High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics

Kejin Wei,[1,2,3,4,*] Wei Li,[1,2,3,*] Hao Tan,[1,2,3] Yang Li,[1,2,3] Hao Min,[1,2,3] Wei-Jun Zhang,[5] Hao Li,[5] Lixing You,[5] Zhen Wang,[5] Xiao Jiang,[1,2,3] Teng-Yun Chen,[1,2,3] Sheng-Kai Liao,[1,2,3] Cheng-Zhi Peng,[1,2,3,6] Feihu Xu,[1,2,3,†] and Jian-Wei Pan[1,2,3,‡]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China*
[2]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*
[3]*Shanghai Research Center for Quantum Sciences, Shanghai 201315, China*
[4]*Guangxi Key Laboratory for Relativistic Astrophysics, School of Physics Science and Technology, Guangxi University, Nanning 530004, China*
[5]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*
[6]*QuantumCTek Co., Ltd., Hefei, Anhui 230088, China*

(Received 19 February 2020; revised 29 April 2020; accepted 3 June 2020; published 10 August 2020)

Measurement-device-independent quantum key distribution (MDI QKD) removes all detector side channels and enables secure QKD with an untrusted relay. It is suitable for building a star-type quantum access network, where the complicated and expensive measurement devices are placed in the central untrusted relay and each user requires only a low-cost transmitter, such as an integrated photonic chip. Here, we experimentally demonstrate a 1.25-GHz silicon photonic chip-based MDI QKD system using polarization encoding. The photonic chip transmitters integrate the necessary encoding components for a standard QKD source. We implement random modulations of polarization states and decoy intensities, and demonstrate a finite-key secret rate of 31 bit/s over 36-dB channel loss (or 180-km standard fiber). This key rate is higher than state-of-the-art MDI QKD experiments. The results show that silicon photonic chip-based MDI QKD, benefiting from miniaturization, low-cost manufacture, and compatibility with CMOS microelectronics, is a promising solution for future quantum secure networks.

DOI: 10.1103/PhysRevX.10.031030 Subject Areas: Quantum Information

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is a key technology for building nodal networks which are believed to be a crucial stepping stone toward a quantum Internet. So far, existing QKD networks [3–7] need the central relays to be trusted [e.g., Fig. 1(a)], which is a critical security drawback [1,2]. Fortunately, the measurement-device-independent (MDI) QKD protocol [8] (see also Ref. [9]) can remove all side channels of the measurement devices [10], and it is practical with current technology. MDI QKD has been widely implemented toward long distance [11,12], high secret key rate [13], field test [14,15], asymmetric channels [16,17], and so forth [18–20]. Recently, an efficient MDI scheme, twin-field QKD [21], was proposed to overcome the repeaterless key-rate bound.

Chip-based QKD has attracted great attention [22–30], due to its advantages of compact size and low cost. Particularly, silicon that relies on well-established fabrication techniques is well suited for on-chip photonic QKD components, and it has been exploited to implement several QKD protocols, including decoy-state BB84 [23–26], high dimension [27], continuous variable [28,29], and so forth [22,30].

The combination of silicon photonic chips and MDI QKD enables a remarkably new network-centric [7] or quantum-access [6] structure with an *untrusted* relay. As illustrated in Fig. 1(b), in the chip-based MDI QKD network, each user only needs a compact transmitter chip, whereas the relay holds the expensive and bulky measurement system (and quantum memory [31]) which are shared by all users. Importantly, this structure can bypass the challenging technique for intergrading single-photon

*These authors contributed equally to this work.
†feihuxu@ustc.edu.cn
‡pan@ustc.edu.cn

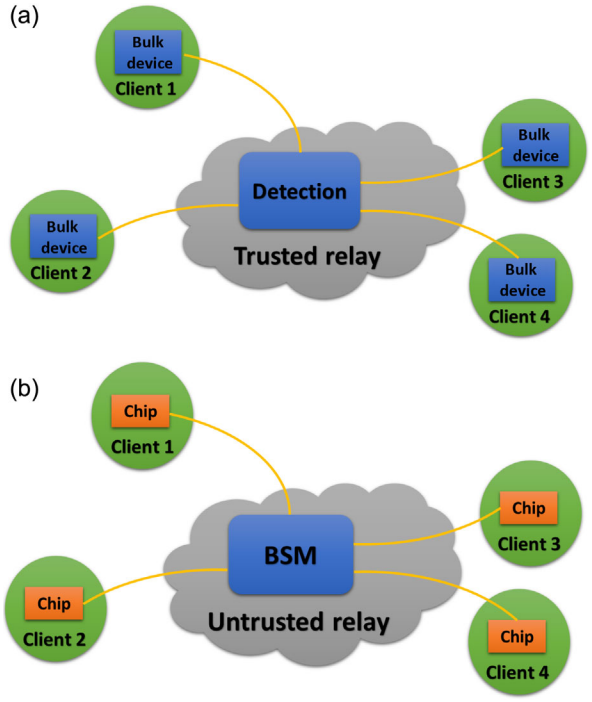

FIG. 1. (a) Schematic of a conventional quantum access network based on BB84 [6]. The central relay needs to be trustful, where the measurement devices are vulnerable to quantum attacks. (b) Schematic of the proposed star-type chip-based MDI QKD network. Each client holds only a compact, low-cost transmitter chip, and the central relay performs the Bell-state measurement (BSM). MDI QKD enables secure QKD with an untrusted relay.

detectors on chip [32,33], since the users do not need to do the quantum detection. Overall, the chip-based MDI QKD network enables a promising solution for low-cost, scalable QKD networks with an untrusted relay.

Here, we experimentally demonstrate a 1.25-GHz, silicon-chip-based, polarization-encoding MDI QKD system. Each user possesses a photonic chip transmitter, which integrates the QKD encoding components of intensity modulator, polarization modulator, and variable optical attenuator. The chips are manufactured by standard Si photonic platforms, packaged with thermoelectric cooler (TEC), and designed compactly for the purpose of commercial production. With two chip transmitters, we implement MDI QKD with random modulations of decoy intensities and polarization qubits, and demonstrate a finite-key secret rate of 31 bit/s over 36-dB channel loss. In addition, we obtain a key rate of 497 bit/s over 140-km commercial fiber spools. The achieved key rate is higher than those of previous MDI QKD experiments [11–15,18,19] (see Table I).

TABLE I. Comparison of state-of-the-art MDI QKD experiments.

Reference	Clock rate (MHz)	Channel loss (dB)	Key rate (bit/s)	Finite key
Tang *et al.* [18]	10	2.0	25	10^{-3}
Tang *et al.* [11]	75	9.9	67	10^{-9}
Valivarthi *et al.* [19]	20	16.0	100	Asymptotic
Yin *et al.* [12]	75	19.5	1380	10^{-10}
Comandar *et al.* [13]	1000	20.4	4567[a]	10^{-10}
This work	1250	20.4	6172[b]	10^{-10}
		28.0	268	10^{-10}
		36.0	31	10^{-10}

[a]No random modulations.
[b]Simulated experiment.

