maximum pairing length is $L_{\max}$. The detector dark count is about 34 Hz, corresponding to a rate of 2.72×10^{-8}/pulse. The detection efficiency is $\eta_d = 62.46\%$ including the insertion loss of 0.58 dB. The error-correction efficiency is $f = 1.1$. The security parameter is $\epsilon = 10^{-10}$.

	101 km	202 km	304 km	407 km
μ	0.309	0.338	0.531	0.429
ν	0.032	0.035	0.053	0.038
η	4.32×10^{-2}	6.80×10^{-3}	7.43×10^{-4}	2.18×10^{-4}
N	5.07×10^{11}	2.10×10^{12}	6.33×10^{12}	7.66×10^{13}
$L_{\max}$	500	1000	2000	2000

do not pair the corresponding clicks. For a short distance (101 km), the successful detection probability is high and the average pairing length is small, so we pick up $L_{\max} = 500$. The average pairing length is larger for a longer distance (202 km), so we pick up $L_{\max} = 1000$. For the cases of 304 and 407 km, we pick up $L_{\max} = 2000$, considering pairs with $l > 2000$ have a relatively high X-basis error rate and contribute little to the final key rate. We give the detailed results in Supplemental Material [24].

The key rates for different transmission distances are presented in Fig. 3. Here, the Z-basis error rate is in the order of 10^{-4} with the two Sagnac rings and the intensity modulator, giving over 40 dB of extinction ratio for the signal and vacuum states. We also compare the experimental results with numerical simulations along with

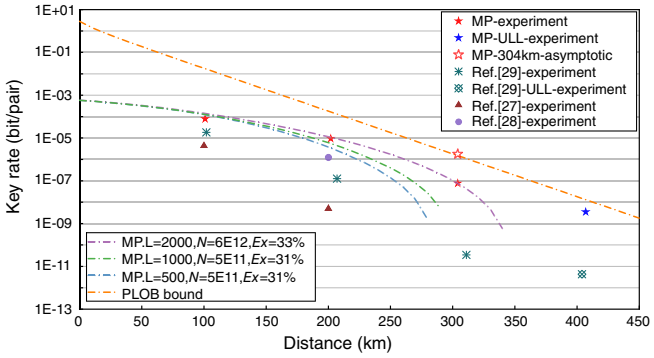

FIG. 3. Key-rate performance. The experimental rate-distance performance of MP QKD, compared with the theoretical simulations, along with the existing two-mode MDI QKD experimental results [28–30] and the linear key rate bound [31]. Data points marked by red and blue stars are key rates of our system using commercial fibers and ultralow loss (ULL) fibers, respectively. We also calculate the asymptotic key rate for the 304 km case based on the experimental data, marked by a hollow red star. Here, N is the total number of QKD rounds, L is the maximum pairing length, and E_X is the X-basis error rate. The theoretical expectation curves are simulated under different maximum pairing lengths, data sizes, and X-basis error rates.

previous experiments. As shown in the key-rate figure, the ratio between the key rate and the square root of the transmittance is given by $[(7.75 \times 10^{-5})/(4.32 \times 10^{-2})] = 1.80 \times 10^{-3}$ for 101 km and the ratio is $[(9.34 \times 10^{-6})/(6.80 \times 10^{-3})] = 1.37 \times 10^{-3}$ for 202 km. The results show that under the intercity communication distances (101 and 202 km), the key rate-transmittance relation of our system follows $R = O(\sqrt{\eta})$ rather than $O(\eta)$, indicating a quadratic improvement in the key rate.

For longer communication distances, even with higher X-basis error rates caused by larger phase fluctuations, the system can still maintain a key rate-transmittance relationship well above $R = O(\eta)$. Our system realizes key rates of 19.2 and 0.769 bits per second, respectively, via 304 km and 407 km fibers, 3 orders of magnitude higher than those of the existing MDI QKD experiments [30]. Besides, we calculate the asymptotic key rate of the 304 km case with the experimental data and show that our system has the potential to break the linear key rate bound [31]. For the one-mode MDI QKD schemes, the key rate is zero under the same setting since the phase differences between Alice and Bob are almost random without global phase locking. We give more comparison and discussion in Supplemental Material [24].

