Phase-Reference-Free Experiment of Measurement-Device-Independent Quantum Key Distribution

Chao Wang, Xiao-Tian Song, Zhen-Qiang Yin,* Shuang Wang,† Wei Chen, Chun-Mei Zhang, Guang-Can Guo, and Zheng-Fu Han

Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei 230026, China and Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

(Received 20 June 2015; published 15 October 2015)

Measurement-device-independent quantum key distribution (MDI QKD) is a substantial step toward practical information-theoretic security for key sharing between remote legitimate users (Alice and Bob). As with other standard device-dependent quantum key distribution protocols, such as BB84, MDI QKD assumes that the reference frames have been shared between Alice and Bob. In practice, a nontrivial alignment procedure is often necessary, which requires system resources and may significantly reduce the secure key generation rate. Here, we propose a phase-coding reference-frame-independent MDI QKD scheme that requires no phase alignment between the interferometers of two distant legitimate parties. As a demonstration, a proof-of-principle experiment using Faraday-Michelson interferometers is presented. The experimental system worked at 1 MHz, and an average secure key rate of 8.309 bps was obtained at a fiber length of 20 km between Alice and Bob. The system can maintain a positive key generation rate without phase compensation under normal conditions. The results exhibit the feasibility of our system for use in mature MDI QKD devices and its value for network scenarios.

DOI: 10.1103/PhysRevLett.115.160502 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex

Quantum key distribution (QKD) [1–5] provides an optimal way for two distant parties (Alice and Bob) to share secret keys because of its unconditional security, which has been proven in several ways with different theoretical models [6–10]. However, the gaps between theoretical models and practical setups may compromise the security of QKD implementations, resulting in various security loopholes [11–13]. Many efforts have been made to achieve loophole-free QKD with practical devices [14–17]. The measurement-device-independent (MDI) QKD protocol [18,19], in contrast to conventional QKD systems, does not rely on any assumption of measurement devices; thus, it is intrinsically immune to all detector-side-channel attacks. Only assumptions on sources are needed in the MDI system [18–24]. MDI QKD has received considerable attention in recent years owing to its balance between security and practicability. Several experimental demonstrations [25,26] and long-distance stable systems [27] of MDI QKD protocol have been performed. These efforts have promoted the development of the MDI QKD protocol and have demonstrated its feasibility for multiuser communication and even star-type networks [28].

Among these demonstrations, whether a time-bin phase coding system or polarization coding system is used, the photons from Alice and Bob must be kept indistinguishable, and the reference frames should be strictly aligned. Take the phase coding system for example; the phase reference frame is the relative phase difference between two arms, which is equivalent to the path length difference. This value is strongly affected by temperature perturbations and platform jounces, which result in notable deviations in state preparations and Bell-state-measurement results. An additional phase-reference-frame aligning system is typically introduced to avoid this problem. For example, in some phase-coding systems [25,27], an additional laser and detector may be required to compensate for the phase drift between Alice and Bob in the practical setup. In a polarization coding system, Alice and Bob modulate photons into the four BB84 polarization states. Any polarization deviation of Alice or Bob will lead to system errors. Thus, it is essential to keep the rectilinear bases (horizontal and vertical) of all users strictly aligned to the polarizing axes of the polarization beam splitter on Charlie's side [26] to make the system work properly. Although these additional alignment parts appear feasible, they increase the complexity of the MDI QKD system, which may lead to potentially dangerous blemishes that Eve may employ [29,30]. Moreover, particularly in a QKD network based on the MDI scheme, the alignment of the multireference frame is a critical technical challenge owing to the complex conditions and will result in expensive overheads.

As a possible solution to the frame-aligning problem, qubits encoded into rotationally invariant states based on a decoherence-free subsystem can be introduced in some QKD schemes [31–33]. However, detector-side-channel attacks of these schemes have not yet been discussed. Moreover, multiphoton (degree) entangled states are

required in this case, which is challenging and inefficient in practical implementations.

