Experimental Measurement-Device-Independent Quantum Key Distribution

Yang Liu,[1] Teng-Yun Chen,[1] Liu-Jun Wang,[1] Hao Liang,[1] Guo-Liang Shentu,[1] Jian Wang,[1] Ke Cui,[1] Hua-Lei Yin,[1] Nai-Le Liu,[1] Li Li,[1] Xiongfeng Ma,[2,*] Jason S. Pelc,[3] M. M. Fejer,[3] Cheng-Zhi Peng,[1] Qiang Zhang,[1,†] and Jian-Wei Pan[1,‡]

[1]*Department of Modern Physics and Hefei National Laboratory for Physical Sciences at Microscale, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[2]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, People's Republic of China*

[3]*E. L. Ginzton Laboratory, Stanford University, 348 Via Pueblo Mall, Stanford, California 94305, USA*

(Received 21 April 2013; published 23 September 2013)

Quantum key distribution is proven to offer unconditional security in communication between two remote users with ideal source and detection. Unfortunately, ideal devices never exist in practice and device imperfections have become the targets of various attacks. By developing up-conversion single-photon detectors with high efficiency and low noise, we faithfully demonstrate the measurement-device-independent quantum-key-distribution protocol, which is immune to all hacking strategies on detection. Meanwhile, we employ the decoy-state method to defend attacks on a nonideal source. By assuming a trusted source scenario, our practical system, which generates more than a 25 kbit secure key over a 50 km fiber link, serves as a stepping stone in the quest for unconditionally secure communications with realistic devices.

DOI: 10.1103/PhysRevLett.111.130502 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex

Throughout history, every advance in encryption has been defeated by advances in hacking with severe consequences. Quantum cryptography [1,2] holds the promise to end this battle by offering unconditional security [3–5] when ideal single-photon sources and detectors are employed. In practice, however, the gap between ideal devices and realistic setups has been the root of various security loopholes [6–8], which have become the targets of many attacks [9–16]. Tremendous efforts have been made towards loophole-free quantum key distribution (QKD) with practical devices [17,18]. However, the question of whether security loopholes will ever be exhausted and closed still remains.

In conventional QKD, such as prepare-and-measure protocols, the sender Alice sends quantum states encoded with key information (qubits) to the receiver Bob, who then measures them, as shown in Fig. 1(a). A malicious eavesdropper Eve may intercept and manipulate the quantum signals traveling in the channel and forward tampered signals to Bob. In a typical security proof of QKD [6], one assumes that Eve performs manipulation on the Hilbert space of qubits. Since the photons have degrees of freedom other than the one used for key information encoding, Eve might take advantage of the side-channel information. For example, when an efficiency mismatch exists between detectors [9], Eve can steal some information of the key by shifting the arrival times of the quantum signals at Bob, which is called a time-shift attack [10]. More attacks can be launched if other degrees of freedom are considered: for instance, the detector blinding attack [13,16] exploits the detector's after-gate pulses and dead time.

Measurement-device-independent (MDI) QKD [19,20] protocols close all loopholes on detection at once. In fact, the detectors in a MDI QKD setup can even be assumed to be in Eve's possession. As shown in Fig. 1(b), Alice and Bob encode the key information onto their own quantum states independently and then send them to the detection station for a Bell-state measurement (BSM). The quantum signals from two arms interfere in a beam splitter and are then detected by two detectors. Certain postselected coincidence events are used as the raw key. As discussed in Ref. [19], even if Eve controls the measurement site, she cannot gain any information on the final key without being noticed. The security of MDI QKD is based on the time-reversed version of entanglement-based QKD protocols