II. SETUP

Figure 2(a) shows the schematic of our chip-based MDI QKD experiment. Using pulsed laser-seeding technology [34] where a master gain-switched laser (Master) injects photons into the cavity of a slave gain-switched laser (Slave) through a circulator (Circ), Alice and Bob each generate low-jitter phase-randomized light pulses at a repetition rate of 1.25 GHz and a center wavelength of 1550 nm. The generated pulses are passed through a 10-GHz bandwidth filter to remove noise. With these sources, we observe stable Hong-Ou-Mandel interference with a visibility up to 48.4% (see Appendix C 1), which ensures the required indistinguishability of independent laser sources for MDI QKD.

The generated pulses are coupled into a Si photonic transmitter chip which integrates together an intensity modulator, a polarization modulator, and a variable optical attenuator. The components are realized by an in-house design (via Quantum CTek), and they consist of several interferometric structures [see Fig. 2(b)] which exploit standard building blocks offered by the IMEC foundry. The multimode interference (MMI) couplers act as symmetric beam splitters, and the thermo-optics modulators (TOMs) with approximate kilohertz bandwidth, and carrier-depletion modulators (CDMs) with approximate gigahertz bandwidth act as phase modulators. Specifically, the intensity modulator, which is used to generate decoy state with different intensities, is realized by the first Mach-Zehnder interferometer (MZI) containing both TOMs and CDMs. The next component is the variable optical attenuator (VOA), consisting of a *p-i-n* (PIN) diode for current injection across-section of the Si waveguide and being used to attenuate the pulses to single-photon levels. The tunable attenuation is controlled by applying differential biased voltage to the TOMs with an attenuation up to 110 dB. The output of VOA is connected to the polarization modulator (POL) which is realized by combining an inner MZI with two external CDMs ending in the polarization rotator combiner (PRC). The PRC is fabricated by using a two-dimensional grating structure [25,30]. The POL can prepare the four BB84 states, $|\psi\rangle = (|H\rangle + e^{i\theta}|V\rangle)/\sqrt{2}, \theta \in \{0, \pi/2, \pi, 3\pi/2\}$, where $\theta \in \{0, \pi\}$ $(\theta \in \{\pi/2, 3\pi/2\})$ represents the state in Z (X) basis in MDI QKD implementation.

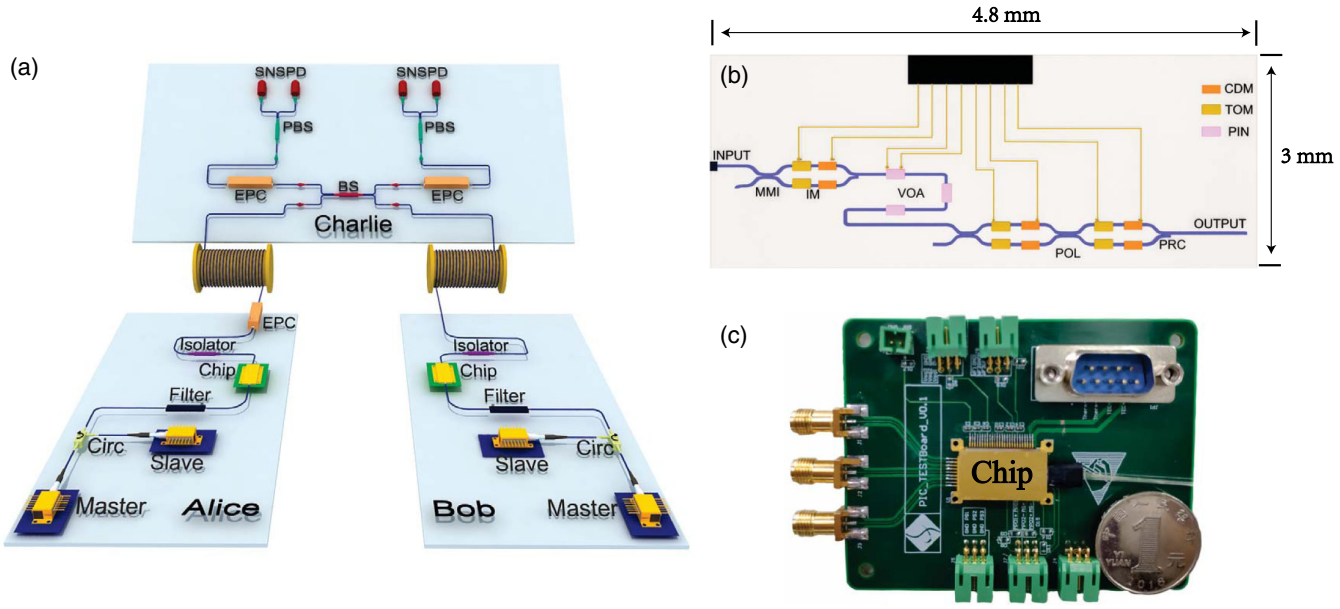

FIG. 2. (a) Experimental setup of chip-based MDI QKD. Alice and Bob each possess a master gain-switched laser (master) which injects photons into the cavity of a slave gain-switched laser (slave) through a circulator (circ) to generate low-jitter phase-randomized light pulses at a repetition rate of 1.25 GHz. The generated pulses are coupled into a silicon photonic transmitter chip (chip) which integrates together an intensity modulator, variable optical attenuator, and polarization modulator. The Bell-state measurements are performed by the untrusted relay Charlie who comprises a beam splitter (BS), two electric polarizing controllers (EPCs), two polarizing beam splitters (PBSs) and four superconducting nanowire single-photon detectors (SNSPDs). (b) The schematic of the Si chip. All components are fabricated using standard Si blocks, including multimode interference (MMI) couplers, thermo-optics modulators (TOMs), carrier-depletion modulators (CDMs), and polarization rotator combiner (PRC). (c) Image of the packaged chip soldered to a compact control board.

The chip has a footprint size of 4.8×3 mm^2 and is packaged with a commercial TEC. A precision and compact temperature controller is designed to drive the TEC. With this design, the chip provides a stable polarization encoding and decoy-state modulation. The observed quantum bit error rate (QBER) maintains at low values over several hours of operation (see Fig. 3). The packaged chip with a total volume of $20 \times 11 \times 5$ mm^3 is soldered to a standard 9×7 cm^2 printed circuit board, as shown in Fig. 2(c). With dedicated layout, the chip is easily assembled by using commercial foundry, providing a low-cost, portable, stable, and miniaturized device for MDI QKD.

To realize MDI QKD, Alice and Bob send their encoding pulses to Charlie, who performs a BSM on the incoming pulses. Charlie's measurement setup comprises a 50/50 beam splitter (BS), two electronics polarization controllers (EPCs), two polarizing beam splitters, and four superconducting nanowire single photon detectors (SNSPDs) with detection efficiency 53% and dark counts 50 Hz. The detection events are registered using a high-speed time tagger where a successful coincidence induces a projection into one of the two Bell states $|\psi^{\pm}\rangle = 1/\sqrt{2}(|HV\rangle \pm |HV\rangle)$.

