Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution

Zhiyuan Tang,* Zhongfa Liao, Feihu Xu, Bing Qi,† Li Qian, and Hoi-Kwong Lo
Centre for Quantum Information and Quantum Control,
Department of Physics and Department of Electrical and Computer Engineering,
University of Toronto, Toronto, Ontario, Canada M5S 3G4
(Received 15 January 2014; published 14 May 2014)

We demonstrate the first implementation of polarization encoding measurement-device-independent quantum key distribution (MDI-QKD), which is immune to all detector side-channel attacks. Active phase randomization of each individual pulse is implemented to protect against attacks on imperfect sources. By optimizing the parameters in the decoy state protocol, we show that it is feasible to implement polarization encoding MDI-QKD with commercial off-the-shelf devices. A rigorous finite key analysis is applied to estimate the secure key rate. Our work paves the way for the realization of a MDI-QKD network, in which the users only need compact and low-cost state-preparation devices and can share complicated and expensive detectors provided by an untrusted network server.

DOI: 10.1103/PhysRevLett.112.190503 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex

Quantum key distribution (QKD) allows two parties, normally referred to as Alice and Bob, to generate a private key even in the presence of an eavesdropper, Eve [1]. With perfect single photon sources and perfect single photon detectors, the security of QKD is guaranteed by quantum mechanics. However, such perfect devices are not available today and the security of QKD cannot be guaranteed in a real life implementation. For example, attenuated coherent laser pulses are commonly used in practical QKD setups, which makes the QKD system vulnerable to a photon-number-splitting attack. Fortunately, it has been shown that the unconditional security of QKD can still be assured with phase randomized weak coherent pulses [2]. Furthermore, by applying decoy state techniques [3], secure key rates can be dramatically increased in practical implementations [4]. Nonetheless, other imperfections in practical QKD systems still present loopholes that can be exploited by Eve to steal the secret key [5,6]. We remark that most of the identified security loopholes are due to imperfections in detection systems [5].

Much effort has been put towards building loophole-free QKD systems with practical devices. Nonetheless, existing approaches such as security patches [7] and device-independent QKD (DI-QKD) [8] are either *ad hoc* or are impractical with current technology due to their extremely low key rates [9].

Fortunately, measurement-device-independent QKD (MDI-QKD), which removes all loopholes in detectors [10], has been proposed as an alternative solution. Although in MDI-QKD, the assumption of almost-perfect state preparation cannot be removed, finite basis-dependent flaws can be tolerated and taken care of [11] using the quantum coin idea [2]. A typical (polarization encoding) MDI-QKD setup is illustrated in Fig. 1.

Proof-of-principle demonstrations of MDI-QKD with time-bin encoding [12] and polarization encoding [13] have been reported. In these two demonstrations, two-photon interference between two independent sources over long optical fibers were demonstrated, bringing the practical application of MDI-QKD a step closer. However, these two demonstrations did not really distribute random key bits between two parties, and thus were not full MDI-QKD demonstrations. Additionally, phase randomization of weak coherent pulses [14], a crucial assumption in the security proofs of decoy state QKD [3], was neglected in these two demonstrations, leaving the systems vulnerable to attacks on the weak coherent sources [15]. A full demonstration of time-bin phase encoding MDI-QKD was reported in Ref. [16].