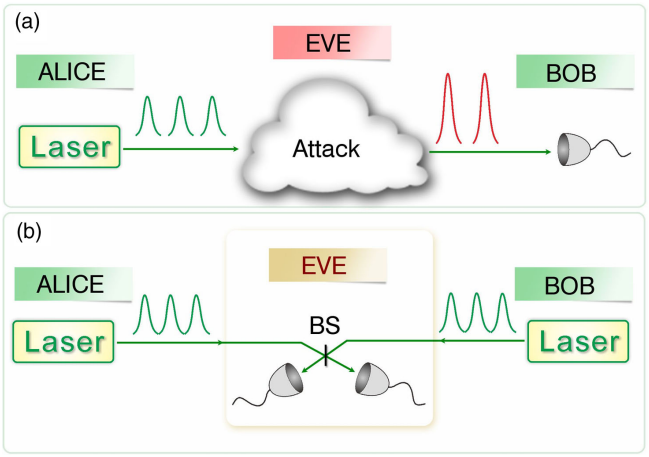

FIG. 1 (color online). (a) Conventional prepare-and-measure QKD setup, where Alice sends qubits to Bob through an insecure quantum channel, controlled by Eve. (b) MDI QKD setup, where Alice and Bob each sends quantum signals to Eve for measurement.

[21,22], which is naturally immune to any attack on detection. To avoid photon-number-splitting attacks [23], the decoy-state method [24] is adopted in the original proposal of MDI QKD. We remark that the main security assumption we adopt for our MDI QKD system is the usage of trusted sources: phase randomized coherent states with intensity modulations.

Several attempts have been devoted to the experimental realization of MDI QKD [19,25,26]. However, none of these experiments has faithfully implemented the decoy-state method and hence cannot guarantee the security of the final key. A faithful demonstration of MDI QKD remains experimentally challenging.

In our experimental realization, we implement the time-bin phase-encoding MDI QKD scheme [19,20], as shown in Fig. 2(a). Alice and Bob first randomly prepare their time-bin qubits in one of the two bases, denoted by Z and X. If the Z basis is used, the key bit is encoded in time bin 0 or time bin 1 by an amplitude modulator (AM). If the X basis is used, the key bit is encoded into the relative phases 0 or π between the two time bins by a phase modulator (PM). Another AM is used to vary the average photon number per pulse, chosen from the values of 0, 0.1, 0.2, and 0.5, for the decoy-state method. After the first two AMs, the average photon numbers in the X and Z bases are different. Hence, a third AM is used to normalize the average photon numbers in the two bases.

Each party sends quantum signals to the measurement station for partial BSM. A successful BSM event occurs when the two qubits interfere perfectly in a beam splitter and the two detectors have a coincidence at alternative time bins. Then, in the Z basis, a valid BSM always results in complementary bits between Alice and Bob, as is the case for the X basis when each pulse contains only one photon. The multiphoton component in the coherent-state pulse may cause accidental coincidence, which introduces a 50% bit error rate in the X basis. After the announcement from the measurement site, Alice and Bob will compare their basis choices and select out the sifted key. Then, they can perform postprocessing to extract a final secure key.

A critical aspect to this experiment is the indistinguishability of the signal pulses generated by the two independent laser sources, mainly in three dimensions: spectrum, timing, and polarization. Any mismatch in these dimensions would introduce errors in the X basis. First, the wavelength difference between Alice and Bob's pulses needs to be small compared to the bandwidth of the laser pulse. In our system, we utilize a 1 MHz shared time reference from a field-programable gate array to modulate two independent distributed feedback laser diodes to produce Alice and Bob's signal pulses. The pulse width is about 2 ns, and its wavelength centers at 1550.200 nm, with a FWHM of about 10 pm. By adjusting the temperature control precisely, the laser's central wavelength can be set to a precision of about 0.1 pm, which is small enough to keep the error rate low. Second, the temporal modes of Alice and Bob's pulses should be overlapped precisely. We monitor the arrival times of the two lasers by an 80 GHz

