Surpassing the rate-transmittance linear bound of quantum key distribution

Xiao-Tian Fang\textsuperscript{1,2,*}, Pei Zeng\textsuperscript{3,*}, Hui Liu\textsuperscript{1,2,*}, Mi Zou\textsuperscript{1,2}, Weijie Wu\textsuperscript{3}, Yan-Lin Tang\textsuperscript{4}, Ying-Jie Sheng\textsuperscript{4}, Yao Xiang\textsuperscript{4}, Weijun Zhang\textsuperscript{5}, Hao Li\textsuperscript{5}, Zhen Wang\textsuperscript{5}, Lixing You\textsuperscript{5}, Ming-Jun Li\textsuperscript{6}, Hao Chen\textsuperscript{6}, Yu-Ao Chen\textsuperscript{1,2}, Qiang Zhang\textsuperscript{1,2}, Cheng-Zhi Peng\textsuperscript{1,2,4}, Xiongfei Ma\textsuperscript{3}, Teng-Yun Chen\textsuperscript{1,2}, and Jian-Wei Pan\textsuperscript{1,2}

\textsuperscript{1}Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
\textsuperscript{2}CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
\textsuperscript{3}Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China
\textsuperscript{4}QuantumCTek Corporation Limited, Hefei, Anhui 230088, China
\textsuperscript{5}State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China
\textsuperscript{6}Corning Incorporated, Corning, New York 14831, USA
*These authors contributed equally to this work.

Quantum key distribution (QKD)\textsuperscript{[1,2]} offers a long-term solution to establish information-theoretically secure keys between two distant users. In practice, with a careful characterization of quantum sources and the decoy-state method\textsuperscript{[3,5]}, measure-device-independent quantum key distribution (MDI-QKD)\textsuperscript{[6]} provides secure key distribution. While short-distance fibre-based QKD has already been available for real-life implementation\textsuperscript{[7]}, the bottleneck of practical QKD lies on the limited transmission distance. Due to photon losses in transmission, it was believed that the key generation rate is bounded by a linear function of the channel transmittance, $O(\eta)$, without a quantum repeater\textsuperscript{[8,9]}, which puts an upper bound on the maximal secure transmission distance\textsuperscript{[10,11]}. Interestingly, a new phase-encoding MDI-QKD scheme, named twin-field QKD\textsuperscript{[12]}, has been suggested to beat the linear bound, while another variant, named phase-matching quantum key distribution (PM-QKD), has been proven to have a quadratic key-rate improvement\textsuperscript{[13,14]}, $O(\sqrt{\eta})$. In reality, however, the intrinsic optical mode mismatch of independent lasers, accompanied by phase fluctuation and drift, impedes the successful experimental implementation of the new schemes. Here, we solve this problem with the assistance of the laser injection technique and the phase post-compensation method. In the experiment, the key rate surpasses the linear key-rate bound via 302 km and 402 km commercial-fibre channels, achieving a key rate over 4 orders of magnitude higher than the existing results in literature\textsuperscript{[14]}. Furthermore, with a 502 km ultralow-loss fibre, our system yields a secret key rate of 0.118 bps. We expect this new type of QKD schemes to become a new standard for future QKD.

In conventional point-to-point QKD, such as the BB84 protocol\textsuperscript{[1]}, the sender Alice encodes key information into quantum states and sends them to the receiver Bob for detection. Whereas in MDI-QKD, Alice’s and Bob’s positions are symmetric. They both send out encoded optical pulses to a measurement site owned by Charlie, who interferes the pulses and publicly announces the results to correlate Alice’s and Bob’s key information. The security of MDI-QKD does not depend on how Charlie realizes the measurement or announces the results. As a result, this scheme is immune to all attacks on the detection and hence owns a higher security level in practice.

In quantum communication, attenuated lasers are widely used as photon sources, which can be described by weak coherent states, $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{k=0}^{\infty} \frac{\alpha^k}{k!} |k\rangle$, superpositions of $k$-photon states $|k\rangle$. The parameter $\alpha = \sqrt{\mu} e^{i \phi}$ is a complex number, where $\mu = |\alpha|^2$ is the light intensity and $\phi$ is the phase. In the original MDI-QKD\textsuperscript{[6]}, the user encodes the key information into two weak coherent states on two orthogonal optical modes, such as polarization encoding. In the security analysis, only the information carried by the single-photon states can be used for the final key generation. The decoy-state method is widely employed to efficiently extract secret key information\textsuperscript{[3,5]}.

In reality, quantum information carriers, photons, can be easily lost during transmission. Define the transmittance between Alice and Bob $\eta$ to be the probability of a photon being successfully transmitted through the channel and being detected. Hence, in the symmetric setting of MDI-QKD, the transmittance between Alice (Bob) and the measurement site is $\sqrt{\eta}$. Only the detections, caused by Alice’s and Bob’s single-photon states, can be used for secure key generation. Then such detection rate is given by $O(\eta)$, as a natural upper bound of the key rate.

To achieve a better rate-transmittance performance, a new phase-encoding MDI-QKD scheme, named PM-QKD, has been proposed, as shown in Fig.\textsuperscript{[1]} Alice (Bob) encodes the key information into the phase of a coherent state on a single optical mode. In this case, Charlie treats Alice and Bob’s two optical modes as one quantum system and detects the relative phase between them. To do so, Charlie only needs one photon in the joint quantum system.
Therefore, the detection rate is $O(\sqrt{\eta})$. Strict security analysis shows that PM-QKD enjoys a quadratic improvement on the rate-transmittance performance over the original MDI-QKD [13].

**FIG. 1. Schematic diagram of PM-QKD.** Encoder is a device to modulate the intensity $\mu$ and phase $\phi$ of coherent states. The beam splitter and the single photon detectors are used for interference detection. Divide the phases $\phi \in [0, 2\pi]$ into $D$ slices, denoted by $\Delta_j = [\frac{\pi}{D}(2j - 1), \frac{\pi}{D}(2j + 1)]$ with the index $0 \leq j \leq D - 1$. In the experiment, we set $D = 16$. In each round of key distribution, Alice codes a random bit $\kappa_a$ into her coherent state $|\sqrt{\mu_a}e^{i(\kappa_a \pi + \phi_a)}\rangle$; after adding an extra discrete random phase $\phi_b = j_a 2\pi / D$ which is at the center of $j_a$th phase slice $\Delta_{j_a}$. Similarly, Bob encodes $\kappa_b$, $\mu_b$, and $\phi_b$ on his pulse, $|\sqrt{\mu_b}e^{i(\kappa_b \pi + \phi_b)}\rangle$. Alice and Bob then send their pulses to Charlie, who is supposed to interfere these quantum states to measure phase differences. After Charlie announces the detection results, Alice and Bob publicly announce the slice indexes $j_a, j_b$ of the random phases. They post-select the key bits $\kappa_a, \kappa_b$ as the raw key, according to Charlie’s detection results and the sifting scheme depending on $j_a, j_b$, with the phase post-compensation technique.