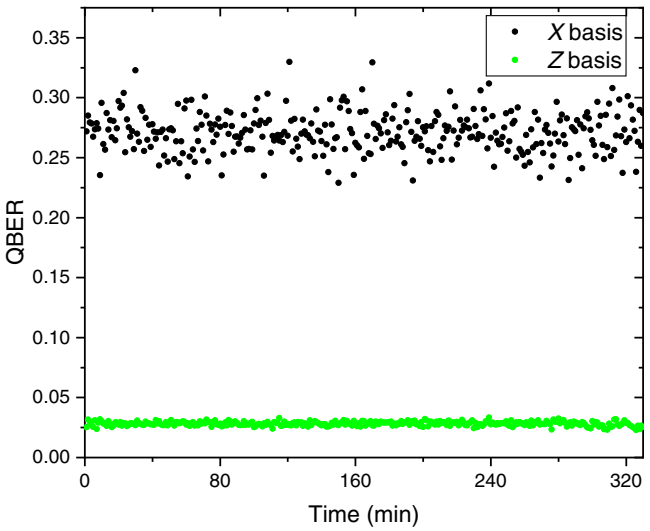

FIG. 3. Observed QBERs in different bases over 36-dB channel loss. The data points are collected without any active adjustment of the system. Each point is calculated by using data collected over a one-minute period. An average QBER of 0.028 ± 0.002 (0.271 ± 0.016) in Z (X) basis is observed over several hours of operation.

For high-rate MDI QKD, an important part is the high-speed electronics for control and synchronization. In our experiment, Alice and Bob each use a homemade cost-effective field-programmable gate array (FPGA) board (see Appendix C 3) to accomplish the electrical controls, including the laser driving, random modulation of intensity modulators (IMs) and polarization modulators (POLs), synchronization of different devices, etc. The specialized electronics enable us to take advantage of the small size of the chips toward a compact MDI QKD system. Each FPGA board is synchronized with Charlie through an electrical cable in our laboratory experiment. For a field implementation, the synchronization could be realized using optical signals through fibers, as demonstrated in Ref. [11]. To share a common polarization reference between Alice and Bob, as well as compensate the polarization drift in the quantum channel, we develop an automatic polarization alignment with electronic polarization controllers, which can rapidly calibrate the polarization reference within half a minute. Further experimental details can be found in Appendix C.

III. RESULTS

We experimentally characterize each of the components in the chip. The bandwidth of the CDM reaches about 21 GHz which is measured by using a vector network analyzer. The IM provides a static extinction ratio (ER) of about 30 dB and a dynamic ER of about 20 dB. We characterize the produced polarization state with measurement devices in Charlie. The EPCs are adjusted so that each PBS is aligned to rectilinear and diagonal bases, respectively. We obtain an average polarization ER of about 23 dB. The attenuation of the VOA ranges from 0 to about 110 dB. The performance of the chip is sufficient for a low-error, high-rate MDI QKD. Figure 3 shows the observed QBER. We obtain an average QBER of $2.8\% \pm 0.2\%$ ($27.1\% \pm 1.6\%$) in Z (X) basis over several hours of stable operations. Note that the theory value of the QBER in X basis for two weak coherent pulses is 25%; our experimental value remains close to the theory.

Using the described setup, we perform a series of MDI QKD experiments using the four-intensity decoy-state protocol [35]. Finite-key effects are carefully addressed using the standard error analysis approach [36]. In the finite-key scenario [37] with a failure probability of 10^{-10}, we perform a full optimization of the implementation parameters by exploiting the joint constrains for statistical fluctuations [35] (see Appendix A). The experimental results are plotted in Fig. 4. The data points are first collected by using optical attenuators to emulate the attenuation of standard single-mode fibers (0.2 dB/km). At the total loss of 28 dB (corresponding to 140 km fiber), we run the system for 7.7 h and send a total of 3×10^{13} pulse pairs from each client. The finite-key secret rate is 268 bit/s. At the total loss of 36 dB (corresponding to 180 km fiber), to maximize the key rate, we slightly enhance the bias current of SNSPDs, resulting in a higher detection efficiency (62%) but a lower maximum counting rate. We achieve a finite-key secret rate of 31 bit/s in 10 h of system operation time. Next, we replace the optical attenuators with two commercial fiber spools of 70 km each (corresponding to about 27 dB total loss), and obtain an asymptotic secret key rate of 497 bit/s which is close to the finite-key one obtained from the optical attenuators. Appendix B shows the detailed experiment values.

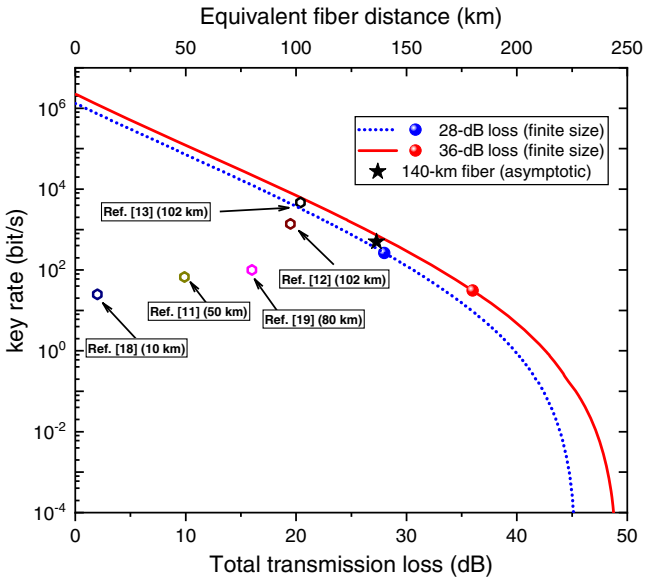

FIG. 4. Secure key rates with different transmission loss. The blue and red points show the experimental results with a total transmission loss of 28 and 36 dB, respectively. The black star is the asymptotic key rate obtained using two 70-km commercial fiber spools. The red solid lines and the blue dot lines are theoretical simulations tailored to the corresponding experimental conditions. We also plot the highest finite key rates of current MDI QKD experiments with polarization encoding (navy diamond [18] and black diamond [13]) and time-bin encoding (dark yellow diamond [11], magenta diamond [19], and brown diamond [12]).

To illustrate the progress entailed by our results, we include in Fig. 4 the highest key rate of selection of existing MDI QKD experiments. See Table I for a detail comparison. In the table, our rate at 20.4 dB was emulated using the measured experimental parameters; this is due to the limited count rates of our SNSPDs which can be easily resolved using the commercial high-count-rate ones (e.g., Single Quantum and Quantum Opus). Although a gigahertz MDI QKD was reported in Ref. [13] with avalanche photodiodes, random modulations of decoy intensities and polarization states were not implemented there. In this sense, apart from the

chip-based implementation, our experiment is the first gigahertz MDI QKD with random modulations. Moreover, our experiment represents the highest reported key rate for MDI QKD.