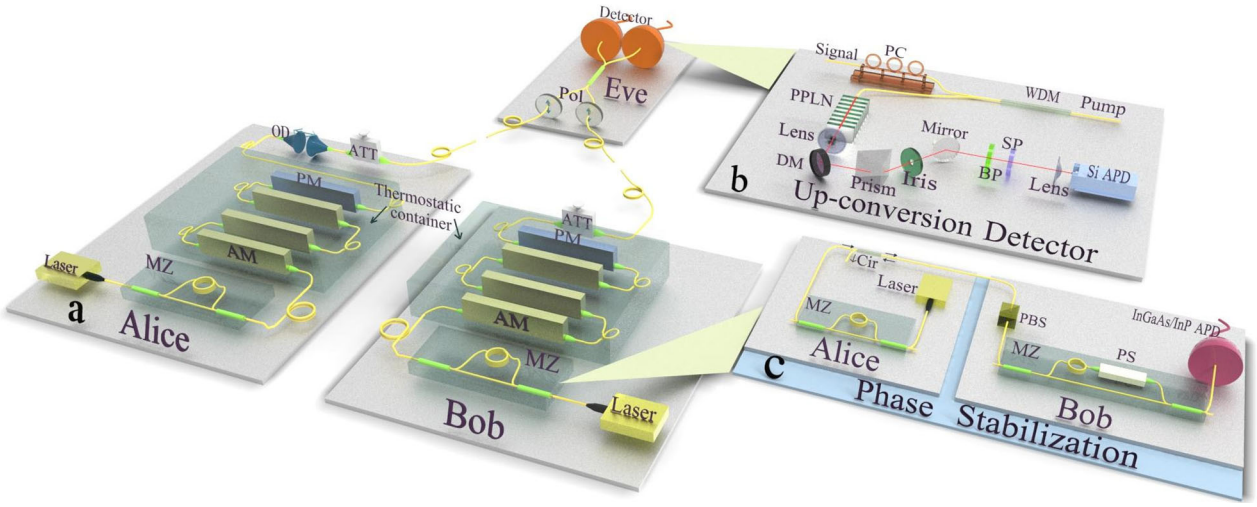

FIG. 2 (color online). (a) Diagram of our MDI QKD setup. Alice passes her laser pulses through an unbalanced MZ interferometer, with an arm difference of 6 m, to generate two time-bin pulses. A PM and three AMs are used to encode the qubit and generate decoy states. All the modulations are controlled by quantum random number generators. In order to reduce the temperature fluctuation, we put all the modulators into thermostatic containers. Bob's encoding system is the same as Alice's. The pulses are then attenuated by an attenuator (ATT) and send out via fiber links from Alice and Bob to the measurement site. After traveling through 25 km fiber spools of each arm and polarizers (Pol), signal pulses from two sides interfere at a 50:50 fiber beam splitter (BS) for a partial BSM. The output photon is detected by up-conversion detectors and recorded with a time interval analyzer. (b) Diagram of an up-conversion single-photon detector. PC, polarization controller; DM, dichroic mirror; BP, band pass filter; and SP, short pass filter. (c) Phase stabilization setup. Cir, circulator; PS, phase shifter; and PBS, polarizing beam splitter.

oscilloscope and use an optical delay (OD) in Alice's station to adjust the timing. The resolution of the OD is better than 10 ps, and the time jitter of the laser pulses is also around 10 ps, which is small compared to the pulse width of 2 ns. Third, the polarization of the quantum signals may rotate during the channel transmission due to the fiber birefringence. In front of the interference beam splitter, we insert a polarization controller and a polarizer in each arm to make the polarization indistinguishable. Experimental details are shown in Sec. III of the Supplemental Material [27].

The relative phase between the two arms of the Mach-Zehnder (MZ) interferometer may fluctuate with temperature and stress, which introduces further errors in the X basis. We use an additional fiber between Alice and Bob for feedback to stabilize the interferometer phases. By sending highly attenuated light from another laser source from Alice's MZ interferometer through Bob's MZ interferometer, we monitor the power at one of the outputs of Bob's interferometer with a single-photon InGaAs/InP avalanche photodiode (APD). The feedback is implemented by using a phase shifter inside Bob's MZ interferometer, as shown in Fig. 2(c).

