Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks

A. Rubenok,[1,2] J. A. Slater,[1,2] P. Chan,[1,3] I. Lucio-Martinez,[1,2] and W. Tittel[1,2]

[1]*Institute for Quantum Science and Technology, University of Calgary, Calgary, Alberta T2N 1N4, Canada*
[2]*Department of Physics and Astronomy, University of Calgary, Calgary, Alberta T2N 1N4, Canada*
[3]*Department of Electrical and Computer Engineering, University of Calgary, Calgary, Alberta T2N 1N4, Canada*

(Received 9 April 2013; published 23 September 2013)

Several vulnerabilities of single-photon detectors have recently been exploited to compromise the security of quantum-key-distribution (QKD) systems. In this Letter, we report the first proof-of-principle implementation of a new quantum-key-distribution protocol that is immune to any such attack. More precisely, we demonstrated this new approach to QKD in the laboratory over more than 80 km of spooled fiber, as well as across different locations within the city of Calgary. The robustness of our fiber-based implementation, together with the enhanced level of security offered by the protocol, confirms QKD as a realistic technology for safeguarding secrets in transmission. Furthermore, our demonstration establishes the feasibility of controlled two-photon interference in a real-world environment and thereby removes a remaining obstacle to realizing future applications of quantum communication, such as quantum repeaters and, more generally, quantum networks.

DOI: 10.1103/PhysRevLett.111.130501 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Dv, 42.50.Ex

Quantum key distribution (QKD) promises the distribution of cryptographic keys whose secrecy is guaranteed by fundamental laws of quantum physics [1,2]. Starting with its invention in 1984 [3], theoretical and experimental QKD have progressed rapidly. Information theoretic security, which ensures that secret keys can be distributed even if the eavesdropper Eve is only bounded by the laws of quantum physics, has been proven under various assumptions about the devices of the legitimate QKD users Alice and Bob [4,5]. Furthermore, experimental demonstrations employing quantum states of light have meanwhile resulted in key distribution over more than 100 km distance through optical fiber [6] or air [7], QKD networks employing trusted nodes [8], as well as in commercially available products [9].

However, it became rapidly clear that some of the assumptions made in QKD proofs were difficult to meet in real implementations, which opened side channels for eavesdropping attacks. The most prominent examples are the use of quantum states encoded into attenuated laser pulses as opposed to single photons [10] and, more recently, various possibilities for an eavesdropper to remotely control or monitor single-photon detectors [11–14]. Fortunately, both side channels can be removed using appropriately modified protocols. In the first case, randomly choosing between so-called signal or decoy states (quantum states encoded into attenuated laser pulses with different mean photon numbers) allows one to establish a secret key strictly from information conveyed by single photons emitted by the laser [15–17]. (We remind the reader that an attenuated laser pulse comprising on average μ photons contains exactly one photon with probability $P_1(\mu) = \mu e^{-\mu}$ [10].) Furthermore, the recently proposed measurement-device-independent (MDI) QKD protocol [18] (for closely related work, see Ref. [19]) additionally ensures that controlling or monitoring detectors, regardless of by what means, does not help the eavesdropper to gain information about the distributed key. Note that while the two most prominent side channels are removed by MDI-QKD, others remain open and have to be closed by means of appropriate experimental design (see the Supplemental Material [20]).

The MDI-QKD protocol is a clever time-reversed version of QKD based on the distribution and measurement of pairs of maximally entangled photons [21]: In the idealized version, Alice and Bob randomly and independently prepare single photons in one out of the four qubit states $|\psi\rangle_{A,B} \in [|0\rangle, |1\rangle, |+\rangle, |-\rangle]$, where $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$. The photons are then sent to Charlie, who performs a Bell-state measurement, i.e., projects the photons' joint state onto a maximally entangled Bell state [22]. Charlie then publicly announces the instances in which his measurement resulted in a projection onto $|\psi^-\rangle \equiv 2^{-1/2}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$ and, for these cases, Alice and Bob publicly disclose the bases (z, spanned by $|0\rangle$ and $|1\rangle$, or x, spanned by $|\pm\rangle$) used to prepare their photons. (They keep their choices of states secret.) Identifying quantum states with classical bits (e.g., $|0\rangle, |-\rangle \equiv 0$, and $|1\rangle, |+\rangle \equiv 1$) and keeping only events in which Charlie found $|\psi^-\rangle$ and they picked the same basis, Alice and Bob now establish anticorrelated key strings. (Note that a projection of two photons onto $|\psi^-\rangle$ indicates that the two photons, if prepared in the same basis, must have been in orthogonal states.) Bob then flips all his bits, thereby converting the anticorrelated strings into correlated ones. Next, the so-called x key is formed out

