Entanglement swapping with independent sources over an optical-fiber network

Qi-Chao Sun,[1,2,3] Ya-Li Mao,[2,3] Yang-Fan Jiang,[2,3] Qi Zhao,[4] Si-Jing Chen,[5] Wei Zhang,[6] Wei-Jun Zhang,[5] Xiao Jiang,[2,3] Teng-Yun Chen,[2,3] Li-Xing You,[5] Li Li,[2,3] Yi-Dong Huang,[6] Xian-Feng Chen,[1] Zhen Wang,[5] Xiongfeng Ma,[4,*] Qiang Zhang,[2,3,†] and Jian-Wei Pan[2,3,‡]

[1]*Department of Physics and Astronomy, Shanghai Jiao Tong University, Shanghai, 200240, China*

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

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

[4]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084, 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]*Tsinghua National Laboratory for Information Science and Technology, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China*

(Received 20 June 2016; published 6 March 2017)

Establishing entanglement between two remote systems by the method of entanglement swapping is an essential step for a long-distance quantum network. Here we report a field-test entanglement swapping experiment with two independent telecommunication band entangled photon-pair sources over an optical fiber network in Hefei. The two sources are located at two nodes that are 12.5 km apart and the Bell-state measurement is performed at a third location which is connected to the two source nodes with 14.7-km and 10.6-km optical fibers, respectively. The observed average visibility is 79.9 ± 4.8%, which is sufficient for the violation of Bell inequalities. Furthermore, with the swapped entanglement, we demonstrate a source-independent quantum key distribution, which is also immune to any detection attacks at the measurement site.

DOI: 10.1103/PhysRevA.95.032306

Entanglement swapping [1] was first proposed to provide an event-ready entanglement for Bell tests [2,3]. Two particles, each of which is half of an entangled pair, become entangled by performing a joint Bell state measurement (BSM) on the other two halves of the entangled pairs [1]. It can be also treated as a more general quantum teleportation [4], since a mixed state instead of a pure state is teleported in an entanglement swapping. Notably, compared to quantum teleportation, a unique feature of entanglement swapping is that the two initially independent particles become entangled without any direct interaction. Besides its interest for the fundamental study of quantum theory, entanglement swapping, together with quantum memory and entanglement distillation, offers a quantum repeater technique [5,6] that provides a mean to establish entanglement over long distances. A quantum repeater is an essential element in a quantum network, where the shared entanglement can be used for various tasks, such as quantum key distribution (QKD) [7], teleportation [4], and quantum computing [8].

For all these purposes in a quantum network, it is critical that the entangled pairs are created independently in spatially separated nodes and interfere with each other after transmission. To date, photons are known to be the most suitable carriers to transmit quantum information due to their flying nature and robustness against decoherence. Since the mid-1990s, various photonic entanglement swapping experiments have been demonstrated [9–15]. However, in most of the previous demonstrations of entanglement swapping, the two entangled photon-pair sources were pumped by the same femtosecond laser and placed close to each other [9,10]. The two sources should be synchronized to achieve interactions between photons generated at distant nodes. Pioneering studies have been conducted to synchronize two sources that are pumped independently in a laboratory [11–13,16]. Due to difficulties in guaranteeing the indistinguishability of the photons after they are transmitted through a realistic channel, a field test of entanglement swapping with independent sources has only recently been realized [17]. The wavelength of the photons used in this study was 637 nm, which makes it difficult to extend the transmission distance to long distances because of losses in the optical fiber.