The performance of QKD systems is determined to a great extent by the quality of single-photon detectors, mainly in two aspects—efficiency and noise. In comparison to the conventional QKD, MDI QKD requires twofold coincidence detection instead of single-fold click. Then, the channel transmittance, and hence the key rate, has quadratic dependence on the detector efficiency. Thus, high-efficiency single-photon detectors are required for MDI QKD. Under room temperature, an up-conversion single-photon detector can provide the highest quantum efficiency in a telecom band. However, its dark count used to be more than 100 kHz, which limits its application in QKD. Here, we utilize long-wave pump technology [28] to suppress detector dark counts by 2 orders of magnitude. In our setup, the signal photon is mixed with a strong pump at 1940 nm in a wavelength division multiplexing (WDM) coupler and is sent to a fiber-pigtailed periodically poled lithium niobate (PPLN) waveguide, where the pump and signal interact via the sum-frequency generation process, as shown in Fig. 2(b). The PPLN waveguide is a 52-mm-long reverse-proton-exchange waveguide with a poling period of 19.6 μm. A Peltier cooler-based temperature-control system is used to keep the waveguide's temperature at 30 °C to maintain the phase-matching condition. We observe a maximum depletion of a 1550 nm input signal of 99%, with a total internal conversion efficiency around 85% limited by the waveguide propagation losses. The generated 862 nm photons are collected by an antireflection-coated objective lens and are separated from the pump and spurious light using a combination of a short pass filter, a dichroic mirror, a prism, and a spatial filter. The light is then focused onto a commercial silicon (Si) APD with a detection efficiency of 40% at this wavelength. Using a pump power of 200 mW, the total-system detection efficiency is 20%, with a dark count rate of approximately 1 kHz, which can meet the stringent requirements for MDI QKD.

At the measurement site, Eve announces the detection events when two detectors click in two different time bins. Alice and Bob postselect their key bits as the raw data according to Eve's announcement. To extract the final secure key out of the raw data, we follow the postprocessing procedure presented in the Supplemental Material [27]. When Alice and Bob, respectively, use the average photon numbers μ and ν, the key rate is given by the standard decoy-state formula [19,24]

$$R \geq Q_{11}[1 - H(e_{11})] - I_{\mathrm{EC}}, \qquad I_{\mathrm{EC}} = Q_{\mu\nu} f H(E_{\mu\nu}), \tag{1}$$

where I_{EC} is the cost of error correction, depending on the overall gain ($Q_{\mu\nu}$) and error rate ($E_{\mu\nu}$), f is the error correction efficiency (instead of implementing error correction, we estimate the key rate by taking $f = 1.16$, which can be realized by the low-density parity-check code), $H(e) = -e\log_2(e) - (1-e)\log_2(1-e)$ is the binary Shannon entropy function, and Q_{11} (e_{11}) is the gain (phase error rate) when both sources generate single-photon states.

In the experiment, we run our MDI QKD system for 59.5 h. Figure 3(a) shows the sifted key bits and error rates in the Z and X bases with different average photon numbers. From Fig. 3(a), one can see that the error rates in the Z basis $E_{\mu\nu}$ are less than 0.5%, when the intensities μ and ν are not 0. With the error rates (of decoy and signal states) in the X basis, we can upper bound the Z-basis phase error rate e_{11}, which is 24.6%. (For single-photon states, the bit error probability in the X basis is the same as the phase error probability in the Z basis.) Meanwhile, we lower bound the yield $Y_{11} \geq 1.77 \times 10^{-4}$ and hence the gain $Q_{11} = \mu\nu e^{-\mu-\nu} Y_{11}$ when both sources generate single-photon states in the Z basis. Then, we evaluate the final secure key rate by Eq. (1), as shown in Fig. 3(b), from which one can see that the main cost of the data postprocessing comes from the non-single-photon components and privacy amplification. Details of the key rate evaluation can found in the Supplemental Material [27].