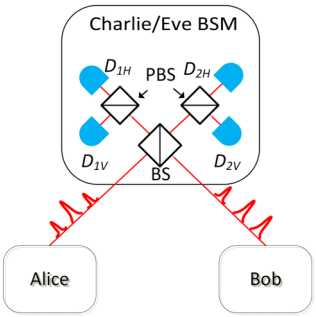


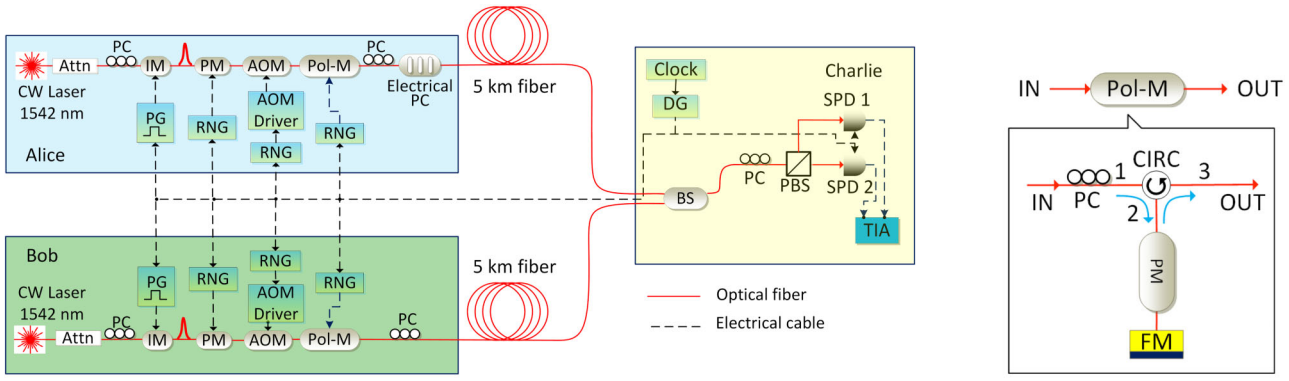
FIG. 1 (Color online) (color online). A typical MDI-QKD setup. Alice and Bob send out polarization encoded weak coherent pulses (with decoy states) to Charlie or Eve, who is supposed to perform partial Bell state measurements (BSMs) and broadcast the BSM results to Alice and Bob. A partial BSM can be realized using a beam splitter (BS), polarizing beam splitters (PBSs), and single photon detectors.

Despite the above demonstrations showing that MDI-QKD is a promising solution to the security problems of practical QKD, there are a few questions to be answered regarding the practical implementation of MDI-QKD. First, the only full demonstration of MDI-QKD in Ref. [16] utilized expensive and specialized up-conversion single photon detectors, which are currently only available to a handful of research groups and not yet commercially available. This has raised some concerns on the practicality of MDI-QKD [17]. Second, a full demonstration of polarization encoding MDI-QKD with rigorous finite-key analysis is still missing. While phase or time-bin encoding is preferred in the conventional BB84 protocol to avoid the problem of random birefringence fluctuations in optical fibers, polarization management is still required in time-bin encoding MDI-QKD in order to maintain polarization indistinguishability [12,16]. On the other hand, it is easier to implement polarization encoding as it does not require maintaining interferometric stability that would be necessary in time-bin encoding. Therefore polarization encoding may be more favourable when implementing MDI-QKD in a network setting in the future, as it can simplify setups of the end users. Polarization encoding is also a common choice in free-space QKD, especially ground-to-satellite QKD.

In this Letter, we report an experimental demonstration of polarization encoding MDI-QKD with active phase randomization over 10 km of a telecom single-mode fiber. Key bits, bases, and pulse intensities are randomly chosen as required in a true QKD demonstration, and a rigorous finite key analysis is performed to evaluate the key rate. Experimental parameters (intensities and probability distributions of signal and decoy states) are optimized numerically. Our demonstration employs only standard off-the-shelf components, implying that MDI-QKD is compatible with today's technology. We also present a systematic method to align polarization reference frames between two separate parties, which is challenging in a fiber-based QKD system.

We implement MDI-QKD with two decoy states over 10 km of telecommunication fiber. We perform a numerical simulation to optimize the performance [18]: average photon numbers are chosen to be $\mu = 0.3$ for the signal state, $\nu = 0.1$ and $\omega = 0.01$ for the two decoy states; the ratio of the numbers of pulses sent out with intensities μ, ν, and ω is set to be $4:9:7$. Details of the numerical simulation and optimization can be found in the Supplemental Material [19]. Active phase randomization is implemented to defend against attacks on the imperfect weak coherent sources.

Figure 2(a) shows the schematic of our polarization encoding MDI-QKD experiment. Alice and Bob each possess a cw frequency-locked laser (Clarity-NLL-1542-HP, wavelength ~1542 nm). The laser light is attenuated and modulated by a $LiNbO_3$ intensity modulator (IM) to generate weak coherent pulses at a repetition rate of 500 kHz. The global phase of each pulse is modulated by a phase modulator (PM), which is driven by a 12-bit arbitrary waveform generator (labelled as RNG) that outputs random voltages uniformly distributed between 0 and $2V_\pi$. Therefore, the phase of each pulse is randomized in the range of $[0, 2\pi]$. To implement the decoy state protocol, intensities of the pulses are randomly modulated by an acousto-optic modulator (AOM) to generate signal and decoy states.