Here we employ telecommunication band time-bin entangled photon-pair sources and realize entanglement swapping with two independent sources separated by 12.5 km, as shown in Fig. 1. Time-bin entangled photon-pairs can be generated by pumping a nonlinear media with two consecutive laser pulses with well-defined relative phases. Usually, the two consecutive laser pulses are created by passing a laser pulse through an unbalanced Mach-Zehnder interferometer (MZI) [10,18]. In our experiment, both Alice and Bob use an electro-optic modulator (EOM) to directly carve a continuous wave (CW) laser beam emitted by a distributed feedback laser diode into two consecutive pulses. The time delay between the two pulses is $\tau = 1$ ns, which is much smaller than the coherent time of the CW laser (~300 μs). Therefore, the relative phase between the two laser pulses is $\theta = 2\pi\nu\tau$, where ν is the frequency of the CW laser. After being amplified by an erbium-doped fiber amplifier and filtered by cascaded dense wavelength division-multiplexing (DWDM) filters to remove

[*] xma@tsinghua.edu.cn

[†] qiangzh@ustc.edu.cn

[‡] pan@ustc.edu.cn

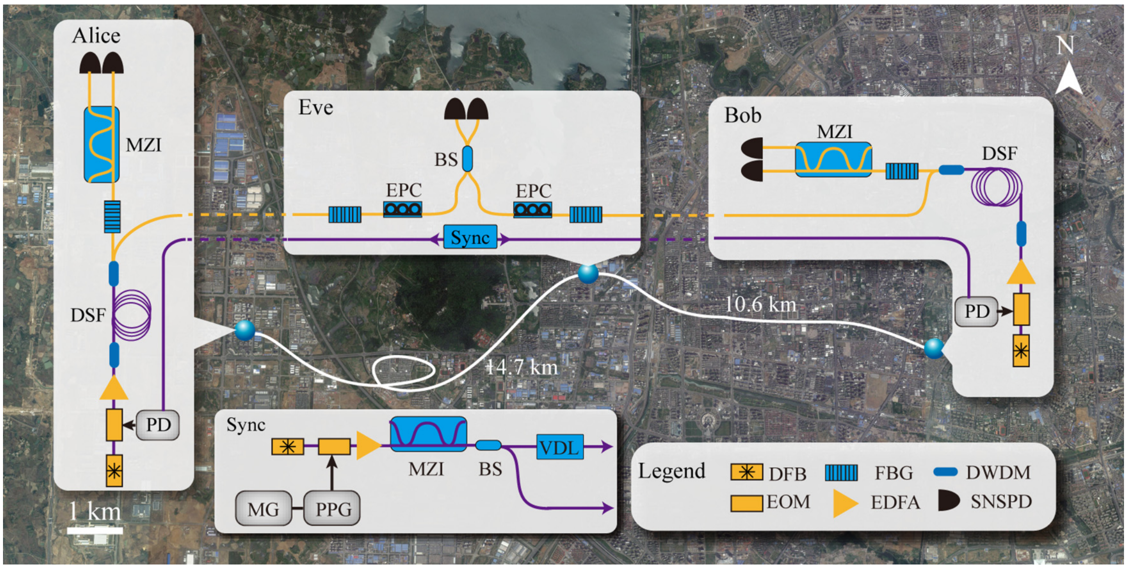

FIG. 1. Bird's-eye view and schematic of entanglement swapping in the Hefei optical fiber network. The locations of Alice (Hefei Innovation Industrial Park), Bob (University of Science and Technology of China), and Eve (Hefei Software Park) are marked on the satellite image. Alice and Bob are separated by 12.5 km and connected to Eve using 14.7-km and 10.6-km deployed optical fibers, respectively. Both Alice and Bob prepare time-bin-entangled photon pairs, measure the idler photons, and send their twin signal photons to Eve for BSM. The synchronization signals (Sync) are generated by Eve and then distributed to Alice and Bob through the optical fibers. The single photons and strong laser pulses are transmitted in different optical fibers, represented by the yellow line and purple lines, respectively.

the amplified spontaneous emission noise photons, the two laser pulses are fed into a 300-m-long dispersion shifted fiber cooled by liquid nitrogen, where a photon pair can be generated via the four-wave-mixing process. The quantum state of the photon pair is a superposition of two-photon states with different emission times denoted by t_0 and t_1, respectively, $|\phi\rangle = \frac{1}{\sqrt{2}}(|t_0,t_0\rangle + e^{2i\theta}\,|t_1,t_1\rangle)$.