of all key bits for which Alice and Bob prepared their photons in the x basis; its error rate is used to bound the information an eavesdropper may have acquired during photon transmission. Furthermore, Alice and Bob form the z key out of those bits for which both picked the z basis. Finally, they perform error correction and privacy amplification [1,2] to the z key, which results in the secret key.

As in the entanglement-based protocol, the time-reversed version ensures that Eve cannot gain information by eavesdropping photons during transmission or by modifying the device that generates entanglement—either the source of photon pairs or the projective two-photon measurement, respectively—without leaving a trace [23,24]. Furthermore, the outstanding attribute of the MDI-QKD protocol is that it decorrelates detection events (here indicating a successful projection onto the $|\psi^-\rangle$ Bell state) from the values of the x- and z-key bits and hence the secret key bits. In other words, all side channels related to the detection setup, regardless of whether they are actively attacked or passively monitored, do not help Eve gain information about the secret key.

For two reasons, the described procedure is, unfortunately, difficult to implement, first of which is the lack of practical single-photon sources. However, it is possible to replace the true single photons by attenuated laser pulses of varying mean photon number (i.e., signal and decoy states, as introduced above) and to establish the secret key using information only from joint measurements at Charlie's that stem from Alice and Bob both sending single photons [25]. This procedure results in the same security against eavesdropping as the conceptually simpler one discussed above. The secret key rate S distilled from signal states is then given by [18]

$$S \geq Q_{11}^z[1 - h_2(e_{11}^x)] - Q_{\mu\sigma}^z f h_2(e_{\mu\sigma}^z), \qquad (1)$$

where $h_2(X)$ denotes the binary entropy function evaluated on X, and f describes the efficiency of error correction with respect to Shannon's noisy coding theorem. Furthermore, Q_{11}^z, e_{11}^x, $Q_{\mu\sigma}^z$, and $e_{\mu\sigma}^z$ are gains (Q, the probability of a projection onto $|\psi^-\rangle$ per emitted pair of pulses) and error rates (e, the ratio of erroneous to total projections onto $|\psi^-\rangle$) in either the x or z basis for Alice and Bob sending single photons (denoted by the subscript 11) or for pulses emitted by Alice and Bob with mean photon number μ and σ (denoted by the subscript $\mu\sigma$), respectively. While the latter are directly accessible from experimental data, the former have to be calculated using a decoy-state method [18,25] (see the Supplemental Material [20]).

The second issue that makes an implementation difficult is the necessity of a Bell-state measurement (BSM) [26], which is a crucial element for MDI-QKD as well as future quantum repeaters and networks. However, this two-photon interference measurement has not yet been demonstrated with photons that were generated by independent sources and have traveled through separate deployed fibers (i.e., fibers that feature independent changes of propagation times and polarization transformations). To implement the BSM, one requires that these photons be indistinguishable, i.e., arrive simultaneously within their respective coherence times, with equal polarization, and feature sufficient spectral overlap. Yet, due to time-varying properties of optical fibers in a real-world environment, significant changes to photons' indistinguishability can happen in less than a minute, as depicted in Fig. 1. Furthermore, the carrier frequencies of the signals generated at Alice's and Bob's generally vary. These instabilities make real-world Bell-state measurements without stabilization by means of active feedback impossible.