Despite the promising qualities of PM-QKD on both security and performance, the experimental implementation is very challenging. In PM-QKD, the interference results at the measurement result should reflect the difference between Alice’s and Bob’s encoded phases. In practice, an essential requirement is to match the phases of coherent states generated by two remote and independent lasers. The coherent states of Alice $|\sqrt{\mu_a}e^{i(\kappa_a \pi + \phi_a)}\rangle$ and Bob $|\sqrt{\mu_b}e^{i(\kappa_b \pi + \phi_b)}\rangle$ could have different phase references due to phase drift and fluctuation. Define the reference deviation $\delta_{\phi}$ to be the phase difference when both Alice and Bob set $\kappa_a(\kappa_b) = 0$ and $\phi_a(\phi_b) = 0$. There are three main factors determining the value of $\delta_{\phi}$, fluctuations of the laser initial phases, fibre lengths, and laser frequencies. Take the 1550 nm telecom light through a 200 km fibre for example, either a tiny change of transmission time, say by $10^{-15}$ s corresponding to a 200 nm optical length, or a small deviation of the angular frequency, say by 1 kHz, will cause a significant phase drift. Note that, there are several recent experiments which make efforts to deal with these challenges in order to demonstrate the advantages of the new type of MDI-QKD schemes [15–18].

In this work, we implement PM-QKD with the setup shown in Fig. 2. In order to suppress the fluctuations of the laser initial phases and frequencies, we employ the laser injection technique [19]. The setups on Alice’s and Bob’s sides are exactly the same. Below, we take Alice’s side for example. The master laser in between Alice and Bob, with 3 kHz line-width and 1550.12 nm centre wavelength, emits a seed light which goes through a long fibre to lock Alice’s distributed feedback laser. Alice’s laser generates optical pulses with a clock rate of 312.5 MHz. Two Sagnac rings are employed to modulate pulses into four different intensities. The pulses with the largest intensity are used as reference pulses for phase estimation, while the other three pulses are used as the signal state, weak decoy state, and vacuum state to implement the decoy-state method. The extinction ratio between the signal state and the vacuum state is about 20 dB. Two phase modulators are employed to modulate 16 different phases. Details of the laser injection technique and the phase estimation are presented in Appendix A and B.

The pulses from Alice and Bob are transmitted through long optical fibres and interfered at the measurement site. The interference results are detected by two superconducting nanowire single photon detectors. The dark count is about 10 counts per second and the detector efficiency is about 40%. The total detection efficiency reduces to about 23% owing to 1.2 dB insertion loss and 25% non-overlapping between signal and detection windows. Two stabilization systems are inserted before interference to filter out the noise caused by the nonlinear effect of the fibre and stabilizing the incident pulses. Details of the implementation are presented in Appendix D.

Due to fibre fluctuation, there exists a slow phase drift between Alice and Bob. In the case when the phase fluctuates slowly, pulses nearby share similar values of the reference deviation $\delta_{\phi}$. Inspired by this observation, we employ a simple phase post-compensation technique [20]. During the experiment, Alice and Bob send reference pulses and quantum pulses periodically. The reference pulse is typically more than one order of magnitude stronger than the quantum pulse. They use reference pulses to estimate which slice $j_b$ the reference deviation $\delta_{\phi}$ lies in, according to interference results. They use quantum pulses to perform the PM-QKD experiment. After obtaining measurement results, Alice
and Bob publicly announce the random phase slices $j_a, j_b$ of the signal pulses. They calculate $j_s = j_a - j_b + j_δ$ for raw key sifting, where $j_δ$ works as the post-compensation shift. Clearly, if $j_δ$ accurately reflects the real-time reference deviation of the system, perfect interference will happen when $j_s = 0$ or $j_s = 8$. Note that the estimated phase slice indexes $j_δ$ are only used in the post-processing, which frees us from active phase locking during the state transmission. Furthermore, compared with active locking, where the phase can only be locked well when $\phi_S$ keeps stable during the whole process of phase estimation and feedback, the phase post-compensation method can tolerate faster fluctuation, as long as $\phi_S$ does not change much in the time between the reference and quantum pulses.

In the security analysis of PM-QKD[13], due to the random phases Alice and Bob modulated on their coherent states, the joint state can be decomposed into odd and even total photon number components, $\rho^{\text{odd}}_{AB}$ and $\rho^{\text{even}}_{AB}$. Denote the proportions of detection caused by $\rho^{\text{odd}}_{AB}$ and $\rho^{\text{even}}_{AB}$ as $q^{\text{odd}}$ and $q^{\text{even}}$, respectively, and obviously, $q^{\text{odd}} + q^{\text{even}} = 1$. In fact, the information leakage in PM-QKD is shown to be independent of channel disturbance. As a result, the privacy is only related to $q^{\text{even}}$, irrelevant to the bit error rate. The final key length is given by

$$K = M_\mu [1 - H(q^{\text{even}})] - l_{\text{cor}},$$

where $H(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$ is the binary entropy function. Here, we consider the case where Alice and Bob use the same intensities of coherent states. The subscript $\mu$ represents the signal states with $\mu_a = \mu_b = \mu/2$. The raw key length $M_\mu$ is the number of detection events caused by signal states when Alice and Bob match their phases, $j_s = 0$ or 8. The even photon component ratio $q^{\text{even}}$ can be efficiently estimated by decoy state methods[3][5].
The error correction cost $l_{\text{cor}}$ can be usually estimated by a function of bit error rate $E_\mu$, $l_{\text{cor}} = fM_\mu H(E_\mu)$, where $f$ is the error correction efficiency depending on $E_\mu$. The key rate is defined by $R = K/N$, where $N$ is the number of QKD rounds. Details of the decoy state method and the security analysis by considering the finite data size effects are presented in Appendix [E].

In order to further improve the key rate, one can take advantage of the data with mismatched phases. Note that the phase-mismatched signals of $j_s = 1, 9$ can be regarded as the ones with a fixed misalignment $\phi_s = 2\pi/D$, which results in a larger bit error rate compared with the phase-matched signals of $j_s = 0, 8$. The raw keys with different $j_s$ have the same $q_{\text{even}}$ in Eq. (4) and hence the same privacy. More explicitly, Alice and Bob can categorize the data from signal states into $D/2$ groups, where the data of $j_s = 0, 8$ are in the 0-th group, the data of $j_s = 1, 9$ are in the 1-st group, etc. Alice and Bob can correct errors in each data group separately and perform privacy amplification altogether. Of course, if the error rate in a group is too large, they can simply discard that group of data.

We perform the experiment via 101, 201, 302, 402 km standard optical fibres and a 502 km ultralow-loss optical fibre. The experiment parameters and results are presented in Fig. 3, from which one can see that the key rate-transmittance relation follows $R = O(\sqrt{\eta})$ as a contrast with the linear rate-transmittance bound. Specifically, the experimental results beat the linear bound at the distances of 302 and 402 km. Take the 302 km fibre case as an example, with the same channel transmission and detection efficiency, the linear key-rate bound is given by $R_{\text{lin}} = 5.44 \times 10^{-7}$. Our experiment yields a key rate of $R = 6.74 \times 10^{-7}$, with a failure probability of $\epsilon = 1.68 \times 10^{-10}$, when all the mismatched data is used. The key rate is 24.0% higher than the bound. In the case of 302 km, the data with mismatched phases has a significant contribution to the overall key rate, which is 72.6% larger than the value with only the phase-matched group considered. Notably, our achieved key rate is three orders of magnitude higher than the asymptotic key rate of the original MDI-QKD scheme [6].

Meanwhile, we obtain a positive key rate at 502 km experiment with an ultralow-loss optical fibre, beating the current record of 421 km fibre communication distance of QKD [11]. The channel loss of 502 km experiment is 81.7 dB and the total loss is 87.1 dB. This new loss-tolerance record is comparable with the high-orbital satellite link loss in free space.