The created photon-pairs are fed into another set of cascaded DWDM filters to single out paired idler photons (1,555.73 nm) and signal photons (1,549.36 nm) with pump photons suppressed by 115 dB. The signal photons are sent to Eve for a partial BSM by interfering them on a 50:50 beam splitter (BS). Therefore, the signal photons from Alice and Bob should be indistinguishable in degrees of freedom, such as spatial mode, polarization, spectrum, and temporal mode. The fact that all the photons are generated and transmitted in a single mode fiber guarantees the spatial indistinguishability. Each input port of the BS is equipped with an electronic-controlled polarization controller to automatically calibrate the polarization of photons. To make the signal photons have identical spectra and the same single temporal mode, both the signal photons and the idler photons are further filtered with fiber Bragg gratings with a bandwidth of 4 GHz. This value is approximately half that of the pump pulses, which means that, in theory, the state purity of the signal photons is 99.4%.

In addition, the interference also requires a temporal overlap of the two signal photons on the BS. To synchronize the two sources, Eve generates driven signals for the two sources and distributed them to the two sources through optical fibers. She uses a microwave generator to provide a 12.5-GHz clock for a pulse pattern generator (PPG), which drives an EOM to carve a CW laser into pulses with a repetition rate of 300 MHz. The pulse width is approximately 75 ps, which is determined by the minimum pulse width of the PPG. After passing through an unbalanced MZI with a 1-ns path difference, each laser pulse is split into two consecutive laser pulses. Then the laser pulse train is sent to Alice and Bob through optical fiber and detected using 45-GHz photodetectors to generate driving signals for their EOMs. As a field test, even if the two sources are synchronized, the arrival time of the signal photons fluctuates because the length of the optical fiber changes dramatically due to influences in the real world. Eve monitors the arrival times of the signal photons and automatically compensate the relative delay between the arrival times using a variable delay line. This synchronization scheme is valid as long as Alice and Bob can generate pump laser pulses with pulse widths smaller than the coherent time of the photon pairs. Therefore, one of the limitations of the maximum synchronization distance is the chromatic dispersion. The scheme with driven signals distributed by a third party between the two sources can double the maximum synchronization distance compared to that used in Ref. [18]. Note that the chromatic dispersion can be compensated by using a dispersion compensating fiber and a chirped fiber Bragg grating so this configuration is feasible for synchronizing independent sources separated by 100 km.

In the BSM, Eve only discriminates the Bell state $|\Psi^-\rangle_s^{A,B} = \frac{1}{\sqrt{2}}(|t_0t_1\rangle_s^{A,B} - |t_1t_0\rangle_s^{A,B})$ with the two signal photons sent by Alice and Bob detected in difference output ports of the BS and in different time bins. As a result, the corresponding idler photons are projected to an entangled state $|\Psi^-\rangle_i^{A,B} = \frac{1}{\sqrt{2}}(|t_0t_1\rangle_i^{A,B} - |t_1t_0\rangle_i^{A,B})$. Actually, the idler photons are measured immediately and locally after their generation, while the signal photons are transmitted through 14.7-km and 10.6-km optical fibers before being detected. Therefore, the entanglement between the idler photons is generated *a posteriori* [19].

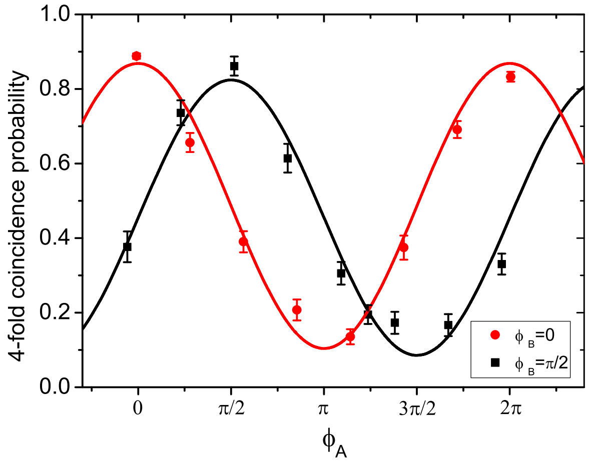

FIG. 2. Fourfold coincidence count probabilities as a function of the phase of Alice's MZI. The error bars indicate one standard deviation calculated from measured counts assuming Poissonian detection statistics. Each data point is accumulated for more than 10 h. The visibilities of the fitted curve are 81.2 ± 6.2% and 78.6 ± 7.3% for measured results with $\phi_B = 0$ and $\phi_B = \pi/2$, respectively.