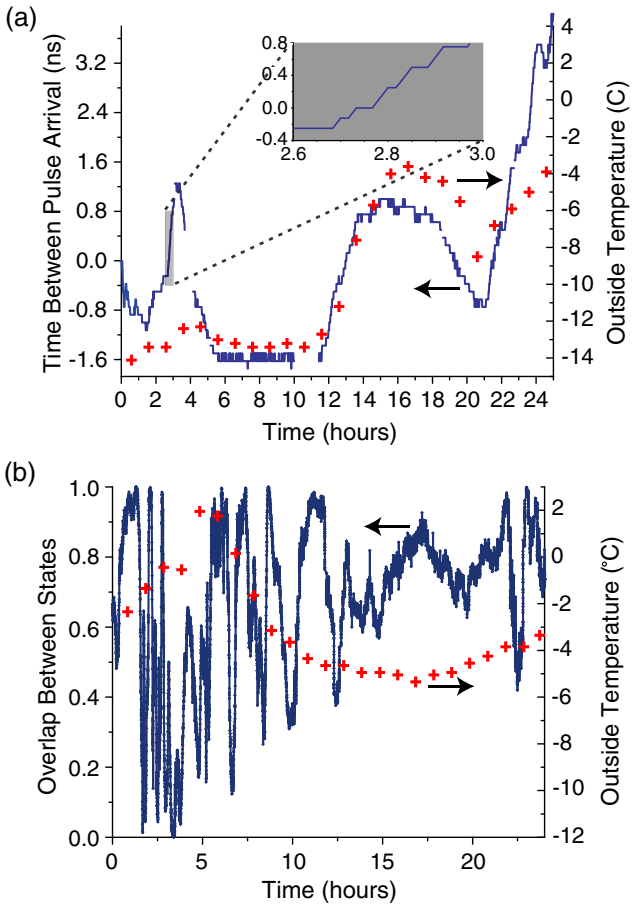

FIG. 1 (color online). (a) Drift of differential arrival time. Variation of the arrival time difference of attenuated laser pulses emitted at Alice's and Bob's after propagation to Charlie. (b) Variation in the overlap of the polarization states of originally horizontally polarized light (emitted by Alice and Bob) after propagation to Charlie. Both panels include temperature data (crosses), showing a correlation between variations of indistinguishability and temperature. In addition, despite local frequency locks, the difference between the frequencies of Alice's and Bob's lasers varied by up to 20 MHz per hour (not shown).