**FIG. 3. Experimental parameters and results.** a. Main panel, the experimental rate-distance performance of PM-QKD, comparing with the theoretical expectation and the linear key rate bound [9]. The data points marked by cross and star are, respectively, the key rate without and with the usage of phase-mismatched signals. Inset, error rate against total loss. The solid line shows the bit error rate in the theoretical model, and the crosses show the experiment data. b. The bit error rate with respect to the experiment time in the 302 km experiment. Each data point represents a number of $3.31 \times 10^7$ effective clicks which are collected in 21.91 minutes on average. The blue dots and red dots show the bit error rate for data with phase difference $\phi_d = 0$ and 1, respectively. c. Parameters used in the experiment and theoretical simulation. Note that, the listed value of the dark count rate $p_d$, the detection efficiency $n_{\text{det}}$, misalignment error $e_d$, and the fibre loss of PM-QKD are used for numerical simulation. The corresponding experimental values depend on the specific environment, which are listed in Appendix [E].
Our results show that PM-QKD system is stable and economical, which facilitates the promotion of practical QKD. In the future, we expect to use the phase post-compensation technique to keep the system robust by increasing the system repetition frequency and enhancing the detectors’ performance. Also, we expect that the design of PM-QKD experiment will be helpful for the construction of quantum repeater[21, 22], as well as extending the reach of the quantum internet.

FUNDING INFORMATION

This work has been supported by the National Key R&D Program of China (Grant No. 2017YFA0303903 and No. 2017YFA0304000), the Chinese Academy of Science, the National Fundamental Research Program, the National Natural Science Foundation of China (Grant No. 11875173, No. 61875182 and No. 11674193), Anhui Initiative in Quantum Information Technologies, and Fundamental Research Funds for the Central Universities (WK2340000083).

ACKNOWLEDGMENTS

We acknowledge H. Zhou for the insightful discussions.

AUTHOR CONTRIBUTIONS

All authors contributed extensively to the work presented in this paper.

AUTHOR INFORMATION

Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of this article at www.nature.com/nature.

Appendix A: Phase drift estimation

Rather than using extra devices to lock the phase, here we apply the phase estimation method to estimate the drifted phase, as shown in Fig. 4. Here, Alice and Bob need not obtain the exact value of the real-time phase deviation \( \phi_\delta \), but only an estimation of the slice number \( j_\delta \) for post-compensation. Moreover, the estimation of \( j_\delta \) does not need to be announced in a real-time manner. Instead, it can be announced during the sifting process, as a post-selection shift factor. This makes our protocol practical without active feedback.

![Phase estimation technique](image)

**FIG. 4. Phase estimation technique.** The pulses with a repetition rate of 312.5 MHz are grouped into trains, each containing 625 pulses. The period of pulse trains is about 2 \( \mu \)s. In each train, there are two reference pulse regions and two quantum pulse regions. Alice loads the 0 and \( \pi/2 \) phase on her pulses in the former and latter reference pulse region, respectively. A recovery region without pulses is at the end of every reference pulse region, where the detector systems recover to the optimal working condition.

In the reference pulse region, Alice and Bob send reference pulses to Charlie, who interferes them and announces the results. They use the interference results to estimate the phase slice difference between two reference pulses, \( \phi_\delta \).
The right detector click ratio $P_r$ after interference is

$$\frac{n_r}{n_r + n_l} \approx P_r = \frac{1 + \cos \phi_\delta}{2},$$

(A1)

where $n_r$ and $n_l$ are the counts of the right and left detector clicks, respectively. With this ratio, one can classify the phase fluctuation $\phi_\delta$ to the phase slices $\Delta_{j\delta}$ marked by $j\delta$ according to the detection ratio.

Note that, since the phase deviation $\phi_\delta$ and $(2\pi - \phi_\delta)$ yield the same $P_r$, Alice and Bob cannot discriminate these two cases from the ratio $P_r$. To solve this problem, Alice loads a $\phi_0 = \pi/2$ phase on the pulses in the latter reference pulse region, making the phase difference to be $\phi_\delta + \pi/2$, and hence $P_r = \frac{1 - \sin \phi_\delta}{2}$. In that case, one can distinguish the phase slice $j\delta$ from $(16 - j\delta)$. With the interference results $P_r$ from the case $\phi_0 = 0$ and $\phi_0 = \pi/2$, Alice and Bob can estimate $j\delta$ accurately, as shown in Fig. 5.

![Phase estimation region](image)

FIG. 5. Phase estimation region. The blue, green, red and orange region denotes four phase quadrants ranging from $[0, \pi/2), [\pi/2, \pi), [\pi, 3\pi/2)$, and $[3\pi/2, 2\pi)$. The solid line shows the theoretic detection probability $P_r$ with the initial phase difference $\phi_0$ of the reference pulse is set to 0, while the dashed line shows $P_r$ when $\phi_0 = \pi/2$. From these two estimated $P_r$ values, one can infer the $j\delta$ value with no degeneracy.

In order to yield an accurate estimation of $j\delta$, sufficient detection counts of the reference pulses are required. According to the transmittance and phase drift velocity, one should properly set the intensity and time duration of the reference pulse and the system repetition frequency.

**Appendix B: Laser injection technique**

The fluctuation of reference deviation $\phi_\delta$ is mainly caused by three factors: the initial phase fluctuation of the lasers, the optical length fluctuation, and the fluctuation of the laser frequencies. In order to minimize the fluctuation caused by the first and the third factors, we apply the laser injection technique.

As shown in Fig. 6a, a narrow line-width continuous wave laser at Charlie side works as the master laser, while DFB laser at Alice’s (same as Bob’s) side works as the slave laser. The seed light generated by the master laser is divided into two parts and sent to the two slave lasers through long fibres, which induces stimulated emission. In this case, the wavelength and phase of the light generated by the slave laser are the same as the seed light, which results in slower fluctuation of laser initial phases. For a local experiment test, interference results of pulses generated by slave lasers shows that the phase difference of two locked slave lasers fluctuates in a relatively low speed, which is presented in Fig. 6b. Here, the residual phase noise and fluctuation mainly come from the spontaneous emission in the slave lasers. Though the phase will fluctuate faster when the fibre gets longer, we can still get an effective phase estimation in this case.

In the 101, 201, 302 km experiments, the master laser is put at the middle point between Alice and Bob’s laser. The fibres used to transmit seed light and the signal light are different but with the same length. Due to the limited power of the master laser and low transmittance value, in the 402 km and 502 km experiments, we place the master laser and the slave lasers locally.

**Appendix C: PM-QKD protocol**

In Box [C], we explicitly present the phase-matching quantum key distribution (PM-QKD) scheme implemented in the experiment. We divide the phase space $0 \sim 2\pi$ into $D$ slices and denote the $j$-th slice as $\Delta_j = \left[ \frac{\pi}{D}(2j-1), \frac{\pi}{D}(2j+1) \right]$.
The central phase of $j$-th slice is $\phi_j = \frac{2\pi}{D}j$.