As an alternative, the reference-frame-independent (RFI) QKD protocol was proposed to eliminate the requirements of frame alignment [34]. Verification tests and practical applications of this protocol have been investigated in several ways [35–38]. Yin *et al.* proposed the RFI MDI QKD protocol, which is immune to detector-side-channel attacks [39,40]. In this study, we successfully implement this protocol with a time-bin phase coding system, which confirms the feasibility of RFI MDI QKD with slow, time-varying phase drifting and makes the MDI protocol safer, more compact, and more promising for future use.

We denote the Z basis consisting of $|0\rangle$ and $|1\rangle$, the X basis consisting of $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$, and the Y basis consisting of $|+i\rangle = 1/\sqrt{2}(|0\rangle + i|1\rangle)$ and $|-i\rangle = 1/\sqrt{2}(|0\rangle - i|1\rangle)$, where $|0\rangle$ and $|1\rangle$ represent the time-bin states traveling along the short and long arm, respectively. In RFI-MDI QKD, the Z basis is well defined, namely, $Z_A = Z_B$ for Alice and Bob. The X basis and the Y basis may vary with the slow phase drifting factor β as follows:

$$X_B = \cos\beta X_A + \sin\beta Y_A, \tag{1}$$

$$Y_B = \cos\beta Y_A - \sin\beta X_A. \tag{2}$$

$$\beta = (\beta_A + \beta_B)/2, \tag{3}$$

where $X_{A(B)}$, $Y_{A(B)}$, $Z_{A(B)}$ are Alice's (Bob's) local measurement frames for the X, Y, and Z bases, respectively. $\beta_{A(B)}$ is the deviation of the practical reference frame from the ideal one of Alice (Bob), which is the phase drifting in our time-bin phase coding system. Thus, we can write $1/\sqrt{2}(|0\rangle + e^{i\beta_{A(B)}}|1\rangle)$ instead of $|+\rangle$, $1/\sqrt{2}(|0\rangle - e^{i\beta_{A(B)}}|1\rangle)$ instead of $|-\rangle$, $1/\sqrt{2}(|0\rangle + ie^{i\beta_{A(B)}}|1\rangle)$ instead of $|+i\rangle$, and $1/\sqrt{2}(|0\rangle - ie^{i\beta_{A(B)}}|1\rangle)$ instead of $|-i\rangle$ because of the frame misalignment.

Alice and Bob randomly prepare their quantum states in the X, Y, and Z bases and send them to Charlie through the quantum channel. Charlie receives the photons and tries to project them into the Bell state $|\Psi^-\rangle$. According to the postselection results, Alice and Bob exchange their basis information and obtain $Y^{1,1}_{ZZ(XX,YY,XY,YX)}$ and $e^{1,1}_{ZZ(XX,YY,XY,YX)}$, which are the yields and error rates when Alice and Bob prepare the single-photon state in the Z-$Z(X$-X, Y-Y, X-Y, Y-$X)$ basis, respectively. Then, the quantity C can be defined as

$$\begin{aligned} C &= \langle X_A X_B\rangle^2 + \langle Y_A Y_B\rangle^2 + \langle X_A Y_B\rangle^2 + \langle Y_A X_B\rangle^2 \\ &= (1 - 2e^{1,1}_{XX})^2 + (1 - 2e^{1,1}_{YY})^2 \\ &\quad + (1 - 2e^{1,1}_{XY})^2 + (1 - 2e^{1,1}_{YX})^2. \end{aligned} \tag{4}$$

The C value does not vary with β_A or β_B, and without the existence of eavesdroppers and other system errors, the quantity C reaches its maximum value of 2. Therefore, the C value can be used to estimate Eve's information, and the secure key rate could be described as

$$R \geq P^{1,1}_{ZZ} Y^{1,1}_{ZZ}[1 - I_E(C)] - Q^{\mu,\mu}_{ZZ} f H(e^{\mu,\mu}_{ZZ}), \tag{5}$$

