Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network

Yan-Lin Tang,[1,2] Hua-Lei Yin,[1,2] Qi Zhao,[3] Hui Liu,[1,2] Xiang-Xiang Sun,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[4] Si-Jing Chen,[4] Lu Zhang,[4] Li-Xing You,[4] Zhen Wang,[4] Yang Liu,[1,2] Chao-Yang Lu,[1,2] Xiao Jiang,[1,2,*] Xiongfeng Ma,[3,†] Qiang Zhang,[1,2,‡] Teng-Yun Chen,[1,2,§] and Jian-Wei Pan[1,2,‖]

[1]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Shanghai 201315, China*
[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[4]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

(Received 29 October 2015; revised manuscript received 6 January 2016; published 4 March 2016)

Quantum cryptography holds the promise to establish an information-theoretically secure global network. All field tests of metropolitan-scale quantum networks to date are based on trusted relays. The security critically relies on the accountability of the trusted relays, which will break down if the relay is dishonest or compromised. Here, we construct a measurement-device-independent quantum key distribution (MDIQKD) network in a star topology over a 200-square-kilometer metropolitan area, which is secure against untrustful relays and against all detection attacks. In the field test, our system continuously runs through one week with a secure key rate 10 times larger than previous results. Our results demonstrate that the MDIQKD network, combining the best of both worlds—security and practicality, constitutes an appealing solution to secure metropolitan communications.

DOI: 10.1103/PhysRevX.6.011024 Subject Areas: Quantum Information

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] can, in principle, offer information-theoretical security between two remote parties, guaranteed by the fundamental laws of quantum mechanics. The last three decades have witnessed tremendous advances in both theoretical developments and successful experimental demonstrations of various quantum cryptographic systems. Moreover, QKD networks of various topologies have emerged and extended to more users in larger domains [3–8]. To increase the scalability of these networks, the architectures often adopt the idea of sharing, and thus a star-type network is preferable for sharing the most expensive resource—single-photon detectors [8], as shown in Fig. 1(a). With such a topological structure, it is straightforward to directly add more users with low hardware requirements.

From the security point of view, the existing star-type networks have to assume the central relays to be trustful, which is a critical shortcoming. Once the relay is dishonest,

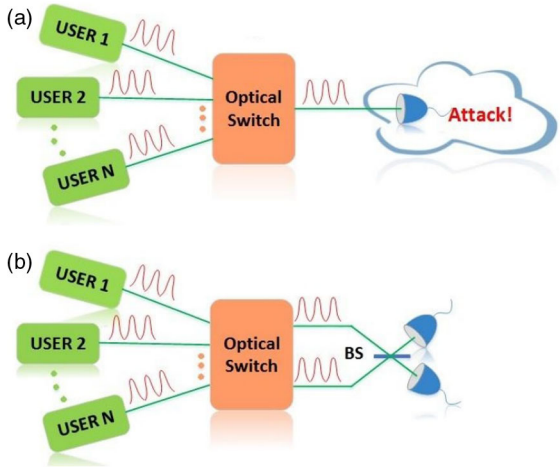


FIG. 1. (a) Schematic of a conventional QKD network with detectors as the shared resources, which are vulnerable to detection attacks. (b) Schematic of star-type MDIQKD network, in which the shared detectors can even be controlled by Eve but without any leakage of key information.

*jiangx@ustc.edu.cn
†xma@tsinghua.edu.cn
‡qiangzh@ustc.edu.cn
§tychen@ustc.edu.cn
‖pan@ustc.edu.cn

the security of the whole network is down. Furthermore, an honest relay with imperfect devices still suffers from various attacks that exploit the loopholes caused by the gap between the idealized devices assumed in the security proof and the realistic ones [9]. Indeed, single-photon detectors can be difficult for legitimate users to characterize precisely but easy for technology-advanced eavesdroppers to exploit a certain imperfection to attack [10,11]. It is important to note that in all previous network implementations, trustful relays are utilized, which constitutes the weakest point of security.

Remarkably, the MDIQKD protocol [12], inspired by the time-reversed entanglement-based QKD protocol [13–15], can close all the detection loopholes. In addition, MDIQKD is intrinsically suitable for a star-type network architecture with measurement devices placed at the central relay, as depicted in Fig. 1(b). Since its security does not rely on any assumption on measurement, the MDIQKD network even allows the eavesdroppers to have full control of the relay without compromising the security. Therefore, the MDIQKD networks are able to solve the security loophole existing in the conventional starlike QKD networks and almost all existing quantum networks.