Suppose the phase references of Alice and Bob are different $\phi_a(0)$, $\phi_b(0)$. Moreover, we denote the phase variation in the fibre as $\phi_f$. Before Eve’s interference, the phase difference between Alice and Bob’s pulses is

$$\phi_a + \phi_a(0) - (\phi_b + \phi_b(0)) + \phi_f = \phi_a - \phi_b + (\phi_a(0) - \phi_b(0)) + \phi_f = \phi_a - \phi_b + \phi_f \approx (j_a - j_b + j_\delta)\frac{2\pi}{D},$$

and hence the phase difference belongs to the $(j_a - j_b + j_\delta)$-th slice. Suppose $\phi_\delta$ fluctuates slowly with respect to time. By the interference of coherent pulses, Alice and Bob can estimate $\phi_\delta$ accurately. In this case, for the data with $j_\delta = 0$, the interference should be nearly perfect, with small quantum bit error rate. Note that, the sifting strategy does not affect the security of PM-QKD. It only affects the error correction efficiency.

Appendix D: Experiment detail of PM-QKD

1. Laser injection details

As is shown in Fig. 7, the continuous wave emitted from the master laser (Realphoton Technology Ltd.) are split by a PMBS and transmitted through long fibres and finally injected into Alice and Bobs slave laser (Agilecom Ltd.). To achieve a good laser injection result, we apply the Erbium doped fiber amplifier (EDFA) to amplify the light intensity and the dense wavelength division multiplexer (DWDM) to filter the side band noise. After that, a fiber Bragg grating (FBG) inserted before injection is used to block the light with unexpected wavelength. A photoelectric diode (PD) is used to monitor the intensity of injection wave for avoiding that Charlie (or Eve) controls the output of the slave laser by manipulate the injection wave. The optical pulses at the width of 400 ps generated by the slave laser.

2. Encoding and measurement devices

In accordance with random bit values generated beforehand, two Sagnac rings [23] (SR1-2) are employed to modulate the intensities of reference state and three decoy states while two phase modulators (PM1-2) are employed to modulate encoding phases and random phases. The circulator followed are utilized to prevent Trojan horse attack. Note that the pulse into the SR is split into two pulses by the polarization-maintaining beam splitter (PMBS), one of which travels clockwise and the other travels anticlockwise. The PM in the SR adjusts and loads the phase only on one of the two pulses every round so that the output pulses intensity could be modulated when they meet again on the PMBS. To avoid the disturbance on the encoding process, the backward output pulses will be removed by the Circ.
State preparation: Alice randomly generates a key bit \( \kappa_a \), and picks a random phase \( \phi_{ja} \) from the set \( \{ j \frac{2\pi}{D} \}_{D=1}^{D-1} \), and the intensity \( \mu_{ia} \) from the set \( \{ 0, \nu/2, \mu/2 \} \). She then prepares the coherent state \( |\sqrt{\mu_{ia}}e^{(\phi_{ja} + \pi \kappa_a)}\rangle_A \). Similarly, Bob generates \( \kappa_b \), \( \phi_{jb} \), \( \mu_{ib} \) and then prepares \( |\sqrt{\mu_{ib}}e^{(\phi_{jb} + \pi \kappa_b)}\rangle_B \).

Measurement: Alice and Bob send their optical pulses, \( A \) and \( B \), to an untrusted party, Eve, who is expected to perform an interference measurement and record the detector \( (L \) or \( R) \) that clicks.

Announcement: Eve announces her detection results. Then, Alice and Bob announce the random phases and intensities \( j_a, \mu_{ia} \) and \( j_b, \mu_{ib} \), respectively.

Phase estimation: From time to time, Alice and Bob generate strong coherent pulses with \( \phi_{ja} = \phi_{jb} = 0 \) and send to Eve. Eve is supposed to interfere these pulses and estimate the phase difference \( \phi_d \) between these two pulses. Eve announces the phase slice number \( j_b \) of \( \phi_d \).

Alice and Bob repeat the above steps for \( N \) times. After that, they perform the following data post-processing procedures.

Sifting: When Eve announces a successful detection, (a click from exactly one of the detectors \( L \) or \( R \)), Alice and Bob keep \( \kappa_a \) and \( \kappa_b \). Bob flips his key bit \( \kappa_b \) if Eve’s announcement was an \( R \) click. Then, Alice and Bob group the signals by \( j_b = (j_a - j_b + j_b) \mod D \). If \( j_b \in [0, \frac{D}{2}] \), Bob flips his key bit \( \kappa_b \). After that, Alice and Bob merge the data with \( j_s \) and \( j_s + \frac{D}{2} \), with \( j_s = 0, 1, \ldots, \frac{D}{2} - 1 \).

Parameter estimation: For all the raw data that they have retained, Alice and Bob record the detect number \( M_{ja,ib} \) of different intensity combinations \( \{ \mu_{ia}, \mu_{ib} \} \) and phase group \( j_s \). They then estimate the phase error number among all the clicked signal rounds \( n_s^\mu \) in the phase group \( j_s \) using the methods in Section 2.

Key distillation: For the signals with \( \mu_{ia} = \mu_{ib} = \frac{\mu}{2} \), Alice and Bob group them by the phase difference \( j_s \). Then they perform error correction and error verification on the raw key data of each group \( j_s \), respectively. They then perform privacy amplification on the sifted key bits to generate private key.

Box 1 | PM-QKD protocol

State preparation: Alice randomly generates a key bit \( \kappa_a \), and picks a random phase \( \phi_{ja} \) from the set \( \{ j \frac{2\pi}{D} \}_{D=1}^{D-1} \), and the intensity \( \mu_{ia} \) from the set \( \{ 0, \nu/2, \mu/2 \} \). She then prepares the coherent state \( |\sqrt{\mu_{ia}}e^{(\phi_{ja} + \pi \kappa_a)}\rangle_A \). Similarly, Bob generates \( \kappa_b \), \( \phi_{jb} \), \( \mu_{ib} \) and then prepares \( |\sqrt{\mu_{ib}}e^{(\phi_{jb} + \pi \kappa_b)}\rangle_B \).

Measurement: Alice and Bob send their optical pulses, \( A \) and \( B \), to an untrusted party, Eve, who is expected to perform an interference measurement and record the detector \( (L \) or \( R) \) that clicks.

Announcement: Eve announces her detection results. Then, Alice and Bob announce the random phases and intensities \( j_a, \mu_{ia} \) and \( j_b, \mu_{ib} \), respectively.

Phase estimation: From time to time, Alice and Bob generate strong coherent pulses with \( \phi_{ja} = \phi_{jb} = 0 \) and send to Eve. Eve is supposed to interfere these pulses and estimate the phase difference \( \phi_d \) between these two pulses. Eve announces the phase slice number \( j_b \) of \( \phi_d \).

Alice and Bob repeat the above steps for \( N \) times. After that, they perform the following data post-processing procedures.

Sifting: When Eve announces a successful detection, (a click from exactly one of the detectors \( L \) or \( R \)), Alice and Bob keep \( \kappa_a \) and \( \kappa_b \). Bob flips his key bit \( \kappa_b \) if Eve’s announcement was an \( R \) click. Then, Alice and Bob group the signals by \( j_b = (j_a - j_b + j_b) \mod D \). If \( j_b \in [0, \frac{D}{2}] \), Bob flips his key bit \( \kappa_b \). After that, Alice and Bob merge the data with \( j_s \) and \( j_s + \frac{D}{2} \), with \( j_s = 0, 1, \ldots, \frac{D}{2} - 1 \).