To verify successful entanglement swapping, Alice and Bob perform projection measurements on idler photons using two unbalanced MZIs with path differences of 1 ns. All the photons in our experiment are detected with superconducting nanowire single photon detectors (SNSPDs), and the detection signals are measured using time-to-digital converters (TDCs) with 4-ps time resolutions. The TDCs are synchronized with 10-MHz clocks generated at Eve's node and distributed to Alice and Bob through optical fibers (not pictured in Fig. 1). The fourfold coincidence counts of the detection results of the idler photons in Alice and Bob's nodes, and those of the signal photons at Eve's node, show a clear interference fringe, as shown in Fig. 2. The average visibility of the fitted curves is 79.9 ± 4.8%. This corresponds to a fidelity of 84.9 ± 3.6% [$F = (3V + 1)/4$] and infers a violation of the Clauser-Horne-Shimony-Holt Bell inequality by more than two standard deviations, provided the swapped photons are in the Werner state [3,20].

The visibility allows the swapped entanglement to be used directly for some quantum communication purposes without further distillation. Indeed, we use the swapped entanglement as a resource to demonstrate QKD. The relative phase of the MZIs of Alice and Bob are set to 0. Therefore, the idler photons are randomly detected in the time basis, $\{|t_0\rangle, |t_1\rangle\}$, and the energy basis, $\{(|t_0\rangle \pm |t_1\rangle)/\sqrt{2}\}$. Alice and Bob can extract a secure key from their local measurement results conditioned on the BSM outcomes following the Bennett-Brassard-Mermin92 protocol [21].

From the viewpoint of security, implementing entanglement swapping in QKD can remove many side channels in practice. Even though QKD can in principle provide information-theoretical security, practical QKD systems suffer from side-channel attacks that exploit the device imperfections. Recently, detector side-channel attacks have been removed by employing the measurement-device-independent (MDI) QKD protocol [22]. However, potential loopholes still exist on the source side. For instance, if the photon source is not well prepared according to the security proof model, source attacks would be possible [23]. In our QKD setting, the local measurements of Alice and Bob can be treated as preparing the quantum states of the photons by measuring their paired photons. The security of the final key does not rely on how faithful Eve performs the BSM or announces the results. Hence, this is essentially an MDIQKD. Moreover, the local detection systems on Alice and Bob's sides are disconnected from the quantum channels via entangled photon sources. Eve cannot get aware of the local measurements. In fact, an entangled source can be used as a basis-independent source [24,25]. Therefore, our QKD setting enjoys both MDI and source-independent security properties.

TABLE I. The number of sifted key bits (N) and the error rate (e_b). The superscripts e, t, and tot denote values in the energy basis, time basis, and both of them together, respectively.

N^{tot}	N^e	N^t	e_b^e	e_b^t	e_b^{tot}
5096	2485	2611	0.09980	0.09575	0.09772

Following the security proof from Koashi and Preskill [24], the final key rate is given by

$$R \geqslant Q[1 - fH(e_b) - H(e_p)], \tag{1}$$

where Q is the sifted key rate; f is the error correction efficiency (we use $f = 1.16$ here); e_b and e_p are the bit and phase error rates, respectively; and $H(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$ is the binary entropy function. The estimation of the phase error rate is the key to the security analysis [26]. Due to the symmetry between the complementary bases, the phase error rate of one basis can be estimated from the bit error rate of the other basis. The details of the analysis are shown in the Appendix A.

