Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber

Hua-Lei Yin,[1,2] Teng-Yun Chen,[1,2] Zong-Wen Yu,[3,4] Hui Liu,[1,2] Li-Xing You,[5] Yi-Heng Zhou,[2,3] Si-Jing Chen,[5] Yingqiu Mao,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[5] Hao Chen,[6] Ming Jun Li,[6] Daniel Nolan,[6] Fei Zhou,[7] Xiao Jiang,[1,2] Zhen Wang,[5] Qiang Zhang,[1,2,7,*] Xiang-Bin Wang,[2,3,7,†] and Jian-Wei Pan[1,2,‡]

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

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*

[4]*Data Communication Science and Technology Research Institute, Beijing 100191, China*

[5]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

[6]*Corning Incorporated, Corning, New York 14831, USA*

[7]*Jinan Institute of Quantum Technology, Jinan, Shandong 250101, China*

(Received 30 June 2016; published 2 November 2016)

Measurement-device-independent quantum key distribution (MDIQKD) with the decoy-state method negates security threats of both the imperfect single-photon source and detection losses. Lengthening the distance and improving the key rate of quantum key distribution (QKD) are vital issues in practical applications of QKD. Herein, we report the results of MDIQKD over 404 km of ultralow-loss optical fiber and 311 km of a standard optical fiber while employing an optimized four-intensity decoy-state method. This record-breaking implementation of the MDIQKD method not only provides a new distance record for both MDIQKD and all types of QKD systems but also, more significantly, achieves a distance that the traditional Bennett-Brassard 1984 QKD would not be able to achieve with the same detection devices even with ideal single-photon sources. This work represents a significant step toward proving and developing feasible long-distance QKD.

DOI: 10.1103/PhysRevLett.117.190501

Quantum key distribution (QKD) can provide unconditional secure communication between two distant parties [1]. Even though the significance of QKD is undisputed, its feasibility has been questioned due to certain limitations in the practical application of real-life QKD systems. It is a common belief that the lack of a perfect single-photon source and the existence of detection losses will handicap the feasibility of QKD by creating security loopholes and distance limitations [2,3]. The measurement-device-independent QKD (MDIQKD) [4,5] with the decoy-state method [6–8] negates the security threats of both the imperfect single-photon source and detection losses.

Enormous efforts focusing on MDIQKD have been experimentally made in labs [9–18], field tests [9,19], and over networks [20]. Currently, the longest transmission record for MDIQKD is 200 km [12]. Thereinto, at metropolitan scale distances (∼100 km), a key rate of several bits per second (bps) can be achieved, which does not appear to meet the requirements for practical applications. Conversely, one of the advantages of QKD [21] is its ability to generate fresh secure keys for instantaneous use. This demands appreciable final key generation on a time scale of seconds. However, prior MDIQKD experiments have shown that if statistical fluctuations are taken into consideration, one needs large data sizes to reach a substantial final key rate [9–20]. In particular, the number of total pulses at each side, N_t, is assumed to be 10^{12} or even larger [22]; therefore, for a 75-MHz system [12], it would take more than 4 hours to accumulate a sufficient amount of data.

Several parameter optimization methods have been proposed to solve this problem [23–25]. However, to fundamentally improve the key rate and distance, only optimizing the parameters is not sufficient. For long-distance MDIQKD, large effects from statistical fluctuations severely undermine efficiency when estimating the phase error rate. Considering statistical fluctuations from different sources jointly [25] is important, and the worst-case joint estimation for both the yield s_{11} and the bit error rate e_{11} of the single-photon pairs [26] directly leads to the final key rate. Here, we implement a new type of asymmetric four-intensity decoy-state MDIQKD protocol [26]. Each party exploits three different intensities 0, μ_x, and μ_y in the X basis, and only one intensity μ_z in the Z basis. The yield of the single-photon pairs, s_{11}, can be calculated from the observed gain of each two-pulse source in the X basis,