Parameter estimation: For all the raw data that they have retained, Alice and Bob record the detect number \( M_{ja,ib} \) of different intensity combinations \( \{ \mu_{ia}, \mu_{ib} \} \) and phase group \( j_s \). They then estimate the phase error number among all the clicked signal rounds \( n_s^\mu \) in the phase group \( j_s \) using the methods in Section 2.

Key distillation: For the signals with \( \mu_{ia} = \mu_{ib} = \frac{\mu}{2} \), Alice and Bob group them by the phase difference \( j_s \). Then they perform error correction and error verification on the raw key data of each group \( j_s \), respectively. They then perform privacy amplification on the sifted key bits to generate private key.

(circulator) in the SR. Because of the same fiber in which two pulses travel, the clockwise and counter-clockwise paths are insensitive to any length drifts or stress and temperature variation of the fiber within propagation time. In that case, the SR is so stable that the intensity feedback device is unnecessary.

In Charlie’s measurement device, to make sure that the polarization of two pulses are indistinguishable, we utilize two PBSs before interfere to filter unexpected part. The reflection port of each PBS is monitored by the SNSPD with detection efficiency of 20% and dark count rate of 100 cps. Charlie adjusts the DC loaded in the EPC in real time to minimize and stabilize the detection count of SNSPD so the incident pulses intensity for interfere maintains maximum. Note that since we have to send strong reference pulses which is described in Appendix A, we always have enough pulses intensity for the polarization feedback system even the fiber length is up to 500 km, and Our feedback system works well with less than 1% loss of the incident pulse intensity.

The detector efficiency of SNSPD1 and SNSPD2 is about 40% in 101, 201, 302 and 402 km experiments, while in 502 km experiment, we enhance the efficiency of two detectors to 46% and 75% for better performance. To get a higher interference visibility, we set a 25% non-overlap between the signal and detection window. The insertion loss of Charlie’s measurement device is about 1.2 dB.

3. Synchronization systems

The entire system are synchronized by two arbitrary-function generators (Tektronix, AFG3253) which is not shown in Fig. 1. Three 100 KHz electric signals in phase are modulated by two arbitrary-function generators. The delay between any two of them is adjustable. Alice, Bob and Charlie use one of them to regenerate their own 312.5 MHz system clock, respectively. To overlap the independent signal pulses from Alice and Bob precisely, we need to develop the time calibration system. First, Charlie measures the arriving time of the optical pulses from Alice and Bob with a time-to-digital converter (TDC), respectively. Then she adjusts the time delay between the electric signals from
FIG. 7. Detailed setting of PM-QKD with the nonlocal laser locking system.

the arbitrary-function generator according to the calculation of the averaged arriving time. Due to the long optical fiber length drifting, we have to proceed a time calibration every 30 minutes. The total timing calibration precision is about 20 ps which is precise enough for the implement.

Appendix E: Finite-size parameter estimation

Here we list the formulas to estimate the key length $K$, the phase error number, and the corresponding failure probability. The detailed finite-size security analysis of PM-QKD is in Ref. [24].

1. Key length formula

In the experimental PM-QKD protocol introduced in Appendix C, Alice and Bob group the signals by the phase difference $j_s$. For the signals in group $j_s$, the key length is

$$K^{(j_s)} = M^{(j_s)}[1 - H(q^{even(j_s)})] - l^{(j_s)}_{cor},$$

(E1)

where $M^{(j_s)}$ is the clicked rounds when Alice and Bob both send out signal lights with $\mu_{ia} = \mu_{ib} = \mu/2$ in the group $j_s$. $q^{even(j_s)}$ is the estimated fraction caused by the even state

$$q^{even(j_s)} = \frac{M^{even(j_s)}}{M^{(j_s)}},$$

(E2)

where $M^{even(j_s)}$ is clicked rounds caused by even photon component in the $M^{(j_s)}$ with estimation method introduced in Appendix E 2.

The error correction cost, given by $l^{(j_s)}_{cor}$, can usually by estimated by a function of bit error rate $E^{(j_s)}$ among the signals of group $j_s$,

$$l^{(j_s)}_{cor} = f M^{(j_s)} H(E^{(j_s)}),$$

(E3)
where $f$ is the error correction efficiency, determined by the error rate $E_{\mu}^{(j)}$ and the specific error correction method. If $E_{\mu}^{(j)}$ is too large, the cost $l_{cor}^{(j)}$ may be larger than the generated key length $M_{\mu}^{(j)}(1 - H(q_{\mu}^{even}(j)))$. In this case, Alice and Bob directly abandon this group of data.

The overall key length for all the phase group $j_s$ is

$$K = \sum_{j_s = 0}^{D/2 - 1} \max\{K(j_s), 0\}. \quad (E4)$$

Note that, the information leakage is only related to the fraction $q_{\mu}^{even(j_s)}$, irrelevant to the bit error rate. Therefore, the overall information leakage depends on the even photon component in the clicked signals for all the phase group.

In practice, the data post-processing procedure can be improved. Alice and Bob can first perform error correction separately, with respect to different phase group $j_s$. If the error rate is too large, they can simply discard that group of data. Denote the group set $J$ to be the set of group indeces $\{j_s\}$ where the data is left. That is, if $j_s \in J$, then the phase group $j_s$ is kept for key generation. For all the left phase groups in set $J$, Alice and Bob estimate the even photon fraction $q_{\mu}^{even(J)}$. They then perform privacy amplification among the left data altogether. Of course, Alice and Bob should properly set the group set $J$ to maximize the key length.

With the improved post-processing procedure, the key length for the left phase groups is

$$K = M_{\mu}^{(J)}[1 - H(q_{\mu}^{even(J)})] - f \sum_{j_s \in J} M_{\mu}^{(j_s)} H(E_{\mu}^{(j_s)}), \quad (E5)$$

where $M_{\mu}^{(J)}$, $q_{\mu}^{even(J)}$ are, respectively, the clicked rounds and estimated even photon fractions for the left data.

2. Decoy-state estimation

The core of parameter estimation step is to estimate the phase error number $M_{\mu}^{even(J)}$ in the signal state group set $J$ with $\mu_s = \mu_w = \mu/2$. According to the security analysis in Ref. [23], $M_{\mu}^{even(J)}$ is bounded by

$$M_{\mu}^{even(J)} = 1 - \sum_{k:odd} M_{\mu}^{s(J)} \geq 1 - M_{\mu}^{(J)}, \quad (E6)$$

where $M_{\mu}^{s(J)}$ is the $k$-photon clicked number in the group set $J$ of signal lights.

In experimental PM-QKD protocol, Alice and Bob set the signal, weak decoy and vacuum light with preset ratio $r_s, r_w, r_{vac}$. To estimate $M_{\mu}^{(J)}$, Alice and Bob perform the following decoy-state process,

1. To record the sending round number when Alice and Bob both send out signal, weak decoy or vacuum pulses, denoted as $\{N_s, N_w, N_{vac}\}$; and the number of according single-clicked rounds (including the rounds with error), denoted as $\{M_s, M_w, M_{vac}\}$.