The experimental data were accumulated for 89 h, and the results are shown in Table I and Fig. 3. The total number of bits of the sifted key is 5096. The error rate in the energy basis is consistent with the average visibility of the correlation fringe according to the relation $e = (1 - V)/2$. Due to the slight difference between the error rates of sifted key in the two bases, the secure key rates were evaluated for the two bases separately. In postprocessing, we applied the Gottesman-Lo security analysis method using two-way classical communication [27]. See the Appendix B for details. As shown in Fig. 3(b), 118 bits of secure key were distilled from the sifted key.

In our experiment, the average photon-pair number per two consecutive pump pulses was approximately 0.03, which upper-bounded the visibility to approximately 84%. The rest of the degradation can be attributed to the imperfection of the synchronization and the devices, such as BS and MZIs. As our system was automatically stabilized, we can decrease the intensity of the entangled photon pairs and extend the measurement time if higher visibility is required. The count rate is limited by the intensity of the photon-pairs, detection efficiency, and the loss of the sources. The detection efficiency of the SNSPDs was about 0.65 in Eve's node and 0.5 in the other two nodes with dark count rates of approximately 100 Hz. The insertion loss of filters with is about 10 dB for each path. Note that the count rate can be improved by using state-of-the-art devices instead of commercial ones. Moreover, compared to the laboratory experiments, the count rate in our experiment is further decreased by the transmission losses in

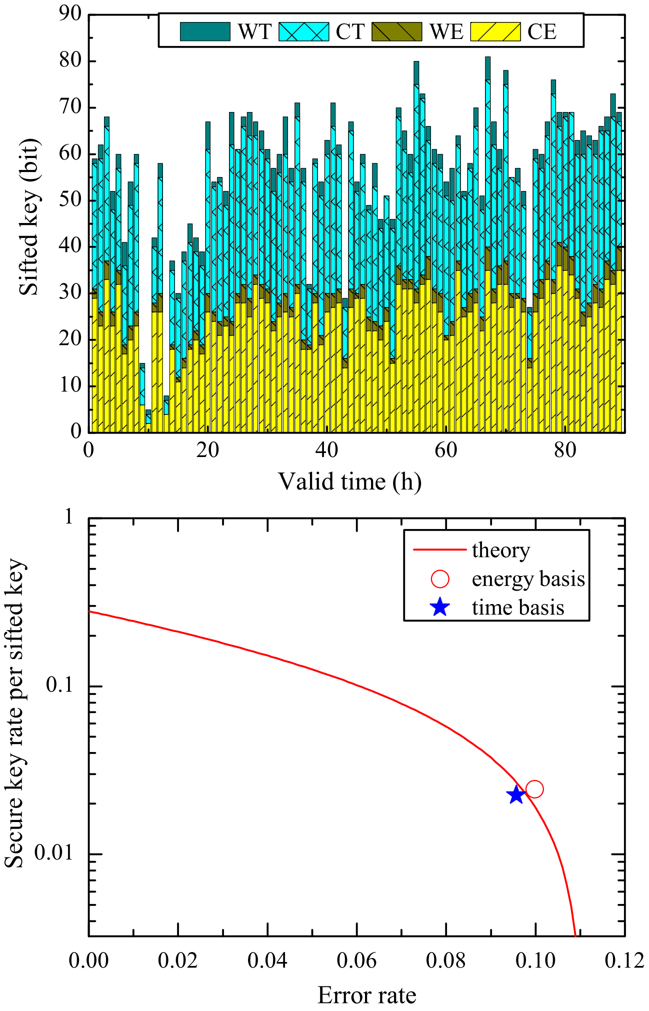

FIG. 3. Experimental results. (a) Sifted key in the time basis (T) and the energy basis (E) per hour, with the numbers of wrong (W) and correct (C) bits. (b) Secure key rate per sifted key with one B step of the entanglement swapping based QKD as well as the simulation result. The circle and star correspond to the experimental result in the energy basis (60 bits) and the time basis (58 bits), respectively. In the simulation, $N^e = N^t = 2500$ and $e_b^e = e_b^t$.

the optical fiber, which is approximately 3 dB for the Alice-Eve link and 6 dB for the Bob-Eve link.