Up till now, many efforts have been devoted to proof-of-principle experimental demonstrations of the MDIQKD protocol [16–20]. Further experiments, accounting for long-distance, high-loss field tests as well as high-visibility interference with an optically seeded laser, have also been reported [21–24]. Nevertheless, these are all limited to point-to-point configurations. Note that, in the field test of MDIQKD [23], three nodes are used, but the relay node does not share any key information and cannot be seen as a user. The MDIQKD network is theoretically discussed [25,26] but has yet to be developed. When extending to a network, quantum channels in a field environment may be very difficult to stabilize. In addition, the network system may need complicated and expensive resources for stabilization. Thus, a real-life network implementation is crucial for enabling and extending practical applications of MDIQKD.

II. CONFIGURATION DESCRIPTION

Here, we experimentally demonstrate a three-user, four-node MDIQKD network within the city of Hefei, China. The network deployment is shown in Fig. 2, which includes an untrusted relay R and three users, $U1$, $U2$, and $U3$, located in four different places. The deployed fiber lengths (channel losses) between the three users and the relay are 17 km (5.1 dB), 25 km (9.2 dB), and 30 km (8.1 dB), respectively. We employ an 8-by-4 mechanical optical switch to route the three users to the relay by an autocontrol command, with a low connection loss around 1 dB per channel. The outputs of the switch are connected to a fiber beam splitter (BS) for the Bell state measurement (BSM). Within the star-type topology, any user pair ($U1-U2$, $U1-U3$, $U3-U2$) can get access to the BSM setup to run MDIQKD, which works as a quantum telephone exchange.

A. Technical challenge

We emphasize that the MDIQKD network is not a straightforward upgrade of the previous point-to-point system [17,21]. There are significant new technical challenges in the network implementation. The first one is reference-frame calibration. Because of the phase fluctuation [16,17], the reference frame needs to be calibrated in a timely manner. In the previous point-to-point experiments [17,21], we utilized an additional fiber link between the two users and one phase-stabilization laser (PSL) for this purpose. To scale up for networking applications, the demand of fiber links increases quadratically with the user number. In addition, each new user needs an additional PSL with its wavelength locked to the signal laser.

We use a scalable and efficient structure [23] of phase stabilization suitable for phase calibration. As shown in Fig. 3(a), a pulsed PSL is placed in the relay and passes through a reference asymmetrical Mach-Zehnder interferometer (AMZI) with a delay of 6.5 ns. It is divided by BS and then sent to the three users through three additional fibers, respectively. After the user's AMZI, two commercial power meters record the two output interference intensities. Their measurement ratio provides a feedback signal to compensate the phase shift of AMZI by the phase shifter inside each user's AMZI. In this arrangement, the required fiber resources increase only linearly with the user number, which is a significant reduction compared to that in point-to-point structure. In addition, only one PSL, placed in the relay and shared by all the users, is needed.

The other critical challenge is to maintain the indistinguishability of all the users' lasers. For a point-to-point system, a high-speed feedback system [21] was developed for this purpose, where the two lasers are calibrated and locked via a feedback loop. However, in the network, any two users can be switched upon request. Once switched, the two lasers must be calibrated immediately to guarantee that their timing, spectrum, and polarization mode are indistinguishable. Furthermore, the optical switch will change the lasers' arriving time and polarization when it is connected.

In our network, we randomly switch any two users to the relay BSM per two hours; i.e., we need to recalibrate all the lasers' modes per 2 hours. For the timing synchronization and polarization stabilization, we adopt the feedback system in our previous system [21] (see Appendix A). For the wavelength calibration, in the point-to-point system, we previously utilized an optical spectrum analyzer (OSA) to calibrate and give feedback to the wavelength. Here, we measure the Hong-Ou-Mandel (HOM) interference with