Our experiment shows that the MP QKD scheme owns clear advantages over the existing MDI QKD implementations, especially in the regime of metropolitan and intercity distances. We anticipate the MP QKD system and similar designs to improve the performance of quantum communication networks. Also, we expect that the design of the MP QKD experiment will be helpful for the construction of quantum repeaters [32,33], as well as extending the reach of the quantum internet.

In the future, the scheme has a few potential directions to explore. First, in terms of instrument hardware, increasing the system repetition rate is more beneficial to improving the key rate of the MP QKD scheme compared with other MDI QKD schemes. A higher repetition rate leads to shorter time intervals between the pulses. Hence, the users can choose a larger pairing interval to obtain more pairs. In addition, this is advantageous to the phase reference estimation and results in a lower X-basis error rate. The users can also use frequency multiplexing to achieve a similar goal since one can pair detection events from different spectrum channels in the mode-pairing scheme. Other improvements, such as narrowing the linewidth, or improving the stability, will also help increase the key rate further. Theoretically, applying more efficient pairing strategies could also benefit the key rate. Because of the low click probability caused by the low intensity and phase matching of the X-basis pairs, the number of them is relatively small, which affects the accuracy of parameter estimation. One possible solution is that re-pairing the clicks that fail to pair during key mapping stage. Intuitively, the pairing process does not reveal anything about the final

key bits, so repairing X-basis pairs should not affect security.

The authors acknowledge Y. Yan and G. Liu for the insightful discussions and B. Bai and J. Zhang for providing assistance on electronics. This work has been supported by the National Key R&D Program of China (Grants No. 2017YFA0303903 and No. 2019QY0702), the Chinese Academy of Science, the National Fundamental Research Program, the National Natural Science Foundation of China (Grants No. 11875173, No. 61875182, and No. 12174216), Anhui Initiative in Quantum Information Technologies, and Fundamental Research Funds for the Central Universities (WK2340000083).

H.-T. Z. and Y. H. contributed equally to this work.

*xma@tsinghua.edu.cn
†tychen@ustc.edu.cn
‡pan@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, 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, Phys. Rev. Lett. **67**, 661 (1991).
[3] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] M. Peev *et al.*, New J. Phys. **11**, 075001 (2009).
[6] M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011).
[7] 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, Phys. Rev. X **6**, 011024 (2016).
[8] T.-Y. Chen *et al.*, npj Quantum Inf. **7**, 134 (2021).
[9] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen *et al.*, Nature (London) **589**, 214 (2021).
[10] H. Zhou, K. Lv, L. Huang, and X. Ma, IEEE/ACM Trans. Netw. **30**, 1328 (2022).
[11] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).
[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[13] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[14] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[15] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature (London) **557**, 400 (2018).
[16] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Nat. Photonics **13**, 334 (2019).
[17] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **123**, 100505 (2019).
[18] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **124**, 070501 (2020).
[19] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li *et al.*, Nat. Photonics **14**, 422 (2020).
[20] Y. Mao, P. Zeng, and T.-Y. Chen, Adv. Quantum Technol. **4**, 2000084 (2021).
[21] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu *et al.*, Nat. Photonics **15**, 570 (2021).
[22] P. Zeng, H. Zhou, W. Wu, and X. Ma, Nat. Commun. **13**, 3903 (2022).
[23] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, PRX Quantum **3**, 020315 (2022).
[24] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.130.030801 for detailed mode-pairing quantum key distribution protocol, the causes of phase differences, actions taken to estimate phase differences, the test results, and raw data of the experiment.
[25] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[26] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[27] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[28] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Optica **7**, 238 (2020).
[29] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. Paraiso, M. Lucamarini, Z. Yuan, and A. Shields, npj Quantum Inf. **7**, 58 (2021).
[30] 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, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **117**, 190501 (2016).
[31] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[32] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[33] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).