2. Based on an inverted usage of Chernoff bound introduced in Appendix E3, to calculate $\{E^U(\tilde{M}_s), E^L(\tilde{M}_w)\}_a$, where $a = s, w, vac$ as signal, weak decoy and vacuum pulse, and estimate the failure probability $\epsilon_1$. Calculate the $\{E^U(\tilde{Q}_s), E^L(\tilde{Q}_w)\}_a$ by

$$\tilde{Q}_a = \frac{M_a}{N_a}. \quad (E7)$$

3. Calculate the minimal $Y_1^{*L}$ based on $\{E^U(\tilde{Q}_s), E^L(\tilde{Q}_w)\}_a$ and the following formula,

$$Y_1^{*L} \geq \frac{\mu}{\mu \nu - \nu^2} \left( E^L[Q_{\nu s}]e^\nu - E^U[Q_{\nu s}]e^\nu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} E^U[Q_{\nu vac}] \right). \quad (E8)$$

calculate $\tilde{M}_k^L$ by

$$\tilde{M}_k = N_k^{\infty} \tilde{Y}_k^{*}, \quad (E9)$$
where

$$N_k^\infty = N \sum_a P^a(k)(r^a)^2,$$  \hspace{1cm} (E10)

are the asymptotic rounds of sending pulses with photon number \(k\). \(P^a(k)\) is the Poisson distribution when the intensity setting is \(a\).

4. Based on a direct usage of Chernoff bound introduced in Appendix E3 to calculate \((M_1^{\ell(J)})^L\) and estimate the failure probability \(\epsilon_2\).

As a result, Alice and Bob can obtain an lower bound estimation of \(M_1^{\ell(J)}\) with failure probability \(\epsilon_1 + \epsilon_2\). From Eq. (E6), we can bound the phase error number \(M_\mu^{\text{even}(J)}\).

3. Chernoff-Hoeffding bound

Here we present the methods to evaluate \(\mathbb{E}(\bar{M}^a)\) from \(M^a\) and evaluate \(M_1^s\) from \(M_1^\ell\) using Chernoff bounds.

To evaluate \(\mathbb{E}(\bar{M}^a)\) from \(M^a\), we inversely use the Chernoff bounds based on Bernoulli variables. We briefly summarize the results in Ref. [25]. For the observed value \(\chi\), we set the lower and upper bound of estimated \(\mathbb{E}(\chi)\) as \(\{\mathbb{E}^L(\chi), \mathbb{E}^U(\chi)\}\). Denote

$$\mathbb{E}^L(\chi) = \frac{\chi}{1 + \delta^L}, \quad \mathbb{E}^U(\chi) = \frac{\chi}{1 - \delta^U}. \hspace{1cm} (E11)$$

The failure probability of the estimation \(\mathbb{E}(\chi) \in [\mathbb{E}^L(\chi), \mathbb{E}^U(\chi)]\), given by the Chernoff bound, is

$$\epsilon = e^{-\chi g_2(\delta^L)} + e^{-\chi g_2(\delta^U)}, \hspace{1cm} (E12)$$

where \(g_2(x) = \ln(1 + x) - x/(1 + x)\).

To evaluate \(M_1^s\) from \(M_1^\ell\), we directly apply the Chernoff bounds. Suppose the direct sampling expectation value of \(M_1^s\) is given by \(\mathbb{E}(M_1^s) = p_1^s M_1\). For the expected value \(\mathbb{E}(\chi)\), we set the lower and upper bound of the estimated \(\chi\) as \(\{\chi^L, \chi^U\}\). Denote

$$\chi^L = (1 - \delta^L)\mathbb{E}(\chi), \quad \chi^U = (1 + \delta^U)\mathbb{E}(\chi). \hspace{1cm} (E13)$$

The failure probability of the estimation \(\chi \in [\chi^L, \chi^U]\), given by the Chernoff bound, is

$$\epsilon = e^{-(\delta^L)^2\mathbb{E}(\chi)/(2 + \delta^L)} + e^{-(\delta^U)^2\mathbb{E}(\chi)/(2 + \delta^U)}. \hspace{1cm} (E14)$$

In practice, we can preset the lower bound and upper bound \(\{\mathbb{E}^L(\chi), \mathbb{E}^U(\chi)\}\) or \(\{\chi^L, \chi^U\}\) by assuming a Gaussian distribution on \(\chi\) first,

$$\mathbb{E}^L(\chi) = \chi - n_\alpha \sqrt{\mathbb{E}(\chi)}, \quad \mathbb{E}^U(\chi) = \chi + n_\alpha \sqrt{\mathbb{E}(\chi)}, \hspace{1cm} (E15)$$

$$\chi^L = \chi - n_\alpha \sqrt{\mathbb{E}(\chi)}, \quad \chi^U = \chi + n_\alpha \sqrt{\mathbb{E}(\chi)},$$

where \(n_\alpha\) is a preset parameter to determine the estimation precision. After that, we calculate the failure probabilities by Eq. (E12) and Eq. (E14).

Appendix F: Simulation formulas and detailed results

Here we list the formulas used to simulate the key rate of PM-QKD and MDI-QKD in Fig. 3 in Main Text. The channel is modeled to be a pure loss one and symmetric for Alice and Bob with transmittance \(\eta\) (wit the detector efficiency \(\eta_d\)) taken into account.
1. Gain, yield and error rate of PM-QKD

In PM-QKD, the \(k\)-photon the yield \(Y_k\) is (Eq. (B13) in Ref. [13])
\[
Y_k \approx 1 - (1 - 2p_d)(1 - \eta)^k,
\]
and the gain \(Q_\mu\) when \(\mu_a = \mu_b = \mu/2\), is (Eq. (B14) in Ref. [13])
\[
Q_\mu \approx 1 - (1 - 2p_d)e^{-\eta \mu}.
\]

The even signal fraction \(q^\text{even}_\mu\) is bounded by
\[
q^\text{even}_\mu \leq 1 - Y_1.
\]

For the coherent lights with intensities \(\mu_a - \mu_b = \mu/2\) and phase difference \(\phi_a - \phi_b = \phi_\delta\), the bit error rate is (Eq. (B21) in Ref. [13])
\[
E_{\mu}(\phi_\delta) \approx e^{-\eta \mu}[p_d + \eta \mu \sin^2(\phi_\delta/2)].
\]

In the simulation in Fig. 3 in Main Text, we directly set \(e_d(0) = 5.3\%\) and only consider the data with matched phases. The bit error rate is,
\[
E_{\mu}(0) \approx [p_d + \eta \mu e_d(0)]e^{-\eta \mu / Q_\mu}.
\]

2. Simulation formulas for MDI-QKD protocols

The key rate of MDI-QKD is [6]
\[
R_{MDI} = \frac{1}{2}\{Q_{11}[1 - H(e_{11})] - fQ_{\text{rect}} H(E_{\text{rect}})\},
\]
where \(Q_{11} = \mu_a \mu_b e^{-\mu_a - \mu_b} Y_{11}\) and 1/2 is the basis sifting factor. We take this formula from Eq. (B27) in Ref. [20]. In simulation, the gain and error rates are given by

\[
Y_{11} = (1 - p_d)^2 \frac{\eta_a \eta_b}{2} + 2(2\eta_a + 2\eta_b - 3\eta_a \eta_b)p_d + 4(1 - \eta_a)(1 - \eta_b)p_d^2,
\]
\[
e_{11} = e_0 Y_{11} - e_0 - e_d(1 - p_d^2)\frac{\eta_a \eta_b}{2},
\]
\[
Q_{\text{rect}} = Q_{\text{rect}}^{(C)} + Q_{\text{rect}}^{(E)},
\]
\[
Q_{\text{rect}}^{(C)} = 2(1 - p_d)^2 e^{-\mu'/2}[1 - (1 - p_d)e^{-\eta_\mu \mu_a/2}][1 - (1 - p_d)e^{-\eta_\mu \mu_b/2}],
\]
\[
Q_{\text{rect}}^{(E)} = 2p_d(1 - p_d)^2 e^{-\mu'/2}[I_0(2x) - (1 - p_d)e^{-\mu'/2}] + E_{\text{rect}} Q_{\text{rect}} = e_d Q_{\text{rect}}^{(C)} + (1 - e_d)Q_{\text{rect}}^{(E)}.
\]

