PHYSICAL REVIEW A **93**, 030302(R) (2016)

Experimental round-robin differential phase-shift quantum key distribution

Yu-Huai Li,[1,2] Yuan Cao,[1,2] Hui Dai,[1,2] Jin Lin,[1,2] Zhen Zhang,[3] Wei Chen,[1,2] Yu Xu,[1,2] Jian-Yu Guan,[1,2] Sheng-Kai Liao,[1,2] Juan Yin,[1,2] Qiang Zhang,[1,2] Xiongfeng Ma,[3] Cheng-Zhi Peng,[1,2] and Jian-Wei Pan[1,2]

[1]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Shanghai 201315, China*

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

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

(Received 20 July 2015; published 23 March 2016)

In conventional quantum key distribution (QKD) protocols, security is guaranteed by estimating the amount of leaked information. Such estimation tends to overrate, leading to a fundamental threshold of the bit error rate, which becomes a bottleneck of practical QKD development. This bottleneck is broken through by the recent work of round-robin differential phase-shift (RRDPS) protocol, which eliminates the fundamental threshold of the bit error rate. The key challenge for the implementation of the RRDPS scheme lies in the realization of a variable-delay Mach–Zehnder interferometer, which requires active and random choice of many delays. By designing an optical system with multiple switches and employing an active phase stabilization technology, we successfully construct a variable-delay interferometer with 127 actively selectable delays. With this measurement, we experimentally demonstrate the RRDPS protocol and obtain a final key rate of 15.54 bps with a total loss of 18 dB and an error rate of 8.9%.

DOI: 10.1103/PhysRevA.93.030302

In the Bennett-Brassard-1984 (BB84) quantum key distribution (QKD) protocol [1], the sender, Alice, sends a quantum signal through an untrusted quantum channel. The receiver, Bob, measures the received quantum signal and obtains the raw key. Due to device imperfections, environmental interference, and possible eavesdropping, the raw keys obtained by Alice and Bob may not be identical or private. In security analysis, the disturbance of the quantum signal is quantified by the bit flip error rate, e_{bit}, and the amount of leaked information is quantified by the phase error rate, e_{ph} [2]. To ensure that the final keys are identical and secure, proper postprocessing should be performed. After performing error correction, to remove the disturbances, one should apply privacy amplification, which removes the leaked information. The final key generation rate per raw key bit is given by [3]

$$R = 1 - H(e_{\mathrm{bit}}) - H(e_{\mathrm{ph}}). \tag{1}$$

When the error rates, e_{bit} and e_{ph}, exceed certain thresholds, the key rate becomes zero or negative and hence no secure keys can be generated.

Security is guaranteed by the Heisenberg uncertainty principle in BB84 QKD protocol, which ensures that any attempt at eavesdropping in the quantum channel inevitably causes quantum signal disturbances. Therefore, the leaked information obtained by an eavesdropper, Eve, can be upper bounded by the disturbance of the signal. Due to its symmetry, the phase error rate is estimated by the bit error rate, $e_{\mathrm{ph}} = e_{\mathrm{bit}}$, and hence, the final key rate in Eq. (1), is given by $R = 1 - 2H(e_{\mathrm{bit}})$. When $e_{\mathrm{bit}} > 11\%$, the final key rate approaches 0. Hence, the bit error rate threshold for the BB84 protocol is 11% using the above postprocessing method. Note that with other postprocessing techniques [4], a higher bit error rate threshold can be obtained. Nevertheless, a fundamental limitation on the error rate threshold exists [5] in general. It is widely believed that secure QKD cannot be achieved when the background is too large in comparison to the signal. In practice, especially in the application of free-space communication, the strength of the background comes from the major noise source, such as detector dark counts and environment lighting, can be considered to be a constant, whereas the strength of the signal exponentially decreases as the transmission distance increases. Hence, the error rate threshold puts a fundamental limit on the secure transmission distance. From a realistic point of view, most disturbances are caused by environmental noises and device imperfections, rather than eavesdropping. Thus, the amount of leaked information is often overestimated, which is the root for the limit on the error rate threshold.