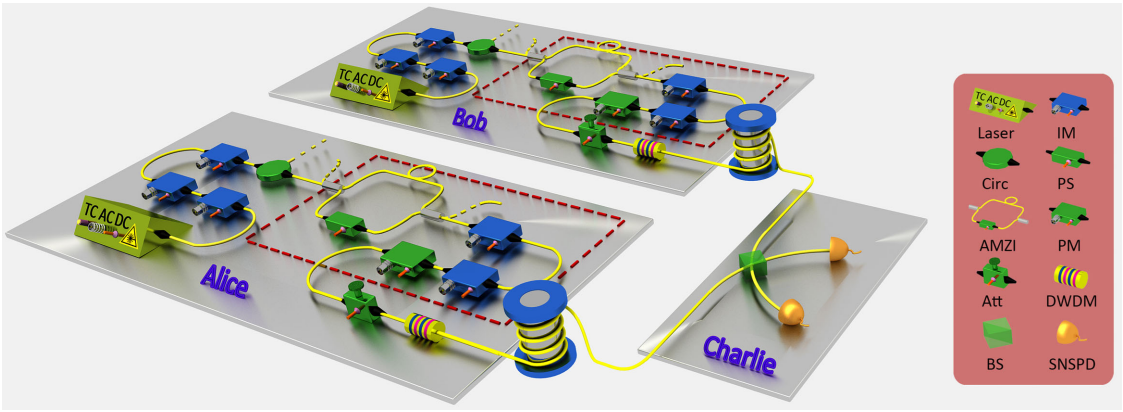

FIG. 1. Experimental setup for the MDIQKD system. Alice's (Bob's) phase randomized weak coherent state pulses are modulated into four decoy-state intensities via two intensity modulators (IM). An asymmetrical Mach-Zehnder interferometer (AMZI), two IMs, and one phase modulator (PM) encode time-bin phase qubits. A circulator (Circ) is used to isolate the laser with the quantum signal. A phase shifter (PS) is used to compensate the relative phase fluctuation of two AMZIs. The first IM is used to better format the signal pulse; the following two IMs are used to modulate the decoy state, and the final two IMs are used for time-bin qubit encoding. TC, temperature controller; AC, alternating current; DC, direct current; Att., attenuator; DWDM, dense wavelength division multiplexer; BS, beam splitter; SNSPD, superconducting nanowire single-photon (SP) detector.

specifically the sources oo, ox, xo, oy, yo, xx, and yy, while source zz sending out signals in the Z basis is used to distill the final key. Given the total number of pulses, the channel loss, and the system parameters, we can choose the values of μ_x, μ_y, and μ_z and their corresponding probability distributions p_x, p_y, and p_z carefully via a global optimization of all the parameters to maximize the final key rate [26].

Figure 1 schematically shows our experimental setup for MDIQKD, which consists of two identical legitimate users, Alice and Bob, and an unreliable relay, Charlie. Alice and Bob exploit internally modulated lasers to generate phase randomized weak coherent state (WCS) optical pulses. The pulse laser is temperature tunable and can be used to adjust the wavelength to implement two-photon interference. To ensure the high visibility of the two-photon interference, an extra IM is used to cut off the overshoot rising edge of the optical pulse. In our experiment, the two-photon interference visibility is more than 46%. The FWHM of the optimized optical pulse is 2.5 ns at a clock frequency of 75 MHz and a wavelength of 1550.12 nm. On each side, two IMs, a PM, and an AMZI are combined to form a time-bin phase qubit encoder [12]. The AMZI divides the laser pulse into two time bins separated by a 6.37 ns time delay. Meanwhile, two additional IMs are used to add decoy states according to our optimization method [26]. The intensity arrangements and the probability distribution are optimized according to the different transmission fiber distances. All these modulators are independently controlled via random numbers generated beforehand. In the cases of 102 and 155 km, the random numbers were generated in previous QKD experiments, while in the cases of longer distances, we use a pseudorandom number generator due to the large data sizes. The corresponding radio-frequency signals originate from a self-made digital to analog converter based on a field programmable gate array. An electrical variable optical Att reduces the pulse intensity to the single-photon level. Just before sending the optical pulses through the quantum channel fiber, a DWDM filters spontaneous emission noise from the laser.