Similar to standard QKD experiments, our chip-based source presents small device imperfections. First, the intensity fluctuations are less than 0.9%, which indicates the good stability of the chip-based intensity modulator. Second, the polarization dependent loss is smaller than 0.8 dB, which has a negligible effect to the key rate [38]. Third, the phase-modulation errors are less than 0.18 for a π-phase modulation [39]. Fourth, for our high-speed modulation, the pattern effect for the intensity deviations of adjacent pulses is less than 12%. The security issue of pattern effect, together with the countermeasures, has been proposed in Ref. [40]. Note that in the future, these source imperfections can be included in the key-rate calculation by following the recent security proofs [41,42].

IV. DISCUSSIONS

We have demonstrated a high-speed chip-based MDI QKD system where both clients possess a low-cost Si photonic transmitter chip. The transmitter can be further integrated with the laser based on wire bounding or the substrate of indium phosphide or hybrid integration [43,44]. This can construct a compact chip-scale QKD transmitter. We perform a complete demonstration of polarization-encoding MDI QKD and distill finite-key secret rates higher than previous experiment. This work paves the way for a low-cost, wafer-scale manufactured MDI QKD system, and represents a key step toward building quantum networks with untrusted relays.

ACKNOWLEDGMENTS

We thank Jianhong Liu, Pan Gong, Yan-Lin Tang, Wenyuan Wang for enlightening discussions. This work was supported by the National Key Research and Development (R&D) Plan of China (under Grants No. 2018YFB0504300 and No. 2017YFA0304000), the National Natural Science Foundation of China (under Grants No. 61771443 and No. 61705048), the Anhui Initiative in Quantum Information Technologies, the Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), the Chinese Academy of Sciences, the Shanghai Science and Technology Development Funds (No. 18JC1414700) and the Fundamental Research Funds for the Central Universities (No. WK2340000083).

Note added.—Recently, we become aware of a related work in Ref. [45]. Our work uses polarization encoding and low-cost Si substrate at a clock rate of 1.25 GHz, with a careful finite-key consideration and an implementation of random modulations of decoy states and polarization qubits. Reference [45] uses time-bin encoding and InP substrate at a clock rate of 0.25 GHz, without the implementation of random modulations and the finite-key consideration, but it integrates the lasers on chip.

APPENDIX A: FOUR-INTENSITY MDI QKD

In experiment, the EPCs are carefully aligned for state preparation and detection in the $Z = \{|0\rangle, |1\rangle\}$ basis and $X = \{|+\rangle, |-\rangle\}$ basis. Here, $|0\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, $|1\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$, $|+\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, and $|-\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$. Our experiment adopts the four-intensity decoy-state protocol [35]. There are three intensities $\{\mu, \nu, \omega\}$ in the X basis for the decoy-state analysis and one signal intensity $\{s\}$ in the Z basis for secret key generation. We consider the symmetric channel loss where Alice and Bob used the same parameters. One can refer to Refs. [16,17] for the case of asymmetric channel loss. Including the probabilities P for each intensity, both Alice and Bob use the same group of six parameters $[s, \mu, \nu, P_s, P_\mu, P_\nu]$. We perform a full optimization of parameters [36]. For statistical fluctuations, we use the *joint constrains* where the same observables are combined and treated together, as proposed in Ref. [35]. This can produce a higher key rate than independent constrains. Finally, the secret key is extracted using the formula,

$$R = P_s^2\{s^2 e^{-2s} Y_{11}^{X,L}[1 - h(e_{11}^{X,U})] - f_e Q_{ss}^Z h(E_{ss}^Z)\}, \quad \text{(A1)}$$

where Q_{ss}^Z and E_{ss}^Z are the gain and the QBER in the Z (signal) basis, P_s is the probability of signal state, $Y_{11}^{X,L}$ and $e_{11}^{X,U}$ are the lower bound of single-photon yield and the upper bound of single-photon QBER estimated by the decoy state statistics in the X basis, h is the binary entropy function, and f_e is the error-correction efficiency which is set to 1.16.

APPENDIX B: DETAILED EXPERIMENTAL RESULTS

The detailed experimental results are listed in Table II.

APPENDIX C: EXPERIMENTAL DETAILS

1. Source

Each of Alice and Bob consists of two nearly identical gain-switched lasers, of which the wavelengths are stabilized using homemade tunable temperature controllers. The lasers are distributed feedback diodes, which have wavelength sensitivity over temperature 90 pm/K. The resolution of the temperature controller is 1 mK. The central wavelength of the master laser is set at 1549.68 nm, and the

TABLE II. Total gains and error gains of Bell state $|\psi^{\pm}\rangle$. The notation Q_{ij} and E_{ij} denotes the total gains and error gains from Alice's source i and Bob's source j, respectively.

Attenuation (dB)	28.0	36.0
Distance (km)	140	180
N	3.0×10^{13}	4.5×10^{13}
P_s	0.607	0.488
P_μ	0.030	0.038
P_ν	0.267	0.350
P_ω	0.096	0.124
s	0.207	0.141
μ	0.197	0.188
ν	0.035	0.036
ω	0	0
Q_{ss}	67 610 084	6 305 857
$Q_{\mu\mu}$	258 557	115 035
$Q_{\nu\nu}$	606 196	388 040
$Q_{\mu 0}$	49 091	138 680
$Q_{0\mu}$	102 736	87 576
$Q_{\nu 0}$	69 561	26 574
$Q_{0\nu}$	47 406	44 947
Q_{00}	6	0
E_{ss}	1 851 744	178 909
$E_{\nu\nu}$	160 177	104 895
$E_{\nu 0}$	34 705	13 227
$E_{0\nu}$	23 637	22 647
E_{00}	4	0
s_{11}	8.98×10^{-5}	2.43×10^{-5}
e_{11}	0.068	0.089
Key rate per pulse	1.29×10^{-7}	2.47×10^{-8}

wavelength of the slave laser is slowly tuned by adjusting its temperature. To ensure the two independent laser pulses have the same spectral property, we employ an optical spectrum analyzer to acquire the central wavelength of Alice's and Bob's laser pulses, and then match them by elaborately adjusting one of the user's temperatures and driving currents. During the experiment, the relative wavelength is actively stabilized by using a highly accurate proportional-integral-derivative temperature circuit that has a temperature stability of 3 mk. With these procedures, the wavelength of Alice's and Bob's slave laser is well matched and the relative wavelength difference is stable over several hours, as shown in Fig. 5.

