

Experimental Side-Channel-Secure Quantum Key Distribution

Chi Zhang,^{1,2,3} Xiao-Long Hu,⁴ Cong Jiang,³ Jiu-Peng Chen,^{1,2,3} Yang Liu,^{1,2,3} Weijun Zhang^{①,5}, Zong-Wen Yu,⁶
 Hao Li,⁵ Lixing You,⁵ Zhen Wang,⁵ Xiang-Bin Wang^{①,2,3,4,*}, Qiang Zhang^{①,1,2,3,†} and Jian-Wei Pan^{1,2,‡}

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


²Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics,
 University of Science and Technology of China, Shanghai 201315, China

³Jinan Institute of Quantum Technology, Jinan, Shandong 250101, China

⁴State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University,
 Beijing 100084, China

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

⁶Data Communication Science and Technology Research Institute, Beijing 100191, China

 (Received 9 March 2021; revised 20 August 2021; accepted 14 April 2022; published 13 May 2022)

Quantum key distribution can provide unconditionally secure key exchange for remote users in theory. In practice, however, in most quantum key distribution systems, quantum hackers might steal the secure keys by observing the side channels in the emitted photons, such as the photon frequency spectrum, emission time, propagation direction, spatial angular momentum, and so on. It is hard to prevent such kinds of attacks because side channels may exist in many dimensions of the emitted photons. Here we report an experimental realization of a side-channel-secure quantum key distribution protocol which is not only measurement-device independent, but also immune to all side-channel attacks to the photons emitted from Alice's and Bob's labs. We achieve a secure key rate of 1.73×10^{-6} per pulse through 50 km fiber spools.

DOI: 10.1103/PhysRevLett.128.190503

Introduction.—The cyber security today is protected by the modern cryptography, which is based on the computational complexity assumption. This assumption, however, might be challenged by the progress in algorithm [1] or super computer [2,3]. Besides, hackers may steal the information from side channels instead of decrypting the ciphered message. For example, one can attack the communication terminals that store the secret bits by detecting the physical effects like time shift [4], power consumption [5], electromagnetic leak [6], sound variation [7], etc.

Guaranteed by basic principles of quantum mechanics [8], quantum key distribution (QKD) generates information theoretically secure keys [9–16] even if hackers have the most powerful attacks that physical laws permit. However, side channels may appear in practical QKD systems due to device imperfections [15], leading to potential security loopholes. Actually, device imperfections, especially those in the detections, are the most serious threat to “prepare-and-measure” QKD systems, such as time-shift attack [17,18], detector-blinding attack [19,20], detector-after-gate attack [21], and so on. Luckily, this can be solved by measurement-device-independent QKD (MDIQKD) [22–29], which is immune to all attacks to measurement devices. But the problem of side channels from the source still exists, leaving potential loopholes. Though the security

is proven with the ideal encoding state, it can still be undermined when there is difference in the side channels of the emitted photons. For example, in a protocol using polarization encoding or phase encoding, there can be imperfections in side-channel space such as the frequency spectrum, the light emission time, etc. These imperfections are highly possible, because the encodings in the source inevitably operate on a larger space. For example, the intensity modulation in the source may also affect the timing and frequency of the pulse. In such cases, the eavesdropper may acquire the secure keys by monitoring the side channels only, without affecting the encoding space. As a simple example, the eavesdropper may distinguish the intensity by monitoring the wavelength. Thus, the side channels actually undermine the security of practical QKD systems, say, Eve may hide her presence perfectly in performing the side-channel attack.