where $I_E(C) = (1 - e^{1,1}_{ZZ})H[(1+u)/2] + e^{1,1}_{ZZ}H[(1+v)/2]$, $v = [\sqrt{C/2 - (1 - e^{1,1}_{ZZ})^2 u^2}/e^{1,1}_{ZZ}]$, and $u = \min[\sqrt{C/2}/(1 - e^{1,1}_{ZZ}), 1]$. $Q^{\mu,\mu}_{ZZ}$ and $e^{\mu,\mu}_{ZZ}$ are the overall gain and error rate, respectively, when Alice and Bob both send signal states in the Z basis, and $Y^{1,1}_{ZZ}$ and $e^{1,1}_{ZZ}$ denote the yield and error rate, respectively, when both Alice and Bob send single-photon states in the Z basis. $P^{1,1}_{ZZ}$ is the probability that Alice and Bob both send single-photon states in the Z basis. $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Parameter f is the error correction efficiency. (Corresponding to the typical error rates in our experiment, the average efficiency of our CASCADE program is 1.16. So we use this value for our secure key rate estimation.)

Our experimental setup is shown in Fig. 1. The laser lights on Alice and Bob's side are first chopped into pulses by intensity modulators (IMs) with a temporal width of 2.5 ns. The lasers (Wavelength References Clarity-NLL-1542-HP) employed in our system are frequency locked to a molecular absorption line with a center wavelength of

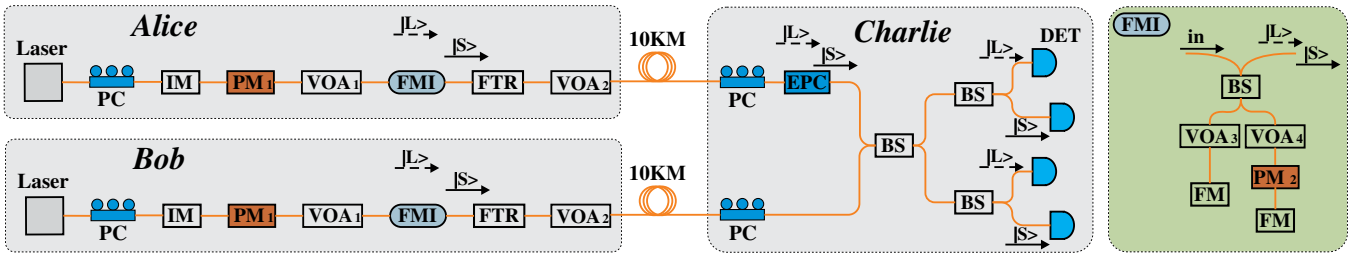

FIG. 1 (color online). Diagram of our RFI MDI QKD system. Laser, continuous-wave laser; PC, polarization controller; EPC, electronic polarization controller; IM, intensity modulator for wave chopping; VOA, variable optical attenuator; BS, beam splitter; PM, phase modulator; FM, Faraday mirror; FMI: Faraday-Michelson interferometer; FTR, band pass filter; DET, detector.

1542.38 nm. The center wavelength accuracy of 0.0001 nm (approximate frequency difference of 10 MHz) and frequency linewidth of approximately 400 MHz after wave chopping guarantee that the two separately generated lasers have sufficient overlap in the spectrum.

Then, active phase randomizations are implemented by phase modulators (PM_1) to avoid imperfect-source attacks [42,43]. For quantum state preparation, Faraday-Michelson interferometers (FMIs) with a 4.9 m difference in the two arms are used, where VOA_3 and VOA_4 dominate the basis choice, which indicates that if either VOA_3 or VOA_4 is set to low loss with the other set to high loss, only a short arm or long arm pulse can be passed through; thus, the Z basis state is prepared in this case. If VOA_3 and VOA_4 in FMI are both set to low loss, the X or Y basis state is prepared in this case, and phase modulators PM_2 determine the relative phase information of the two time bins. Compared with the Mach-Zehnder interferometer, the greatest benefit of the FMI system is the stability of the relative polarization between the two time-bin pulses; thus, we do not need to pay extra attention to the polarization difference between two arms, particularly in long-distance communication.