The master laser and the slave laser are individually driven by 500-ps and 200-ps square-wave pulses. With the laser-seeding technology, each user generates low-jitter laser pulses at a repetition rate of 1.25 GHz. An electrical delay in steps of 1 ps allows a perfect temporal overlap of two lasers. The seeding photons are injected into the cavity of the slave laser via a circulator. With the seeding photons, the slave lasers generate low-jitter phase-randomized light pulses with a pulse width of about 100 ps. The generated

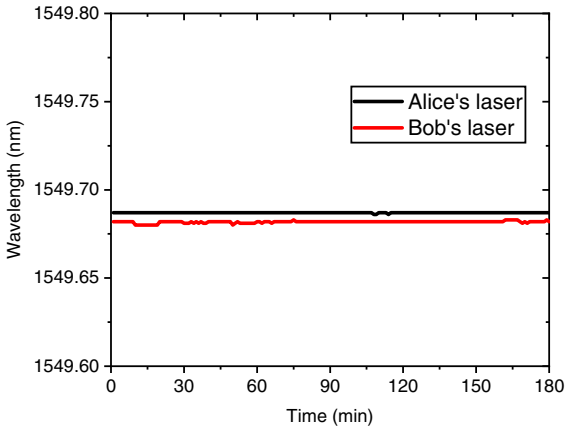

FIG. 5. Observed wavelength of laser pulses at each user over time.

pulses pass through a filter with a bandwidth of 10 GHz to reduce frequency chirp. To test the visibility of the setup, we perform a two-photon interference experiment. The photon count rate is attenuated to ~3.5 MHz per detector. Data are collected for 100 s with a coincidence time window of 600 ps. As shown in Fig. 6(a), we obtain a visibility of 48.4%.

In our implementation, we find that the main factors limiting the interference visibility are the laser frequency chirp and the time jitter. In particular, frequency chirp plays a more important role [34]. In our experiment, two single gain-switched lasers may not produce a good interference visibility. However, by using two delicately tuned spectral filters (with about 10-GHz bandwidth), we find that the obtained visibility in Fig. 6(b) is comparable to that achieved by the master-slave configuration. Notice that the spectral filters are mature techniques from chip integration. This suggests that our transmitters could further be reduced and be further integrated using hybrid integration technology [43,44].

2. Si transmitter chip

The generated pulses are coupled into a Si photonic transmitter chip which integrates together an intensity

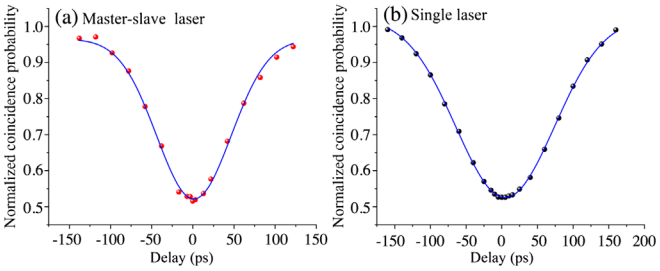

FIG. 6. Hong-Ou-Mandel interference between two gain-switch lasers using different laser sources. (a) A dip with visibility 48.4% is obtained with master-slave laser using laser-seeding technology. (b) The achieved visibility is 47.4% with single laser source together with spectral filtering.

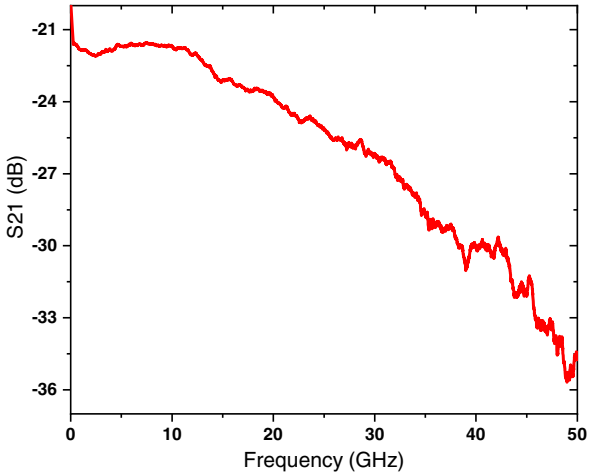

FIG. 7. S21 curve of CDM. A 3-dB bandwidth of about 21 GHz is achieved.

modulator, and polarization modulator, and variable optical attenuator.

A CDM, acting as a phase modulator, is a key component in our chip. The bandwidth of the CDM must be subtly estimated since it has a crucial role on the performance of IMs and POLs. We measure the bandwidth of the CDM by using a vector network analyzer. As shown in Fig. 7, we achieve a 3-dB bandwidth of about 21 GHz.

The IM is realized by the first Mach-Zehnder interferometer (MZI). While the microring's structure features a lower peak voltage and a smaller footprint [23], it requires a very careful temperature control. In contrast, the MZI structure has better temperate stability than microrings. By applying multilevel radio frequency (rf) signal to the CDMs, the intensities are randomly modulated according to four different intensity choices. In experimental characterization, a static extinction ratio (ER) of 29.7 ± 0.1 dB is achieved with an applied dc voltage of 0.97 V. In the dynamic ER test, we first trigger the IMs with 625-MHz rf signals and get an ER of 21.5 ± 0.1 dB. Then, we enhance the repetition rate of rf signals to 1.25 GHz, and an ER of 19.8 ± 0.1 dB is obtained. The decline of the ERs with rising repetition rate is caused by electronic jitter. To further test its performance, we randomly drive the IM with four different rf voltages at a repetition rate of 1.25 GHz, which are generated by our homemade FPGA control board (see Fig. 11). As shown in Fig. 8, the four voltage levels produce four intensities which can be used for signal state (s) and three decoy states (μ, ν, ω). We also quantify the fluctuations of each intensity. The largest fluctuation of 0.9% is observed in ν states. This low fluctuation indicates the good stability of the chip-based IM.

The next component is the variable optical attenuator, consisting of a PIN diode for current injection cross-section of the waveguide and being used to attenuate the pulses to single-photon levels. In our chip, we have three cascade-connected VOAs and each VOA provides an about 38-dB

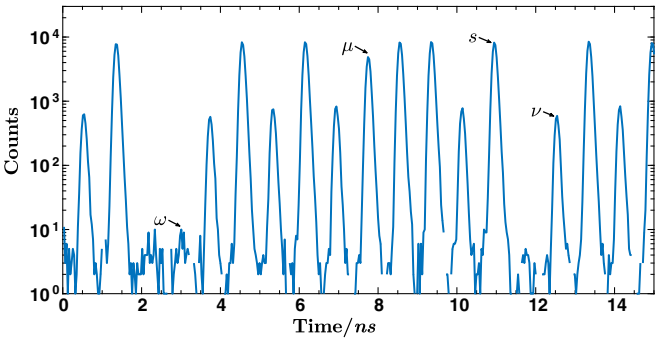

FIG. 8. Histogram measurement of different intensities using the chip. Four varying intensities can be used for signal (s) and three decoy states (μ, ν, ω).

dynamic range. Figure 9 shows the tuning ranges of one of the VOAs, which could provide 38.0 dB of attenuation. By applying differential dc-biased voltage to the PIN, the max attenuation is up to about 110 dB. The applied attenuation has a good accuracy. For example, at a driver voltage of 1.5 V, the obtained attenuation is 9.50 ± 0.01 dB. The stability of the attenuation is ensured by an accurate temperature feedback control of the chip.