(a) (b)

FIG. 2 (Color online) (color online). (a) Experimental setup of polarization encoding MDI-QKD. Alice and Bob prepare phase randomized weak coherent pulses with attenuators (Attn), intensity modulators (IM) and phase modulators (PM). Decoy states are prepared by acousto-optic modulators (AOM) and key bits are encoded using polarization modulators (Pol-M). Pulses are sent to Charlie for Bell state measurements. A coincidence between two single photon detectors (SPDs) indicates a successful projection into the $|\psi^+\rangle$ state. Abbreviations of other components: PC, polarization controller; Electrical PC: electrical polarization controller; PG, electrical pulse generator; RNG, random number generator; DG, delay generator; BS, beam splitter; PBS, polarizing beam splitter; TIA, time interval analyzer. (b) Schematic of the polarization modulator: CIRC, optical circulator; PM, phase modulator; FM, Faraday mirror. See the text for details.

Key bits are encoded into polarization states of weak coherent pulses by a polarization modulator (Pol-M), whose design is proposed in Ref. [20]. The schematic of the polarization modulator, consisting of an optical circulator, a phase modulator, and a Faraday mirror, is shown in Fig. 2(b). Optical pulses are launched via the optical circulator into the phase modulator with polarization at 45° from the optical axis of the phase modulator's waveguide. By modulating the relative phase $\Delta\phi$ between the two principal modes of the waveguide, four BB84 polarization states can be generated: horizontal H ($\Delta\phi = 0$), vertical V ($\Delta\phi = \pi$), left-hand circular L ($\Delta\phi = \pi/2$), and right-hand circular R ($\Delta\phi = -\pi/2$). The first two form the rectilinear (Z) basis and the latter two form the circular (X) basis. Polarization mode dispersion and temperature-induced variation of polarization states inside the Pol-M setup can be compensated when pulses are reflected by a Faraday mirror with a 90° rotation in polarization, thus achieving stable polarization modulation.

Alice and Bob need to have a shared polarization reference frame. They first use polarization controllers to align their rectilinear polarization states to the polarizing axes of Charlie's polarizing beam splitter. Alice's horizontal polarization state is also aligned to either the fast or slow axis of a fiber squeezer in the electrical polarization controller. A dc voltage is applied on this squeezer to change the phase retardation between the fast and slow components. This is equivalent to a unitary transformation where Alice's rectilinear polarization states remain unchanged, while the circular polarization states are rotated about the H-V axis on the Poincaré sphere. The voltage is adjusted such that their circular bases are aligned.

The misalignment is around 1% in our experiment. The polarization can remain stable for more than one hour, and is realigned every hour during the experiment. More details of the polarization alignment and stability are given in the Supplemental Material [19].

All the PMs, AOMs, and Pol-Ms are independently driven by random number generators (function generators with prestored random numbers [21] generated by a quantum random number generator [22]). An electrical delay generator (DG) located in Charlie's setup synchronizes all the RNGs and the electrical pulse generators (PGs) driving the IMs. A synchronization clock signal can be sent through the fiber using wavelength division multiplexing [23] in future field implementations of MDI-QKD.

In this experiment, it is critical to assure that the weak coherent pulses independently prepared by Alice and Bob are indistinguishable at Charlie's beam splitter in terms of spectrum and arrival time. We solve this problem by using two frequency-stabilized lasers, whose wavelengths are independently locked to the P16 line of a C13 acetylene gas cell (integrated in each laser by the manufacturer) at around 1542.38 nm. This guarantees the frequency difference between Alice's laser and Bob's laser is within 10 MHz, while the temporal width of the pulse is about 1 ns (FWHM), corresponding to a bandwidth of about 1 GHz. Note that frequency locking to other telecom wavelengths is feasible: absorption lines of hydrogen cyanide cover the entire C band from 1530 to 1560 nm [24], and absorption lines of carbon monoxide covers the L band from 1560 to 1630 nm [25]. The arrival time of the pulses can be independently controlled by the DG with a resolution of 50 ps, and the timing jitter of the electronic devices is about 100 ps (rms). Therefore, we can guarantee that the two independently prepared pulses have sufficient overlap in both time and spectrum.

Alice and Bob send their pulses through a 5 km fiber spool to Charlie, who performs Bell state measurements on the incoming pulses. Charlie's measurement setup consists of a 50:50 beam splitter (BS), a polarizing beam splitter (PBS), and two commercial InGaAs/InP single photon detectors (SPDs, detection efficiency ~10%, dead time = 25 μs, dark count probability per gate $\sim 5 \times 10^{-5}$). Because of the limited number of available detectors, we choose to detect photons at the outputs of one PBS only. A coincidence between these two detectors (defined as when both SPDs click within 10 ns, measured by a time-interval analyzer, TIA) in this setup corresponds to a successful projection into the triplet state $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$.