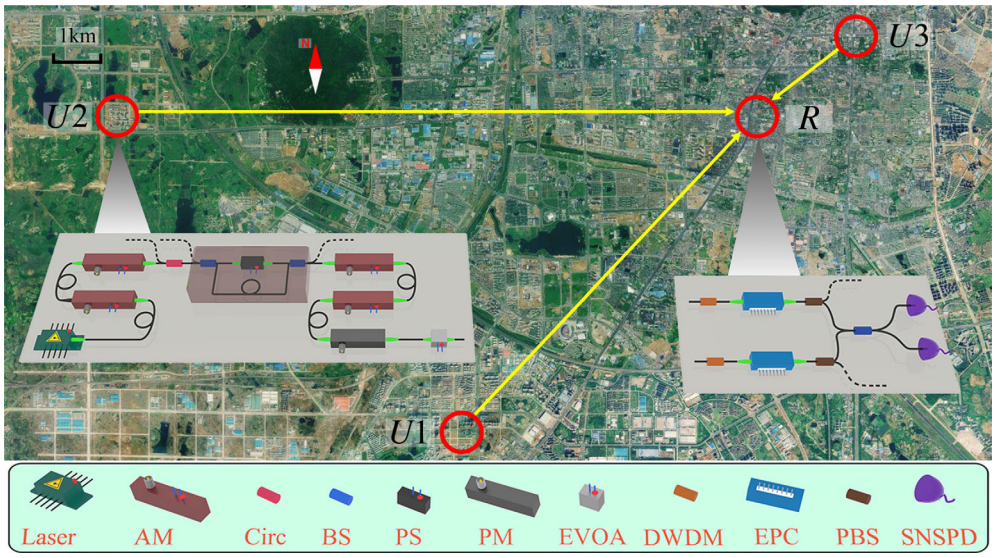


FIG. 2. Birds-eye view of the MDIQKD network topology. User $U1$ is placed in an administrative committee (AC) $(N31°47'5'', E117°12'58'')$, user $U2$ at the Animation Industry Park in Hefei (AIP) $(N31°50'6'', E117°7'52'')$, and user $U3$ in an office building (OB) $(N31°50'57'', E117°16'50'')$. In addition, a central relay R placed in the campus of the University of Science and Technology of China (USTC) $(N31°50'8'', E117°15'47'')$ is shared by all the users. The users' setup and the relay's BSM setup are shown in the inset. In the user's side, we utilize an internally modulated signal laser and modulate the decoy intensity according to the vacuum + weak decoy scheme by an amplitude modulator (AM). Then, we adopt a circulator, an asymmetrical Mach-Zehnder interferometer (AMZI), three AMs, and one phase modulator (PM) to encode qubits. The idle ports of circulators and beam splitters for the AMZI are exploited for phase synchronization and feedback, which are represented by the dashed line. After being attenuated by an electrical variable optical attenuator (EVOA), the signal laser pulses are sent via the deployed fiber to the relay comprised of an interference BS and two superconducting nanowire single-photon detectors (SNSPDs). Before the BSM, we adopt a dense wavelength division multiplexor (DWDM) in each input of the BS to block the stray light in the fiber, and we insert an electric polarization controller (EPC) and a polarization beam splitter (PBS) for polarization alignment.

the BSM setup and utilize the visibility of the HOM dip as the feedback signal. When the time and polarization are calibrated, the HOM visibility depends on the wavelength difference of the two lasers. Then, we adjust the wavelength by tuning the temperature of the input signal lasers. As shown in the inset of Fig. 3(b), by scanning the wavelength, we can observe a clear HOM dip. Using this method, we can take advantage of the existing BSM equipment, without the need for other instruments such as the OSA. Furthermore, as the HOM dip can reflect the overall interference condition, it is also an efficient way to calibrate all the interference parameters, including the wavelength difference.

B. Theoretical optimization

In our experiment, we optimize the system parameters [27], including the decoy-state parameter and basis choice setting [28], to increase the secure key rate. This optimization is based on the system parameters of the MDIQKD network with a high-quality transmitter system and a high-efficiency detection system. The MDIQKD transmitter at the user side and the BSM setup in the relay are illustrated in Fig. 2. Each user has the same configuration, adopting a signal laser internally modulated at 75 MHz, with a central wavelength of 1550.12 nm and a pulse width of 2.5 ns. With decoy-state optimization, the laser-pulse probabilities of the vacuum state, weak decoy state, and signal state are 16%, 58%, and 26%, and their intensities are modulated by AM1 into 0, $\nu = 0.1$, and $\mu = 0.33$, respectively. Each user employs the time-bin phase-encoding scheme [29], in which only the raw data in the Z basis are used for final key generation, and those in the X basis are used for phase-error estimation. The signal state is encoded in the Z basis. For the weak decoy state, 63% is encoded in the X basis and 37% in the Z basis. We utilize an AMZI, three AMs (AM2–AM4), and one PM to encode qubits. The modulators, AM2, AM3, and PM, are used to encode basis, and AM4 is used to normalize the two bases' average photon numbers. AM2 and AM3 beneficially help to further improve the extinction ratio of the vacuum state in the decoy-state scheme. The signal laser pulses are attenuated to single-photon level by an EVOA.

After passing through the deployed fiber routed to the relay by an optical switch, the laser pulses are interfered in the BSM setup. Before the BSM, we insert two DWDMs with 0.7-dB loss to block the background light. The BSM is then implemented with an interference BS and two SNSPDs [30] operated at 2.1 K with system-detection