Next, Alice and Bob send their pulses through the optical fibers to Charlie's measurement site. Charlie is symmetrically located with respect to Alice and Bob; therefore, the distances mentioned in this paper are twice the distance between Alice and Charlie. A BS and two SNSPDs constitute a Bell state measurement device. The SNSPDs operate at 2.05 K and provide detection efficiencies of 66% and 64% at a dark count rate of 30 counts per second. We postselect the singlet Bell state $|\Psi^-\rangle$ when the two detectors coincide at two alternative time bins. The efficiency of the time window is approximately 85%, which is an optimal trade-off between the raw key rate and the error rate of X basis.

Achieving a stable and enduring MDIQKD system is not a trivial task. Our system needs to achieve rigorous timing and clock synchronization over the long transmission distance; however, we must also solve technical complications to establish indistinguishability and calibration for the phase reference frames of Alice and Bob (see Supplemental Material [27]). In our setup, therefore, we use automatic feedback systems to calibrate the time for the laser modulation and to optimize the spectrum and polarization of the two independent laser pulses from Alice and Bob.

One of the most outstanding properties of the four-intensity method [26] is its key rate optimization. Here we experimentally demonstrate this feature with a 102 km standard optical fiber spool. Given a failure probability of 10^{-10}, the key rate ranges from 321 to 7.9 bps with the

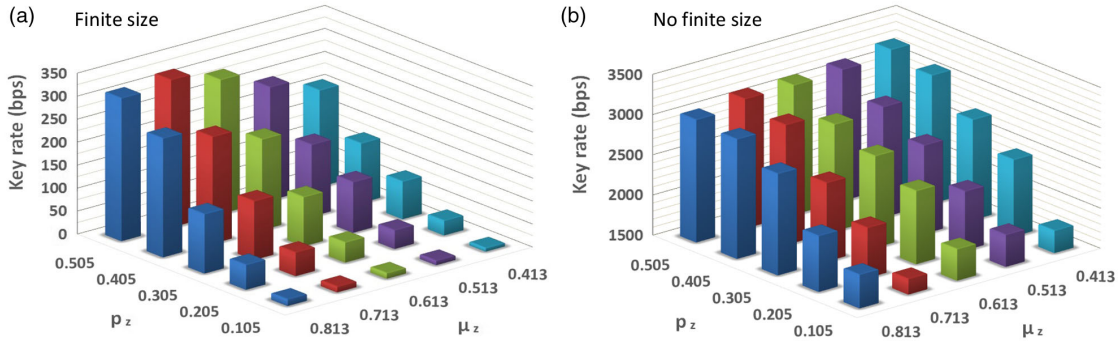

FIG. 2. MDIQKD key rates versus the intensities, μ_z, and probabilities, p_z. (a) The key rates of a 102 km standard fiber with a 10-minute data accumulation time. By varying the signal state intensities, μ_z, and probabilities, p_z, we can achieve key rates from 321 to 7.9 bps with a failure probability of 10^{-10}. (b) The key rates of the same experimental data without the finite size effect. The key rates are more than 1.5 kbps for all signal state intensities, μ_z, and probabilities, p_z.

different input values of μ_z and p_z. Details of the key rate analysis are shown in the Supplemental Material. Given the same device, the key rate can vary greatly depending on different parameters; see Fig. 2(a). Note that the accumulation time and the data size for each point are 10 minutes and 4.5×10^{10}, respectively, which are much more efficient than the 130 hours and 3.51×10^{13} data size of the previous experiment [12], while the key rate in this work is 2 orders of magnitude higher than the previous one at 100 km [12]. Meanwhile, as shown in Fig. 2(b), without considering the finite size effect, the key rate can approach 3 kbps for the same fiber length and data accumulation time. This key rate is enough for voice telephone with one-time pad encryption [29].

To achieve longer distances, we increase the accumulation time. For example, in the case of a 311 km standard fiber, we run the system for 336.6 hours and a total of 9.09×10^{13} pulse pairs are sent from each side in the experiment. Tens of thousands of data are collected. Setting the failure probability to 10^{-10}, we can theoretically acquire 3135 bits for our final key.