In classical communication, according to Shannon's communication theory, information can transform through a noisy channel even if the background noise is very strong compared with the signal, and hence, the threshold of the bit error rate tends to be 50% [6]. One might wonder whether a QKD scheme can also tolerate an error rate as high as 50%. The question has been answered affirmatively by recent work on the round-robin differential phase-shift (RRDPS) protocol [7,8], which breaks through the fundamental threshold of the bit error rate and indicates another potential direction for the development of the field of quantum cryptography. The RRDPS protocol is essentially evolved from the differential phase-shift protocol [9–15]. Surprisingly, with the new protocol, secure key can be generated even if the bit flip error rate is close to 50%. As pointed out in the original theoretical work [7], the key rate formula shown in Eq. (1) still applied for the RRDPS protocol using the privacy amplification. However, there is a technical challenge facing this new QKD scheme, namely, a variable-delay Mach-Zehnder interferometer must be developed. Here, we successfully construct such an interferometer with 127 actively selectable delays ($L = 128$), and use it to experimentally demonstrate the RRDPS QKD.

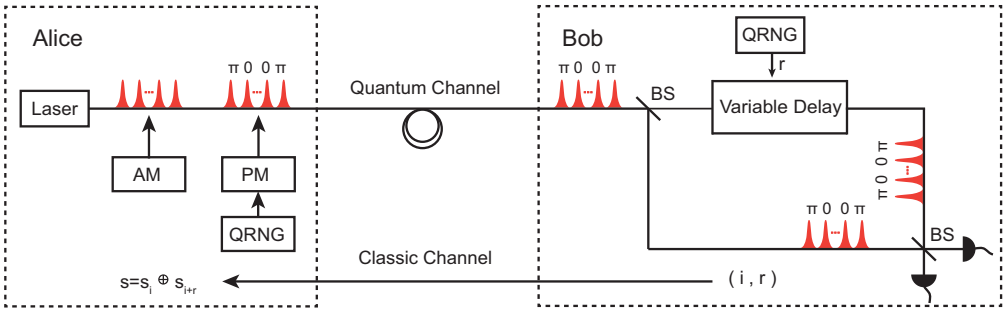

FIG. 1. Schematic of the RRDPS QKD proposal. *State preparation*: Alice generates an L-pulse train by modulating a narrow linewidth continuous-wave laser with an AM. Then, she applies a random phase shift, 0 or π, to each pulse. After attenuating the intensity to a quantum value, Alice sends the L-pulse train to Bob. *Measurement*: Bob generates a random number, $r \in \{1,2,\ldots,L-1\}$, and splits the received pulse train with a BS. He applies a delay of r pulses to one of the split trains, interferes them, and obtains a detection on pulse i. The detection result reveals the relative phase between pulses i and $i+r$ as a key bit $s_i \oplus s_{i+r}$. *Announcement*: Bob announces i and r so that Alice can calculate the corresponding key bit $s_i \oplus s_{i+r}$. AM: amplitude modulator; PM: phase modulator; BS: beam splitter; QRNG: quantum random number generator.

The schematic diagram of the RRDPS QKD scheme is shown in Fig. 1. Alice prepares a pulse train containing L pulses, encodes her (random) key information into the phase of each pulse, 0 or π, and sends it to Bob, who splits it into two with a beam splitter. Bob randomly shifts one of the split pulse trains by r' pulses where $1 \leqslant r' \leqslant L-1$, and uses it to interfere with the other split pulse train. Bob uses another random bit c to define $r = r'$ for $c = 0$, while $r = L - r'$ for $c = 1$ [7], so that each pair of pulses has the same detection probability. The key rate of the RRDPS QKD protocol is given by [8]