Recently, Wang *et al.* proposed an interesting side-channel-secure protocol [30]. This protocol is not only immune to all attacks in the side-channel space of emitted photons, such as the attacks on the imperfections of the frequency spectrum, emission time, nonideal propagation direction, spatial angular momentum, etc, but also closes all potential loopholes in detection, by adapting the measurement-device-independent architecture, so it has a high security level. Say, the protocol is secure under whatever

attacks to photons emitted from Alice's and Bob's labs, while Alice and Bob only need to prepare their source states correctly in operational space (the photon number space). The only potential attack Eve can implement is the attack against Alice's or Bob's setup inside their labs such as a Trojan-horse attack through actively modifying the source inside Alice's and Bob's labs by sending light. This can be prevented by isolating the secure zone with proper isolation. In the protocol, coherent state without any phase randomization is used as the source, so the decoy-state assumption is not required; Alice and Bob only decide on sending or not sending the coherent state for encoding, so no more modulations are needed in the experiment. The only assumption in the protocol is the perfect vacuum. The theoretically proved side channel security of the emitted photons and the simple operation in encoding are the essential differences between the side-channel-secure QKD [30] and the twin-field QKD (TF-QKD) [31], including the sending-or-not-sending (SNS) protocol [32]. There are other protocols to achieve the side-channel-secure protocols security [23,33–35], but this protocol [30] is the only one that can be implemented with commercial products and reach long distance.

Here, we experimentally realize the side-channel-secure QKD [30] over different distances. Secure key rate of 1.73×10^{-6} per pulse is achieved over 50 km. Precise wavelength control and fast phase compensation have been utilized to accurately control and estimate the phase difference in the single-photon interference of two independent laser sources.

Protocol.—We adopt the protocol with phase reference pulses and phase postselection in Ref. [30] for our experiment. As discussed in Ref. [30], by this option, instead of using active phase compensation, we postselect those effective events with a condition that sufficiently limits small phase errors. In this protocol, we assume the vacuum is perfect and the upper bound of the intensity of the coherent state is known. For completeness, we write the full protocol here:

Step 1. At each time window, Alice (Bob) prepares a non-random phase coherent state $|\alpha_A\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} [(\sqrt{\mu}e^{i\gamma_A})^n / \sqrt{n!}] |n\rangle$ ($|\alpha_B\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} [(\sqrt{\mu}e^{i\gamma_B})^n / \sqrt{n!}] |n\rangle$), where $\alpha_A = \sqrt{\mu}e^{i\gamma_A}$ ($\alpha_B = \sqrt{\mu}e^{i\gamma_B}$). With probability ε , Alice (Bob) decides on *sending* and she (he) sends out the coherent state $|\alpha_A\rangle$ ($|\alpha_B\rangle$) to Charlie and puts down a classical bit value 1 (0) locally; with probability $1 - \varepsilon$, she (he) decides on *not sending* and she (he) does not send out anything and puts down a classical bit value 0 (1) locally. These pulses (coherent states or vacuum) are called signal pulses. She (He) also prepares a strong reference pulse time multiplexed with the signal pulses. The phases of the reference pulses are modulated periodically and this will be presented in detail later. No matter what she (he) decides, she (he) always sends the reference pulse to Charlie. They define a \tilde{Z} window as a time window when either Alice or Bob decides on sending and the other decides on not sending.

Note.—Different from the decoy-state method requiring phase-randomized coherent states, here Alice and Bob are required to use the nonrandom phase coherent states. Their initial individual phases (γ_A and γ_B) are fixed during the whole experiment. The reference pulse is introduced only to carry the information about the phase, which is allowed to be known by Eve according to the protocol. It has nothing to do with either the bit value or the state of the signal pulse (except the phase). Thus the introduction of reference pulse does not affect the security.

Step 2. Charlie measures the signal pulses at the measurement station between Alice and Bob and announces which detector clicks. If one and only one detector clicks, this time window is regarded as an *effective time window*. In addition, he measures the reference pulses and announces the phase difference δ between Alice's and Bob's pulses to learn the phase shifts in the channels. It is shown schematically in Fig. 1.

Step 3. According to Charlie's measurement results, Alice and Bob keep the bits from *all* events in which the phase difference δ satisfies the condition

$$|\delta| < \Delta, \quad (1)$$

where Δ is the relative phase difference threshold, and they announce the bit values of other bits, and then discard them. Here, $|x|$ means the degree of the minor angle enclosed by the two rays that enclose the rotational angle of degree x , e.g., $|-15\pi/8| = |15\pi/8| = \pi/8$.

Step 4. Among the preserved bits, Alice and Bob take a random subset u , through classical communication, to do error test and parameter estimation. They announce all bit values in set u through classical channel. They discard the bits from the set u after the error test, and the set of remaining bits is called the set v .