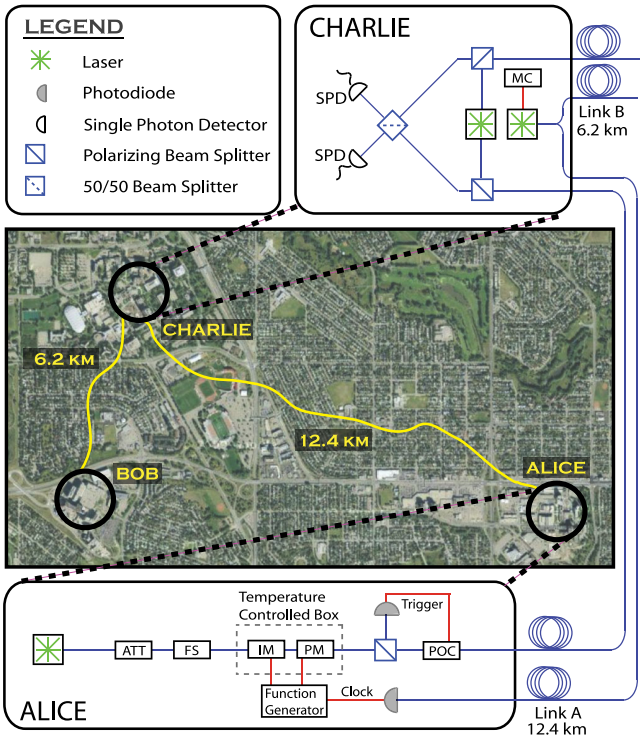

FIG. 2 (color online). Aerial view showing Alice (located at SAIT Polytechnic), Bob [located at the University of Calgary (U of C) Foothills campus] and Charlie (located at the U of C main campus). Also shown is the schematic of the experimental setup. Optically synchronized using a master clock (MC) at Charlie's, Alice and Bob (not shown; setup identical to Alice's) generated time-bin qubits at a 2 MHz rate encoded into Fourier-limited attenuated laser pulses using highly stable continuous-wave lasers at 1552.910 nm wavelength, temperature-stabilized intensity and phase modulators (IM and PM), and variable attenuators (ATT). The two temporal modes defining each time-bin qubit were of 500 ps (FWHM) duration and were separated by 1.4 ns. The qubits traveled through 12.4 and 6.2 km of deployed optical fibers to Charlie, where a 50/50 beam splitter followed by two gated (10 μs dead time) InGaAs single-photon detectors (SPD) allowed projecting the bipartite state onto the $|\psi^-\rangle$ Bell state. (This projection occurred if the two detectors indicate detections with a 1.4 ± 0.4 ns time difference.) The MC, the polarization controller (POC), and Alice's frequency shifter (FS) are used to maintain indistinguishability of the photons upon arrival at Charlie. These three feedback systems are detailed in the Supplemental Material [20]. The individual setups for measurements using spooled fiber (arrangement (i)) are identical.

Hence, to enable MDI-QKD and pave the way for quantum repeaters and quantum networks, we developed the ability to track and stabilize photon arrival times and polarization transformations as well as the frequency difference between Alice's and Bob's lasers during all measurements (for more information, see the Supplemental Material [20]). In order to ensure the indistinguishability of photons arriving at Charlie's and to allow, for the first time, Bell-state measurements in a real-world environment, we developed and implemented three stabilization systems (see Fig. 2): fully automatic polarization stabilization, manual adjustment of photon arrival time, and manual adjustment of laser frequency. Note that automating the frequency and timing stabilization systems is straightforward, particularly if the active control elements are placed in Charlie's setup.

We verified that we could indeed maintain the indistinguishability of the photons by frequently measuring the visibility V_{HOM} of the so-called Hong-Ou-Mandel dip [27] (a two-photon interference experiment that is closely related to a BSM). On average, we found $V_{\mathrm{HOM}} = 47\% \pm 1\%$, which is close to the maximum value of 50% for attenuated laser pulses with a Poissonian photon number distribution [28], and thereby confirm that real-world two-photon interference is possible.

To assess the feasibility of MDI-QKD, we implemented a proof-of-principle demonstration of MDI-QKD using the decoy-state protocol proposed by Wang [25]. This protocol requires that Alice and Bob choose between three different mean photon numbers: two nonzero values referred to as signal and decoy as well as vacuum. We performed our experiments over four different distances (henceforth referred to as setups) comprising two different arrangements (see Fig. 2): (i) Alice, Bob, and Charlie are located within the same lab, and Alice and Bob are connected to Charlie via separate spooled fibers of various lengths and loss. (ii) Alice, Bob, and Charlie are located in different locations within the city of Calgary, and Alice and Bob are connected to Charlie by deployed dark fibers of 12.4 and 6.2 km length, respectively. The fiber lengths and loss in each setup are listed in Table I.

For each setup, we prepared all four combinations of Alice and Bob picking a state from the z basis (i.e., $|\psi\rangle_{A,B} \in [|0\rangle, |1\rangle]$, where $|0\rangle$ and $|1\rangle$ denote time-bin

TABLE I. Length and loss (ℓ_A, l_A, ℓ_B, l_B) of the individual fiber links used to connect Alice and Charlie, and Charlie and Bob, respectively, for all tested setups. The table also lists the total length ℓ (not to be confused with l, which denotes loss) and total loss $l = l_A + l_B$ (in dB). The last line details measurements outside the laboratory with deployed fiber.

Setup	Fiber	ℓ_A (km)	l_A (dB)	ℓ_B (km)	l_B (dB)	Total length ℓ (km)	Total loss l (dB)
i(a)	Spool	22.85	4.6	22.55	4.5	45.40	9.1
i(b)	Spool	30.98	6.8	34.65	6.9	65.63	13.7
i(c)	Spool	40.80	9.1	40.77	9.1	81.57	18.2
ii	Deployed	12.4	4.5	6.2	4.5	18.6	9.0