The output of VOA is connected to the POL which is realized by combining two MZI structures. The amplitude ratio between the two arms of the second MZI is controlled by dc-voltage biasing the TOMs in the first MZI. The second MZI ends with a polarization rotator combiner (PRC) (it is achieved by using a two-dimensional grating structure [25,30]), which converts the transverse-electric polarized light in one of its inputs into the transverse-magnetic polarized light, which is recombined with the light from the other input at the output. The relative phases of the two inputs of the PRC are modulated by the CDMs in the second MZI. Therefore, we obtain the four states

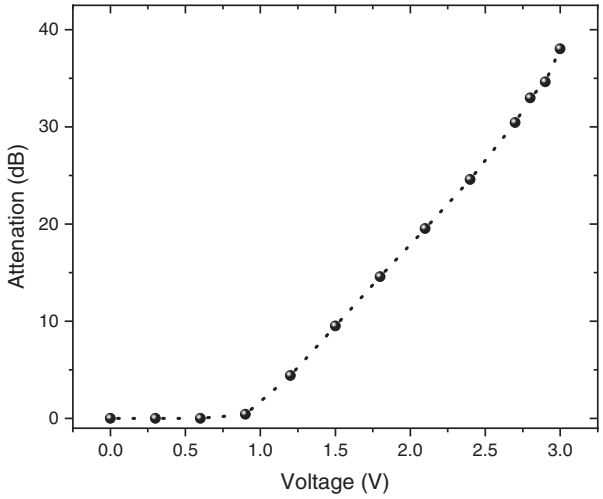

FIG. 9. Measured attenuation versus dc voltage. The maximum attenuation is 38 dB with applying a voltage of 3 V. The error bars are smaller than the data points.

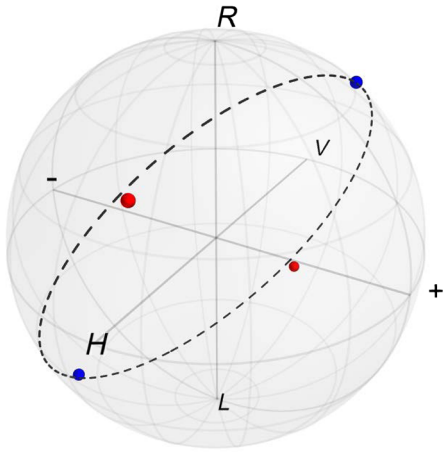

FIG. 10. Measured polarization states on Bloch sphere. The dots represent the produced states by the polarization modulator in chip.

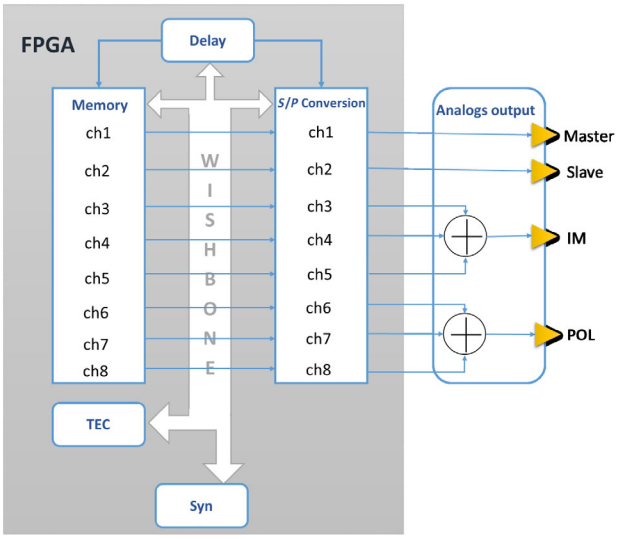

FIG. 11. Architecture of the electronics board. The dash box denotes a FPGA, which can be divided into several modules.

required by the protocol as follows. First, we create the polarization $(|H\rangle + |V\rangle)/\sqrt{2}$ by dc-voltage biasing the TOMs in the inner MZI. Then, by applying different levels of rf signal on the CDM in one arm of the PRC, a $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ phase shift is imposed to one of the arms of PRC, creating the one of polarization states $|\psi\rangle = (|H\rangle + e^{i\theta}|V\rangle)/\sqrt{2}$.

We characterize the produced states by using a polarimeter system (Thorlabs PAX1000). As shown in Fig. 10, with appropriate rf signals, we prepare four polarized states in conjugate bases, exhibiting a good ER (about 26 dB) and a high degree of polarization (about 0.993). Then, we measure the produced states with the measurement device in Charlie. The EPCs are adjusted so that each PBS is aligned to rectilinear and diagonal bases, respectively. With rf voltages between 0 and 7.5 V, we obtain an average polarization ER of about 23 dB, which is sufficient for a low-error MDI QKD operation.

3. Electronic control board

Figure 11 shows the architecture of the FPGA board (see an image in Fig. 12), which mainly consists of a memory module, parallel to serial conversion module (S/P conversion), delay module, thermoelectric cooler (TEC) module, synchronization module (Syn), and analog output module. All the modules (except the analogs output module) are implemented on a Xilinx Kintex-7 FPGA. Eight digital channels are able to generate signals with a 10-GHz sampling rate. Among them, two sets of channels (3, 4, 5 and 6, 7, 8) are synthesized to output multilevel signals for driving IM and POL, respectively.

The memory module provides 64 kb for eight digital channels each to storage waveform. The S/P conversion module is used to convert the parallel data to high-speed serial data. The delay module can adjust the delay of each channel. It has a resolution of 1 ps which provides a perfect overlap of the laser pulses and accurate intensity or polarization modulations. The analog output is used to amplify the signals from the FPGA, generating dc-coupled, return-to-zero encoding and four-amplitude pulse trains with the maximum amplitude of 7.5 V. It contains three MAX3942 whose outputs are combined via three 25 Ω resistors and connected to the amplifier HMC659 via the forth 25 Ω resistor. The combination of these 25 Ω resistors can meet the impedance matching requirements of all devices to form a broadband matched network. The TEC module generates all signals for thermoelectric controls, such as the lasers. The Syn module is designed to create up to four delayed-output pulse sequences precisely synchronized to internal or external clock. Using this pulse sequence, we can synchronize all stations in our setup. The further details of the design of the control circuit board can be found in Ref. [46].

4. Polarization alignment

Alice and Bob need to share a common polarization reference as well as compensate the polarization drift in the

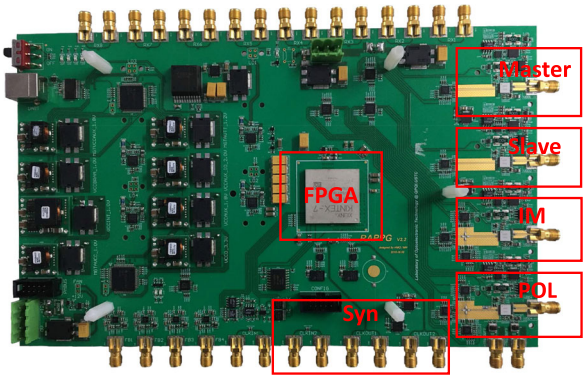

FIG. 12. Image of the electronics board.