VOA_1 is proposed to modulate the pulses into three different intensities for decoy state technology. In our experiment, one signal state with a mean photon number of $\mu = 0.635$, one decoy state with a mean photon number of $\nu = 0.04$, and a vacuum state with a mean photon number ω of nearly 0 (limited by the attenuation depth of VOA_1) are used, which have been comprehensively optimized through numerical simulations. VOA_2 is used for single-photon-level attenuation as well as power adjustment between the Z basis state and the X and Y basis states, which ensures the conformity of the mean photon number between bases. A band pass filter (center wavelength of 1542.38 nm and linewidth of 0.25 nm) is employed to purify the signals and eliminate stray light from other optical components.

The encoded pulses from Alice and Bob are then sent to Charlie through a 10 km spooled fiber at the same time. The entire system is working at a repetition frequency of 1 MHz. In our experiment, state preparation devices, detectors, and random numbers are all triggered by a fine-tuned sync signal of 10 ps resolution, so the preparation and detection of two pulses can be precisely controlled.

TABLE I. Experimental data of total gains (a) and total error rates (b) with different mean photon numbers in the Z basis.

(a)

	ω_{Alice}	ν_{Alice}	μ_{Alice}
ω_{Bob}	1.8473×10^{-10}	1.8489×10^{-8}	7.6988×10^{-7}
ν_{Bob}	1.8133×10^{-8}	5.2622×10^{-7}	8.6503×10^{-6}
μ_{Bob}	6.4881×10^{-7}	8.7524×10^{-6}	1.1975×10^{-4}

(b)

	ω_{Alice}	ν_{Alice}	μ_{Alice}
ω_{Bob}	0.5	0.5038464	0.4944358
ν_{Bob}	0.4929414	0.0391894	0.0528204
μ_{Bob}	0.5019247	0.0783674	0.0139244

Apart from timing and spectrum alignments, the polarization of pulses from two parties also should be regulated to keep the photons indistinguishable for the Bell state measurement. Experimentally, Charlie periodically checks the polarization of pulses from Alice every 30 min, and if deviation exists, rectification is implemented using an electronic polarization controller (General Photonics PCD-M02-4X polaRITE 3).

Then, a partial Bell state measurement is performed with a beam splitter and four commercial InGaAs/InP single-photon detectors (Qasky WT-SPD100), whose average efficiency is 12% and whose average dark count rate is approximately 9.61×10^{-6} per gate, with a gate width of 2.5 ns. The dead time of the detectors is set to 5 μs to depress after-pulse generation. Once a coincident occurs in two different time bins at both outputs of the beam splitter, it can be proven that Alice and Bob share a Bell state $|\Psi^-\rangle$ at this time. Therefore, both Alice and Bob will be informed of the detection results and obtain their secure keys after basis sifting and postprocessing.

We collect all successful $|\Psi^-\rangle$ projections in all bases with different mean photon numbers. The data information in the Z basis are shown in Table I.

We use the analytical equations given by Xu *et al.* [44] to evaluate the lower bound $Y^{1,1}_{ZZ,L}$ and upper bound $e^{1,1}_{ZZ,U}$ of the Z basis:

$$\begin{aligned} Y^{1,1}_{ZZ,L} \geq{}& \frac{1}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_a-\nu_a)} \\ &\times [(\mu_a^2-\omega_a^2)(\mu_b-\omega_b)(Q^{\nu,\nu}_{ZZ}e^{(\nu_a+\nu_b)}+Q^{\omega,\omega}_{ZZ}e^{(\omega_a+\omega_b)}-Q^{\nu,\omega}_{ZZ}e^{(\nu_a+\omega_b)}-Q^{\omega,\nu}_{ZZ}e^{(\omega_a+\nu_b)}) \\ &-(\nu_a^2-\omega_a^2)(\nu_b-\omega_b)(Q^{\mu,\mu}_{ZZ}e^{(\mu_a+\mu_b)}+Q^{\omega,\omega}_{ZZ}e^{(\omega_a+\omega_b)}-Q^{\mu,\omega}_{ZZ}e^{(\mu_a+\omega_b)}-Q^{\omega,\mu}_{ZZ}e^{(\omega_a+\mu_b)})], \end{aligned} \tag{6}$$