A total number of $N = 1.69 \times 10^{11}$ pulses are sent out in the experiment. After that we perform key sifting, and measure gains and quantum bit error rates (QBERs) with different intensities in both bases from the sifted key. The results are listed in Tables I and II. In MDI-QKD with weak coherent pulses, measurements are taken in the rectilinear basis, so QBERs in the rectilinear and circular bases are asymmetric [10]. The QBERs in the rectilinear basis are due to misalignment of polarization in the system, and detectors' dark counts. In an ideal case with no misalignment and dark counts, $E^Z = 0$. Therefore, small QBERs should be expected as long as polarizations are aligned properly. On the other hand, due to multi-photon components in weak coherent pulses, the QBERs in the circular basis are higher. An erroneous projection onto the Bell state

TABLE I. Experimental values of gains $Q^W_{I_A I_B}$ ($\times 10^{-4}$) with intensities I_A and I_B in basis $W \in \{X, Z\}$. Errors shown represent 3 standard deviations.

	Rectilinear (Z) basis			Circular (X) basis		
	I_A					
I_B	μ	ν	ω	μ	ν	ω
μ	0.466 ±0.005	0.160 ±0.002	0.0225 ±0.0008	0.903 ±0.006	0.410 ±0.003	0.254 ±0.003
ν	0.155 ±0.002	0.0531 ±0.0008	0.0070 ±0.0003	0.397 ±0.003	0.102 ±0.001	0.0312 ±0.0007
ω	0.0214 ±0.0008	0.0067 ±0.0003	0.0009 ±0.0001	0.246 ±0.003	0.0317 ±0.0007	0.0014 ±0.0001

TABLE II. Experimental values of QBERs $E^W_{I_A I_B}$ with intensities I_A and I_B in basis $W \in \{X, Z\}$. Errors shown represent 3 standard deviations.

	Rectilinear (Z) basis			Circular (X) basis		
	I_A					
I_B	μ	ν	ω	μ	ν	ω
μ	0.018 $\pm$0.001	0.032 $\pm$0.002	0.17 $\pm$0.01	0.262 $\pm$0.004	0.326 $\pm$0.005	0.465 $\pm$0.009
ν	0.031 $\pm$0.002	0.040 $\pm$0.003	0.16 $\pm$0.02	0.322 $\pm$0.005	0.261 $\pm$0.006	0.43 $\pm$0.02
ω	0.16 $\pm$0.01	0.16 $\pm$0.02	0.23 $\pm$0.07	0.469 $\pm$0.009	0.43 $\pm$0.02	0.32 $\pm$0.07

can occur if one user sends out a vacuum pulse and the other sends out a pulse of two photons. In this case, a successful projection onto the Bell state does not generate any correlated key bit between Alice and Bob. A QBER of 25% in the circular basis is expected, even if there is no misalignment or dark counts.

A lower bound of the secure key rate is given by [10]

$$R \geq q\{p_{11} Y_{11}^{Z,L}[1 - H(e_{11}^{X,U})] - Q_{\mu\mu}^{Z} f(E_{\mu\mu}^{Z}) H(E_{\mu\mu}^{Z})\}, \quad (1)$$

where q is the probability that both Alice and Bob send out signal states in the Z basis; $p_{11} = \mu^2 e^{-2\mu}$ is the conditional probability that both Alice and Bob send out single photon states given that they both send out signal states; $f(E_{\mu\mu}^{Z}) > 1$ is the efficiency of error correction; $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy; the gain $Q_{\mu\mu}^{Z}$ and QBER $E_{\mu\mu}^{Z}$ are measured directly from the sifted key and given in Tables I and II; $Y_{11}^{Z,L}$ is a lower bound of the yield of single photon states in the Z basis, and $e_{11}^{X,U}$ is an upper bound of the QBER of single photon states in the X basis. Both $Y_{11}^{Z,L}$ and $e_{11}^{X,U}$ are estimated using an analytical method with two decoy states [18]. We take the finite key effect [26] into account when estimating $Y_{11}^{Z,L}$ and $e_{11}^{X,U}$: considering 3 standard deviations, we find a lower bound of the yield $Y_{11}^{Z,L} = 4.1 \times 10^{-4}$ and an upper bound of the QBER $e_{11}^{X,U} = 15.1\%$. Table III summarizes parameters used for key rate estimation. We can estimate that a secure key of length $L = NR = 1600$ bits can be extracted.

The large phase error rate e_{11}^{X} and low key rate is mostly due to the relatively small data size and therefore large statistical fluctuations in gains and QBERs shown in Tables I and II. Furthermore, a relatively large portion of the pulses are sent as decoy states and only 1% are pulses that both Alice and Bob send out as signal states in the rectilinear basis that can be used for key generation.