$$R = Q[1 - H(e_{\text{bit}}) - H_{\text{PA}}], \tag{2}$$

where R is the final key bit per L-pulse train. Experimentally, the average number of valid detections per L-pulse train, Q, can be measured directly. In the Supplemental Material, we show the estimation of the privacy amplification term H_{PA} [16]. The privacy amplification term H_{PA} is a function of L, which approaches 0 if L approaches the infinity as we have discussed in the Supplemental Material. Thus, e_{bit} can take any value below 50%. Because the privacy amplification term does not depend on the parameters related to signal disturbance, the RRDPS protocol is in principle highly robust against channel disturbance for a large L and provides a new route towards QKD over long distances and under a much harsher environment [7,8].

In our experiment, we demonstrate the RRPDS QKD protocol with $L = 128$, which can tolerate a bit error rate up to 30%, which is far above the upper limit of 11% in the decoy state BB84 QKD protocol [17–24]. The setup is shown in Fig. 2. On the sender side, a continuous-wave (cw) external cavity laser (ECL) is employed as the optical source. The central wavelength of the ECL is 1550.12 nm, with a linewidth below 2 kHz, which offers a coherence time greater than 500 μs. This cw laser is modulated by an amplitude modulator (AM, Photline 10 GHz) to produce a 128-pulse train. The pulses, with a full width at half maximum of 300 ps, are separated by 2 ns. Thus, the overall duration of a pulse train (also a round) is about 256 ns. A phase modulator (PM, Photline 10 GHz) is employed to encode a random phase shift, 0 or π, into each pulse.

On the receiver side, a Mach-Zehnder interferometer with variable delay is constructed to perform different interference measurements, as shown in Fig. 2. The required delay time is a discrete value in the sequence {2 ns,4 ns, ...,254 ns}. The seven delay gates, denoted as DG_i for $i \in \{1,\ldots,7\}$, which can delay optical pulses for a time of 2^i ns, are arranged so as to achieve the 127-value variable delays. The length of each delay path is carefully adjusted to ensure that pulses with and without delays can overlap well. Meanwhile, the coupling efficiency of each pair of collimators is above 90% so as to ensure the intensity of pulses passing through different numbers of delay gates as closely as possible. The seven delay gates are controlled by a seven-bit random number. Each delay gate is constructed of a Pockels cell, a fiber, or free-space link with specific length and two polarizing beam splitters (PBSs). The Pockels cell contains two rubidium titanate phosphate crystals and is controlled by a customized high-voltage pulse generator to achieve fast switching between 0 V and half-wave voltage, which is around 2100 V. For each one of the delay gates, if a randomly selected control bit is 0, the pockels cell will not affect the received pulses which allow the received pulses to pass through the output PBS without delay. If the control bit is 1, the Pockels cell will be driven by the half-wave voltage to convert the polarization state of arrived photons from horizontal ($|H\rangle$) to vertical ($|V\rangle$). Thus, the pulses will be reflected by the output PBS and propagate through the delay link. The delay gate of 2 ns (DG_1) is obtained by a free-space link of ~0.6 m. Other delay gates of longer than 2 ns are obtained by fiber links with appropriate lengths. After being reflected by the input PBS, the pulses pass through the half-wave voltage Pockels cell again, leading to the polarization being reverted to $|H\rangle$ and passed through the output PBS. These seven delay gates are distributed in both arms of the interferometer to balance the transmittance. Some PBSs are shared between two neighboring gates.