$$e^{1,1}_{ZZ,U} \leq \frac{1}{(\nu_a-\omega_a)(\nu_b-\omega_b)Y^{1,1}_{ZZ,L}} \times \left[e^{(\nu_a+\nu_b)}Q^{\nu,\nu}_{ZZ}e^{\nu,\nu}_{ZZ}+e^{(\omega_a+\omega_b)}Q^{\omega,\omega}_{ZZ}e^{\omega,\omega}_{ZZ}-e^{(\nu_a+\omega_b)}Q^{\nu,\omega}_{ZZ}e^{\nu,\omega}_{ZZ}-e^{(\omega_a+\nu_b)}Q^{\omega,\nu}_{ZZ}e^{\omega,\nu}_{ZZ}\right], \tag{7}$$

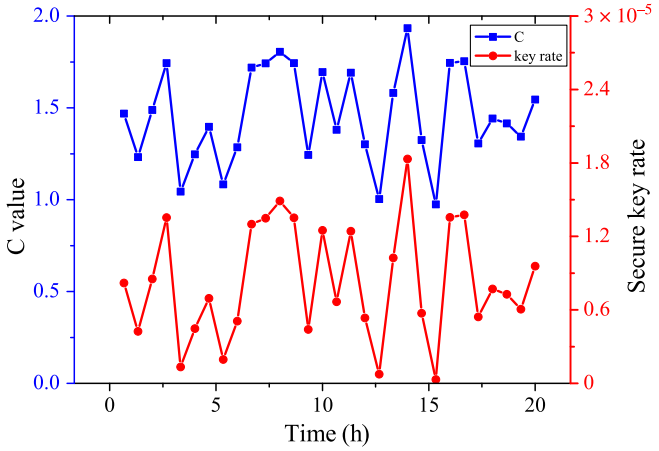

FIG. 2 (color online). C value and secure key rate over time.

where $Q_{ZZ}^{i,j}$ and $e_{ZZ}^{i,j}$ $(i,j=\mu,\nu,\omega)$ represent the total gain and total error rate when Alice and Bob send pulses with mean photon numbers of i and j, respectively.

With the data above, we obtain $Y_{ZZ,L}^{1,1}=2.843\times10^{-4}$ and $e_{ZZ,U}^{1,1}=7.548‰$. Compared to the simulation values of $Y_{ZZ,\mathrm{ideal}}^{1,1}=3.423\times10^{-4}$ and $e_{ZZ,\mathrm{ideal}}^{1,1}=1.098‰$ according to practical setups, $e_{ZZ,U}^{1,1}$ is considerably higher than expected. This can be principally explained by the imperfection of light wave chopping. Owing to the typical extinction ratio of IMs of approximately 25 dB, we could not cut off the long arm pulse entirely when we let the short arm pulse through in the Z basis, which gives rise to a notable error rate. In this case, if Alice and Bob both send signal state μ in the Z basis, the total error rate in our system would be $e_{ZZ}^{\mu,\mu}\approx0.0124$, which is close to the experimental result of 0.0139.

The same method is applied to estimate error rates in the X-X, X-Y, Y-X, and Y-Y bases for the C value. In our experiment, each C value is evaluated using 2×10^9 emitted light pulses while the phase reference β is relatively stable. The relative final secure key rate is evaluated according to Eq. (5). The final results vary with time, as shown in Fig. 2.

The clear fluctuations of the C value and secure key rate are primarily due to the statistical fluctuations of the gains $Q_{ZZ}^{\nu,\nu}$ and error rates $e_{ZZ}^{\nu,\nu}$ of decoy state because of the low repetition rate of our system. Considering that both $Q_{ZZ}^{\nu,\nu}$ and $e_{ZZ}^{\nu,\nu}$ vary within their 3 standard deviations, the C value changes from 1.22 to 2.0, and the final secure key rate changes from 2.58×10^{-6} to 2.17×10^{-5}, which varies widely between the maximum and minimum, according to the numerical simulations in the ideal case.

