Experimental measurement-device-independent quantum key distribution with imperfect sources

Zhiyuan Tang, Kejin Wei, Olinka Bedroya, Li Qian, and Hoi-Kwong Lo

Phys. Rev. A **93**, 042308 — Published 6 April 2016

DOI: 10.1103/PhysRevA.93.042308

Experimental Measurement-Device-Independent Quantum Key Distribution with Imperfect Sources

Zhiyuan Tang,[1,*] Kejin Wei,[1,2] Olinka Bedroya,[1] Li Qian,[1] and Hoi-Kwong Lo[1]

[1] *Centre for Quantum Information and Quantum Control*
Department of Physics & Department of Electrical and Computer Engineering
University of Toronto, Toronto, Ontario, M5S 3G4, Canada
[2] *School of Science and State Key Laboratory of Information Photonics and Optical Communications,*
Beijing University of Posts and Telecommunications, Beijing, 100876, People's Republic of China

Measurement-device-independent quantum key distribution (MDI-QKD), which is immune to all detector side-channel attacks, is the most promising solution to the security issues in practical quantum key distribution systems. Though several experimental demonstrations of MDI-QKD have been reported, they all make one crucial but not yet verified assumption, that is there are no flaws in state preparation. Such an assumption is unrealistic and security loopholes remain in the source. Here we present, to our knowledge, the first MDI-QKD experiment with the modulation error taken into consideration. By applying the loss-tolerant security proof by Tamaki *et al* (Phys. Rev. A 90, 052314 (2014)), we distribute secure keys over fiber links up to 40 km with imperfect sources, which would not have been possible under previous security proofs. By simultaneously closing loopholes the detectors and a critical loophole - modulation error in the source, our work shows the feasibility of secure QKD with practical imperfect devices.

PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex

Quantum key distribution (QKD), in principle, offers unconditional security based on the laws of quantum physics rather than computational complexity [1]. However, it has been realized that, due to the gap between the security proofs [2] and real-life implementations, practical QKD systems are vulnerable to various attacks [3].

Device-independent QKD (DI-QKD) [4], was proposed to remove all assumptions of the internal working of devices of QKD. The security of DI-QKD is based on the loophole-free Bell test. Despite a number of recent experimental demonstrations of loophole-free Bell test [5], DI-QKD is impractical at practical distances (20-30 km of telecom fiber) due to its low key rate of about 10^{-10} bit per pulse [6]. Fortunately a protocol, namely the Measurement-Device-Independent QKD (MDI-QKD), whose security is built on the time-reversed entanglement QKD [7] , has been proposed [8] to remove all potential security loopholes in the detection side, the most vulnerable part of a QKD system (See also [9]). Several MDI-QKD demonstrations using polarization [10, 11] and time-bin phase [12] encoding have been reported. More recently, MDI-QKD over 200 km [13], a field test [14], a network demonstration [15], and an implementation with 1 GHz clock rate [16] have been reported, highlighting the practicality of this protocol. MDI-QKD with continuous variables has also been proposed [17]. The concept of measurement-device independence has also been applied in other areas of quantum information, including entanglement witness [18] and quantum coin tossing [19].

It is conceivable that MDI-QKD [8] will be widely adopted in the near future. Since MDI-QKD is intrinsically immune to all detector side-channel attacks, eavesdroppers will shift their focus from hacking the detectors to hacking the sources, which are not protected in MDI-QKD. Several theoretical studies on MDI-QKD with imperfect sources have been reported [20].

A crucial assumption in discrete-variable MDI-QKD is that the source employed must be trusted. An ideal trusted source need to satisfy two conditions: first, the source only emits single photons; second, information should be encoded without flaws. However, these two conditions cannot be satisfied perfectly with today's technology. First, phase-randomized weak coherent pulses (WCPs) rather than single-photon sources are widely used in most QKD (including BB84 and MDI-QKD) demonstrations. Fortunately, it has been shown that unconditional security can still be achieved with phase-randomized WCPs [21]. Furthermore, the performance can be significantly improved with the decoy state method [22]. Second, encoding quantum states onto optical pulses has inherent errors due to the finite inaccuracies in practical encoding devices. However, such errors are ignored in all previous discrete-variable MDI-QKD demonstrations [10–14]. It is unrealistic to ignore all those errors because they may lead to security loopholes that a eavesdropper might conceivably exploit to launch attacks.

Such state preparation flaws can be taken care of using the quantum coin idea [21, 23]. However, this approach assumes the worst case in which an eavesdropper can enhance the flaws by channel loss, and therefore the performance is not loss tolerant. The study in [23] shows that highly accurate state preparations are required in MDI-QKD.

Recently, Tamaki *et al* have proposed a loss-tolerant security proof [24] that can take modulation error - a

* ztang@physics.utoronto.ca

most crucial flaw in a QKD source, into consideration. The loss-tolerant protocol is secure against the most general type of attacks. For ease of discussion, the intuition behind the security of the loss-tolerant protocol can be understood for the example of the unambiguous state discrimination (USD) attack. The idea is that, as long as the states are encoded in 2-dimensional qubits [25], it is impossible for Eve to launch a USD attack. Therefore Eve cannot enhance state preparation flaws of qubits by channel loss. The performance of QKD can thus be dramatically improved even when the state preparation flaws are considered. This idea has been applied to both the BB84 protocol and the three-state prepare-and-measure protocol [26], and an experimental demonstration is reported in [27].

It is noteworthy that this security proof can be applied to MDI-QKD. In this paper, we extend the work in [24] and present an experimental demonstration of MDI-QKD with state preparation imperfections over fiber links of 10 km and 40 km. By closing an important potential loophole in MDI-QKD, we achieved improved security compared to previous demonstrations.

The contributions of this paper are as follows. First and most importantly, in contrast to previous MDI-QKD demonstrations [10–14] which unrealistically assume perfect state preparations, we carefully optimize the state preparation to minimize the preparation flaws and perform a complete characterization of the states using quantum state tomography. For the first time, we include the state preparation flaws into secure key rate estimation. We highlight that this would not have been possible under previous security proofs [21, 23]. Second, the analysis in [24] only applies to the asymptotic case with an infinite number of decoy states and an infinitely long key. We present the theory (see Appendix A) which shows how the loss-tolerant protocol can be applied to MDI-QKD in a realistic setting, where only a finite number of decoy states and a key of finite length are available. Third, we improve the key generation speed by increasing the system repetition rate from 500 kHz [10] to 10 MHz and employing free-running single-photon detectors with 20% quantum efficiency. These technological improvements enable us to get a positive key rate within a reasonable time frame, even when finite-key effects and encoding flaws are taken into account, and thus demonstrate the practicality of the protocol.

We first briefly explain the loss-tolerant MDI-QKD protocol. Alice (Bob) randomly encodes her (his) key bits into one of the three polarization states $\{\rho_{0_Z}, \rho_{1_Z}, \rho_{0_X}\}$, where ρ_{i_α} is the density matrix of the polarization state of single photons corresponding to the bit value $i \in \{0, 1\}$ in the basis $\alpha \in \{Z, X\}$. She (He) then sends her (his) encoded WCPs to an untrusted third party, Eve, who can be an eavesdropper, to do Bell state measurements (BSMs). After a sufficient number of key bits have been transmitted, Eve announces the BSM results to Alice and Bob. Alice and Bob also announce their basis choices over a public authenticated channel and generate a sifted key. By revealing part of the sifted key, they can estimate the bit error rate in the Z basis and perform error correction.

We apply the decoy state method [28] to estimate the gain of single photons in the Z basis. The phase error rate of single photons e_{11}^X, which quantifies the information leakage to an eavesdropper, is estimated from the transmission rates of fictitious states using the rejected data analysis [24]. Privacy amplification can then be performed to generate a secret key.

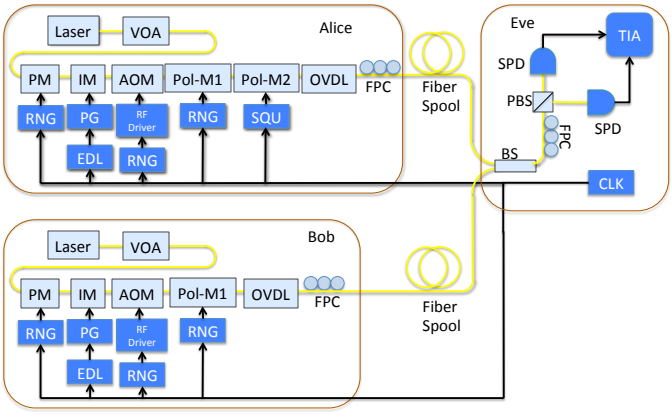

FIG. 1. (Color online). Schematic of the experiment. VOA: variable optical attenuator; PM: phase modulator; IM: intensity modulator; AOM: acousto-optic modulator; Pol-M:polarization modulator; BS: beam splitter; FPC: fiber polarization controllers; PBS: polarizing beam splitter; SPD: single-photon detector; TIA: time interval analyzer; RNG: random number generators; PG: pulse generators; EDL: electrical delay line; SQU: square wave generator; OVDL: optical variable delay line.

Fig.1 shows the schematic of our experiment. Alice and Bob each have a CW laser whose wavelength is independently locked to the P16 line of a C13 acetylene gas cell (integrated in Alice's and Bob's lasers by the manufacturer) at 1542.38 nm. The frequency locking ensures that the frequency difference between Alice's and Bob's lasers is within 10 MHz, guaranteeing the spectral indistinguishability. The laser light is attenuated by a variable optical attenuator (VOA) down to single-photon level at the output of Alice's / Bob's system. Its phase is randomized by a phase modulator into 1000 discrete random phases distributed uniformly in $[0, 2\pi]$, which gives performance close to the case of continuous phase randomization [29]. The amplitude of the light is modulated by an intensity modulator (IM) to generate phase-randomized weak coherent pulses at a repetition rate of $f = 10$ MHz, with a full width at half maximum (FWHM) of around 2.5 ns.

Each pulse's intensity is randomly modulated by an acousto-optic modulator (AOM). We implement the 2-decoy protocol, i.e., each pulse's amplitude is modulated to either the signal state or one of the two decoy states.

Key bits are encoded into the polarization states of the optical pulses by a polarization modulator (Pol-M). The

Pol-M consists of a phase modulator, an optical circulator, and a Faraday mirror. Polarization modulation is achieved by bi-directional modulation of the phase difference of the TE and TM components of the waveguide in the phase modulator. Details of the Pol-M setup can be found in [10, 30]. In the three state protocol, each pulse's polarization is randomly modulated to one of the three BB84 states: the horizontal state ρ_{0_Z}, the vertical state ρ_{1_Z}, and the diagonal state ρ_{0_X}. We fine tuned the voltages on the Pol-Ms to minimize the preparation flaws of these states. See Appendix B for details.