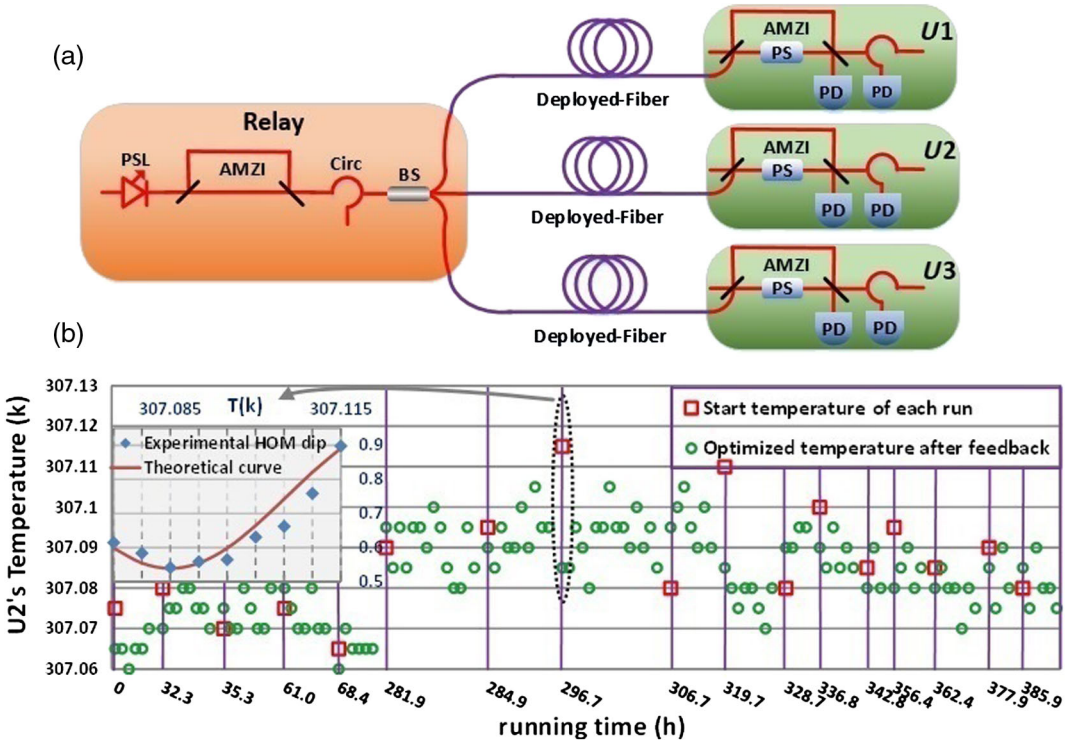


FIG. 3. (a) The structure of the phase-feedback scheme. A PSL placed in the relay passes through a reference AMZI with 6.5-ns delay and a circulator. It is divided into three parts by BS and then sent to each user's AMZI, connected by an additional fiber, respectively. After the user's AMZI, two photon detectors (here, we use commercial power meters) record the two output interference intensities and then provide a feedback signal to compensate the phase shift of AMZI by the phase shifter inside each user's AMZI. (b) The wavelength calibration result via measuring HOM interference. The different vertical zone represents different runs of MDIQKD. The x axis represents the system running time, and the y axis represents the temperature for U2's laser in the case of user pair ($U3 - U2$). Every green circle and red square point defines optimized temperature after a HOM dip measurement and the start temperature of each run. The inset shows the experimental HOM dip curve that we measure by scanning the temperature.

efficiencies of 64% and 66% and a dark count rate of 100 Hz. The inner insertion loss of the BS is 1.4 dB. The partial BSM postselects the $|\psi\rangle^-$ Bell state, when the two detectors in the two output arms of the BS have a coincidence detection at two alternative time bins. We set an efficient time window of 1.7 ns to achieve a good interference.

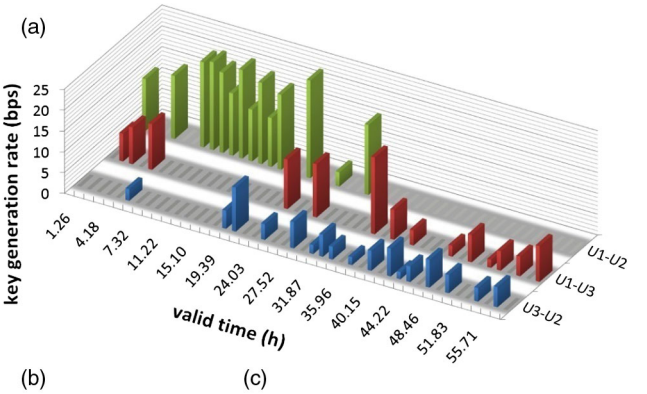
C. Experimental results

With the BSM results announced by the untrusted relay, the two users run the basis shift by postselecting the raw data when they choose the same basis. Then, the two users categorize the data according to vacuum-, decoy-, and signal-state labels and evaluate the gains and bit error rates in each case. All the data from the Z basis, consisting of nine cases, will be used for secure key extraction. The secure key rate formula is given by [12]