For comparison, we implement MDIQKD at the different distances of 102, 155, 207, 259, and 311 km. The optimized experimental parameters are listed in Table I. Specifically, at a distance of 207 km, we obtain a key rate of 9.55 bps, which is more than 500 times higher than that of an earlier experiment [12] for the same accumulation time. Of this huge increase, a factor of approximately 50 is due to the four-intensity method [25,26] and the device improvements and optimizing the time window can further increase the key rate by approximately ten times. The device improvements include improving the SNSPD's detection efficiency and decreasing the insertion loss of the Bell state measurement system. A narrower time window reduces the bit error rate of the X basis, but also reduces the detection efficiency. We adjust the length of the time window to find an optimal point for the highest secure key rate. The achieved key rates at various distances are shown in Fig. 3. The data size for each data point is listed in Table I. It is interesting that given the same device at a distance of 311 km, no secure key can be generated using the traditional passive BB84 protocol, even if we do not consider statistical fluctuations and assume that an ideal SP source is applied.

Consider a passive BB84 protocol with an ideal SP source. Let p_X (p_Z) be the probability of BS to reflect (transmit) the incident light to the measurement port of the X (Z) basis. Let d, η, and S_ω be the dark count rate of the detector, the overall efficiency, and the gain of the ω basis ($\omega = Z, X$), respectively. Exploiting the linear loss model, the gain and bit error rate of the ω basis are $S_\omega = \eta p_\omega + 2d(1-d)(1-\eta p_\omega)$ and $e_w = d(1-d)(1-\eta p_w)/S_w$, respectively, where we assume no alignment errors or insertion losses. In our experimental setup, the loss in a

TABLE I. Optimized intensities (μ_α) and probabilities (p_α) for each distance in our experimental setup.

Distance	102 km	155 km	207 km	259 km	311 km	404 km
μ_z	0.891	0.864	0.757	0.677	0.453	0.413
μ_y	0.189	0.191	0.203	0.267	0.363	0.302
μ_x	0.049	0.058	0.059	0.064	0.083	0.073
p_z	0.827	0.789	0.731	0.509	0.409	0.315
p_y	0.025	0.038	0.042	0.068	0.101	0.110
p_x	0.128	0.154	0.201	0.388	0.439	0.529
N_t	2.05×10^{12}	2.03×10^{12}	3.61×10^{13}	3.55×10^{13}	9.09×10^{13}	6.04×10^{14}

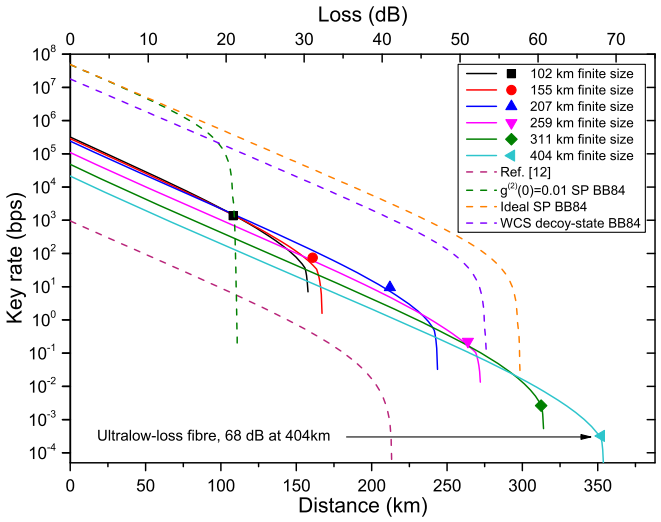

FIG. 3. Experimental results. The experimental results (symbols) agree well with the theoretical simulations (solid lines) with a maximum transmission distance of 404 km via ultralow-loss optical fiber and 311 km via standard optical fiber. For comparison, we include simulations for the balanced basis passive Bennett-Brassard 1984 (BB84) protocol using ideal SP sources, the practical SP with $g^{(2)}(0) = 0.01$ without the decoy-state method, the WCS with the decoy-state method, and the results of Ref. [12] shown as the dotted lines. Note that even though the MDIQKD produces lower key rates than the BB84 protocol, it can offer greater secure transmission distances.