Step 5. Alice and Bob distill (by conducting error correction and privacy amplification) the effective bits from the set v , with the asymptotic key rate for the number of final bits

$$n_F = n_{\tilde{Z}}[1 - H(\bar{e}^{ph})] - f n_v H(E_v), \quad (2)$$

where $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the entropy function; $n_{\tilde{Z}}(n_v)$ is the number of remaining effective bits from \tilde{Z} windows (all time windows) in set v ; \bar{e}^{ph} is the

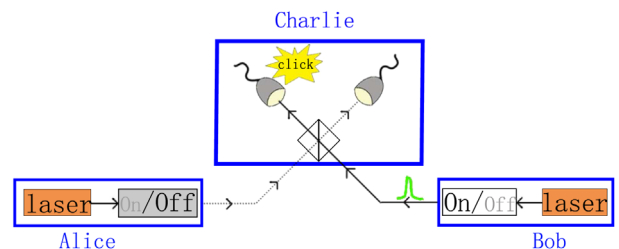


FIG. 1. A schematic illustration of the side-channel-secure QKD protocol.

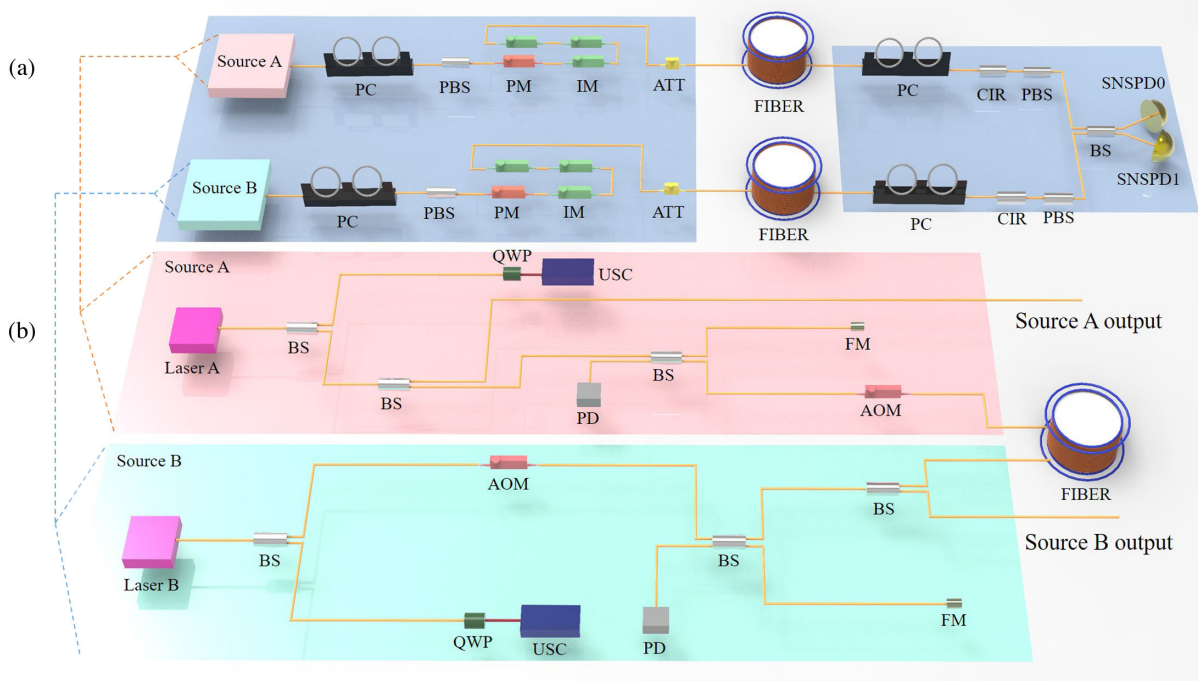


FIG. 2. (a) Experimental setup. Alice and Bob modulate the phase-locked lasers with a phase modulator (PM) and three intensity modulators (IM1, IM2, IM3). The PM is used to encode the reference pulses; the intensity modulator IM1 is used to set sending or not sending of the signal, while IM2 and IM3 are used to set the intensities between the reference and signal pulses. Additional attenuators (ATTs) in the secure zones are calibrated to set the proper output photon intensity. Charlie interferes and measures the light from Alice and Bob with superconducting nanowire single-photon detectors. Polarization controller (PC), polarization beam splitter (PBS), circulator (CIR), beam splitter (BS). (b) Alice and Bob lock the wavelength of their lasers with a frequency-locking system [37]. The light transmits through an additional 50 km fiber. Acousto-optic modulator (AOM); Faraday mirror (FM); photodiode (PD); quarter wave plate (QWP); ultrastable cavity (USC).

upper bound of the phase-flip error rate for bits in effective \tilde{Z} windows in set v ; f is the correction efficiency factor which we set $f = 1.1$, and E_v is the bit-flip error rate of effective bits in set v . The values of $n_{\tilde{z}}$ and \bar{e}^{ph} can be obtained by the observed data of the set u asymptotically.

Equivalently, the key rate (per pulse) can be written as

$$R = \frac{1}{N_t} \{n_{\tilde{z}}[1 - H(\bar{e}^{ph})] - fn_v H(E_v)\}, \quad (3)$$

where N_t is the total number of signal pulses that Alice (Bob) sends. The details of the calculation of the key rate are shown in the Supplemental Material [36].