The key challenge here is to simultaneously stabilize the Mach-Zehnder interferometer with all possible delays in the subwavelength order, to perform high visibility interference measurements. To suppress mechanical vibration and temperature drift from the optical table and air, we employ a frame with thermal insulating and high-damping materials to envelop the interferometer. With these passive phase stabilization methods,

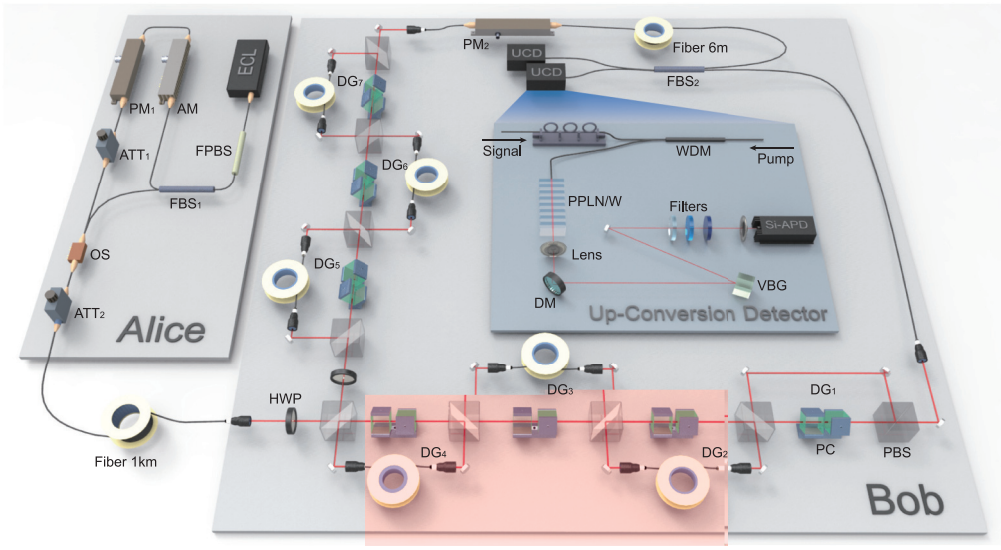

FIG. 2. Experimental setup. The 128-pulse trains are generated by the ECL and the AM on the sender side and encoded randomly a phase shift, 0 or π, into each pulse by the PM_1. The FBS_1 is employed to split the laser into the pulse trains and the phase stabilization light. OS is used to choose the pulse trains or phase stabilization light to be transmitted periodically. After transmitting in the 1-km fiber channel, the pulse trains arrive at the receiver side. Then, the receiver's variable-delay Mach-Zehnder interferometer with 127 settings, which are realized by the seven optical delay gates, implements the interference measurement on the pulse trains. After interferometry, the pulses are detected by two custom up-convert single photon detectors. ECL: external cavity laser; AM: amplitude modulator; PM: phase modulator; ATT: attenuator; (F) PBS: (fiber) polarizing beam splitter; FBS: fiber beam splitter; OS: optical switch; HWP: half-wave plate; PC: Pockels cell; DG: delay gate; WDM: wavelength division multiplexing.

127 kinds of unequal-arm interferometers can maintain a visibility above 96% for a time period of the order of 10 s, depending on the delay r. The residual phase instability is mainly due to the drift of the central wavelength of the laser. Therefore, to implement a complete experimental demonstration of RRDPS QKD protocol, an active phase stabilization technique is required. On the sender side, an additional path without modulation of AM and PM (known as a "phase stabilization light") with a relatively greater intensity of about 60 million photons per second, is introduced by a fiber beam splitter (FBS) and an optical switch. The phase stabilization light is switched on for 340 ms/s to calibrate the interferometers. The remaining 660 ms/s is used for QKD. During phase stabilization, the 127 delays are traversed by