Alice's and Bob's pulses are sent through 2 separate fiber spools to Eve for Bell state measurements (BSMs). BSMs require indistinguishability between Alice and Bob's pulses in all degrees of freedom (except polarization, which is used for encoding). The spectral indistinguishability can be guaranteed by frequency locking in the laser as discussed above (the frequency difference of 10 MHz is much less than the bandwidth of a transform-limited pulse of 2.5 ns). To achieve the temporal indistinguishability, arrival times of Alice's and Bob's pulses are controlled by two passive electrical delay lines (EDLs) and two optical variable delay lines (OVDLs). The EDLs, which can adjust the delay of the the clock signal driving the intensity modulators (and thus the arrival time of the pulses), have a resolution of 0.5 ns and a range of 63.5 ns, and are used for coarse temporal alignments. The relative delay is further finely adjusted by the OVDLs with a resolution less than 10 ps, which is much smaller than the pulses' width of 2.5 ns FWHM.

Alice and Bob need to establish a common polarization reference frame. To achieve this, they first align their Z basis (ρ_{0_Z} and ρ_{1_Z}) to the polarizing axes of the PBS in Eve's BSM setup. Alice has an extra polarization modulator (Pol-M2). This modulator modulates the relative phase between $|H\rangle$ (ρ_{0_Z}) and $|V\rangle$ (ρ_{1_Z}). This is equivalent to a unitary rotation about the $H-V$ axis on the Poincaré sphere, and the amount of rotation depends on the voltage applied on Pol-M2. Alice adjusts the voltage such that her diagonal state ρ_{0_X} is aligned to that of Bob.

Alice and Bob's pulses interfere at the 50/50 beam splitter and are sent to a polarizing beam splitter (PBS), whose outputs are connected to two free running InGaAs/InP single-photon detectors (SPDs, ID220) with 20% quantum efficiency and a dark count rate of 2 kHz. Times of the detection events are recorded by a time interval analyzer (TIA). Within each period (100 ns), a 7 ns window is chosen (by calibrating the arrival times of optical pulses) to post-select detection events. Therefore, over 90% of the dark count noise can be removed and the effective dark count probability per window is around 1.5×10^{-5}. A coincidence between these two detectors implies a successful projection onto the triplet Bell state $|\Psi^+\rangle=(|HV\rangle+|VH\rangle)/\sqrt{2}$.

We characterize the polarization states $\rho_{0_Z},\rho_{1_Z},\rho_{0_X}$ prepared by the Pol-Ms using quantum state tomography. We perform projective measurements by sending the polarization-encoded photons to a polarization analyzer (HP8169A), which consists of a half-wave plate (HWP), a quarter-wave plate (QWP), and a polarizer (POL). Angles of the waveplates and the polarizer are driven by electrical motors with an accuracy of $\pm0.1°$. A SPD is connected to the output of the polarizer for detections. Each input state ρ_{j_α}, $j_\alpha\in\{0_Z,1_Z,0_X\}$, is projected into the following polarization states: $|H\rangle$ (horizontal), $|V\rangle$ (vertical), $|D\rangle$ (diagonal), and $|R\rangle$ (right-hand circular), and counts are accumulated for 10 s for each projective measurement. Density matrices can then be reconstructed using the maximum likelihood technique [31].

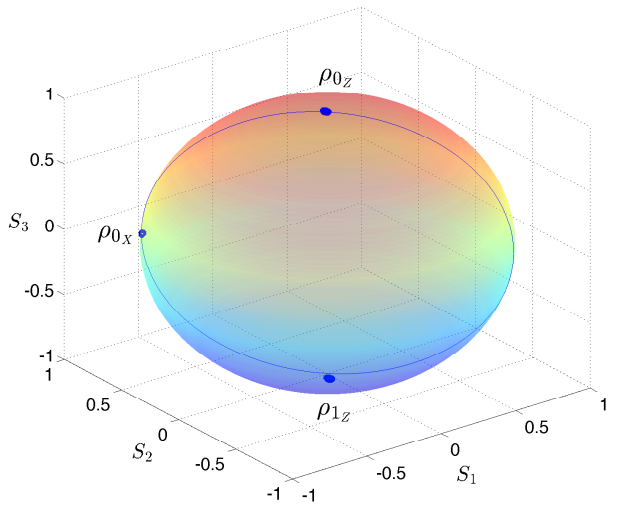

FIG. 2. (Color online).Results of quantum state tomography. Density matrices are represented by their Stokes parameters and plotted on the Poincaré sphere. The Stokes parameters (S_1,S_2,S_3) of the states are: ρ_{0_Z} (-0.0032 $\pm$0.0042, 0.0106 $\pm$0.0055, 0.9994 $\pm$0.0002); ρ_{1_Z} (-0.0375 $\pm$0.0040, -0.0662 $\pm$0.0052, -0.9962 $\pm$0.0005); ρ_{0_X} (-0.6963 $\pm$ 0.0028, 0.7163 $\pm$ 0.0016, -0.0128 $\pm$ 0.0029).

Errors in the quantum state tomography are mostly due to the following factors: errors in counting statistics, errors in the projection states, and drifts of the source's intensity and input state. We monitor the intensity during the experiment, and do not observe significant drift in intensity. The drift in input states is due to the random unitary transformation induced by the short fiber connecting the encoding system and the polarization analyzer. We characterize the stability and find that the input states remain relatively stable within the span of the quantum state tomography measurement. We therefore only consider the first two errors. Errors in counting statistics follow the Poisson distribution. Errors in projection states are due to errors in setting waveplates' angles, which follow the Gaussian distribution with an accuracy of $\pm0.1°$. We use Monte-Carlo method [31] to estimate the errors in the density matrices. Additional sets of data are generated numerically using the above distributions. Each set of data (consisting of counts and

waveplate angles) is used to generate a density matrix by the maximum likelihood technique. We generate 1,000 additional simulated results for each state ρ_{j_α} to get the error distributions of the Stokes parameters. The reconstructed density matrices together with their errors are shown in Fig.2.

We quantify the overlap between two states ρ_{j_α} and ρ_{s_β} by $F(\rho_{j_\alpha}, \rho_{s_\beta})^2$, where $F(\rho_{j_\alpha}, \rho_{s_\beta}) = Tr[\sqrt{\sqrt{\rho_{j_\alpha}}\rho_{s_\beta}\sqrt{\rho_{j_\alpha}}}]$ is the fidelity between ρ_{j_α} and ρ_{s_β}. The overlap between the states ρ_{0_Z} and ρ_{1_Z} is $F(\rho_{0_Z}, \rho_{1_Z})^2 = 0.0024 \pm 0.0006$ (whereas the ideal overlap is 0), and the overlaps between ρ_{0_X} and ρ_{0_Z}, and between ρ_{0_X} and ρ_{1_Z}, are $F(\rho_{0_X}, \rho_{0_Z})^2 = 0.4994 \pm 0.0030$ and $F(\rho_{0_Z}, \rho_{1_Z})^2 = 0.4963 \pm 0.0028$, respectively (whereas the ideal overlaps are 0.5). These results are comparable to other reported results in commercial [27] and research [32] QKD systems. Further details of the state characterization can be found in the Appendix B.

We implement the three state loss-tolerant MDI-QKD over 10 km and 40 km of SMF-28 optical fibers.

In the 10-km demonstration, Alice and Bob are each connected to Eve by a 5-km fiber spool. We optimize the intensities and probability distributions of the signal and decoy states using the model in [28]. The intensity of the signal state is chosen to be $\mu = 0.20$ photon per pulse, and the intensities for the two decoy state are $\nu_1 = 0.03$ and $\nu_2 = 0$ photon per pulse. The probability to send out the signal state μ and the decoy states ν_1 and ν_2 are $P_\mu = 0.3$, $P_{\nu_1} = 0.4$, and $P_{\nu_2} = 0.3$, respectively. The probabilities to send out the states ρ_{0_Z}, ρ_{1_Z}, and ρ_{0_X} are $P_{0_Z} = 0.25$, $P_{1_Z} = 0.25$, and $P_{0_X} = 0.5$, respectively. A total of $N = 6 \times 10^{11}$ pulses are sent out.

The lower bound of the secure key rate is given by [8]

$$R \geq Q_Z^{11,L}[1 - h(e_X^{11,U})] - Q_Z^{\mu\mu} f(E_Z^{\mu\mu}) h(E_Z^{\mu\mu}), \qquad (1)$$

where $Q_Z^{11,L}$ is the lower bound of the gain of single-photon states given that both Alice and Bob send out signal states μ in the Z basis, $e_X^{11,U}$ is the upper bound of the phase error rate of single-photon components, $Q_Z^{\mu\mu}$ is the gain when both of them send signal states, $E_Z^{\mu\mu}$ is the quantum bit error rate (QBER) of the signal states in the Z basis, $f(E_Z^{\mu\mu}) = 1.16$ is the efficiency of error correction, and $h(x) = -x log_2(x) - (1-x) log_2(1-x)$ is the Shannon entropy. The values of $Q_Z^{\mu\mu}$ and $E_Z^{\mu\mu}$ are directly measured from the sifted key, and are shown in Table I.

The value of $Q_Z^{11,L}$ is estimated using the decoy state method [28, 33]. We consider 3 standard deviations of statistical fluctuations for finite-key analysis, and find $Q_Z^{11,L} = 3.96 \times 10^{-5}$.

With the Stokes parameters of the encoded states, we upper bound the phase error rate $e_X^{11,U} = 18.9\%$ using the rejected data analysis [24] and the decoy state method. We can then lower bound the secure key rate $R \geq 2.48 \times 10^{-6}$ bit per signal pulse. The number of pulses where both Alice and Bob send signal states μ in the Z basis is $N_Z^{\mu\mu} = 1.35 \times 10^{10}$, and a private key of length $L = N_Z^{\mu\mu} R = 33.8$ kbits is generated.

The high phase error rate is due to the small key size in this demonstration. We also estimate the key rate without finite-key correction, as shown in Table I. Besides, we perform a proof-of-principle demonstration at 40 km. Intensities of the signal and decoy states are the same as those in the 10 km demonstration. The key rate is estimated without finite-key correction.

As a comparison, we simulate the performance of MDI-QKD with source flaws using the three-state loss-tolerant analysis and the GLLP analysis[21, 23]. The result is shown in Fig.3, which indicates that no secure key can be generated using the GLLP analysis, even for an infinitely long key.

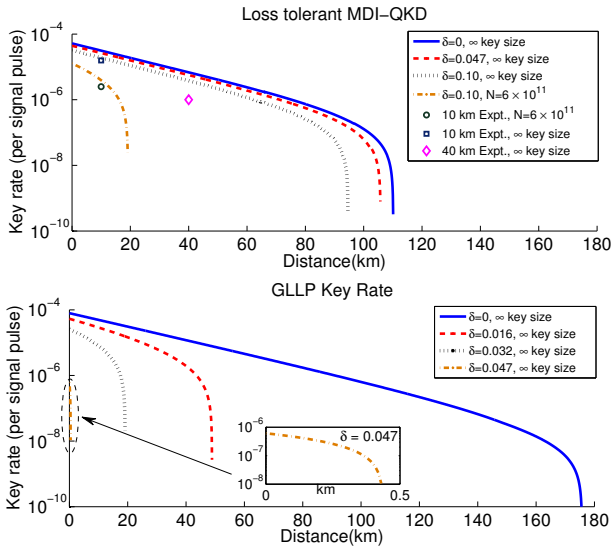

FIG. 3. (Color online). The upper figure shows the simulated and experimental key rates of the loss-tolerant MDI-QKD protocol, for both the infinitely long key case and the finite-key case. We use $\frac{\delta}{\pi}$ to quantify the relative modulation error. See Appendix D for the definition of δ. The modulation error $\delta = 0.1$ corresponds to $F(\rho_{0_Z}, \rho_{1_Z}) = 0.0025$, which is close to our experimental value. The lower figure shows the simulated key rates for an infinitely long key under the GLLP analysis. The results show that the loss-tolerant protocol gives a positive key rate for realistic values of encoding flaws, while no key can be generated with the GLLP proof. We use our experimental parameters for simulation.