The essential idea of the side-channel-secure QKD protocol [30] is that a real-life source is secure if there exists a quantum process that can map a virtual ideal source, which is proved secure, to this real-life source. In our experiment, Alice and Bob each emits only one coherent state and one vacuum state, and the vacuum state has no side channel. Such a process that transforms the ideal source to the real-life source must exist. Thus, the protocol with a real-life source is still secure even if there is side channel in the coherent state.

Experiment.—Our experimental setup is schematically shown in Fig. 2(a). We use the time-frequency dissemination technology to accurately control the phase difference in the single-photon interference of two independent laser sources. Intensity modulators are used to control the “sending” and “not sending” encoding. Finally, high performance superconducting nanowire single-photon detectors are used to meet the high efficiency requirement of the pulses.

First, stable lasers with exact wavelength are required in the remote single-photon interference in our experiment. The wavelengths of Alice’s and Bob’s independent lasers are locked with the time-frequency transmission technology [37], through additional 50 km fiber spools shown in Fig. 2(b). Alice uses a commercial sub-Hz laser source with a central wavelength of 1550.1665 nm and it is internally locked into her cavity; Bob uses a commercial kilo-Hz fiber laser, locked to an ultra-low-expansion (ULE) glass cavity with Pound-Drever-Hall (PDH) technique [38,39]. The final linewidth is approximately 1 Hz with a central wavelength of 1550.1674 nm. Obviously, the frequency difference of two laser sources about 112 MHz still exists. Therefore, at Bob’s station, we insert an acoustic-optic modulator (AOM) with a tunable carrier frequency to

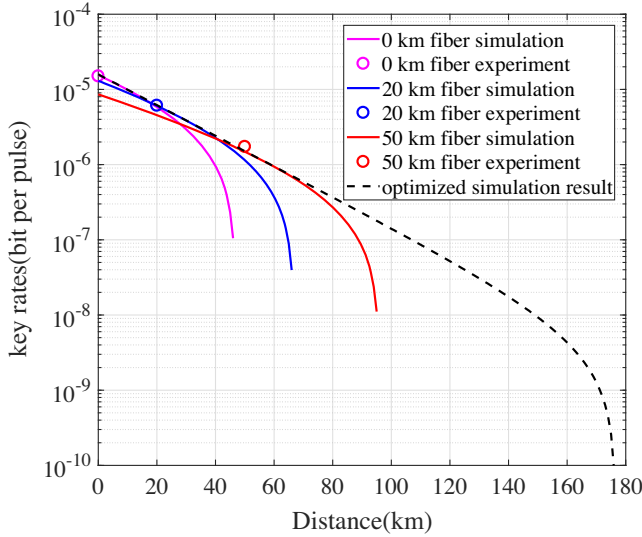


FIG. 3. Secure key rates. The magenta, blue, and red circles represent the experimental key rates over 0, 20, and 50 km fiber spools accordingly. The solid magenta, blue, and red curves show the simulated key rates under three fixed intensities which we applied in three experiments respectively. The dashed black curve illustrates the optimized simulation results point by point.

compensate the frequency difference in real time. The phase noise via the 50 km fiber spools is cancelled in real time using another AOM with a carrier frequency of 40 MHz by Alice.