TABLE III. Parameters used to estimate the secure key rate.

q	p_{11}	$Y_{11}^{Z,L}$	$e_{11}^{X,U}$	$Q_{\mu\mu}^{Z}$	$E_{\mu\mu}^{Z}$	f
0.011	0.0494	4.1×10^{-4}	0.151	4.66×10^{-5}	0.018	1.16

The key generation rate can be substantially improved by increasing the repetition rate: first, more pulses can be sent out in a reasonable time frame, leading to tighter bounds in estimating Y_{11}^{Z} and e_{11}^{X}; second, given a large data size, we can reduce the portion of pulses sent as decoy states and more pulses can be sent out in signal states for key generation. The speed of our system is limited by the performance of our SPDs. Our simulation [27] shows that, with commercial single photon detectors gating up to 100 MHz, the key rate (with the finite key effect taken into consideration) can be up to 1 kbps over 50 km of optical fiber; moreover, by using state-of-the-art superconducting single photon detectors with over 90% quantum efficiency [28], the key rate can be as high as 100 kbps. Futhermore, by using four detectors rather than two, we can get at least a fourfold increase in the key rate. With a larger data size, more standard deviations can also be applied in the statistical analysis, therefore a tighter security bound can be achieved.

In summary, we have demonstrated the first polarization encoding MDI-QKD experiment over 10 km of optical fiber, with active phase randomization implemented to defeat attacks on imperfect sources. Our work shows that, with commercial off-the-shelf optoelectronic devices, it is feasible to build a QKD system immune to detector side-channel attacks. Our demonstration is a promising result towards the realization of a detector side-channel-free QKD network, in which users only need to possess handy hardware to prepare polarization qubits. Our work can also be extended to free space polarization encoding MDI-QKD with an untrusted satellite in the future.

We thank W. Cui and M. Curty for enlightening discussions, H. Xu for his assistance in the experiment, and V. Burenkov for his comments in the presentation of this Letter. Financial support from NSERC Discovery Grant, NSERC RTI Grant, and Canada Research Chairs Program is gratefully acknowledged.

*ztang@physics.utoronto.ca
†Present address: Quantum Information Science Group, Computational Sciences and Engineerng Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee, 37831-6418, USA.

[1] C. H. Bennett and G. Brassard, in *IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, Banglore, India, 1984) pp. 175–179; A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[2] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[3] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[4] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); D. Rosenberg, J. Harrington, P. Rice, P. Hiskett, C. Peterson, R. Hughes, A. Lita, S. Nam, and J. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007); C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).

[5] Y. Zhao, C.-H. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010); I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011); N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011); H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).

[6] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[7] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Opt. Express **20**, 18911 (2012); Z. Yuan, J. Dynes, and A. Shields, Nat. Photonics **4**, 800 (2010).

[8] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (IEEE, Washington, DC, 1998) p. 503; A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[9] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

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

[11] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).

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

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

[14] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).

[15] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[16] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).

[17] J. Cartwright, Science News, "Quantum Cryptography is Safe Again," August 2013, http://news.sciencemag.org/physics/2013/08/quantum-cryptography-safe-again. In this news, Grégoire Ribordy, CEO of ID Quantique, a company that makes commercial QKD systems, says, "The short answer is that it (MDI-QKD) is very interesting, although it is not yet mature enough to implement, from a practical point of view."

[18] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).

[19] See Supplemental Material http://link.aps.org/supplemental/10.1103/PhysRevLett.112.190503 for details on polarization alignment and stability, two photon interference, finite-key analysis, and numerical simulation, which includes Ref. [29].

[20] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, New J. Phys. **11**, 095001 (2009).

[21] For perfect security, a new set of random numbers should be loaded on to the function generator when the prestored random numbers are used up. Because the on-board memories of the function generators are finite, and it is time consuming to load random numbers onto the function generator, the random numbers are reused and updated every one hour. However, the random pattern loaded on each function generator is unique and independent.

[22] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).

[23] A. Tanaka *et al.*, Opt. Express **16**, 11354 (2008).

[24] W. C. Swann and S. L. Gilbert, J. Opt. Soc. Am. B **22**, 1749 (2005).

[25] W. C. Swann and S. L. Gilbert, J. Opt. Soc. Am. B **19**, 2461 (2002).

[26] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[27] M. Curty *et al.*, arXiv:1307.1081.

[28] F. Marsili *et al.*, Nat. Photonics **7**, 210 (2013).

[29] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).