In conclusion, we have realized entanglement swapping with two independent entangled photon-pair sources 12.5 km apart and experimentally demonstrated QKD with the swapped entanglement. The QKD experiment with this scheme enjoys both MDI and source-independent security properties. We need to point out that the security of such a scheme is not fully device-independent, which requires extremely high detection efficiencies [28–30]. The underlying security assumption is that Alice and Bob's local detector efficiencies are independent of the basis choices [31], which offers basis-independent sources [24,25]. This assumption can be guaranteed when the entangled source is single-mode or the local measurement device follows the squashing model [32]. Therefore, our QKD experiment is immune to attacks aimed at the time-energy based Bell inequality test [33], which makes use of the postselection loophole in the Franson-type Bell test [34]. The detection rate in our experiment is not high enough for practical application of QKD. This can be improved by using SNSPDs with higher detection rate, increasing the repetition rate of the system and reduce the loss in our experiment. However, an ultimate method to solve this problem is quantum repeater, which requires entanglement swapping combining with quantum memories [5,6]. Note that our setup can be directly coupled with the Erbium-doped quantum memory [35].

ACKNOWLEDGMENTS

The authors thank H. Lu, X.-L. Wang, Q. Zhou, and H.-L. Yin for enlightening discussions and especially Y. Liu for his useful discussions and comments on the key rate analysis. This work was supported by the National Fundamental Research Program (under Grants No. 2013CB336800 and No. 2011CBA00303), the National Natural Science Foundation of China, the Chinese Academy of Science, the 10000-Plan of Shandong Province, and Quantum Ctek Co., Ltd.

APPENDIX A: PHASE ERROR RATE ESTIMATION

In postprocessing, the phase error rate of one basis can be estimated by the bit error rate of the other basis. Here we take the time basis for example to show how to estimate phase error rate. The analysis for the energy basis is the same. Due to the symmetry between the time and energy bases, in the large-data-size limit, the phase error rate in the time basis, e_p^t, equals the bit error rate of the energy basis, e_b^e,

$$e_p^t = e_b^e = E, \tag{A1}$$

where E is the quantum bit error rate in the energy basis. Considering the statistical fluctuation, there exists a gap between e_b^e and e_p^t. The random sampling method provides an upper bound for this gap with a fixed failure probability ϵ [36,37]; in our security analysis, $\epsilon = 10^{-10}$. Here the Serfling inequality [38] is applied to estimate this gap. The upper bound for e_p^t is as follows:

$$e_p^t \leqslant e_b^e + g(\epsilon, n_e, n_t), \tag{A2}$$

where $g(\epsilon, n_e, n_t)$ is the function of failure probability ϵ, sample size n_e, and the other basis population size n_t.

Considering a finite list of values $x_1, \ldots, x_N$, for any i, $x_i \in [a,b]$, n is the sample size and N is the population. $X_1, \ldots, X_n$ are the values of chosen sample, S_n is the summation of them, $S_n = \sum X_i$, $\mu = \frac{\sum_1^N x_i}{N}$ is the total average value, and $f_n^* = n - 1/N$ is the sampling fraction. For $k > 0$, we have

$$\begin{aligned} P_n(k) &= P(n\mu - S_n \geqslant nk), \\ P_n(k) &\leqslant \exp\left[\frac{-2nk^2}{1 - f_n^*}(b - a)\right]. \end{aligned} \tag{A3}$$

In our case, $e_p^t = \mu$; $e_b^e = S_n/n$; $a = 0$; $b = 1$; n_e and n_t are the numbers of raw key for energy basis and time basis, respectively; $N = n_e + n_t$ is the total raw key, and thus

$$Pr\left(e_p^t \geqslant e_b^e + k\right) \leqslant \exp\left[-k^2 \frac{2n^e(n^e + n^t)}{n^t + 1}\right]. \tag{A4}$$

Consequently, the upper bound for e_p is

$$e_p^t \leqslant e_b^e + \sqrt{\frac{(n^t + 1)\log(1/\epsilon)}{2n^e(n^e + n^t)}} \tag{A5}$$

and

$$g(\epsilon,n_e,n_t) = \sqrt{\frac{(n^t+1)\log(1/\epsilon)}{2n^e(n^e+n^t)}}. \tag{A6}$$