With these narrow linewidth coherent light sources prepared, the next step is to encode. As for signal pulses, only one intensity for sending is required. We use an intensity modulator (IM) to modulate the signal to 240 ps pulse duration for sending and to vacuum for not sending. Based on the experimental conditions, we optimize the coherent state intensity μ and the probability of sending ε . The sending and not sending are determined by previously prepared quantum random numbers, with only one intensity modulation required. While the relative phase between Alice and Bob is not stable: the fluctuation of the fiber length and refractive index directly affect the relative phase; the wavelength difference of the sources may also contribute to the phase drift.

In order to correct the relative phase drift, we adopt strong reference pulses to estimate the relative phase between Alice's and Bob's signal pulses [37]. For every 1 μ s time interval, 100 signal pulses are encoded in the first 400 ns as sending or not sending; then in the following 440 ns, 4 phase encoded reference pulses are sent; the final 160 ns are used as the recovery time for the superconducting nanowire single-photon detectors (SNSPDs), with vacuum states sent.

The relative intensities between signal and reference pulses are modulated with another two IMs. All three IMs are set to vacuum if the signal state is not sending to increase the extinction ratio. To estimate the relative phases

in the fibers, a phase modulator (PM) in Alice's station sets the phase of her reference pulses to $\{0, \pi/2, \pi, 3\pi/2\}$ respectively, while all of Bob's phase reference pulses are set to π . Note that the phase modulation is only applied to Alice's and Bob's reference pulses to estimate relative phase drift in the fibers; the phases of the signals are always set to 0. In another word, the phase modulation works only as an estimation of the reference frame, thus it would not introduce side channels to the system.

The signals from Alice and Bob are transmitted through fiber spools respectively to the measurement station, Charlie. The light is filtered with circulators to eliminate the SNSPD backscattered light. Then polarization controllers and polarization beam splitters are used to correct the polarization before interference at Charlie's beam splitter. The additional loss of the optical components are 4.31 for Alice and 4.32 dB for Bob. The interference results are measured with two SNSPDs with detection efficiencies of 82.0% and 84.0%, and recorded by a time tagger. The dark count rate of the SNSPD is about 3 Hz, or 7.2×10^{-10} in a signal window.

We performed the side-channel-secure QKD over a distance of 0, 20, 50 km standard optical fiber. The total loss of 20 km and 50 km fiber spools is 3.99 and 9.95 dB, respectively, with an attenuation coefficient of 0.2 dB/km. For different fiber lengths, the total number of pulses sent by Alice and Bob is set to 8.82×10^{11} . The valid detections are 291 520 690 and 111 514 074 and 27 979 651 for 0, 20, 50 km. For each pair of signal pulses, the relative phase between Alice's and Bob's signal pulses is calculated with the phase estimation procedure [37]. Next, a threshold of relative phase difference Δ is set. Only the data with the relative phase $|\delta| < \Delta$ are kept as raw keys, as in Eq. (1); for all other detections, Alice and Bob disclosed the bit values to calculate the state of the twin-field after phase post-selection which is

$$\begin{aligned} \rho' = & c_1 |\alpha, \alpha\rangle \langle \alpha, \alpha| + c_2 |\alpha, 0\rangle \langle \alpha, 0| \\ & + c_3 |0, \alpha\rangle \langle 0, \alpha| + c_4 |0, 0\rangle \langle 0, 0|, \end{aligned} \quad (4)$$