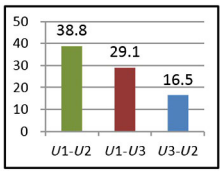
$$R \geq \sum_{a,b\in\{0,\nu,\mu\}} Q_{11}^{ab}[1 - H(e_{11}^{ab})] - Q^{ab} f H(E^{ab}), \quad (1)$$

where 0, ν, μ denote the vacuum, decoy, and signal states, respectively. Q^{ab} and E^{ab} are the overall gain and error rate when two users send states a and b with $a, b \in \{0, \nu, \mu, \}$. The gain and phase-error rate of the single-photon components, Q_{11}^{ab} and e_{11}^{ab}, can be estimated by the decoy-state method with a proper fluctuation analysis [31]. $H(e) = -e\log_2(e) - (1-e)\log_2(1-e)$ is the binary Shannon entropy function. The parameter f is the error correction efficiency, and we use $f = 1.2$ for evaluation. The detailed key rate calculation is shown in Appendix B.

We run the postprocessing for each valid data session of 1 to 2 hours between different user pairs. In the analysis, we fix the failure probability to be 10^{-10}. The secure key rates between different pairs, $U1 - U2$, $U1 - U3$, and $U3 - U2$, in different runs are shown in Fig. 4(a). They are, on average, 17.1 bps in 1 hour ($U1 - U2$), 6.4 bps in 1 hour ($U1 - U3$), and 4.2 bps in 1.5 hours ($U3 - U2$). Furthermore, we analyze the secure key rate by accumulating all the valid data, and we have extracted 38.8 bps in 17.4 hours ($U1 - U2$), 29.1 bps in 14.2 hours ($U1 - U3$), and 16.5 bps in 26.9 hours ($U3 - U2$), as shown in Fig. 4(b). We remark that the results we have achieved are at least 10 times higher than the previous state-of-the-art field test.



(b)



(c)

Client pair	U1-U2	U1-U3	U3-U2
fiber length(km):	17+25	17+30	30+25
fiber loss(dB):	5.1+9.2	5.1+8.1	8.1+9.2
connection loss(dB):	6.2	7	6.2
accumulated time(h):	17.4	14.2	26.9
secure key(b):	2.42E+06	1.49E+06	1.60E+06
secure key rate(bps):	38.8	29.1	16.5

FIG. 4. (a) The secure key rate array of each run with a valid time of 1.0–1.3 hours for user pair $(U1-U2)$, 0.8–1.2 hours for $(U1-U3)$, and 1.2–2.1 hours for $(U3-U2)$. (b) The overall key rate (unit: bps) with accumulated data of each user pair in 17.4 hours $(U1-U2)$, 14.2 hours $(U1-U3)$, and 26.9 hours $(U3-U2)$. (c) The system parameters, including the loss, the accumulation time, and secure key rate, are obtained.

III. CONCLUSION

In this work, we have demonstrated the first MDIQKD network which is secure against untrustful relays and all detection attacks, and also resource efficient in real-world implementation. Comparing to the decoy BB84 system with trustful relay, the MDIQKD network has the advantage of security but with a low key rate. For example, under the same experimental parameters, a decoy BB84 system with trustful relay can generate a key rate around 1 kbits per second. In the future, combining MDIQKD protocol to build up a resource-efficient and untrustful metropolitan network, and standard BB84 protocol to build up the trusted-relay backbone network, we can expect a wide-area QKD network with both practical performance and security.

The multiuser HOM interference technology developed in the experiment can find applications in multiparty entanglement swapping-based quantum communication [32] and a quantum-computing cloud. In a quantum-computing cloud, the users only need to prepare quantum states and share the expensive quantum-computing devices. Furthermore, with the decoy-state source, such a topological setup can also be extended to the blinding quantum computing [33], where the computing station can be untrusted.

ACKNOWLEDGMENTS

The authors would like to thank J. Fan, X. Xie, Z. Cao, and M. Jiang for enlightening discussions, as well as D. Yang and W. Sun for experimental assistance. This work has been supported by the National Fundamental Research Program (under Grants No. 2011CB921300 and No. 2013CB336800), the National Natural Science Foundation of China, the Chinese Academy of Science, the Science Fund of Anhui Province for Outstanding Youth, the 1000 Youth Fellowship program in China, and the Shandong Institute of Quantum Science & Technology Co., Ltd.

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

APPENDIX A: FULLY AUTOMATED FEEDBACK SYSTEM

The time calibration system mainly includes synchronization laser (SynL, 1570 nm) pulses to synchronize the whole system and a programmable delay chip to adjust the time delay of SynL pulses. The polarization stabilization system in each arm of the interference BS in the BSM handles the polarization misalignment of the laser pulse connected to the BSM by the optical switch. It mainly includes an EPC, a PBS, a SNSPD in the reflection port of this PBS, and a polarization-maintained interference BS in the transmission port.