The privacy amplification part is largely affected by the relatively small data size. Here, we have not considered the key cost in authentication, error verification, and efficiency of privacy amplification, which has been shown to be small, typically less than 1000 bits, in a practical system [29]. [Denote this key cost to be k_3, which is defined in Ref. [29]. Let us take an example to see the physical meaning of k_3. Suppose the size of the sifted key after error correction is 500 kbits and the privacy amplification ratio is 90% (after considering the statistical fluctuations). Then, the final key is 50 kbits minus the overhead from the authentication and the efficiency of privacy amplification. This overhead is defined as k_3. Strictly speaking, the final

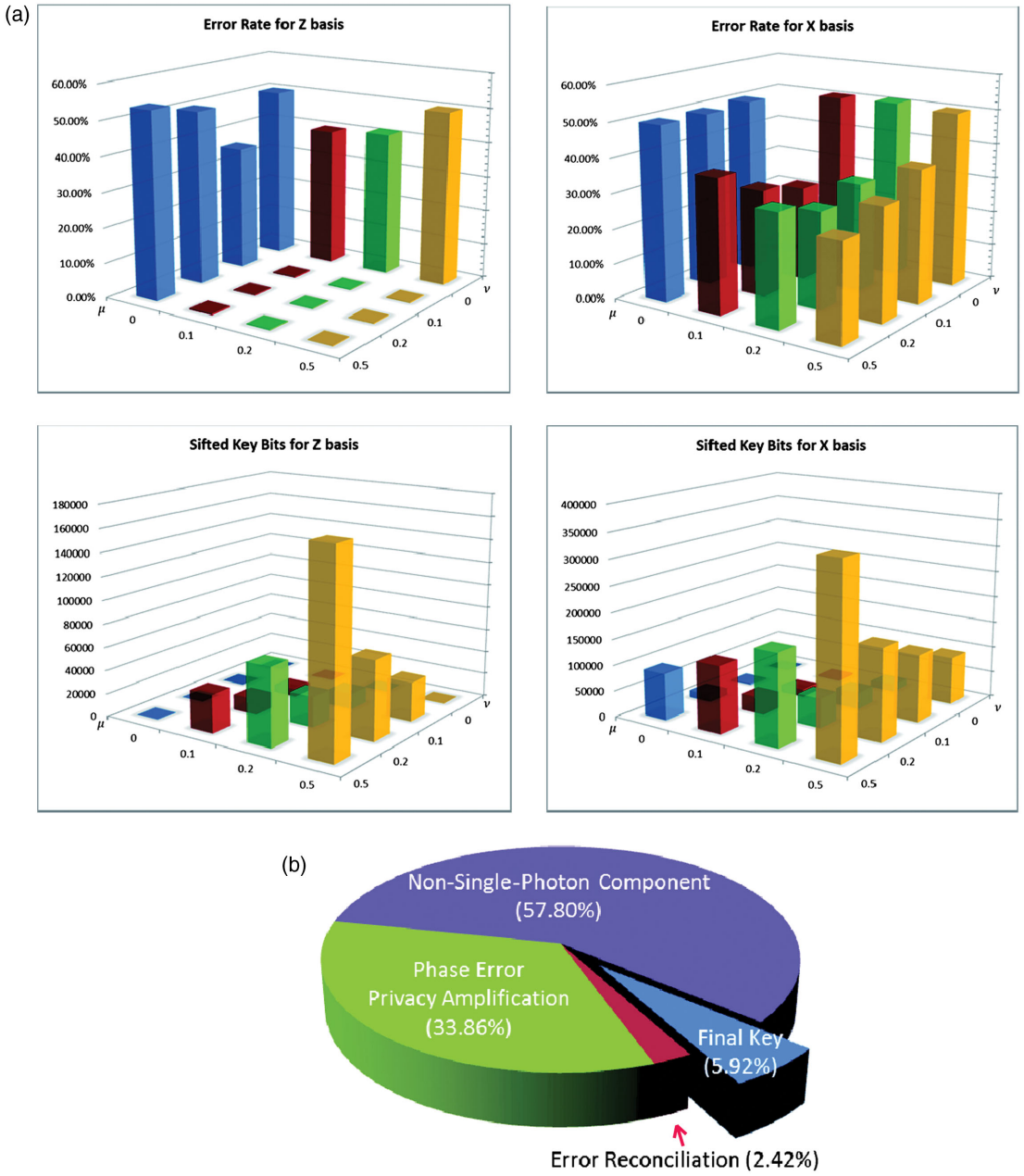

FIG. 3 (color online). (a) Sifted key rate and error rate with different average photon numbers 0, 0.1, 0.2, and 0.5 in both the Z and X bases. The data are collected by running the system for 59.5 h. The relative standard deviations of the data can be found in the Supplemental Material [27]. (b) Extracting a secure key from the raw data. In the data postprocessing, we assume 3 standard deviations for the statistical fluctuation analysis of the decoy-state method. A detailed analysis is given in the Supplemental Material [27].

key size should be $5 \times 10^4 - k_3$. As pointed out in Ref. [29], k_3 is small in a typical QKD system.] Finally, following the postprocessing scheme proposed in Ref. [30] that is summarized in the Supplemental Material [27], we obtain a secure key of 25 517 bits.

We remark that the internal modulation of laser pulses randomizes the phases of the decoy or signal states, which guarantees our system to be secure against the unambiguous-state-discrimination attack [31]. All the components in the source part, as shown in Fig. 2(a), are standard commercial optical devices, which have been properly calibrated. Thus, it is reasonable to assume the side channels on source are well shielded out.

The developed up-conversion single-photon detector with high efficiency and low noise in our experiment can find immediate application in fiber-based quantum technology, an optical time domain reflectometer, a photon-counting lidar, etc. Meanwhile, the technology of interfering two independent lasers, developed in our experiment, is also an essential building block of a quantum

repeater [32] in global quantum communication. Furthermore, the MDI QKD scheme can be extended into a quantum network with a starlike structure [20] conveniently, in which users only need photon sources but not detection systems. The expensive parts of the system, detectors, are only required at the service center, i.e., the measurement site.