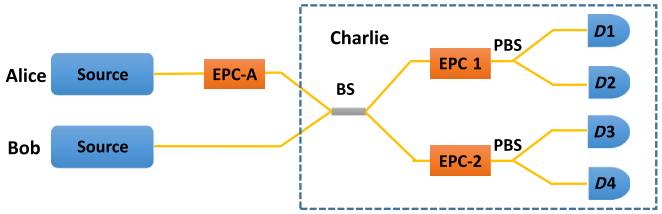

FIG. 13. Schematic of our polarization alignment system. EPC-*A*, EPC-1, EPC-2: electronic polarization controller; BS: beam splitter; PBS: polarization beam splitter; *D*1, *D*2, *D*3, *D*4: superconducting nanowire detector.

quantum channel. Here, we develop an automatic polarization alignment method which rapidly calibrates the polarization reference. Figure 13 shows the schematic of our alignment system, which is extracted from the setup in the main text. The EPCs (QEPC-100, QuantumCTek) have three control channels and the driver voltage of each channel is from 0 to 100 V. The system can be summarized in the following three steps, which can be realized by following the flowchart in Fig. 14.

Step 1: Bob and Charlie share a common reference by adjusting EPC-1 and EPC-2, following the flowchart in Fig. 14(a). The EPCs perform the step-by-step search for the optimal visibility by changing the driver voltage. The step size is initialized at 1 V and it is dynamically adjusted based on the obtained visibility. The timescale for each measurement in determining the visibility is 0.2 s. The threshold is set to 1:1000.

Step 2: Alice aligns her bases by adjusting EPC-A, following the flowchart in Fig. 14(b). The parameters of EPC are similar with that in step 1, except that the threshold of the average visibility is set to 1:200.

Step 3: Charlie aligns one of PBS to the *Z* basis by adjusting EPC-2, following the flowchart in Fig. 14(c). The parameters of EPC are similar to those in step 1, except that the threshold is set to 1:1000.

At last, Alice, Bob, and Charlie automatically share a common polarization reference at an average timescale of 30 s. The time is mainly limited by the searching algorithm, which can be further improved to less than 3 s by using an advanced local search algorithm. To our knowledge, most of previous works on polarization-encoding MDI QKD [13,18] used a manual calibration method. Generally, it takes dozens of minutes for a manual calibration. The system in Ref. [47] presents an automatic polarization procedure, but the method there is different from ours. Note that we perform the experiment in laboratory, where the polarization drift is negligible, as shown in Fig. 15. Thus, we do not actively control the polarization during the data collection. We perform the automatical realignment of the polarization every two hours.

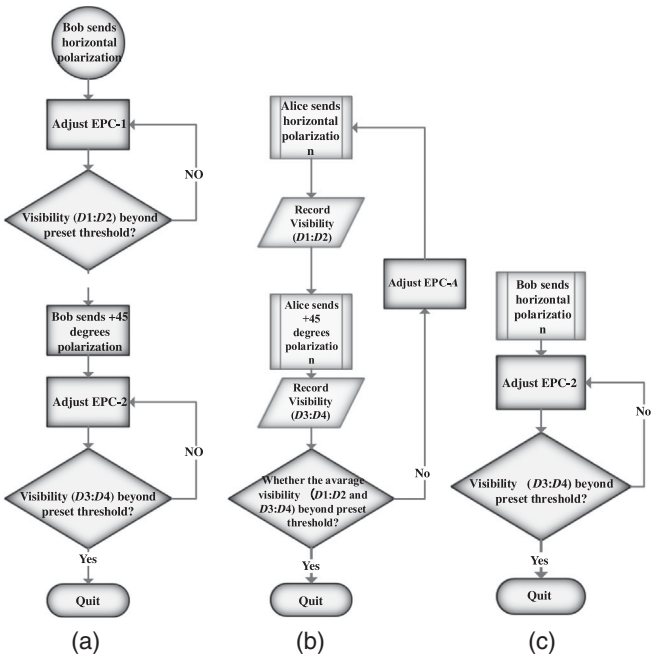

FIG. 14. Flowchart of polarization alignment.

5. Detection

The Bell-state measurement devices are located in Charlie. The synchronization clock is electrically distributed with a tunable time delay in steps of 1 ps. This enables Alice, Bob, and Charlie to electrically compensate any temporal drifts. The projection results are detected with four SNSPDs. The SNSPDs are cooled down to 2.1 K and with an detection efficiency of about 53%, dead time of about 40 ns, time jitter of about 70 ps, and dark counts about 50 Hz. Since the system has a gigahertz repetition rate, which requires that the SNSPD can tolerate a peak

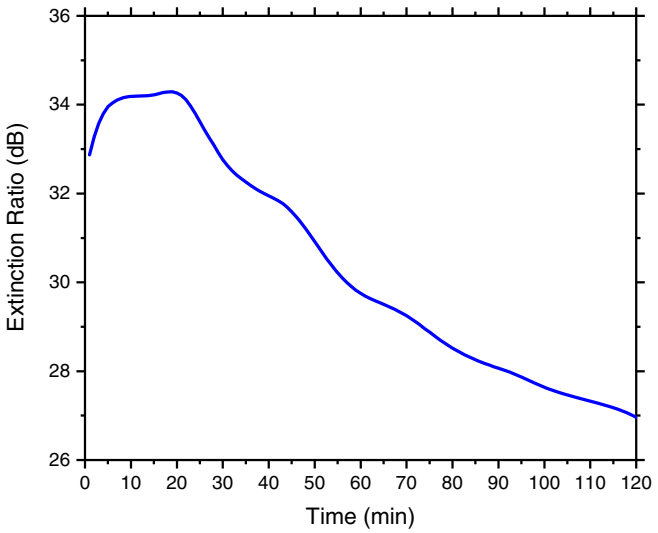

FIG. 15. Polarization stability over a 70-km single-mode fiber spool. Without active polarization control, the polarization can be stable for two hours with a polarization extinction ratio greater than 27 dB.

counting rate of more than 5 MHz. We solve it by inserting a 50-Ω shunt resistor between the dc arm of the bias tee and the ground at room temperature. This improved electrical configuration can prevent the detector from latching at a higher count rate without scarifying the detection efficiency. The outputs of detectors are recorded by a high-speed time-tagging equipment (Time-tagger 20, Swabian Instruments). The time coincidence time window is selected as 600 ps, which is determined by the trade-off between the detection efficiency of SNSPD and the error rate. The position of the coincidence time window is determined via the synchronization between Charlie and Alice or Bob. Detection events of different SNSPDs coincide in the time window are recorded and postselected as successful Bell-state measurements.

[1] H.-K. Lo, M. Curty, and K. Tamaki, *Secure Quantum Key Distribution*, Nat. Photonics **8**, 595 (2014).

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure Quantum Key Distribution with Realistic Devices*, Rev. Mod. Phys. **92**, 025002 (2020).

[3] M. Peev *et al.*, *The SECOQC Quantum Key Distribution Network in Vienna*, New J. Phys. **11**, 075001 (2009).