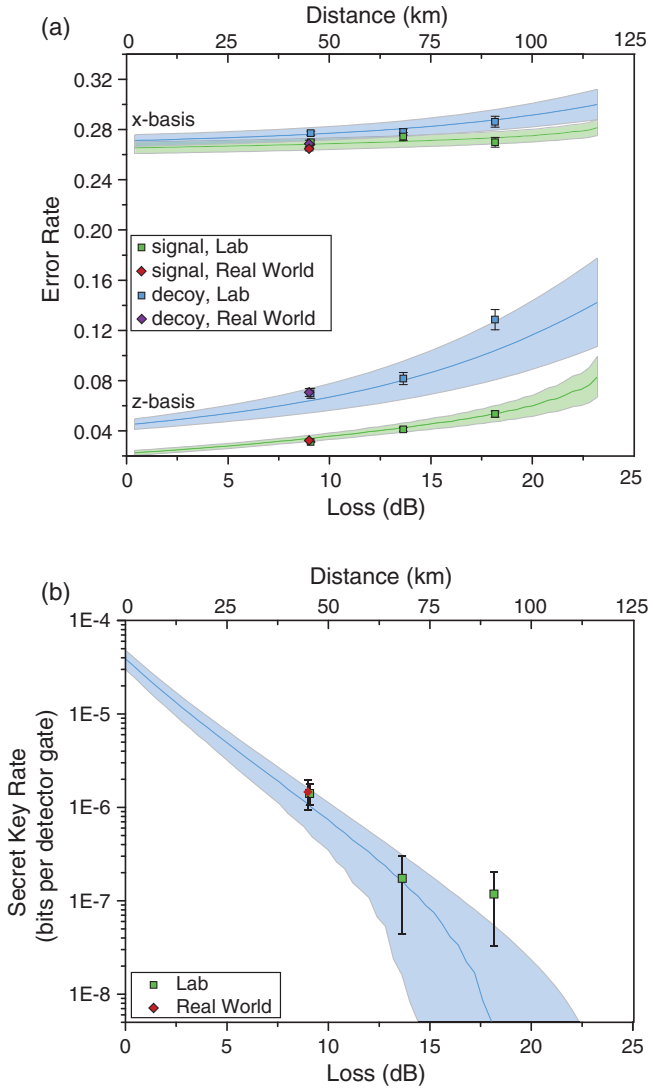

FIG. 3 (color). (a) Measured error rates $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$ for Alice and Bob, either both using signal intensity or both using decoy intensity as a function of total loss $l = l_A + l_B$ (in dB). We note that every other combination of intensities used in the decoy-state analysis requires Alice or Bob (or both) sending vacuum, and thus the error rate is 50% and not plotted. (b) Experimentally obtained and simulated secret key rates as a function of total loss $l = l_A + l_B$ (in dB), with $l_A \cong l_B$, for optimized mean photon numbers. Experimental secret key rates are directly calculated from measured gains and error rates using the decoy-state method [25] (see the Supplemental Material [20] for details). In both panels, the secondary x axis shows distance, assuming a loss of 0.2 dB/km. Diamonds depict results obtained using deployed fibers [see Fig. 2(a)]; all other data were obtained using fiber on spools. Uncertainties (1 standard deviation) were calculated for all measured points, assuming Poissonian detection statistics. We stress that the simulated values, computed using our model [29], do not stem from fits but are based on parameters that have been established through independent measurements. Monte Carlo simulations using uncertainties in these measurements lead to predicted bands as opposed to lines (for more details, see the Supplemental Material [20]).

qubits [22] prepared in an early or late temporal mode) and all four combinations of picking a state from the x basis (i.e., $|\psi\rangle_{A,B} \in [|+\rangle, |-\rangle]$). Measuring all four combinations is necessary to assess the error rates in each basis. Using a detailed model of our MDI-QKD system [29], we calculated the signal and decoy intensities that maximize the secret key rate produced by the decoy-state method for each setup. For our decoy intensity, we generated attenuated laser pulses containing on average $\mu = \sigma = 0.050 \pm 0.001$ photons, and for our signal intensities, we used a mean photon number between 0.25 and 0.5 (the optimal value depends on loss—see the Supplemental Materials [20]). For each of the four distance configurations listed in Table I and for each of the 16 pairs of qubit states, we performed measurements of all nine combinations of Alice and Bob using the signal, decoy, or vacuum intensity. We recorded the number of joint detections in which one detector indicated an early arriving photon (or an early noise count) and the other detector indicated a late arriving photon (or a late noise count), which, for time-bin qubits, is regarded as a projection onto the $|\psi^-\rangle$ state [22]. Depending on the observed detection rates, measurements took between 2 and 35 min. These data yield the gains $Q^z_{\mu\sigma}$ and $Q^x_{\mu\sigma}$ and error rates $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$, a subset of which is plotted in Fig. 3(a). A complete list of gains and error rates is presented in the Supplemental Material [20].