The transmission distance and secure key rate can be significantly improved by increasing the repetition rate [30], which is mainly limited by the detector timing jitter. Our up-conversion detector can be run under a clock rate of 2 GHz [33], with which the transmission distance can go beyond 250 km and the secure key rate can be more than 1 kbps at a distance of 100 km.

The authors would like to thank Y.-A. Chen, M. Curty, H.-K. Lo, B. Qi, Q.-C. Sun, Y.-L. Tang, and B. Zhao for enlightening discussions, especially C.-H. F. Fung for his useful discussions and comments on the key rate analysis. This work has been supported by the National Fundamental Research Program, the National Natural Science Foundation of China, the Chinese Academy of Science, and the Shandong Institute of Quantum Science and Technology Co., Ltd. Y. L. and T.-Y. C. contributed equally to this work.

Note added in proof.—We note that related experimental work has been reported in Ref. [25].

*xma@tsinghua.edu.cn
†qiangzh@ustc.edu.cn
‡pan@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001).
[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[7] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).
[8] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).
[9] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 073 (2007).
[11] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[12] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[14] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[15] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[16] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).
[17] D. Mayers and A. Yao, in *Proceedings of the FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, CA, 1998), p. 503.
[18] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
[19] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[20] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[21] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[22] H. Inamori, Algorithmica **34**, 340 (2002).
[23] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[24] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); X. Wang, Phys. Rev. Lett. **94**, 230503 (2005); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[25] A. Rubenok, J. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[26] T. da Silva, D. Vitoreti, G. Xavier, G. Temporão, and J. von der Weid, arXiv:1207.6345.
[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.130502 for details of the key rate evaluation.
[28] J. Pelc, L. Ma, C. Phillips, Q. Zhang, C. Langrock, O. Slattery, X. Tang, and M. Fejer, Opt. Express **19**, 21 445 (2011).
[29] X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. Chau, Computers and Security **30**, 172 (2011).
[30] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[31] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 0431 (2007).
[32] B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, Phys. Rev. Lett. **98**, 240502 (2007).
[33] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 13 073 (2006).