In summary, we have demonstrated the first MDI-QKD experiment with an important type of source flaws taken into consideration. In contrast to previous demonstrations which assume perfect state modulations without verification, our experiment shows the feasibility of generating secure keys with imperfect states prepared by off-the-shelf devices. The methodology developed here can be applied to high-speed systems [16] and in a network setting [15].

TABLE I. Key rate for loss-tolerant MDI-QKD at 10 km and 40 km. An infinitely long key (∞ in data size) indicates that finite-key effect is not considered when estimating the key rate R.

Distance	Data size	Security bound	$Q_Z^{11,L}$	$e_X^{11,U}$	$Q_Z^{\mu\mu}$	$E_Z^{\mu\mu}$	R (bit per pulse)
10 km	6×10^{11}	10^{-3}	3.96×10^{-5}	0.189	6.31×10^{-5}	0.0178	2.48×10^{-6}
10 km	∞	N/A	4.17×10^{-5}	0.079	6.31×10^{-5}	0.0178	1.57×10^{-5}
40 km	∞	N/A	1.88×10^{-5}	0.122	2.94×10^{-5}	0.0368	1.00×10^{-6}

ACKNOWLEDGMENTS

We thank F. Xu, E. Zhu, and M. Curty for enlightening discussions. Financial support from NSERC Discovery Grant, NSERC RTI Grant, and the Canada Research Chairs Program is gratefully acknowledged.

Appendix A: Upper-bounding phase error rate

1. Rejected data analysis

In this section, we give the algorithm used in the paper to estimate the phase error rate e_X^{11} using the rejected data analysis as proposed in [24].

In the actual three-state MDI-QKD protocol, Alice and Bob send the untrusted third party Eve photons encoded in one of the three polarization states. Let $|\phi_{j_\alpha}\rangle_{A_eE}$ be the purification of the state ρ_{E,j_α} sent by Alice to Eve, where $j_\alpha\in\{0_Z,1_Z,0_X\}$, and the subscripts A_e and E represent the extended system possessed by Alice and the system to be sent to Eve, respectively. Sending the state $\rho_{E,0_Z}$ ($\rho_{E,1_Z}$) to Eve by Alice is equivalent to preparing the tripartite state of systems A, A_e, E

$$|\Psi\rangle_{AA_eE}=\frac{1}{\sqrt{2}}(|0_Z\rangle_A|\phi_{0_Z}\rangle_{A_eE}+|1_Z\rangle_A|\phi_{1_Z}\rangle_{A_eE}) \quad \text{(A1)}$$

followed by a projective measurement on system A in the Z basis with an outcome of 0 (1), and sending system E to Eve.

Likewise, sending ρ_{0_Z} (ρ_{1_Z}) to Eve by Bob is equivalent to preparing the tripartite state $|\Psi\rangle_{BB_eE'}$ with systems B, B_e, and E',

$$|\Psi\rangle_{BB_eE'}=\frac{1}{\sqrt{2}}(|0_Z\rangle_B|\phi_{0_Z}\rangle_{B_eE'}+|1_Z\rangle_B|\phi_{1_Z}\rangle_{B_eE'}), \quad \text{(A2)}$$

followed by a projective measurement on system B in the Z basis with outcome 0 (1), and sending system E' to Eve.

Now consider the following virtual protocol. Alice prepares the state $|\Psi\rangle_{AA_eE}$, measures system A in the X basis with outcome $j\in\{0,1\}$, and sends Eve the system E. The state sent to Eve can be written as

$$\hat{\sigma}^{vir}_{E,j_X}=Tr_{AA_e}[\hat{P}(|j_X\rangle_A)\mathbb{I}_{A_eE}\hat{P}(|\Psi\rangle_{AA_eE})], \quad \text{(A3)}$$

where $\hat{P}(x)=|x\rangle\langle x|$, and $|j_X\rangle=1/\sqrt{2}(|0_Z\rangle+(-1)^j|1_Z\rangle)$. Similarly, Bob prepares the state $|\Psi\rangle_{BB_eE}$, measures system B in the X basis with outcome $s\in\{0,1\}$, and sends Eve the system E' whose state is given by

$$\hat{\sigma}^{vir}_{E',s_X}=Tr_{BB_e}[\hat{P}(|s_X\rangle_B)\mathbb{I}_{B_eE'}\hat{P}(|\Psi\rangle_{BB_eE'})], \quad \text{(A4)}$$

where $|s_X\rangle=1/\sqrt{2}(|0_Z\rangle+(-1)^s|1_Z\rangle)$.

The phase error rate of single photon components is determined by the transmission rates of the fictitious states:

$$e_X^{11}=\frac{Y^{\Psi^+,vir}_{0_X1_X}+Y^{\Psi^+,vir}_{1_X0_X}}{Y^{\Psi^+,vir}_{0_X0_X}+Y^{\Psi^+,vir}_{1_X1_X}+Y^{\Psi^+,vir}_{0_X1_X}+Y^{\Psi^+,vir}_{1_X0_X}}. \quad \text{(A5)}$$

where $Y^{\Psi^+}_{j_Xs_X}$ is the probability that Alice and Bob send Eve the virtual states $\hat{\sigma}_{E,j_X}$ and $\hat{\sigma}_{E',s_X}$, respectively, and Eve gets a successful Bell state measurement with outcome $|\Psi^+\rangle=(|H\rangle|V\rangle+|V\rangle|H\rangle)/\sqrt{2}$, which is given by

$$Y^{\Psi^+,vir}_{j_Xs_X}=Tr[\hat{\sigma}^{vir}_{E,j_X}]Tr[\hat{\sigma}^{vir}_{E',s_X}]Tr[\hat{D}_{\Psi^+}\hat{\sigma'}^{vir}_{E,j_X}\otimes\hat{\sigma'}^{vir}_{E',s_X}]. \quad \text{(A6)}$$

In the above equation, the operator $\hat{D}_{\psi^+}$ is Eve's operation corresponding to the BSM with outcome Ψ^+, and the operators $\hat{\sigma'}^{vir}_{E,j_X}$ and $\hat{\sigma'}^{vir}_{E',j_X}$ are the normalized versions of $\hat{\sigma}^{vir}_{E,j_X}$ and $\hat{\sigma}^{vir}_{E',j_X}$ given by

$$\begin{aligned}\hat{\sigma'}^{vir}_{E,j_X}&=\hat{\sigma}^{vir}_{E,j_X}/Tr[\hat{\sigma}^{vir}_{E,j_X}]\\ \hat{\sigma'}^{vir}_{E',j_X}&=\hat{\sigma}^{vir}_{E',j_X}/Tr[\hat{\sigma}^{vir}_{E',j_X}]\end{aligned} \quad \text{(A7)}$$

The density operators of the virtual states $\hat{\sigma}^{vir}_{E,j_X}$ and $\hat{\sigma}^{vir}_{E',s_X}$ can be found from the density operators of the actual states ρ_{j_α}. From Eqs. (A1) and (A3), the virtual state σ_{E,j_X} sent to Eve by Alice is

$$\begin{aligned}\hat{\sigma}^{vir}_{E,j_X}=&Tr_{AA_e}[\hat{P}(|j_X\rangle_A)\mathbb{I}_{A_eE}\hat{P}(|\Psi\rangle_{AA_eE})]\\ =&\frac{1}{4}[(\rho_{E,0_Z}+\rho_{E,1_Z})+(-1)^jTr_{A_e}(|\phi_{1_Z}\rangle_{A_eE}\langle\phi_{0_Z}|_{A_eE}\\ &+|\phi_{0_Z}\rangle_{A_eE}\langle\phi_{1_Z}|_{A_eE})].\end{aligned} \quad \text{(A8)}$$

Let $|\gamma^0_{j_\alpha}\rangle_E$ and $|\gamma^1_{j_\alpha}\rangle_E$ be the eigenvectors of ρ_{E,j_α}, and $|\lambda^0_{E,j_\alpha}|^2$ and $|\lambda^1_{E,j_\alpha}|^2$ be the corresponding eigenvalues. The Schmidt decomposition of $|\phi_{j_\alpha}\rangle_{A_eE}$ is

$$|\phi_{j_\alpha}\rangle_{A_eE}=\lambda^0_{E,j_\alpha}|0\rangle_{A_e}|\gamma^0_{j_\alpha}\rangle_E+\lambda^1_{E,j_\alpha}|1\rangle_{A_e}|\gamma^1_{j_\alpha}\rangle_E \quad \text{(A9)}$$

where $\{|0\rangle_{A_e}|1\rangle_{A_e}\}$ is a basis of Alice's extended system A_e. Note that since Alice possesses the extended system

A_e, she can select the basis $\{|0\rangle_{A_e}|1\rangle_{A_e}\}$ in the purification of ρ_{E,j_α} to optimize the key rate. In this paper, we use the same basis $\{|0\rangle_{A_e}|1\rangle_{A_e}\}$ for the purification of $\rho_{E,0_Z}$ and $\rho_{E,1_Z}$, which is not necessarily the optimal choice. The key rate can be further improved by optimizing the purification, which is left as future work.

Substituting Eq. (A9) into (A8), the virtual state $\hat{\sigma}^{vir}_{E,j_X}$ is

$$\begin{aligned}\hat{\sigma}^{vir}_{E,j_X} = \frac{1}{4}\{&(\rho_{E,0_Z}+\rho_{E,1_Z})\\ &+(-1)^j[\lambda^0_{E,0_Z}\lambda^0_{E,1_Z}(|\gamma^0_{0_Z}\rangle_E\langle\gamma^0_{1_Z}|_E+|\gamma^0_{1_Z}\rangle_E\langle\gamma^0_{0_Z}|_E)\\ &+\lambda^1_{E,0_Z}\lambda^1_{E,1_Z}(|\gamma^1_{0_Z}\rangle_E\langle\gamma^1_{1_Z}|_E+|\gamma^1_{1_Z}\rangle_E\langle\gamma^1_{0_Z}|_E)]\}.\end{aligned} \tag{A10}$$

The density operator σ^{vir}_{E',s_X} (the virtual state sent to Eve by Bob) can be found using the same method.