In summary, we have successfully accomplished the first RFI MDI QKD experiment with a time-bin phase coding system. The rejection of the frame-calibrating part will intrinsically reduce the consumption of resources as well as the potential security flaws of practical MDI systems. We continuously run the system with a timing alignment, polarization alignment, and wave chopping system that operates automatically, and we obtain an average secure key rate of 8.3098×10^{-6} bits per pulse, equivalent to 8.3098 bits per second. Predictably, the secure key generation rate of RFI MDI systems can benefit from a higher clockwork frequency and higher photon detection efficiency. In particular, taking finite-key analysis into account, the robustness and practical security will be greatly improved in the high-speed RFI MDI QKD system.

This work was supported by the Strategic Priority Research Program (B) of the Chinese Academy of Sciences (Grants No. XDB01030100 and No. XDB01030300), the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200) and the National Natural Science Foundation of China (Grants No. 61201239, No. 61475148, No. 61205118, and No. 11304397).

C. W. and X-T. S. contributed equally to this work.

*Corresponding author.
yinzheqi@mail.ustc.edu.cn
†Corresponding author.
wshuang@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179.
[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005).
[4] Z. F. Han, X. F. Mo, Y. Z. Gui, and G. C. Guo, Appl. Phys. Lett. **86**, 221103 (2005).
[5] S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, G. C. Guo, and Z. F. Han, Opt. Lett. **37**, 1008 (2012).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[8] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[9] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[10] H. W. Li, Z. Q. Yin, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Phys. Rev. A **89**, 032302 (2014).
[11] H. W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011).
[12] J. Z. Huang, Z. Q. Yin, S.Wang, H. W. Li, W. Chen, and Z. F. Han, Eur. Phys. J. D **66**, 159 (2012).
[13] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[15] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[16] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[17] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[18] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[19] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[20] Z. Q. Yin, C.-H. Fred 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).
[21] Z. Q. Yin, C.-H. Fred Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Phys. Rev. A **90**, 052319 (2014).
[22] K. Tamaki, H.-K. Lo, C.-H. Fred Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).
[23] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).
[24] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[25] 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.*, Phys. Rev. Lett. **111**, 130502 (2013).
[26] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[27] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).
[28] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[29] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).
[30] Z.-Y. Dong, N.-N. Yu, Z.-J. Wei, J.-D. Wang, and Z.-M. Zhang, Eur. Phys. J. D **68**, 230 (2014).
[31] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).
[32] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[33] T.-Y. Chen, J. Zhang, J.-C. Boileau, X.-M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J.-W. Pan, Phys. Rev. Lett. **96**, 150504 (2006).
[34] A. Laing, V. Scarani, J. G. Rarity, and J. L. OBrien, Phys. Rev. A **82**, 012304 (2010).
[35] W. Y. Liang, S. Wang, H. W. Li, Z. Q. Yin, W. Chen, Y. Yao, J. Z. Huang, G. C. Guo, and Z. F. Han, Sci. Rep. **4**, 3617 (2014).
[36] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. OBrien, and A. O. Niskanen, New J. Phys. **15**, 073001 (2013).
[37] V. DAmbrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, Nat. Commun. **3**, 961 (2012).
[38] J. A. Slater, C. Branciard, N. Brunner, and W. Tittel, New J. Phys. **16**, 043002 (2014).
[39] Z. Q. Yin, S. Wang, W. Chen, H. W. Li, G. C. Guo, and Z. F. Han, Quantum Inf. Process. **13**, 1237 (2014).
[40] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.115.160502, which includes Ref. [41], for more information about RFI MDI QKD.
[41] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[42] H.-K. Lo and J. Preskill, arXiv:quant-ph/0504209.
[43] S. H. Sun, M. Gao, M. S. Jiang, C. Y. Li, and L. M. Liang, Phys. Rev. A **85**, 032304 (2012).
[44] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).