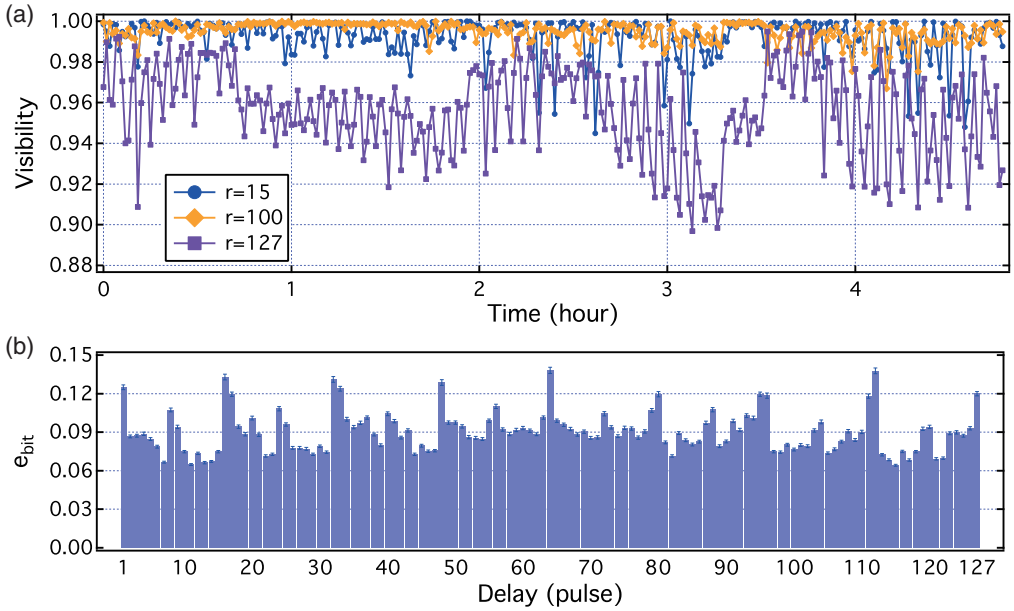

FIG. 3. Experiment result. (a) Phase stability with our active phase stabilization technique over several hours. For most values of r such as $r = 15$ and $r = 100$, the visibility is maintained above 96%. (b) The bit error rate e_{bit} as a function of delay r. The mean error rate is 8.9%. The error rate is approximately reflective symmetric.

TABLE I. Experimental parameters and results.

Total rounds	Sifted key	Q	L	μL	e_{bit}	Final key length
103 679 400	675 937	0.006 52	128	0.8	8.9%	2.441×10^5

activating the specific Pockels cells. PM_2 is deployed to adjust the relative phase between the two arms of the interferometers. For each delay, an optimal compensation voltage of PM_2 is measured and recorded by a custom field programmable gate array in the control board (see Supplemental Material). The recorded compensation voltages are used to keep the relative phase unchanged against different delay selections and central wavelength drift. With the active phase stabilization technique, the visibility of most interferometers can simultaneously be maintained over 96% for hours, as shown in Fig. 3(a).

The photons are detected by two custom up-conversion single photon detectors [25]. By interaction with a 1950 nm pump laser in a periodically poled lithium niobate (PPLN) waveguide, 1550 nm photons are up-converted to 863 nm and then detected by commercial Si-based single photon detectors. The outputs of the single photon detectors are recorded by a high-speed, high-accuracy time-to-digital converter. The overall detection efficiency of the up-conversion detector is around 10%, and the dark count is below 200 counts/s.

We perform this demonstration using a 1-km-long fiber channel. The average photon numbers per pulse and per 128-pulse train are 0.006 25 and 0.8, respectively. The repetition rate of the pulse trains is 10 kHz. With 34% of the time used for calibration, 6600 pulse trains are transmitted per second (see Supplemental Material). The total loss is 18 dB, including 10 dB of detection efficiency and around 8 dB of loss in Bob's interferometer setup. In addition, since only about half of the pulses can overlap and interference after a random delay, the other half of the detected events were discarded. Within 15 709 s, we obtain 675 937 bit sifted keys in total. The bit flip error rates with different delays are shown in Fig. 3(b). Due to the imbalance between the two arms of the interferometer, there are fluctuations of the bit error rates with different delays. Finally, 2.441×10^5 bits of the security key are generated with an 8.9% overall error rate, as shown in Table I. Therefore, the key generation rate is given by 15.54 bps. A numerical simulation was performed to show the secure key rates on the increase of transmission distance, as shown in Fig. 4. Generally, a lower error rate implies a higher final key rate when the other parameters were fixed. In the real experiment, we manage to suppress the error rate down to 8.9%. Note that the configuration used here to build the variable-delay interferometer can be conveniently extended to obtain a larger