We first discuss the case where the states lie in the $X-Z$ plane. In this case, the Stokes parameter $S^Y=0$, and the states $\hat{\sigma'}^{vir}_{E,j_X}$ (with Stokes parameters $(S^{vir,X}_{E,j_X}, 0, S^{vir,Z}_{E,j_X})$ and $\hat{\sigma'}^{vir}_{E',s_X}$ (with Stokes parameters $(S^{vir,X}_{E,j_X}, 0, S^{vir,Z}_{E,j_X})$ can be written as a linear combination of the identity matrix $\hat{\sigma}_I$ and the Pauli matrices $\hat{\sigma}_X, \hat{\sigma}_Z$:

$$\hat{\sigma'}^{vir}_{E,j_X} = \frac{1}{2}(\hat{\sigma}_I + S^{vir,X}_{E,j_X}\hat{\sigma}_X + S^{vir,Z}_{E,j_X}\hat{\sigma}_Z) \tag{A11}$$

$$\hat{\sigma'}^{vir}_{E',s_X} = \frac{1}{2}(\hat{\sigma}_I + S^{vir,X}_{E',s_X}\hat{\sigma}_X + S^{vir,Z}_{E',s_X}\hat{\sigma}_Z) \tag{A12}$$

Define the transmission rate of $\hat{\sigma}_t\otimes\hat{\sigma}_{t'}$, $t,t'\in\{I,X,Z\}$ as

$$q_{\Psi^+|t,t'} = \frac{1}{4}Tr[\hat{D}_{\Psi^+}\hat{\sigma}_t\otimes\hat{\sigma}_{t'}]. \tag{A13}$$

From Eqs. (A6) and (A13), the transmission rate $Y^{\Psi^+}_{j_X s_X}$ can be written as

$$\begin{aligned}Y^{\Psi^+,vir}_{j_X s_X} = &Tr[\hat{\sigma}^{vir}_{E,j_X}]Tr[\hat{\sigma}^{vir}_{E',s_X}]\times(q_{\Psi^+|I\otimes I}+S^{vir,X}_{E',s_X}q_{\Psi^+|I\otimes X}+S^{vir,Z}_{E',s_X}q_{\Psi^+|I\otimes Z}\\ &+S^{vir,X}_{E,j_X}q_{\Psi^+|X\otimes I}+S^{vir,X}_{E,j_X}S^{vir,X}_{E',s_X}q_{\Psi^+|X\otimes X}+S^{vir,X}_{E,j_X}S^{vir,Z}_{E',s_X}q_{\Psi^+|X\otimes Z}\\ &+S^{vir,Z}_{E,j_X}q_{\Psi^+|Z\otimes I}+S^{vir,Z}_{E,j_X}S^{vir,X}_{E',s_X}q_{\Psi^+|Z\otimes X}+S^{vir,Z}_{E,j_X}S^{vir,Z}_{E',s_X}q_{\Psi^+|Z\otimes Z})\end{aligned} \tag{A14}$$

Let $\mathbf{S^{vir}_{j_X s_X}}$ be a row vector and $\mathbf{q}$ be a column vector defined as

$$\mathbf{S^{vir}_{j_X s_X}} = [1, S^{vir,X}_{E',s_X}, S^{vir,Z}_{E',s_X}, S^{vir,X}_{E,j_X}, S^{vir,X}_{E,j_X}S^{vir,X}_{E',s_X}, S^{vir,X}_{E,j_X}S^{vir,Z}_{E',s_X}, S^{vir,Z}_{E,j_X}, S^{vir,Z}_{E,j_X}S^{vir,X}_{E',s_X}, S^{vir,Z}_{E,j_X}S^{vir,Z}_{E',s_X}], \tag{A15}$$

$$\mathbf{q} = [q_{\Psi^+|I\otimes I}, q_{\Psi^+|I\otimes X}, q_{\Psi^+|I\otimes Z}, q_{\Psi^+|X\otimes I}, q_{\Psi^+|X\otimes X}, q_{\Psi^+|X\otimes Z}, q_{\Psi^+|Z\otimes X}, q_{\Psi^+|Z\otimes Z}]^T, \tag{A16}$$

respectively. The expression for the transmission rate $Y^{\Psi^+,vir}_{j_X s_X}$ (Eq. (A14)) can be written as

$$Y^{\Psi^+,vir}_{j_X s_X} = Tr[\hat{\sigma}^{vir}_{E,j_X}]Tr[\hat{\sigma}^{vir}_{E',s_X}]\mathbf{S^{vir}_{j_X s_X}}\mathbf{q}. \tag{A17}$$

Once we know the transmission rates of the Pauli matrices $\mathbf{q}$, we can estimate $Y^{\Psi^+,vir}_{j_X s_X}$ and the phase error rate e^{11}_X. In the next session, we will discuss how to find $\mathbf{q}$ from experimental data.

When the states ρ_{E,j_α} prepared by Alice / Bob do not lie in the $X-Z$ plane, we can always find a reference frame such that the states $\rho_{E,0_Z}$, $\rho_{E,1_Z}$, and $\rho_{E,0_X}$ have a common Stokes parameter S^Y_E (i.e., the Stokes parameters of the state ρ_{E,j_α} is given by $(S^X_{E,j_\alpha}, S^Y_E, S^Z_{E,j_\alpha})$.) We apply the filtering technique described in [24], which shows that, for a state ρ_{E,j_α} with a nonzero S^Y_E, we can equivalently consider the following state with its Stokes parameters given by,

$$(\frac{S^X_{E,j_\alpha}}{f(q)}, 0, \frac{S^Z_{E,j_\alpha}}{f(q)}) \tag{A18}$$

where $f(q)$ is given by

$$f(q) = \frac{2(1-q)q}{1-2q+2q^2} \tag{A19}$$

and q is determined by solving the following equation

$$S^Y_E = \frac{(2q-1)}{(1-2q+2q^2)}. \tag{A20}$$

2. Estimating transmission rates of Pauli matrices from experimental data

In this section, we will show how to estimate the transmission rates of Pauli matrices $\mathbf{q}$ from experimental data. Recall in the three-state MDI-QKD, Alice (Bob) randomly sends Eve one of the three states $\rho_{E,0_Z}$ ($\rho_{E',0_Z}$), $\rho_{E,1_Z}$ ($\rho_{E',1_Z}$), $\rho_{E,0_X}$ ($\rho_{E',0_X}$). As in the previous section, the subscripts E and E' represent the systems sent to Eve by Alice and Bob, respectively.

Let $Y_{j_\alpha s_\beta}^{\Psi^+,11}$ be the *conditional* probability that Eve gets a successful Bell state measurement with outcome Ψ^+ given that Alice sends Eve a single photon of state ρ_{E,j_α} and Bob sends Eve a single photon of state ρ_{E',s_β} (the superscript 11 represent that both Alice and Bob send out single photons). Following the procedures described in the previous section, the transmission rate of the actual states $Y_{j_\alpha s_\beta}^{\Psi^+,11}$ can be written as

$$Y_{j_\alpha s_\beta}^{\Psi^+,11} = \mathbf{S_{j_\alpha s_\beta}} \mathbf{q}, \tag{A21}$$

where $\mathbf{S_{j_\alpha s_\beta}}$ is related to the actual states ρ_{E,j_α} (with Stokes parameters (S_{E,j_α}^X, 0, S_{E,j_α}^Z) and ρ_{E',s_β} (with Stokes parameters (S_{E',s_beta}^X, 0, S_{E',s_β}^Z) as follows:

$$\mathbf{S_{j_\alpha s_\beta}} = [1, S_{E',s_\beta}^X, S_{E',s_\beta}^Z, S_{E,j_\alpha}^X, S_{E,j_\alpha}^X S_{E',s_\beta}^X, S_{E,j_\alpha}^X S_{E',s_\beta}^Z, S_{E,j_\alpha}^Z, S_{E,j_\alpha}^Z S_{E',s_\beta}^X, S_{E,j_\alpha}^Z S_{E',s_\beta}^Z]. \tag{A22}$$

From experiment, we can get the following set of independent linear equations:

$$\begin{aligned}
Y_{0_Z0_Z}^{\Psi^+,11} &= \mathbf{S_{0_Z0_Z}} \mathbf{q}, \\
Y_{0_Z1_Z}^{\Psi^+,11} &= \mathbf{S_{0_Z1_Z}} \mathbf{q}, \\
Y_{1_Z0_Z}^{\Psi^+,11} &= \mathbf{S_{1_Z0_Z}} \mathbf{q}, \\
Y_{1_Z1_Z}^{\Psi^+,11} &= \mathbf{S_{1_Z1_Z}} \mathbf{q}, \\
Y_{0_X0_Z}^{\Psi^+,11} &= \mathbf{S_{0_X0_Z}} \mathbf{q}, \\
Y_{0_X1_Z}^{\Psi^+,11} &= \mathbf{S_{0_X1_Z}} \mathbf{q}, \\
Y_{0_Z0_X}^{\Psi^+,11} &= \mathbf{S_{0_Z0_X}} \mathbf{q}, \\
Y_{1_Z0_X}^{\Psi^+,11} &= \mathbf{S_{1_Z0_X}} \mathbf{q}, \\
Y_{0_X0_X}^{\Psi^+,11} &= \mathbf{S_{0_X0_X}} \mathbf{q}.
\end{aligned} \tag{A23}$$

Define a vector $\mathbf{Y^{\Psi^+,11}}$

$$\begin{aligned}
\mathbf{Y^{\Psi^+,11}} = [&Y_{0_Z0_Z}^{\Psi^+,11}, Y_{0_Z1_Z}^{\Psi^+,11}, Y_{1_Z0_Z}^{\Psi^+,11}, Y_{1_Z1_Z}^{\Psi^+,11}, \\
&Y_{0_X0_Z}^{\Psi^+,11}, Y_{0_X1_Z}^{\Psi^+,11}, Y_{0_Z0_X}^{\Psi^+,11}, Y_{1_Z0_X}^{\Psi^+,11}, Y_{0_X0_X}^{\Psi^+,11}]
\end{aligned} \tag{A24}$$

and a matrix \$

$$\$ = \begin{bmatrix}
\mathbf{S_{0_Z0_Z}} \\
\mathbf{S_{0_Z1_Z}} \\
\mathbf{S_{1_Z0_Z}} \\
\mathbf{S_{1_Z1_Z}} \\
\mathbf{S_{0_X0_Z}} \\
\mathbf{S_{0_X1_Z}} \\
\mathbf{S_{0_Z0_X}} \\
\mathbf{S_{1_Z0_X}} \\
\mathbf{S_{0_X0_X}}
\end{bmatrix}$$

The linear system (A23) can be concisely written as

$$\mathbf{Y^{\Psi^+,11}} = \$\mathbf{q}. \tag{A25}$$

Knowing $\mathbf{Y^{\Psi^+,11}}$ from the experiment, the transmission rates $\mathbf{q}$ can be solved:

$$\mathbf{q} = \$^{-1}\mathbf{Y^{\Psi^+,11}}. \tag{A26}$$

The transmission rates of the virtual states can then be calculated by Eq.(A17), and the phase error rate can be estimated by Eq.(A5).

3. Bounding e_X^{11} with a finite number of decoy states

In the previous two sections, we give the method to estimate the phase error rate e_X^{11} from the $Y_{j_\alpha s_\beta}^{\Psi^+,11}$, which is the yield of single photon components. The parameter $Y_{j_\alpha s_\beta}^{\Psi^+,11}$ can be precisely estimated with an infinite number of decoy states.