For the wavelength calibration, we implement the HOM interference and calculate the coincidence value of the HOM dip, rather than measure the wavelength difference directly by an OSA. The coincidence value of the HOM dip is calculated by $(N_c N_{\mathrm{tot}})/(N_1 N_2)$, where N_c, N_{tot}, N_1, and N_2 represent the coincidence count of two BSM detectors, the total pulse count sent by the laser source, and the detection count of BSM detectors 1 and 2, respectively, over a certain run time and within a certain time window. By scanning the temperature, which increases linearly with the wavelength of our laser (0.8 pm per 0.01 ° centigrade), we can obtain the optimized wavelength. To implement the HOM dip measurement, the two users send their strong laser pulses without any decoy or qubit modulation. In addition, it is preferable for the intensity of the laser pulses arriving at the BSM setup to be close to each other because the coincidence value represents the indispensability considering all the modes. To obtain the wavelength difference more precisely, the coincidence value should be less influenced by the other aspects. To fulfill this purpose, the EVOA on the user's side is utilized to adjust the output intensity in this wavelength calibration procedure. In our experiment, we accumulate about 5 seconds with $N_{1,2} \sim 300\ k$ and accordingly $N_c \sim 600$ per second, which means that less than one photon per pulse sent from each user is enough for precise calculation.

For the phase stabilization, we adopt a pulsed PSL (1550.12 nm) with 2.5-ns pulse width placed in the relay. It passes through an AMZI with 6.5-ns time difference of two paths. Then, a BS divides the pulsed laser into three parts, with each output port connecting to one user. Combined with the synchronization laser pulses by WDM, the PSL pulses are transmitted through an additional fiber link and received by the corresponding user. Separated by another WDM, the PSL pulses pass through the user's AMZI and are monitored

by two commercial power meters in the two interference outputs. The intensity ratio provides a feedback signal to calibrate two AMZIs' phase reference frame by the phase shifter inside each user's AMZI. This arrangement has two advantages in both the scalable structure and the low commercial cost. First, this new structure is preferred for extension, with only one PSL placed in the relay and shared by all the users. In contrast, the structure of the phase stabilization system suitable for point-to-point implementation [21] needs one more feedback laser source when one user joins the network, and all the feedback laser wavelengths should be locked to the signal laser, which increases the technical complexity. Second, we adopt the commercial power meter rather than the gated single-photon detector. On one hand, the power meter is much cheaper and is especially preferred by users. On the other hand, the single-photon detector requires a gate signal with time calibrated according to fiber length shift. However, the power meter requires no extra controlling signal and hence no calibration.

APPENDIX B: THEORETICAL ANALYSIS

Following the Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security analysis [9], we give the detailed procedure for postprocessing and instructions about how to deal with the raw data obtained from the experiments. As a consequence, applying the Chernoff bound fluctuation analysis method, we show the secure key rate calculation for the measurement-device-independent quantum key distribution (MDIQKD) protocol.

We denote some parameters as follows.

(1) N^{ZZ} is the number of pulses when both Alice and Bob prepare quantum states in the Z basis.
(2) M^{ZZ} is the number of successful BSM events when both Alice and Bob prepare quantum states in the Z basis.
(3) E^{ZZ} is the error number in N^{ZZ} events.

When Alice and Bob prepare quantum states in other bases, we can similarly denote (N^{XX}, M^{XX}, E^{XX}), (N^{ZX}, M^{ZX}, E^{ZX}), and (N^{XZ}, M^{XZ} and E^{XZ}).

Alice and Bob send the quantum states encoded in three different intensities, 0, ν, μ, referred to as a vacuum state, a decoy state, and a signal state, respectively. Thus, all the data from the certain basis consisting of nine cases can be shown in a 3×3 matrix. For example, the successful BSM events when both Alice and Bob choose the Z basis are shown in Table I. Considering the basis choice, all the data can be shown in a 6×6 matrix.

TABLE I. M^{ZZ} consists of nine cases.

M^{ZZ}	0	Decoy	Signal
0	M_{00}^{ZZ}	$M_{0\nu}^{ZZ}$	$M_{0\mu}^{ZZ}$
Decoy	$M_{\nu 0}^{ZZ}$	$M_{\nu\nu}^{ZZ}$	$M_{\nu\mu}^{ZZ}$
Signal	$M_{\mu 0}^{ZZ}$	$M_{\mu\nu}^{ZZ}$	$M_{\mu\mu}^{ZZ}$

TABLE II. $M_{0\nu}$ consists of four cases.

	Bob (decoy)	
Alice (vacuum)	Z	X
Z	$M_{0\nu}^{ZZ}$	$M_{0\nu}^{ZX}$
X	$M_{0\nu}^{XZ}$	$M_{0\nu}^{XX}$

After the basis sifting, only the data encoding in the same basis remains. Consequently, we denote

$$Q^Z = \frac{M^{ZZ}}{N^{ZZ}}, \qquad Q^X = \frac{M^{XX}}{N^{XX}},$$
$$EQ^Z = \frac{E^{ZZ}}{N^{ZZ}}, \qquad EQ^X = \frac{E^{XX}}{N^{XX}} \tag{B1}$$

to be the gain and QBER when Alice and Bob coincidentally choose the same basis (Z or X).