APPENDIX B: B-STEP TWO-WAY CLASSICAL COMMUNICATION

In Shor and Preskill's [26] security proof, the maximal tolerable error rate is only 11% with one-way classical communication (1-LOCC). In some practical cases, the bit error rate may be higher, or close to 11%. It is too high to generate keys. Gottesman and Lo's security proof [27] shows that QKD with two-way classical communication can tolerate a much higher bit error rate than that with 1-LOCC. Thus we apply the B step method to perform two-way classical communication and the final key rate after one B step is

$$R \geqslant \frac{p_s}{2} Q[1 - fH(e_b') - H(e_p')], \tag{B1}$$

where e_b' and e_p' are the bit error rate and phase error rate after a B step, respectively, and $p_s = {e_b}^2 + (1-e_b)^2$.

Classically, a B step involves random pairing of the key bits. The strings x_1, x_2 are on Alice'side and y_1, y_2 are on Bob'side. Both Alice and Bob announce the parities, $x_1 \oplus x_2$, $y_1 \oplus y_2$. If their parities are the same, then they keep x_1, y_1; otherwise, they discard all of them. Note that at least half of the raw keys are discarded. After a B step, the bit error rate e_b' and the upper bound for phase error rate e_p' [39] becomes

$$\begin{aligned} e_b' &= \frac{{e_b}^2}{p_s}, \\ e_p' &\leqslant 2\frac{e_p(1-e_p-e_b)}{p_s}. \end{aligned} \tag{B2}$$

[1] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[2] J. Bell, Physics **1**, 195 (1964).

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[4] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[5] H. J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

[7] C. H. Bennett and G. Brassard, in *IEEE International Conference on Computer System and Signal Processing* (IEEE, Los Alamitos, CA, 1984), pp. 175–179.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[9] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[10] H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **71**, 050302 (2005).

[11] T. Yang, Q. Zhang, T. Y. Chen, S. Lu, J. Yin, J. W. Pan, Z. Y. Wei, J. R. Tian, and J. Zhang, Phys. Rev. Lett. **96**, 110501 (2006).

[12] R. Kaltenbaek, R. Prevedel, M. Aspelmeyer, and A. Zeilinger, Phys. Rev. A **79**, 040302 (2009).

[13] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, Nat. Phys. **3**, 692 (2007).

[14] T. Herbst, T. Scheidl, M. Fink, J. Handsteiner, B. Wittmann, R. Ursin, and A. Zeilinger, Proc. Natl. Acad. Sci. USA **112**, 14202 (2015).

[15] R. B. Jin, M. Takeoka, U. Takagi, R. Shimizu, and M. Sasaki, Sci. Rep. **5**, 9333 (2015).

[16] R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, Phys. Rev. Lett. **96**, 240502 (2006).

[17] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Nature **526**, 682 (2015).

[18] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and J.-W. Pan, Nat. Photon. **10**, 671 (2016).

[19] A. Peres, J. Mod. Opt. **47**, 139 (2000).

[20] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Phys. Rev. Lett. **93**, 180502 (2004).

[21] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

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

[23] Y.-L. Tang, H.-L. Yin, X. Ma, Chi-Hang Fred 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).

[24] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[25] X. Ma, C.-H. Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).

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

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

[28] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[29] C. A. Miller and Y. Shi, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2014), pp. 417–426.

[30] Z. Cao, Q. Zhao, and X. Ma, Phys. Rev. A **94**, 012319 (2016).

[31] X. Ma and H.-K. Lo, New J. Phys **10**, 073018 (2008).

[32] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[33] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J. A. Larsson, Sci. Adv. **1**, e1500793 (2015).

[34] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).

[35] E. Saglamyurek, J. Jin, V. B. Verma, M. D. Shaw, F. Marsili, S. W. Nam, D. Oblak, and W. Tittel, Nat. Photon. **9**, 83 (2015).

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

[37] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).

[38] R. J. Serfling, Ann. Statist. **2**, 39 (1974).

[39] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).