In reality, we can only apply a finite number of decoy states, where the value of $Y_{j_\alpha s_\beta}^{\Psi^+,11}$ can not be precisely determined. Instead, we can find an upper bound $Y_{j_\alpha s_\beta}^{\Psi^+,11,U}$, and a lower bound $Y_{j_\alpha s_\beta}^{\Psi^+,11,L}$, either analytically [28, 34] or by linear programming. In this case, the linear system (A23, A25) should be replaced with the following linear inequality:

$$\mathbf{Y^{\Psi^+,11,L}} \leq \$\mathbf{q} \leq \mathbf{Y^{\Psi^+,11,U}}. \tag{A27}$$

where

$$\begin{aligned}
\mathbf{Y^{\Psi^+,11,L}} = [&Y_{0_Z0_Z}^{\Psi^+,11,L}, Y_{0_Z1_Z}^{\Psi^+,11,L}, Y_{1_Z0_Z}^{\Psi^+,11,L}, Y_{1_Z1_Z}^{\Psi^+,11,L}, \\
&Y_{0_X0_Z}^{\Psi^+,11,L}, Y_{0_X1_Z}^{\Psi^+,11,L}, Y_{0_Z0_X}^{\Psi^+,11,L}, Y_{1_Z0_X}^{\Psi^+,11,L}, Y_{0_X0_X}^{\Psi^+,11,L}],
\end{aligned} \tag{A28}$$

and

$$\mathbf{Y}^{\Psi^+,\mathbf{11},\mathbf{U}} = [Y_{0_Z0_Z}^{\Psi^+,11,U}, Y_{0_Z1_Z}^{\Psi^+,11,U}, Y_{1_Z0_Z}^{\Psi^+,11,U}, Y_{1_Z1_Z}^{\Psi^+,11,U}, Y_{0_X0_Z}^{\Psi^+,11,U}, Y_{0_X1_Z}^{\Psi^+,11,U}, Y_{0_Z0_X}^{\Psi^+,11,U}, Y_{1_Z0_X}^{\Psi^+,11,U}, Y_{0_X0_X}^{\Psi^+,11,U}]. \tag{A29}$$

Our task is to find an upper bound of the phase error rate e_X^{11}. The expression of e_X^{11} (Eq. A5) can be rewritten as

$$e_X^{11} = \frac{1}{1 + \frac{Y_{0_X0_X}^{\Psi^+,vir} + Y_{1_X1_X}^{\Psi^+,vir}}{Y_{0_X1_X}^{\Psi^+,vir} + Y_{1_X0_X}^{\Psi^+,vir}}}. \tag{A30}$$

The upper bound of e_X^{11} found by lower bounding $Y_{0_X0_X}^{\Psi^+,vir}+Y_{1_X1_X}^{\Psi^+,vir}$ and upper bounding $Y_{0_X1_X}^{\Psi^+,vir}+Y_{1_X0_X}^{\Psi^+,vir}$:

$$e_X^{11} \leq e_X^{11,U} = \frac{1}{1 + \frac{(Y_{0_X0_X}^{\Psi^+,vir} + Y_{1_X1_X}^{\Psi^+,vir})^L}{(Y_{0_X1_X}^{\Psi^+,vir} + Y_{1_X0_X}^{\Psi^+,vir})^U}}. \tag{A31}$$

Finding a lower bound of $Y_{0_X0_X}^{\Psi^+,vir} + Y_{1_X1_X}^{\Psi^+,vir}$ is equivalent to the following linear programming problem:

$$\min_{q}\{(Tr[\hat{\sigma}_{E,0_X}^{vir}]Tr[\hat{\sigma}_{E',0_X}^{vir}]\mathbf{S_{0_X0_X}^{vir}} + Tr[\hat{\sigma}_{E,1_X}^{vir}]Tr[\hat{\sigma}_{E',1_X}^{vir}]\mathbf{S_{1_X1_X}^{vir}})\mathbf{q}\} \tag{A32}$$

subject to the constraint given by inequality (A27).

Similarly, upper bounding $Y_{0_X1_X}^{\Psi^+,vir} + Y_{1_X0_X}^{\Psi^+,vir}$ is equivalent to the following linear programming problem:

$$\max_{q}\{(Tr[\hat{\sigma}_{E,0_X}^{vir}]Tr[\hat{\sigma}_{E',1_X}^{vir}]\mathbf{S_{0_X1_X}^{vir}} + Tr[\hat{\sigma}_{E,1_X}^{vir}]Tr[\hat{\sigma}_{E',0_X}^{vir}]\mathbf{S_{1_X0_X}^{vir}})\mathbf{q}\} \tag{A33}$$

subject to the constraint (A27).

Appendix B: State characterization

In this session, we discuss the sources of errors involved in preparing the BB84 states, and how we minimize the state preparation errors. We then present the details of state characterization using quantum state tomography.

1. Sources of encoding errors

Fig. 4 shows the schematic of the bi-directional polarization modulator [30]. Optical pulses are launched through an optical circulator to a phase modulator (PM). The polarization of the light is at 45° to the TE axis of the $LiNbO_3$ waveguide inside the PM. When an optical pulse travels through the PM for the first time, a positive voltage $+V$ is applied on the phase modulator. The pulse is reflected by a Faraday mirror (FM) with its polarization rotated by 90°, and travels back. When the pulse travels through the PM for the second time, a negative voltage $-V$ is applied on the PM. Due to the different modulation efficiency in the TE and TM modes, we introduce a phase difference along the TE and TM directions. The output state can be expressed as

$$|\psi\rangle = \frac{|TE\rangle + e^{i\psi}|TM\rangle}{\sqrt{2}}, \tag{B1}$$

where $|TE\rangle$ and $|TM\rangle$ represent the polarization states along the TE and TM directions of the PM's waveguide, and ψ is the phase difference introduced, which depends on the applied voltage. By modulating ψ to $\{0, \pi, \pi/2\}$, we can generate the three states $\{\rho_{0_Z}, \rho_{1_Z}, \rho_{0_X}\}$ needed in our protocol.

Here we discuss the sources of errors in the encoding system that lead to imperfect state preparations.

Power mismatch in TE and TM modes Ideally we want optical pulses to be launched into the PM at an angle of 45° relative to the TE axis of the PM's waveguide. Is this case, the powers along the TE and TM directions are equal, and the output states $\{\rho_{0_Z}, \rho_{1_Z}, \rho_{0_X}\}$ are located on a great circle on the Poincaré sphere. However, optical pulses may be launched at an angle κ other than 45°. In this case, the modulated output state B1 should be rewritten as

$$|\psi\rangle = cos(\kappa)|TE\rangle + sin(\kappa)e^{i\psi}|TM\rangle. \tag{B2}$$

As a result, the output states $\{\rho_{0_Z}, \rho_{1_Z}, \rho_{0_X}\}$ are distributed on a small circle on the Poincaré sphere. In this case, ρ_{0_Z} and ρ_{1_Z} are no longer orthogonal, and their overlap (characterized by $F(\rho_{0_Z}, \rho_{0_Z})^2$, where $F(\rho_{0_Z}, \rho_{0_Z})$ is the fidelity between ρ_{0_Z} and ρ_{1_Z}) is $cos^2(2\kappa)$. This is the dominant error that leads to modulation errors in our encoding system.

Control voltage accuracy The accuracy is limited by the voltage resolution of the signal source driving the

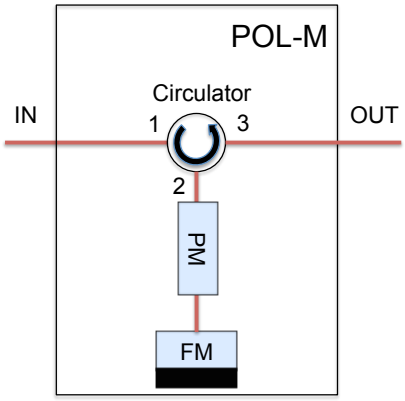

FIG. 4. (Color online). Schematic of the polarization modulator.

PM. In our experiment, the waveform generator driving the PM has an output amplitude of ±5 V and a resolution of 1 mV. The V_π of the PM is around 5 V, which means that error due to limited resolution of the driving voltage is relatively small.

To minimize the errors in the state preparation, we finely scan the voltage applied on the phase modulator at a step of 0.02 V and characterize the corresponding output states. The step size of 0.02 V guarantees that the error due to voltage accuracy is less than 0.4%. Fig. 5 shows different states corresponding to different voltages applied on the polarization modulator. ρ_{0_Z} corresponds to the state when the applied voltage is 0 V. We search around 2.5 V and 5.0 V at a step size of 0.02 V for the states ρ_{0_X} and ρ_{1_Z} with minimum encoding errors. Each point on the Poincaré sphere corresponds one applied voltage. The states are reconstructed using quantum state tomography, as discussed in the next section. Fig. 6 shows the overlap between ρ_{0_Z} and ρ_{0_X}, and the overlap between ρ_{0_Z} and ρ_{1_Z}, with different voltages. The voltage for ρ_{0_X} is chosen such that the overlap between ρ_{0_Z} and ρ_{0_X} is as close to 0.5 as possible, and the voltage for ρ_{1_Z} is chosen such that the overlap between ρ_{0_Z} and ρ_{1_Z} is minimized.

2. Quantum state tomography

Fig.7 shows the setup of the quantum state tomography experiment. Optical pulses encoded in the polarization state $\rho_{j\alpha}$, where $j_\alpha \in \{0_Z, 1_Z, 0_X\}$, are sent to the electrical polarization controller for projective measurements. The projective state $|\psi\rangle$ is given by

$$|\psi\rangle = U^\dagger_{HWP}(\theta)U^\dagger_{QWP}(\phi)|H\rangle. \quad \text{(B3)}$$

The operations $U_{HWP}(\phi)$ and $U_{QWP}(\phi)$ are the unitary transformations by a half wave plate (HWP) and a quarter wave plate (QWP) with fast axes set to θ and ϕ, respectively, which are given by

$$U_{HWP}(\theta) = \begin{bmatrix} cos(2\theta) & sin(2\theta) \\ sin(2\theta) & -cos(2\theta) \end{bmatrix}$$

$$U_{QWP}(\phi) = \begin{bmatrix} cos^2(\phi) + isin^2(\phi) & (1-i)cos(\phi)sin(\phi) \\ (1-i)cos(\phi)sin(\phi) & sin^2(\phi) + icos^2(\phi) \end{bmatrix}$$

.

In the tomography experiment, each state ρ_{j_α} is projected into the following four polarization basis states: horizontal $|H\rangle$, vertical $|V\rangle$, diagonal$|D\rangle$, and right-hand circular $|R\rangle$. The settings of the HWP, QWP, and POL are summarized in Table II. Photons are detected by a single photon detector (SPD1). Another single photon detector (SPD2) is used to monitor the total intensity of the incoming light pulses. The data acquisition time for each projective measurement is $t = 10s$, and the counts are summarized in Table III.