In fact, the vacuum state does not need to distinguish its encoding basis. The cases when one party sends a vacuum state and the other party sends a decoy or signal state need to be redefined. For example, the case when Alice sends a vacuum state and Bob sends a decoy state in the Z basis consists of two subcases, shown in Table II. Consequently, the corresponding gain and QBER are equal to

$$Q_{0b}^Z = \frac{M_{0b}^{XZ} + M_{0b}^{ZZ}}{N_{0b}^{XZ} + N_{0b}^{ZZ}},$$
$$EQ_{0b}^Z = \frac{E_{0b}^{XZ} + E_{0b}^{ZZ}}{N_{0b}^{XZ} + N_{0b}^{ZZ}},$$
$$b \in \{\nu, \mu\}. \tag{B2}$$

These M^{ZZ} are all 3×3 matrices; for example, $M_{0\nu}^{ZZ}$ denotes the successful detection events when Alice sends a vacuum state and Bob sends a decoy state in the Z basis.

We consider the case where Alice and Bob both send vacuum states. The items Q_{00}^Z, EQ_{00}^Z, Q_{00}^X, EQ_{00}^X consist of four cases,

$$Q_{00}^X = Q_{00}^Z = \frac{M_{00}^{XZ} + M_{00}^{ZZ} + M_{00}^{ZX} + M_{00}^{XX}}{N_{00}^{XZ} + N_{00}^{ZZ} + N_{00}^{ZX} + N_{00}^{XX}},$$
$$EQ_{00}^X = EQ_{00}^Z = \frac{E_{00}^{XZ} + E_{00}^{ZZ} + E_{00}^{ZX} + E_{00}^{XX}}{N_{00}^{XZ} + N_{00}^{ZZ} + N_{00}^{ZX} + N_{00}^{XX}}. \tag{B3}$$

From the results in previous work [34], we get the analytical lower bound of Y_{11}^Z and the upper bound of $e_{1,1}^{bx}$ for the MDIQKD system. The lower bound of Y_{11}^Z is

$$Y_{11}^Z \geq \frac{1}{\mu^2\nu^2(\mu - \nu)}[\mu^3(\mathcal{E}(Q_{\nu\nu}^Z)e^{2\nu} + \mathcal{E}(Q_{00}^Z) - \mathcal{E}(Q_{\nu 0}^Z)e^{\nu}$$
$$- \mathcal{E}(Q_{0\nu}^Z)e^{\nu}) - \nu^3(\mathcal{E}(Q_{\mu\mu}^Z)e^{2\mu}$$
$$+ \mathcal{E}(Q_{00}^Z) - \mathcal{E}(Q_{\mu 0}^Z)e^{\mu} - \mathcal{E}(Q_{0\mu}^Z)e^{\mu})], \tag{B4}$$

TABLE III. The number of standard deviations and the corresponding failure probability in standard error analysis and our Chernoff bound analysis.

Deviation	Standard error analysis [36]	Chernoff bound [35]
3σ	2.70×10^{-3}	2.22×10^{-2}
5σ	5.73×10^{-7}	7.45×10^{-6}
7σ	2.56×10^{-12}	4.58×10^{-11}

where we use the upper bound of the Q^Zs with negative signs and the lower bound of the Q^Zs with positive signs to calculate the lower bound of Y_{11}^Z. The upper bound of $e_{1,1}^{bx}$ is

$$e_{1,1}^{bx} \leq \frac{1}{\nu^2 Y_{11}^X} \times [\mathcal{E}(EQ_{\nu\nu}^X)e^{2\nu} + \mathcal{E}(EQ_{00}^X - \mathcal{E}(EQ_{\iota 0}^X)e^{\nu} - \mathcal{E}(EQ_{0\nu}^X)e^{\nu}], \tag{B5}$$

where we use the upper bound of the EQ^Xs with positive signs and the lower bound of the EQ^Xs with negative signs to calculate the upper bound of $e_{1,1}^{bx}$.

Here, all the items with $\mathcal{E}$ need to take fluctuation analysis into consideration. We apply Chernoff bound analysis to estimate these items [31,35]. There are also gaps between Y_{11}^Z and Y_{11}^X, and $e_{1,1}^{bx}$ and $e_{1,1}^{pzab}(a, b \in \{0, \nu, \mu\})$. Random sampling can be applied to calculate these gaps. With a fixed single failure probability ξ, in a MDIQKD system, there are a total of 20ξ types of failure probabilities. Given the number of standard deviations $\sigma = \sqrt{X}$, we use the failure probability as a measure of the statistical fluctuation. In Table III, we show the number of standard deviations and the corresponding failure probability ξ in standard error analysis and our Chernoff bound analysis.