Here,
\[
\mu' = \eta_a \mu_a + \eta_b \mu_b,
\]
\[
x = \frac{1}{2} \sqrt{\eta_a \mu_a \eta_b \mu_b},
\]
where \(\mu'\) denotes the average number of photons reaching Eve’s beam splitter, and \(\mu_a = \mu_b = \mu/2, \eta_a = \eta_b = \eta\). We take these formulas from Eqs. (A9), (A11), (B7), and (B28)-(B31) in Ref. [20].
In 2014, Takeoka et al. derived an upper bound of the key rate of the point-to-point-type QKD protocols \cite{8},

\[ R_{TGW} = - \log_2 \left( \frac{1 - \eta}{1 + \eta} \right). \]  

\[ (F9) \]

Later, Pirandola et al. established a tight upper bound \cite{9},

\[ R_{PLOB} = - \log_2 (1 - \eta), \]  

\[ (F10) \]

which is the linear key-rate bound used in Main Text.

Appendix G: Experimental data

Here we list the experiment data for reference. Table I and II illustrate the data for theoretical parameters, channel condition and the key length calculation. Table III and IV show the sending and received statistics of all the signals. Table V and Table VI shows the detailed data of 101 km experiment with different phase slices setting.

| TABLE I. Parameter setting |
|----------------------------|
| Error correction efficiency | 1.1 |
| Failure probability | \( \sim 1.7 \times 10^{-10} \) |
| Fluctuation factor | 7 |

| TABLE II. Channel condition and key generation |
|-----------------------------------------------|
| Distance (km) | 101 | 201 | 302 | 402 | 502 |
| Channel loss | 1.02E-1 | 1.05E-2 | 1.29E-3 | 1.91E-4 | 8.18E-5 |
| detection loss | 23% | 23% | 23% | 20% | 29% |
| Total loss(double side) | 2.40E-03 | 2.53E-05 | 3.77E-07 | 7.34E-09 | 1.96E-09 |
| Dark count | 2.29E-07 | 5.85E-08 | 7.75E-08 | 3.36E-08 | 1.26E-08 |
| PLOB bound | 3.47E-03 | 3.66E-05 | 5.44E-07 | 1.06E-08 | 2.82E-09 |
| intensity of decoy state(single side) | 0.0179 | 0.0182 | 0.0192 | 0.0177 | 0.0127 |
| intensity of signal state(single side) | 0.0358 | 0.0364 | 0.0384 | 0.0384 | 0.0253 |
| Sending rounds | 1010250633000 | 1001472066000 | 2000013312000 | 19996635312500 | 20003396875000 |
| Aligned bit error rate | 5.31% | 5.75% | 6.06% | 7.00% | 9.80% |
| Key length | 98957100 | 6502240 | 13479300 | 287710 | 33674 |
| Aligned key length | 48529900 | 3440190 | 7809030 | 287710 | 33674 |
| Expansion factor | 2.04 | 1.89 | 1.73 | 1.00 | 1.00 |
| Failure probability | 1.68E-10 | 1.67E-10 | 1.68E-10 | 1.69E-10 | 1.71E-10 |
| Key Rate(bps) | 2.06E+04 | 1.36E+03 | 9.44E+01 | 2.01E+00 | 1.18E-01 |

[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] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[4] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[5] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[6] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
TABLE III. Experimental data of all signals

| Distance (km) | Vacuum state | Decoy state | Signal state |
|--------------|--------------|-------------|--------------|
| 101          | 48107173     | 6975540085  | 836776167162 |
| 201          | 453046887    | 23129235810 | 684363089673 |
| 302          | 2500166415   | 280716154317| 14331523970016|
| 402          | 147832268203 | 1352629545781| 8554989086016|
| 502          | 414356078125 | 3020512928125| 4369313403125|

| Sending rounds | Vacuum state | Decoy state | Signal state |
|----------------|--------------|-------------|--------------|
|                | 48107173     | 6975540085  | 836776167162 |
|                | 453046887    | 23129235810 | 684363089673 |
|                | 2500166415   | 280716154317| 14331523970016|
|                | 147832268203 | 1352629545781| 8554989086016|
|                | 414356078125 | 3020512928125| 4369313403125|

| Received rounds (without alignment) | Vacuum state | Decoy state | Signal state |
|------------------------------------|--------------|-------------|--------------|
| 22                                 | 10           | 430         | 1273         |
| 6036008                            | 23129235810  | 280716154317| 14331523970016|
| 1365570236                         | 6975540085   | 684363089673 |
| 325475042                          | 147832268203 | 8554989086016|
| 414356078125                       | 3020512928125| 4369313403125|

| Received rounds of \(jd=0\) | Vacuum state | Decoy state | Signal state |
|------------------------------|--------------|-------------|--------------|
| 2                            | 5            | 215         | 623          |
| 764808                        | 254969       | 397127      | 240748       |
| 170644117                     | 15018534     | 40698151    | 2982369      |
| 45972                         | 15921        | 28982       | 18418        |
| 9063823                       | 863533       | 2467769     | 208910       |

| Erroneous rounds of \(jd=0\) | Vacuum state | Decoy state | Signal state |
|------------------------------|--------------|-------------|--------------|
| 2                            | 5            | 215         | 623          |
| 764808                        | 254969       | 397127      | 240748       |
| 170644117                     | 15018534     | 40698151    | 2982369      |
| 45972                         | 15921        | 28982       | 18418        |
| 9063823                       | 863533       | 2467769     | 208910       |

| Received rounds of \(jd=1\) | Vacuum state | Decoy state | Signal state |
|------------------------------|--------------|-------------|--------------|
| 2                            | 5            | 215         | 623          |
| 764808                        | 254969       | 397127      | 240748       |
| 170644117                     | 15018534     | 40698151    | 2982369      |
| 45972                         | 15921        | 28982       | 18418        |
| 9063823                       | 863533       | 2467769     | 208910       |

| Erroneous rounds of \(jd=1\) | Vacuum state | Decoy state | Signal state |
|------------------------------|--------------|-------------|--------------|
| 2                            | 5            | 215         | 623          |
| 764808                        | 254969       | 397127      | 240748       |
| 170644117                     | 15018534     | 40698151    | 2982369      |
| 45972                         | 15921        | 28982       | 18418        |
| 9063823                       | 863533       | 2467769     | 208910       |