Below we describe the procedures to reconstruct the density matrices from the data in Table III (see next section) using the maximum likelihood technique [31]. For each projective measurement, counts detected by SPD1 are accumulated for $10s$, and the results are shown in Table I of the main text. The total counts corresponding to the projective measurement to $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|R\rangle$ are denoted as n_H, n_V, n_D, and n_R, respectively. We first

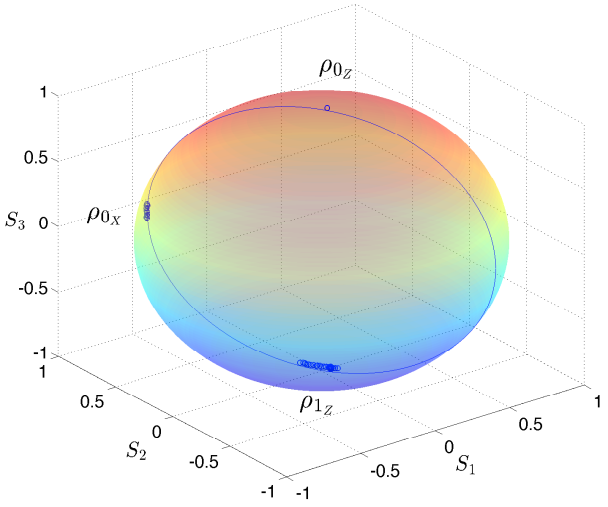

FIG. 5. (Color online). Search of the states with minimum encoding errors. We scan the voltages applied on the polarization modulator to find the states ρ_{0_X} and ρ_{1_Z} with minimum modulation errors.

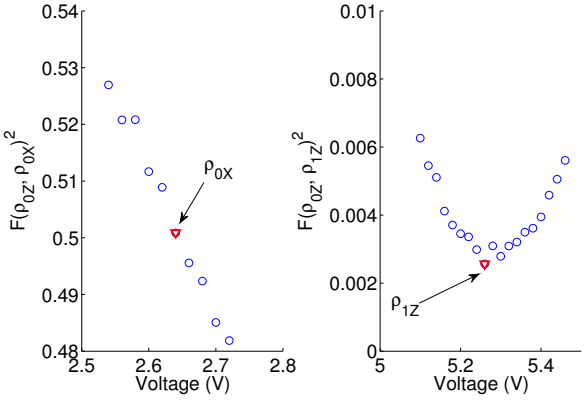

FIG. 6. (Color online). Overlap between ρ_{0_Z} and ρ_{0_X}, and overlap between ρ_{0_Z} and ρ_{1_Z}, with different voltages applied on the Pol-M. The voltage for ρ_{0_X} is chosen to get the overlap between ρ_{0_Z} and ρ_{0_X} as close to 0.5 as possible, and the voltage for ρ_{1_Z} is chosen such that the overlap between ρ_{0_Z} and ρ_{1_Z} is minimized.

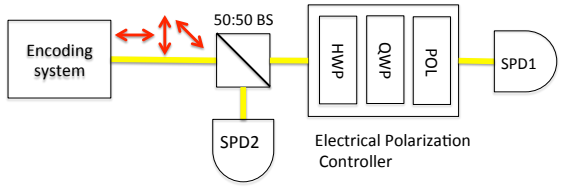

FIG. 7. (Color online). Schematic of the quantum state tomography setup. HWP: half wave plate; QWP, quarter wave plate; POL: polarizer; SPD, single photon detector.

TABLE II. Angles of waveplates and polarizer angles for quantum state tomography.

Projective state	HWP	QWP	POL
$\|H\rangle$	0°	0°	0°
$\|V\rangle$	45°	0°	0°
$\|D\rangle$	22.5°	0°	0°
$\|R\rangle$	0°	45°	0°

calculate a normalized count rate $\tilde{n}_\psi, \psi \in \{H, V, D, R\}$ to correct the impacts of dark counts and deadtime:

$$\tilde{n}_\psi = \frac{n_\psi}{t - n_\psi \tau} - DC \tag{B4}$$

where $t = 10s$ is the data acquisition time, $\tau = 10\mu s$ is the detector deadtime, and $DC = 50Hz$ is the dark count rate. Note that in the above expression, the term $(t - n_\psi\tau)$ gives the total active time of the detector during t, and $\frac{n_\psi}{t-n_\psi\tau}$ gives the counting rate per unit active time.

The density matrix to be reconstructed can be written as

$$\rho_{j_\alpha} = \frac{T_{j_\alpha}^\dagger T_{j_\alpha}}{Tr[T_{j_\alpha}^\dagger T_{j_\alpha}]}. \tag{B5}$$

TABLE III. Raw counts in the quantum state tomography experiment. Counts are accumulated for 10 s.

State	Projected states			
	$\|H\rangle$	$\|V\rangle$	$\|D\rangle$	$\|R\rangle$
ρ_{0_Z}	201311	583	112867	114043
ρ_{1_Z}	982	203500	122028	110687
ρ_{0_X}	114815	117459	35646	38239

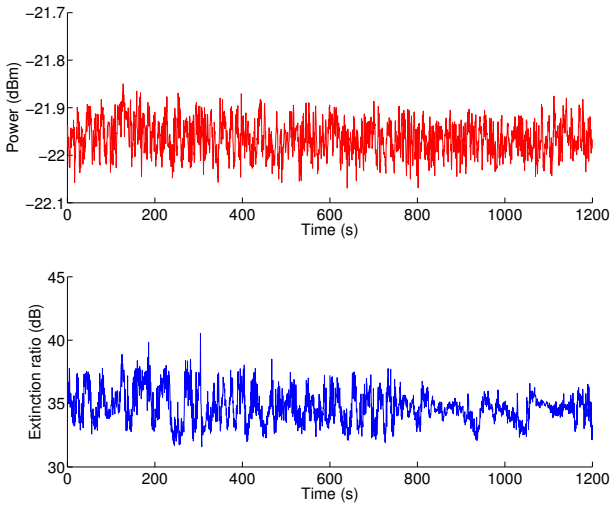

FIG. 8. (Color online). Stability of intensities and input states during the quantum state tomography. The upper figure shows the optical power coming out of the encoding system (intensity was not attenuated to single photon level in this measurement). The lower figure shows the stability test of the input polarization states. Horizontally polarized light coming out of the encoding system is measured at the H/V basis by a polarizing beam splitter. The figure shows the extinction ratio (i.e., the ratio of the power at the H and V output ports), which is around 35 dB over a period of 1200 s. The results show that the intensities and polarization states remain stable within the span of the tomography experiment (< 5 minutes).

where $T_{j_\alpha}^\dagger$ is the conjugate transpose of T_{j_α}, and T_{j_α} is given by

$$T_{j_\alpha} = \begin{bmatrix} t_1 & 0 \\ t_3 + it_4 & t_2 \end{bmatrix}$$

.

The values of t_1, t_2, t_3, and t_4 are determined numerically by minimizing the following likelihood function:

$$L(t_1, t_2, t_3, t_4) = \sum_{\psi=H,V,D,R} \frac{[N\langle\psi|\rho_{j_\alpha}(t_1, t_2, t_3, t_4)|\psi\rangle - \tilde{n}_\psi]^2}{2N\langle\psi|\rho_{j_\alpha}(t_1, t_2, t_3, t_4)|\psi\rangle} \tag{B6}$$

where $N = \tilde{n}_H + \tilde{n}_V$.

To estimate the error distributions, we use Monte Carlo simulations to numerically generate additional data based on the experimental data and errors in the setup. As discussed in the main text, the intensity and input polarization states are relatively stable and no drifts are observed within the span of the tomography measurement. See Fig. and its caption for details.

We therefore consider two sources of errors: errors in counting statistics and errors in the angles of waveplates. To simulate the errors in n_ψ, we assume the detection counts follow the Poisson distribution. In the simulation,

a random number n_ψ^{sim} is generated from the Poisson distribution with mean given by the experimental value n_ψ as an input to the maximum likelihood algorithm.

Errors in setting waveplates' angles lead to projection to a state other than the one intended. Our electrical polarization controller has a accuracy of $\pm 0.1^\circ$ (0.00175 rad) in waveplate angle settings. To model errors in waveplate angles θ and ϕ, random variables θ^{sim} and ϕ^{sim} are generated from the normal distributions $N(\theta, 0.00175^2)$ and $N(\phi, 0.00175^2)$, respectively, where θ and ϕ are the intended angle settings, and $N((\bar{x}, \sigma^2)$ is the Gaussian distribution with mean x and variance σ^2. The state projected into is given by $|\psi^{sim}\rangle = U^\dagger_{HWP}(\theta^{sim})U^\dagger_{QWP}(\phi^{sim})|H\rangle$, where $|H\rangle$ is the horizontal state given by $|H\rangle = [1, 0]^T$.

In each round of simulation, a set of data, including n_ψ^{sim}, θ^{sim}, and ϕ^{sim} , are numerically generated using the distributions described above, and are used to calculate a density matrix using the maximum likelihood method. For each state $\rho_{j\alpha}$, a total of 1×10^3 sets of data are simulated to give the error distribution of the density matrix constructed.

Appendix C: Experimental results

We preformed the loss tolerant MDI-QKD experiment over 10 km and 40 km of optical fibers. The detailed experimental data is presented below.

1. 10 km loss tolerant MDI-QKD

In this section, we present detailed experimental results not covered in the main text.

In the 10 km demonstration, we send a total of 6×10^{11} pulses. The probabilities of sending ρ_{0_Z}, ρ_{1_Z}, and ρ_{0_X} are $P_{0_Z} = 0.25$, $P_{1_Z} = 0.25$, and $P_{0_X} = 0.5$. The intensities of the signal state is $\mu = 0.2$ photon per pulse, and the intensities of the decoy states are $\nu_1 = 0.03$ and $\nu_2 = 0$ photon per pulse.

Table IV shows $Q^{\Psi^+,I_AI_B}_{j_\alpha s_\beta}$, the conditional probability that Eve gets a successful Bell state measurement with outcome Ψ^+ given that Alice sends out a pulse of intensity I_A in the state ρ_{j_α} and Bob sends out a pulse of intensity I_B in the state ρ_{s_β}.

The upper and lower bounds of the yields of single photon components $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ are estimated given the following constraint [33]:

$$Q^{\Psi^+,I_AI_B}_{j_\alpha s_\beta}(1 - \frac{k}{\sqrt{N^{I_AI_B}_{j_\alpha s_\beta} Q^{\Psi^+,I_AI_B}_{j_\alpha s_\beta}}}) \leq \sum_{m,n=0}^{\infty} e^{-I_A-I_B}\frac{{I_A}^m {I_B}^n}{m!n!} Y^{\Psi^+,mn}_{j_\alpha s_\beta} \leq Q^{\Psi^+,I_AI_B,}_{j_\alpha s_\beta}(1 + \frac{k}{\sqrt{N^{I_AI_B}_{j_\alpha s_\beta} Q^{\Psi^+,I_AI_B}_{j_\alpha s_\beta}}}) \quad \text{(C1)}$$

where $Y^{\Psi^+,mn}_{j_\alpha s_\beta}$ is the conditional probability that Eve gets a BSM outcome Ψ^+ given that Alice sends a pulse of m photons in the state ρ_{j_α} and Bob sends a pulse of n photons in the state ρ_{s_β}, and $N^{I_AI_B}_{j_\alpha s_\beta}$ is the number of pulses where Alice sends the state ρ_{j_α} with intensity I_A and Bob sends the state ρ_{s_β} with intensity I_B, and k is the number of standard deviations, which is chosen to be $k = 3$.