[4] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, *Metropolitan All-Pass and Inter-City Quantum Communication Network*, Opt. Express **18**, 27217 (2010).

[5] M. Sasaki *et al.*, *Field Test of Quantum Key Distribution in the Tokyo QKD Network*, Opt. Express **19**, 10387 (2011).

[6] B. Frohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, *A Quantum Access Network*, Nature (London) **501**, 69 (2013).

[7] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, *Network-Centric Quantum Communications with Application to Critical Infrastructure Protection*, arXiv:1305.0305.

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

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

[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination*, Nat. Photonics **4**, 686 (2010).

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

[12] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, *Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fiber*, Phys. Rev. Lett. **117**, 190501 (2016).

[13] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Quantum Key Distribution without Detector Vulnerabilities Using Optically Seeded Lasers*, Nat. Photonics **10**, 312 (2016).

[14] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, *Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks*, Phys. Rev. Lett. **111**, 130501 (2013).

[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, *Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network*, Phys. Rev. X **6**, 011024 (2016).

[16] W. Wang, F. Xu, and H.-K. Lo, *Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks*, Phys. Rev. X **9**, 041012 (2019).

[17] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, *Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels*, Phys. Rev. Lett. **122**, 160501 (2019).

[18] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, *Experimental Measurement-Device-Independent Quantum Key Distribution with Imperfect Sources*, Phys. Rev. A **93**, 042308 (2016).

[19] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, *A Cost-Effective Measurement-Device-Independent Quantum Key Distribution System for Quantum Networks*, Quantum Sci. Technol. **2**, 04LT01 (2017).

[20] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, *Measurement-Device-Independent Quantum Key Distribution Robust against Environmental Disturbances*, Optica **4**, 1016 (2017).

[21] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the Rate-Distance Limit of Quantum Key Distribution without Quantum Repeaters*, Nature (London) **557**, 400 (2018).

[22] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. OBrien, and M. G. Thompson, *Chip-Based Quantum Key Distribution*, Nat. Commun. **8**, 13984 (2017).

[23] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, *Silicon Photonic Transmitter for Polarization-Encoded Quantum Key Distribution*, Optica **3**, 1274 (2016).

[24] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. OBrien, and M. G. Thompson, *Integrated Silicon Photonics for High-Speed Quantum Key Distribution*, Optica **4**, 172 (2017).

[25] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton,

F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, *Metropolitan Quantum Key Distribution with Silicon Photonics*, Phys. Rev. X **8**, 021009 (2018).

[26] T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, *A Modulator-Free Quantum Key Distribution Transmitter Chip*, npj Quantum Inf. **5**, 42 (2019).

[27] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, *High-Dimensional Quantum Key Distribution Based on Multicore Fiber Using Silicon Photonic Integrated Circuits*, npj Quantum Inf. **3**, 25 (2017).

[28] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. Matthews, *A Homodyne Detector Integrated onto a Photonic Chip for Measuring Quantum States and Generating Random Numbers*, Quantum Sci. Technol. **3**, 025003 (2018).

[29] G. Zhang, J. Haw, H. Cai, F. Xu, S. Assad, J. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, *An Integrated Silicon Photonic Chip Platform for Continuous-Variable Quantum Key Distribution*, Nat. Photonics **13**, 839 (2019).

[30] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, *Full Daylight Quantum-Key-Distribution at 1550 nm Enabled by Integrated Silicon Photonics*, arXiv:1907.10039.

[31] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, *Experimental Demonstration of Memory-Enhanced Quantum Communication*, Nature (London) **580**, 60 (2020).

[32] W. H. Pernice, C. Schuck, O. Minaeva, M. Li, G. Goltsman, A. Sergienko, and H. Tang, *High-Speed and High-Efficiency Travelling Wave Single-Photon Detectors Embedded in Nanophotonic Circuits*, Nat. Commun. **3**, 1325 (2012).

[33] F. Najafi, J. Mower, N. C. Harris, F. Bellei, A. Dane, C. Lee, X. Hu, P. Kharel, F. Marsili, S. Assefa, K. K. Berggren, and D. Englund, *On-Chip Detection of Non-Classical Light by Scalable Integration of Single-Photon Detectors*, Nat. Commun. **6**, 5873 (2015).

[34] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, *Interference of Short Optical Pulses from Independent Gain-Switched Laser Diodes for Quantum Secure Communications*, Phys. Rev. Applied **2**, 064006 (2014).

[35] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, *Making the Decoy-State Measurement-Device-Independent Quantum Key Distribution Practically Useful*, Phys. Rev. A **93**, 042324 (2016).

[36] F. Xu, H. Xu, and H.-K. Lo, *Protocol Choice and Parameter Optimization in Decoy-State Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **89**, 052333 (2014).

[37] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, *Finite-Key Analysis for Measurement-Device-Independent Quantum Key Distribution*, Nat. Commun. **5**, 3732 (2014).

[38] C. Li, M. Curty, F. Xu, O. Bedroya, and H.-K. Lo, *Secure Quantum Communication in the Presence of Phase- and Polarization-Dependent Loss*, Phys. Rev. A **98**, 042324 (2018).

[39] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, *Experimental Quantum Key Distribution with Source Flaws*, Phys. Rev. A **92**, 032305 (2015).

[40] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, *Quantum Key Distribution with an Efficient Countermeasure against Correlated Intensity Fluctuations in Optical Pulses*, npj Quantum Inf. **4**, 8 (2018).

[41] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, *Loss-Tolerant Quantum Cryptography with Imperfect Sources*, Phys. Rev. A **90**, 052314 (2014).

[42] M. Pereira, M. Curty, and K. Tamaki, *Quantum Key Distribution with Flawed and Leaky Sources*, npj Quantum Inf. **5**, 62 (2019).

[43] H. Semenenko, P. Sibson, M. G. Thompson, and C. Erven, *Interference between Independent Photonic Integrated Devices for Quantum Key Distribution*, Opt. Lett. **44**, 275 (2019).

[44] C. Agnesi, B. Da Lio, D. Cozzolino, L. Cardi, B. Ben Bakir, K. Hassan, A. Della Frera, A. Ruggeri, A. Giudice, G. Vallone, P. Villoresi, A. Tosi, K. Rottwitt, Y. Ding, and D. Bacco, *Hongoumandel Interference between Independent IIIV on Silicon Waveguide Integrated Lasers*, Opt. Lett. **44**, 271 (2019).

[45] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, *Chip-Based Measurement-Device-Independent Quantum Key Distribution*, Optica **7**, 238 (2020).

[46] X. Liu, M.-Q. Huang, H. Min, G. Jin, X. Jiang, and C.-Z. Peng, *A 5 GHz and 7.5 V Multi-Amplitude Modulator Driving Circuit for Practical High-Speed Quantum Key Distribution*, Rev. Sci. Instrum. **91**, 024705 (2020).

[47] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, *Proof-of-Principle Demonstration of Measurement-Device-Independent Quantum Key Distribution Using Polarization Qubits*, Phys. Rev. A **88**, 052303 (2013).