[7] 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, et al., IEEE Journal of Selected Topics in Quantum Electronics 21, 116 (2014).
[8] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. 5, 5235 (2014).
[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. 8, 15043 (2017).
[10] 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).
[11] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. 121, 190502 (2018).
[12] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature 557, 400 (2018).
[13] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X 8, 031043 (2018).
[14] J. Lin and N. Lütkenhaus, Phys. Rev. A 98, 042332 (2018).
[15] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Nature Photonics , 1 (2019).
[16] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, T.-Y. Chen, L. You, et al., arXiv preprint arXiv:1902.06268 (2019).
[17] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Phys. Rev. X 9, 021046 (2019).
[18] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, arXiv preprint arXiv:1902.10209 (2019).
[19] M. Lipka, M. Parniak, and W. Wasilewski, Applied Physics B 123, 238 (2017).
[20] X. Ma and M. Razavi, Phys. Rev. A 86, 062319 (2012).
[21] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. 71, 4287 (1993).
[22] R. A. Bergh, in Fiber optic and laser sensors X, Vol. 1795 (International Society for Optics and Photonics, 1993) pp. 126–135.
[23] P. Zeng, W. Wu, and X. Ma, Under preparation.
[24] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Phys. Rev. A 95, 012333 (2017).
| Phase Slice | OPD 0   | OPD 1   | OPD 2   | OPD 3   | OPD 4   | OPD 5   | OPD 6   | OPD 7   |
|------------|---------|---------|---------|---------|---------|---------|---------|---------|
|            | DETL    | DETR    | DETL    | DETR    | DETL    | DETR    | DETL    | DETR    |
| 0          | 375744  | 3969399 | 185800  | 414674  | 271002  | 3969399 | 185800  | 414674  |
| 1          | 537284  | 6098291 | 322140  | 6338669 | 513007  | 6265998 | 1125056 | 5733702 |
| 2          | 435376  | 4551069 | 232993  | 4891727 | 365819  | 4882103 | 791599  | 4348193 |
| 3          | 41272   | 508067  | 235091  | 5042261 | 381802  | 4818464 | 1484699 | 3562085 |
| 4          | 430329  | 5080877 | 259194  | 5201990 | 443091  | 5065994 | 911599  | 4348193 |
| 5          | 42237   | 486834  | 276350  | 5083603 | 451102  | 4817269 | 2497162 | 3780426 |
| 6          | 421145  | 478597  | 275524  | 4828410 | 479551  | 4753741 | 1703840 | 2796171 |
| 7          | 469004  | 510467  | 320768  | 5437178 | 511651  | 5188944 | 1066672 | 4749509 |
| 8          | 675823  | 5205534 | 362681  | 5409495 | 497550  | 5391926 | 1025723 | 4774543 |
| 9          | 751984  | 613958  | 434122  | 6560900 | 556244  | 6260261 | 1136504 | 5862130 |
| 10         | 643626  | 477926  | 298356  | 4785353 | 318169  | 4994816 | 666614  | 4464679 |
| 11         | 621568  | 4669051 | 301434  | 5115293 | 304863  | 4937140 | 673244  | 4647285 |
| 12         | 613155  | 473232  | 270746  | 4953558 | 299752  | 5010456 | 667994  | 4535278 |
| 13         | 503642  | 431689  | 236014  | 4700312 | 283689  | 4579890 | 634603  | 4215814 |
| 14         | 49447   | 453118  | 239784  | 4642063 | 306664  | 4583053 | 683584  | 4154620 |
| 15         | 570313  | 5111750 | 287062  | 5418330 | 379937  | 5281927 | 817979  | 4793549 |
| Phase Slice | OPD 8 DETL | OPD 8 DETR | OPD 9 DETL | OPD 9 DETR | OPD 10 DETL | OPD 10 DETR | OPD 11 DETL | OPD 11 DETR | OPD 12 DETL | OPD 12 DETR | OPD 13 DETL | OPD 13 DETR | OPD 14 DETL | OPD 14 DETR | OPD 15 DETL | OPD 15 DETR |
|-------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
| 0           | 16576331   | 462675     | 3698372    | 462675     | 3688286    | 462675     | 3282986    | 668922     | 2818592    | 1292424    | 2062095    | 2827226    | 1419356    | 2827226    | 792026     | 2347682    |
| 1           | 5472601    | 638783     | 580835     | 372595     | 5511681    | 554043     | 5077090    | 1193416    | 4055062    | 2127494    | 3099272    | 3227972    | 2013053    | 4443404    | 1148543    | 5447888    |
| 2           | 4311221    | 508294     | 449892     | 248592     | 426118     | 355970     | 3870006    | 784039     | 3288139    | 1504538    | 2438585    | 2351494    | 1647443    | 3246585    | 925502     | 4016093    |
| 3           | 4281037    | 469627     | 471805     | 247678     | 429168     | 359623     | 3937071    | 823162     | 3203772    | 1539792    | 2421228    | 2124260    | 1588434    | 3304423    | 886645     | 4069628    |
| 4           | 4676434    | 499303     | 471045     | 249121     | 442612     | 359623     | 3937071    | 823162     | 3203772    | 1539792    | 2421228    | 2124260    | 1588434    | 3304423    | 886645     | 4069628    |
| 5           | 4526437    | 447099     | 478054     | 244226     | 453453     | 403877     | 4067129    | 894940     | 3314316    | 1652792    | 2439324    | 2547910    | 1621141    | 3530837    | 904895     | 4423635    |
| 6           | 4560390    | 432379     | 464625     | 241914     | 440915     | 403693     | 3960067    | 897943     | 3209832    | 1635793    | 2415660    | 2567577    | 1591541    | 3547321    | 861669     | 4225159    |
| 7           | 4984117    | 477533     | 517231     | 272093     | 493854     | 452297     | 4357280    | 955027     | 3625455    | 1847187    | 2724208    | 2901542    | 1749707    | 3833764    | 983822     | 4681210    |
| 8           | 5634057    | 567488     | 5895012    | 410723     | 5712734    | 410723     | 5275605    | 912910     | 4492060    | 2649930    | 2256034    | 3710025    | 1318072    | 4493231    | 1382072    | 4493231    |
| 9           | 6054411    | 695599     | 632542     | 393846     | 638054     | 549074     | 584896     | 117938     | 4813596    | 2108247    | 3704310    | 3276566    | 2495890    | 435721     | 152050     | 5486773    |
| 10          | 4426341    | 600914     | 4864008    | 287216     | 4957478    | 335079     | 4497613    | 724541     | 3864613    | 1415560    | 2969011    | 2223641    | 2149296    | 3193987    | 1254639    | 3980210    |
| 11          | 4590026    | 612811     | 5036806    | 289699     | 4908022    | 334996     | 4556779    | 744118     | 3828204    | 1403545    | 3050678    | 2321539    | 2081010    | 3227612    | 1279160    | 4130325    |
| 12          | 4612559    | 610161     | 4835746    | 287826     | 4812024    | 348759     | 4360038    | 744211     | 3795422    | 1449993    | 2895683    | 2295465    | 2048632    | 3271887    | 119245     | 4027685    |
| 13          | 4181277    | 535961     | 4470633    | 271225     | 4335119    | 325771     | 4059576    | 728951     | 3357410    | 1362937    | 2660620    | 2210587    | 1792712    | 3014752    | 109187     | 3880884    |
| 14          | 4221721    | 530266     | 4381533    | 271406     | 4394063    | 364214     | 3946303    | 752179     | 3398431    | 1428086    | 2558102    | 2213075    | 1800125    | 3134338    | 100909     | 3820870    |
| 15          | 4876569    | 606080     | 5261246    | 332588     | 5087582    | 415528     | 4737267    | 9800000    | 3913291    | 1638703    | 3092011    | 2641099    | 2023820    | 3578779    | 1204437    | 4537282    |