An upper bound and a lower bound of $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ are estimated from the constraint in Eq. (C1) using linear programming, and the results are presented in Table V.

We can now find an upper bound of the phase error rate e^U_X by solving the linear programming problems in (A32) and (A33), where the coefficients of the linear system are given by the Stokes parameters of the actual encoded states ρ_{E,j_α} and ρ_{E',s_β}, $j_\alpha, s_\beta \in \{0_Z, 1_Z, 0_X\}$. We search in the sets of states generated by Monte-Carlo simulation and select the one that maximizes $e^U_X = 18.9\%$, which is 4 standard deviations from the mean.

This high phase error rate is mostly due to the small key size. As a comparison, we also estimate e^U_X assuming we have an infinitely long key. That is, we take $N^{I_AI_B}_{j_\alpha s_\beta} = \infty$ when bounding $Y^{\Psi^+,11}_{j_\alpha s_\beta}$, and the results are shown in Table VI. The tighter bounds of $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ lead to an upper bound $e^U_X = 7.9\%$.

2. 40 km loss tolerant MDI-QKD

We perform a demonstration of loss tolerant MDI-QKD over 40 km of optical fiber. The parameters (intensities and probability distributions of signal and decoy states) used are the same as those used in the 10 km demonstration. Table VII shows the values of the gains $Q^{\Psi^+,I_AI_B}_{j_\alpha s_\beta}$. The upper and lower bounds of the yields of single photon components $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ estimated using the constraints in (C1) are shown in Table VIII. As a proof-of-principle demonstration, we do not consider finite key effect when bounding $Y^{\Psi^+,11}_{j_\alpha s_\beta}$. Using the same algorithm, an upper bound of e_X is found to be 12.2%, and the key rate is $R = 1 \times 10^{-6}$ bit per pulse.

Appendix D: MDI-QKD under the GLLP analysis

In this section we show how the key rate under the GLLP analysis is simulated. For simplicity, we assume that the states prepared by Alice and Bob to be identical in the GLLP simulation. We use the error preparation flaw model in [24]. The four BB84 states with preparation flaws δ are given by

$$\begin{aligned}
|\phi_{0_Z}\rangle &= |0_Z\rangle \\
|\phi_{1_Z}\rangle &= -sin\frac{\delta}{2}|0_Z\rangle + cos\frac{\delta}{2}|1_Z\rangle \\
|\phi_{0_X}\rangle &= cos(\frac{\pi}{4}+\frac{\delta}{4})|0_Z\rangle + sin(\frac{\pi}{4}+\frac{\delta}{4})|1_Z\rangle \\
|\phi_{1_X}\rangle &= cos(-\frac{\pi}{4}+\frac{\delta}{4})|0_Z\rangle + sin(-\frac{\pi}{4}+\frac{\delta}{4})|1_Z\rangle
\end{aligned} \tag{D1}$$

where $|0_Z\rangle$ and $|1_Z\rangle$ are the perfect horizontal and vertical states (i.e., $\langle 0_Z|1_Z\rangle = 0$).

Under the GLLP analysis, the imbalance of the quantum coin Δ_{ini} is defined as

$$\Delta_{ini} = \frac{1}{2}[1 - F(\rho_X^A, \rho_Z^A)F(\rho_X^B, \rho_Z^B)], \tag{D2}$$

where $\rho_X^{A(B)}$ and $\rho_Z^{A(B)}$ are the density matrices of states in the X and Z bases prepared by Alice (Bob). The pessimistic assumption of GLLP assumes that Eve can enhance the imbalance of the quantum coin through the loss of single-photon components. As a result, the upper bound of the imbalance Δ is given by

$$\Delta \leq \frac{\Delta_{ini}}{Y^{\Psi^+,11}} \tag{D3}$$

where $Y^{\Psi^+,11}$ is the yield of single photons. The phase error rate e'_X is related to Δ by [24]

$$\sqrt{e'_X} \leq \sqrt{e_X} + 2\sqrt{\Delta}(\sqrt{(1-\Delta)(1-e_X)} - \sqrt{\Delta e_X}) \tag{D4}$$

where e_X is the bit error rate in the X basis, which can be measured directly from the sifted key. In the presence of basis-dependent flaws ($\Delta_{ini} \neq 0$), Δ increases dramatically as the distance increases, leading to a very poor estimation of the phase error rate e'_X.

TABLE IV. Experimental values of $Q_{j_\alpha s_\beta}^{I_A I_B}$ (conditional probability that Eve gets a successful Bell state measurement with outcome Ψ^+ given that Alice sends ρ_{j_α} with intensity I_A and Bob sends ρ_{s_β} with intensity I_B) in the 10 km MDI-QKD experiment.

State	Intensities $I_A I_B$								
$j_\alpha s_\beta$	$\nu_2\nu_2$	$\nu_2\nu_1$	$\nu_2\mu$	$\nu_1\nu_2$	$\nu_1\nu_1$	$\nu_1\mu$	$\mu\nu_2$	$\mu\nu_1$	$\mu\mu$
$0_Z 0_Z$	$(1.65 \pm 0.74) \times 10^{-9}$	$(8.85 \pm 0.58) \times 10^{-8}$	$(8.04 \pm 0.16) \times 10^{-7}$	$(9.52 \pm 0.43) \times 10^{-8}$	$(1.90 \pm 0.06) \times 10^{-7}$	$(1.01 \pm 0.02) \times 10^{-6}$	$(1.02 \pm 0.02) \times 10^{-6}$	$(1.14 \pm 0.02) \times 10^{-6}$	$(2.03 \pm 0.02) \times 10^{-6}$
$0_Z 1_Z$	$(3.47 \pm 0.93) \times 10^{-9}$	$(8.81 \pm 0.45) \times 10^{-8}$	$(8.01 \pm 0.17) \times 10^{-7}$	$(1.11 \pm 0.04) \times 10^{-7}$	$(3.00 \pm 0.02) \times 10^{-6}$	$(2.05 \pm 0.007) \times 10^{-5}$	$(1.15 \pm 0.02) \times 10^{-6}$	$(1.896 \pm 0.006) \times 10^{-5}$	$(1.227 \pm 0.002) \times 10^{-4}$
$0_Z 0_X$	$(1.51 \pm 0.05) \times 10^{-9}$	$(7.25 \pm 0.09) \times 10^{-7}$	$(2.788 \pm 0.006) \times 10^{-5}$	$(9.82 \pm 0.34) \times 10^{-8}$	$(2.24 \pm 0.01) \times 10^{-6}$	$(3.795 \pm 0.007) \times 10^{-5}$	$(9.62 \pm 0.11) \times 10^{-7}$	$(1.032 \pm 0.003) \times 10^{-5}$	$(8.70 \pm 0.01) \times 10^{-5}$
$1_Z 0_Z$	$(2.46 \pm 0.87) \times 10^{-9}$	$(8.70 \pm 0.37) \times 10^{-8}$	$(8.00 \pm 0.16) \times 10^{-7}$	$(9.57 \pm 0.42) \times 10^{-8}$	$(3.02 \pm 0.02) \times 10^{-6}$	$(1.999 \pm 0.006) \times 10^{-5}$	$(1.34 \pm 0.02) \times 10^{-6}$	$(1.963 \pm 0.008) \times 10^{-5}$	$(1.254 \pm 0.002) \times 10^{-4}$
$1_Z 1_Z$	$(3.39 \pm 0.94) \times 10^{-9}$	$(7.77 \pm 0.43) \times 10^{-8}$	$(7.04 \pm 0.14) \times 10^{-7}$	$(1.08 \pm 0.05) \times 10^{-7}$	$(1.85 \pm 0.06) \times 10^{-7}$	$(1.01 \pm 0.02) \times 10^{-6}$	$(1.42 \pm 0.02) \times 10^{-6}$	$(1.53 \pm 0.02) \times 10^{-6}$	$(2.45 \pm 0.02) \times 10^{-6}$
$1_Z 0_X$	$(3.56 \pm 0.65) \times 10^{-9}$	$(6.81 \pm 0.09) \times 10^{-7}$	$(2.790 \pm 0.007) \times 10^{-5}$	$(1.09 \pm 0.03) \times 10^{-7}$	$(2.00 \pm 0.01) \times 10^{-6}$	$(3.626 \pm 0.006) \times 10^{-5}$	$(1.39 \pm 0.01) \times 10^{-6}$	$(1.02 \pm 0.003) \times 10^{-5}$	$(8.21 \pm 0.01) \times 10^{-5}$
$0_X 0_Z$	$(1.98 \pm 0.50) \times 10^{-9}$	$(8.65 \pm 0.33) \times 10^{-8}$	$(8.38 \pm 0.11) \times 10^{-7}$	$(9.13 \pm 0.11) \times 10^{-7}$	$(2.46 \pm 0.01) \times 10^{-6}$	$(1.181 \pm 0.004) \times 10^{-5}$	$(3.437 \pm 0.007) \times 10^{-5}$	$(4.347 \pm 0.007) \times 10^{-5}$	$(9.85 \pm 0.01) \times 10^{-5}$
$0_X 1_Z$	$(2.01 \pm 0.54) \times 10^{-9}$	$(8.47 \pm 0.31) \times 10^{-8}$	$(7.87 \pm 0.11) \times 10^{-7}$	$(8.94 \pm 0.11) \times 10^{-7}$	$(2.38 \pm 0.01) \times 10^{-6}$	$(1.077 \pm 0.003) \times 10^{-5}$	$(3.440 \pm 0.007) \times 10^{-5}$	$(4.269 \pm 0.007) \times 10^{-5}$	$(9.25 \pm 0.01) \times 10^{-5}$
$0_X 0_X$	$(2.18 \pm 0.39) \times 10^{-9}$	$(7.27 \pm 0.06) \times 10^{-7}$	$(2.807 \pm 0.005) \times 10^{-5}$	$(8.95 \pm 0.07) \times 10^{-7}$	$(4.38 \pm 0.01) \times 10^{-6}$	$(4.701 \pm 0.005) \times 10^{-5}$	$(3.522 \pm 0.005) \times 10^{-5}$	$(5.210 \pm 0.005) \times 10^{-5}$	$(1.751 \pm 0.001) \times 10^{-4}$

TABLE V. Lower bounds ($Y^{\Psi^+,11,L}_{j_\alpha s_\beta}$) and upper bounds ($Y^{\Psi^+,11,U}_{j_\alpha s_\beta}$) of $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ in the 10 km experiment. These bounds are estimated assuming 3 standard deviations of statistical fluctuations for finite key analysis.