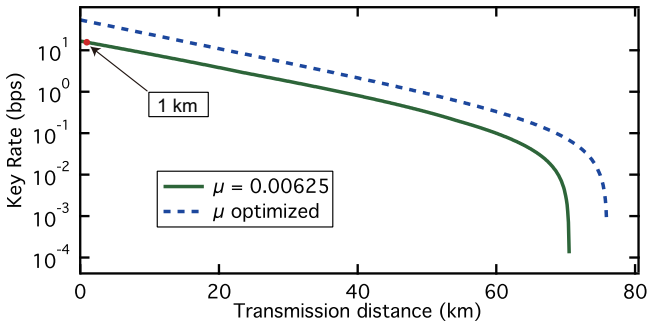

FIG. 4. Simulated secure key rate with current experiment setup. The solid line and the dashed line represent the secure key rate under a fixed and optimized average photon number per pulse separately.

L through adding more choices of delays. In our setup, the choices of L can be doubled for every delay gate increased.

Recently, two other similar RRDPS experiments have been published [26,27] where $L = 5$ and $L = 65$ is realized separately. Our experiment, together with these two experimental implementations, demonstrates the protocol and thus brings a brand new aspect of QKD. Another RRDPS QKD protocol has been proposed and experimentally demonstrated [28]. Different from the original RRDPS protocol, the random delay is chosen passively, while Mach-Zehnder type interference is taken place by the Hong-Ou-Mandel type. The proposal of passive RRDPS QKD is easier to realize a proof-of-principal demonstration, at the cost of performance and practical applicability. Since coherent sources are used for Hong-Ou-Mandel type interference, the bit error rate has a lower bound of 25% [28], which may seriously impact the secure bit rate. On the other hand, a practical system requires two independent lasers in both Alice's and Bob's side, which brings a big challenge on synchronizing. From this perspective, the original RRDPS QKD proposal has advantages for realizing long-distance QKD, especially satellite-ground QKD.

We acknowledge C. Liu and X. Han for their insightful discussions. This work has been supported by CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai Branch, University of Science and Technology of China, by the National Fundamental Research Program (under Grants No. 2011CB921300 and No. 2013CB336800), by the National Basic Research Program of China (under Grants No. 2011CBA00300 and No. 2011CBA00301), the 1000 Youth Fellowship program in China, and the Strategic Priority Research Program on Space Science, the Chinese Academy of Sciences.

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

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175.

[2] Here, if we assume the final key is extracted from the Z basis measure, the bit error rate e_{bit} is the ratio of the key that Alice and Bob disagree on, and the phase error rate e_{ph} is the error ratio when those qubits had been measured in the X basis [29].

[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[4] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[5] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[6] C. Shannon, Math. Rev. (MathSciNet): **MR10**, 133e (1948).

[7] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).

[8] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, arXiv:1505.02481.

[9] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[10] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).
[11] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, New J. Phys. **7**, 232 (2005).
[12] E. Waks, H. Takesue, and Y. Yamamoto, Phys. Rev. A **73**, 012344 (2006).
[13] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 13073 (2006).
[14] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).
[15] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).
[16] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.93.030302 for more details on privacy amplification estimation, the technique of active phase stabilization and time sequence control.
[17] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[18] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[19] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[20] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[21] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[22] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[23] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).
[24] 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).
[25] G.-L. Shentu, J. S. Pelc, X.-D. Wang, Q.-C. Sun, M.-Y. Zheng, M. M. Fejer, Q. Zhang, and J.-W. Pan, Opt. Express **21**, 13986 (2013).
[26] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photonics **9**, 827 (2015).
[27] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photonics **9**, 832 (2015).
[28] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **114**, 180502 (2015).
[29] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).