311 km standard optical fiber is 59.05 dB while the efficiency and dark count rate of the detector are 65% and $d = 7.2 \times 10^{-8}$, respectively. Given that $0 < p_X < 1$ and $p_X + p_Z = 1$, we find $e_X > 7.55\%$ and $e_X + e_Z > 26.25\%$. Therefore, the asymptotic key rate can be given by $1 - H(e_X) - H(e_Z) < 0$, where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon entropy. To make this clearer, we include the theoretical curves of the asymptotic key rates for the balanced basis passive BB84 protocol using the ideal SP, the practical SP [30] with $g^{(2)}(0) = 0.01$ without the decoy-state method, and the WCS with the decoy-state method in Fig. 3.

To extend the transmission limit, we test the key generation with a 404 km ultralow-loss fiber (0.16 dB/km at 1550 nm) provided by Corning Incorporated. Based on the channel loss and accumulation time, we set the optimized experimental parameters to $\mu_z = 0.413$, $\mu_y = 0.302$, $\mu_x = 0.073$, $p_z = 0.315$, $p_y = 0.110$, and $p_x = 0.529$. With an accumulation time of three months, the data collected could be used to generate 2584 key bits with a key rate of 3.2×10^{-4} bps; these results are also shown in Fig. 3. This is by far the longest distance reported for all types of QKD systems [31,32]. Note that, as shown in the Supplemental Material in detail, we have applied the calculation method of Ref. [26] to estimate the final key rate [18]. The same as previous works [9–18], we do not perform the error correction or privacy amplification to generate the specific final key string. Meanwhile, gigabits classical communication data need about 256 bits for authentication [33]. Since the classical communication data in our experiment are less than gigabits and all estimated secure key sizes are larger than 256 bits, our experiment can be seen as a key expansion.

In addition to the long transmission distances, our system generates a 1.38 kbits per second secure finite key at 102 km, therefore constituting a strong candidate for a metropolitan quantum network with an unreliable relay [20]. We can further increase the system performance by increasing the system clock rate [18] and the efficiency of the single-photon detector [34]. Dispersion compensating techniques may be required to improve the key rate when the system clock rate is increased to the order of GHz [18]. In this Letter, the effects of source flaws such as quantum state encoding biases and intensity variation are not considered; however, these are important topics for theoretical and experimental investigations in future QKD.

We thank Y. Tang, X. Xie, and C. Peng for their valuable discussions. This work was supported by the National Fundamental Research Program (under Grant No. 2013 CB336800), the National Natural Science Foundation of China, the Chinese Academy of Science, the 10000-Plan of Shandong Province, the Science Fund of Anhui Province for Outstanding Youth, the National High-Tech Program of China (under Grants No. 2011AA010800 and No. 2011 AA010803), and the QuantumCTek Co., Ltd.

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

*qiangzh@ustc.edu.cn
†xbwang@mail.tsinghua.edu.cn
‡pan@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[4] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[5] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[7] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[8] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[9] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[10] 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, Phys. Rev. Lett. **111**, 130502 (2013).

[11] 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).
[12] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **113**, 190501 (2014).
[13] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[14] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M. D. Shaw, J. A. Stern, S. W. Nam, D. Oblak, Q. Zhou, J. A. Slater, and W. Tittel, J. Mod. Opt. **62**, 1141 (2015).
[15] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).
[16] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Lett. **115**, 160502 (2015).
[17] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, Phys. Rev. A **93**, 042308 (2016).
[18] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nat. Photonics **10**, 312 (2016).
[19] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, IEEE J. Sel. Top. Quantum Electron. **21**, 6600407 (2015).
[20] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Phys. Rev. X **6**, 011024 (2016).
[21] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[22] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[23] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[24] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A **89**, 052333 (2014).
[25] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Phys. Rev. A **91**, 032318 (2015).
[26] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).
[27] See Supplemental Material http://link.aps.org/supplemental/10.1103/PhysRevLett.117.190501, which includes Ref. [28].
[28] H. Chernoff, Ann. Math. Stat. **23**, 493 (1952).
[29] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, Opt. Express **17**, 6540 (2009).
[30] Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu, and J.-W. Pan, Nat. Nanotechnol. **8**, 213 (2013).
[31] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).
[32] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).
[33] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza *et al.*, New J. Phys. **16**, 013047 (2014).
[34] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin *et al.*, Nat. Photonics **7**, 210 (2013).