$j_\alpha s_\beta$	0_Z0_Z	0_Z1_Z	1_Z0_Z	1_Z1_Z	0_X0_Z	0_X1_Z	0_Z0_X	1_Z0_X	0_X0_X
$Y^{\Psi^+,11,L}_{j_\alpha s_\beta}$	0	2.92×10^{-3}	2.97×10^{-3}	0	1.47×10^{-3}	1.44×10^{-3}	1.42×10^{-3}	1.17×10^{-3}	2.98×10^{-3}
$Y^{\Psi^+,11,U}_{j_\alpha s_\beta}$	5.64×10^{-5}	3.41×10^{-3}	3.47×10^{-3}	6.41×10^{-5}	1.86×10^{-3}	1.78×10^{-3}	1.78×10^{-3}	1.54×10^{-3}	3.41×10^{-3}

TABLE VI. Lower bounds ($Y^{\Psi^+,11,L}_{j_\alpha s_\beta}$) and upper bounds ($Y^{\Psi^+,11,U}_{j_\alpha s_\beta}$) of $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ in the 10 km experiment. These bounds are estimated assuming an infinitely long key.

$j_\alpha s_\beta$	0_Z0_Z	0_Z1_Z	1_Z0_Z	1_Z1_Z	0_X0_Z	0_X1_Z	0_Z0_X	1_Z0_X	0_X0_X
$Y^{\Psi^+,11,L}_{j_\alpha s_\beta}$	4.12×10^{-6}	3.08×10^{-3}	3.14×10^{-3}	2.6×10^{-14}	1.62×10^{-3}	1.59×10^{-3}	1.56×10^{-3}	1.31×10^{-3}	3.13×10^{-3}
$Y^{\Psi^+,11,U}_{j_\alpha s_\beta}$	1.77×10^{-5}	3.31×10^{-3}	3.35×10^{-3}	1.18×10^{-5}	1.76×10^{-3}	1.69×10^{-3}	1.69×10^{-3}	1.45×10^{-3}	3.31×10^{-3}

TABLE VII. Experimental values of $Q^{I_AI_B}_{j\alpha s_\beta}$ (conditional probability that Eve gets a successful Bell state measurement with outcome Ψ^+ given that Alice sends ρ_{j_α} with intensity I_A and Bob sends ρ_{s_β} with intensity I_B) in the 40 km MDI-QKD experiment.

State	Intensities I_AI_B								
$j_\alpha s_\beta$	$\nu_2\nu_2$	$\nu_2\nu_1$	$\nu_2\mu$	$\nu_1\nu_2$	$\nu_1\nu_1$	$\nu_1\mu$	$\mu\nu_2$	$\mu\nu_1$	$\mu\mu$
0_Z0_Z	0	$(5.31\pm0.98)\times10^{-8}$	$(4.90\pm0.31)\times10^{-7}$	$(5.48\pm1.03)\times10^{-8}$	$(1.00\pm0.12)\times10^{-7}$	$(5.97\pm0.43)\times10^{-7}$	$(5.87\pm0.48)\times10^{-7}$	$(6.57\pm0.35)\times10^{-7}$	$(1.28\pm0.07)\times10^{-6}$
0_Z1_Z	$(2.65\pm2.65)\times10^{-9}$	$(3.98\pm1.03)\times10^{-8}$	$(5.60\pm0.39)\times10^{-7}$	$(5.73\pm1.15)\times10^{-8}$	$(1.47\pm0.04)\times10^{-6}$	$(9.55\pm0.15)\times10^{-6}$	$(7.06\pm0.43)\times10^{-7}$	$(8.77\pm0.16)\times10^{-6}$	$(5.63\pm0.04)\times10^{-5}$
0_Z0_X	$(1.51\pm1.51)\times10^{-9}$	$(2.93\pm0.16)\times10^{-7}$	$(1.22\pm0.01)\times10^{-5}$	$(5.59\pm0.72)\times10^{-8}$	$(1.02\pm0.03)\times10^{-6}$	$(1.64\pm0.01)\times10^{-5}$	$(5.32\pm0.27)\times10^{-7}$	$(4.76\pm0.07)\times10^{-6}$	$(4.02\pm0.02)\times10^{-5}$
1_Z0_Z	$(5.11\pm3.61)\times10^{-9}$	$(3.91\pm0.95)\times10^{-8}$	$(5.89\pm0.38)\times10^{-7}$	$(5.72\pm1.01)\times10^{-8}$	$(1.28\pm0.05)\times10^{-6}$	$(8.88\pm0.13)\times10^{-6}$	$(1.20\pm0.05)\times10^{-6}$	$(9.28\pm0.14)\times10^{-6}$	$(5.71\pm0.04)\times10^{-5}$
1_Z1_Z	0	$(4.13\pm1.03)\times10^{-8}$	$(4.55\pm0.37)\times10^{-7}$	$(8.92\pm1.41)\times10^{-8}$	$(1.42\pm0.15)\times10^{-7}$	$(8.08\pm0.51)\times10^{-7}$	$(1.15\pm0.05)\times10^{-6}$	$(1.39\pm0.05)\times10^{-6}$	$(3.05\pm0.09)\times10^{-6}$
1_Z0_X	0	$(2.94\pm0.17)\times10^{-7}$	$(1.27\pm0.01)\times10^{-5}$	$(8.32\pm0.91)\times10^{-8}$	$(9.02\pm0.28)\times10^{-7}$	$(1.56\pm0.01)\times10^{-5}$	$(1.29\pm0.04)\times10^{-6}$	$(4.81\pm0.07)\times10^{-6}$	$(3.40\pm0.02)\times10^{-5}$
0_X0_Z	$(4.81\pm2.40)\times10^{-9}$	$(6.07\pm0.75)\times10^{-8}$	$(5.67\pm0.26)\times10^{-7}$	$(4.77\pm0.24)\times10^{-7}$	$(1.19\pm0.03)\times10^{-6}$	$(5.60\pm0.08)\times10^{-6}$	$(1.63\pm0.01)\times10^{-5}$	$(2.06\pm0.02)\times10^{-5}$	$(4.68\pm0.03)\times10^{-5}$
0_X1_Z	$(1.51\pm1.51)\times10^{-9}$	$(5.54\pm0.78)\times10^{-8}$	$(5.30\pm0.27)\times10^{-7}$	$(4.35\pm0.21)\times10^{-7}$	$(1.15\pm0.03)\times10^{-6}$	$(5.05\pm0.07)\times10^{-6}$	$(1.63\pm0.02)\times10^{-5}$	$(1.98\pm0.01)\times10^{-5}$	$(41.3\pm0.02)\times10^{-5}$
0_X0_X	$(2.19\pm1.26)\times10^{-9}$	$(3.12\pm0.14)\times10^{-7}$	$(1.21\pm0.01)\times10^{-5}$	$(4.15\pm0.15)\times10^{-7}$	$(1.99\pm0.03)\times10^{-6}$	$(2.06\pm0.01)\times10^{-5}$	$(1.60\pm0.01)\times10^{-5}$	$(2.45\pm0.01)\times10^{-5}$	$(8.04\pm0.02)\times10^{-5}$

TABLE VIII. Lower bounds ($Y^{\Psi^+,11,L}_{j_\alpha s_\beta}$) and upper bounds ($Y^{\Psi^+,11,U}_{j_\alpha s_\beta}$) of $Y^{\Psi^+,11}_{j_\alpha s_\beta}$ in the 40 km experiment. These bounds are estimated assuming an infinitely long key.

$j_\alpha s_\beta$	0_Z0_Z	0_Z1_Z	1_Z0_Z	1_Z1_Z	0_X0_Z	0_X1_Z	0_Z0_X	1_Z0_X	0_X0_X
$Y^{\Psi^+,11,L}_{j_\alpha s_\beta}$	0	1.54×10^{-3}	1.27×10^{-3}	0	6.92×10^{-4}	7.47×10^{-4}	7.46×10^{-4}	5.86×10^{-4}	1.39×10^{-3}
$Y^{\Psi^+,11,U}_{j_\alpha s_\beta}$	2.36×10^{-6}	1.64×10^{-3}	1.42×10^{-3}	2.77×10^{-5}	8.07×10^{-4}	8.08×10^{-4}	8.15×10^{-4}	6.44×10^{-4}	1.53×10^{-3}

[1] C. H. Bennett and G. Brassard, in *IEEE Internatoional Conference on Computers, Systems, and Signal Processing* (Banglore, India, 1984) pp. 175–179; A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); D. Mayers, J. ACM **48**, 351 (2001); E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptol. **19**, 381 (2006).

[3] Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008); L. Lydersen *et al.*, Nature Photon. **4**, 686 (2010); I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011); N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011); H. Weier *et al.*, New J. Phys. **13**, 073024 (2011); F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010); L. Lydersen, N. Jain, C. Wittmann, O. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. A **84**, 032320 (2011); C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011); A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Phys. Rev. Lett. **112**, 070503 (2014); S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Phys. Rev. A **92**, 022304 (2015); Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[4] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (Washington, DC, 1998) p. 503; A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007); N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010); U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[5] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, *et al.*, Nature **526**, 682 (2015); M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Phys. Rev. Lett. **115**, 250401 (2015); L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Phys. Rev. Lett. **115**, 250402 (2015).

[6] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304 (2011).

[7] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996); H. Inamori, Algorithmica **34**, 340 (2002).

[8] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[9] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[10] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).

[11] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[12] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013); Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).

[13] 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, Phys. Rev. Lett. **113**, 190501 (2014).

[14] 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, IEEE J. Sel. T. Quantum Electron **21**, 6600407 (2015).

[15] 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, ArXiv e-prints (2015), arXiv:1509.08389 [quant-ph].

[16] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, ArXiv e-prints (2015), arXiv:1509.08137 [quant-ph].

[17] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photon. (2015); Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014); X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Phys. Rev. A **89**, 042335 (2014); F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, *ibid.* **9**, 772 (2015); S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *ibid.* **9**, 773 (2015).

[18] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013); P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).

[19] L. Zhao, Z. Yin, S. Wang, W. Chen, H. Chen, G. Guo, and Z. Han, Phys. Rev. A **92**, 062327 (2015).

[20] Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **88**, 062322 (2013); Phys. Rev. A **90**, 052319 (2014); F. Xu, Phys. Rev. A **92**, 012333 (2015).

[21] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).

[22] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005); Y. Zhao *et al.*, Phys. Rev. Lett. **96**, 070502 (2006); D. Rosenberg *et al.*, Phys. Rev. Lett. **98**, 010503 (2007); C.-Z. Peng *et al.*, Phys. Rev. Lett. **98**, 010505 (2007).

[23] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys.

Rev. A **85**, 042307 (2012).
[24] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[25] Bounded dimensionality of the encoding space is also assumed in the semi-device-independent QKD [35]. However loss-tolerant MDI-QKD gives a much higher key rate than semi-device-independent QKD and is thus more practical.
[26] F. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, arXiv:1504.08151 (2015).
[27] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, arXiv:1408.3667 (2014).
[28] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).
[29] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys. **17**, 053014 (2015).
[30] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, New J. Phys. **11**, 095001 (2009).
[31] N. Peters, J. Altepeter, E. Jeffrey, D. Branning, and P. Kwiat, Quant. Inf. Comput. **3**, 503 (2003).
[32] R. Valivarthi *et al.*, J. Mod. Opt. **62**, 1141 (2015).
[33] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[34] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[35] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).