We then computed secret key rates according to Eq. (1) after extracting Q^z_{11} and e^x_{11} using Wang's decoy-state calculation [25] and assuming an error correction efficiency $f = 1.14$ [8]. As shown in Fig. 3(b), all our measurements, both outside and inside the laboratory, and using up to 80 km of spooled fiber between Alice and Bob, output a positive secret key rate. While the secret key rate is currently on the order of 1 Hz, detectors with higher trigger rates [30] and efficiency [31] exist and allow increasing the key rates by several orders of magnitude. Furthermore, using our model [29], we estimate that our setup allows secret key distribution up to a total loss of 18 ± 4.8 dB, which is in agreement with our QKD results. Assuming the standard loss coefficient for telecommunication fibers without splices of 0.2 dB/km, this value corresponds to a maximum distance between Alice and Bob of 90 ± 24 km. Note that moving from our proof-of-principle demonstration to the actual distribution of secret keys requires additional developments, which are detailed in the Supplemental Material [20].

In summary, our proof-of-principle experiment has demonstrated that real-world quantum key distribution with practical attenuated laser pulses and immunity to detector hacking attacks is possible using current technology. Our setup contains only standard, off-the-shelf components, its development into a complete QKD system follows well-known steps [8], and the extension to higher key rates using state-of-the-art detectors [30,31] is straightforward. We also point out that MDI-QKD is well suited for key

distribution over long distances, and we expect that further developments, such as using state-of-the-art detectors, will rapidly push the separation between Alice and Bob beyond 250 km [29]—its current maximum [6]. Finally, we remind the reader that the demonstrated possibility for Bell-state measurements in a real-world environment and with truly independent photons also removes a remaining obstacle to building a quantum repeater, which promises quantum communication such as QKD over arbitrary distances.

The authors thank E. Saglamyurek, V. Kiselyov and TeraXion for discussions and technical support, the University of Calgary's Infrastructure Services for providing access to the fiber link between the University's main campus and the Foothills campus, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates Technology Futures), CFI, AAET and the Killam Trusts.

Note added.—We note that related experimental work has been reported in Refs. [32,33] and, very recently, in Ref. [34].

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] C. H. Bennett and G. Brassard, *Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, 1984*, (IEEE, New York, 1984), p. 175.
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[6] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
[7] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, Th. Scheidl, J. Perdigues, Z. Sodnik, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).
[8] M. Sasaki *et al.*, Opt. Express **19**, 10 387 (2011).
[9] http://www.idquantique.com; http://www.magiqtech.com.
[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[11] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (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] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27 938 (2010).
[15] W. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[16] X. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[17] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[18] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[19] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.130501 for raw data, information on the stabilization systems, the decoy-state analysis, and a discussion on the requirements for QKD.
[21] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[22] W. Tittel and G. Weihs, Quantum Inf. Comput. **1**, 3 (2001).
[23] E. Biham, B. Huttner, and T. Mor, Phys. Rev. Lett. **54**, 2651 (1996).
[24] H. Inamori, Algorithmica **34**, 340 (2002).
[25] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).
[26] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).
[27] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[28] L. Mandel, Phys. Rev. A **28**, 929 (1983).
[29] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, arXiv:1204.0738.
[30] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, Appl. Phys. Lett. **96**, 071101 (2010).
[31] F. Marsili *et al.*, Nat. Photonics **7**, 210 (2013).
[32] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporao, and J. P. von der Weid, arXiv:1207.6345.
[33] 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, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, following Letter, Phys. Rev. Lett. **111**, 130502 (2013).
[34] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, arXiv:1306.6134.