According to the definition of Y_{11}^Z, we know that

$$M_{11}^{Zab} = Y_{11}^Z \mathcal{E}(N_{11}^{Zab}),$$
$$Q_{11}^{Zab} = \frac{M_{11}^{Zab}}{N_{\text{total}}}, a, b \in \{0, \nu, \mu\}, \tag{B6}$$

where N_{11}^Z is the number of pulses encoded in the Z basis when Alice and Bob launch single-photon states at the same time, and N_{total} is the total number of pulses Alice and Bob send.

[1] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, Bangalore, India, 1984), pp. 175–179.

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

[3] J. Qiu, *Quantum Communications Leap out of the Lab*, Nature (London) **508**, 441 (2014).

[4] C. Elliott, *The DARPA Quantum Network*, Quantum Communications and Cryptography (CRC Press, Boca Raton, 2006), pp. 83–102.

[5] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes *et al.*, *The SECOQC Quantum Key Distribution Network in Vienna*, New J. Phys. **11**, 075001 (2009).

[6] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju *et al.*, *Metropolitan All-Pass and Inter-City Quantum Communication Network*, Opt. Express **18**, 27217 (2010).

[7] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, *Field Test of Quantum Key Distribution in the Tokyo QKD Network*, Opt. Express **19**, 10387 (2011).

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

[9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Security of Quantum Key Distribution with Imperfect Devices*, Quantum Inf. Comput. **4**, 325 (2004).

[10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Time-Shift Attack in Practical Quantum Cryptosystems*, Quantum Inf. Comput. **7**, 073 (2007).

[11] 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).

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

[13] E. Biham, B. Huttner, and T. Mor, *Quantum Cryptographic Network Based on Quantum Memories*, Phys. Rev. A **54**, 2651 (1996).

[14] H. Inamori, *Security of Practical Time-Reversed EPR Quantum Key Distribution*, Algorithmica **34**, 340 (2002).

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

[16] 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).

[17] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li *et al.*, *Experimental Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **111**, 130502 (2013).

[18] T. Ferreira 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).

[19] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, *Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **112**, 190503 (2014).

[20] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *High-Rate Measurement-Device-Independent Quantum Cryptography*, Nat. Photonics **9**, 397 (2015).

[21] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan *et al.*, *Measurement-Device-Independent Quantum Key Distribution over 200 km*, Phys. Rev. Lett. **113**, 190501 (2014).

[22] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M. D. Shaw *et al.*, *Measurement-Device-Independent Quantum Key Distribution: From Idea Towards Application*, J. Mod. Opt. **62**, 1141 (2015).

[23] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan *et al.*, *Field Test of Measurement-Device-Independent Quantum Key Distribution*, IEEE J. Selected Topics Quantum Electronics **21**, 6600407 (2015).

[24] 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, *Quantum Cryptography without Detector Vulnerabilities Using Optically-Seeded Lasers*, arXiv:1509.08137.

[25] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, *Discrete and Continuous Variables for Measurement-Device-Independent Quantum Cryptography*, Nat. Photonics **9**, 772 (2015).

[26] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *Reply to "Discrete and Continuous Variables for Measurement-Device-Independent Quantum Cryptography"*, Nat. Photonics **9**, 773 (2015).

[27] 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).

[28] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, *Decoy-State Quantum Key Distribution with Biased Basis Choice*, Sci. Rep. **3**, 2453 (2013).

[29] X. Ma and M. Razavi, *Alternative Schemes for Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **86**, 062319 (2012).

[30] S. Chen, L. You, W. Zhang, X. Yang, H. Li, L. Zhang, Z. Wang, and X. Xie, *Dark Counts of Superconducting Nanowire Single-Photon Detector under Illumination*, Opt. Express **23**, 10786 (2015).

[31] 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).

[32] S. Bose, V. Vedral, and P. L. Knight, *Multiparticle Generalization of Entanglement Swapping*, Phys. Rev. A **57**, 822 (1998).

[33] V. Dunjko, E. Kashefi, and A. Leverrier, *Blind Quantum Computing with Weak Coherent Pulses*, Phys. Rev. Lett. **108**, 200502 (2012).

[34] F. Xu, M. Curty, B. Qi, and H.-K. Lo, *Practical Aspects of Measurement-Device-Independent Quantum Key Distribution*, New J. Phys. **15**, 113007 (2013).

[35] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma (unpublished).

[36] X. Ma, C.-H. F. Fung, and M. Razavi, *Statistical Fluctuation Analysis for Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **86**, 052305 (2012).