where $c_1, c_2, c_3,$ and c_4 is the proportion of the state $|\alpha, \alpha\rangle, |\alpha, 0\rangle, |0, \alpha\rangle,$ and $|0, 0\rangle$ respectively after phase postselection (See Supplemental Material for details about the calculation [36]). After the phase postselection, a portion p_t of the bits are selected as "test bits." The values of the test bits announced by Alice and Bob, as well as the detections, are then used for calculating the number of remaining effective bits in \tilde{Z} window $n_{\tilde{Z}}$ and the upper bound of phase-flip error rate $\bar{\varepsilon}^{ph}$. The test bits are then discarded. In our experiment, the threshold of relative phase difference is set to $\Delta = 30^\circ$ by optimization and the test bits probability is set to $p_t = 0.1$. Results including $n_{\tilde{Z}}$ and $\bar{\varepsilon}^{ph}$ are listed in Supplemental Material [36]. Finally, we acquired secure key rates of 1.50×10^{-5} ,

6.11×10^{-6} , 1.73×10^{-6} per pulse for 0, 20, 50 km fiber length. The key rate obtained in our experiment and the theoretical simulation are plotted in Fig. 3. We note that the actual state is not a perfect vacuum state when Alice (Bob) decides not to send a coherent state due to the finite extinction ratio of IMs. The total extinction ratio of signal to vacuum through three IMs is 70 dB and after taking actual intensity of “vacuum” state into consideration, the secure key rates only decrease by less than 0.1% under the assumption that all sources are stable in the whole space. (See Supplemental Material for detailed calculation [36]). With our experimental parameters, it is predicted that a more than 170 km distribution distance can be achieved with our setup.

Considering the system frequency, the secure key rate is 173 bps at 50 km which is magnitudes smaller than that of 70 kbps of MDIQKD [40], and 10 kbps to 1 Mbps of decoy BB84 protocols [41–43]. The lower key rate is the price for the high practical security, since we have to use very weak coherent state to take the worst-case analysis in this protocol guaranteeing the side-channel-secure property.

In conclusion, we have demonstrated the side-channel-secure QKD protocol experimentally and obtained secure keys over 50 km fiber spools. Our experiment shows that emitted photon state side-channel-free and measurement-device-independent security can be simultaneously achieved in the QKD system with matured existing technologies.

We would like to thank Feihu Xu for insightful discussions. This work was supported by the National Key R&D Program of China (Grants No. 2020YFA0309800, No. 2017YFA0303900, No. 2017YFA0304000), the National Natural Science Foundation of China (T2125010), the Chinese Academy of Science (CAS), Key R&D Plan of Shandong Province (Grants No. 2019JZZY010205, No. 2020CXGC010105), and Anhui Initiative in Quantum Information Technologies.

*xbwang@mail.tsinghua.edu.cn

†qiangzh@ustc.edu.cn

‡pan@ustc.edu.cn

- [1] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, in *Advances in Cryptology—CRYPTO 2017* (Springer, Cham, Switzerland, 2017), pp. 570–596.
- [2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1994), pp. 124–134.
- [3] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA* (1996), pp. 212–219.
- [4] P. C. Kocher, in *Advances in Cryptology—CRYPTO '96*, edited by N. Kobitz (Springer, Berlin and Heidelberg, 1996), pp. 104–113.
- [5] P. Kocher, J. Jaffe, and B. Jun, in *Advances in Cryptology—CRYPTO' 99*, edited by M. Wiener (Springer, Berlin and Heidelberg, 1999), pp. 388–397.
- [6] W. van Eck, *Comput. Secur.* **4**, 269 (1985).
- [7] D. Genkin, A. Shamir, and E. Tromer, in *Advances in Cryptology—CRYPTO 2014*, edited by J. A. Garay and R. Gennaro (Springer, Berlin and Heidelberg, 2014), pp. 444–461.
- [8] W. Wootters and W. Zurek, *Nature (London)* **299**, 802 (1982).
- [9] C. BENNETT, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (1984), pp. 175–179.
- [10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [11] W.-Y. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [12] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [13] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [15] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [16] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [17] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Quantum Inf. Comput.* **7**, 73 (2007).
- [18] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, *Phys. Rev. A* **78**, 042333 (2008).
- [19] V. Makarov, *New J. Phys.* **11**, 065003 (2009).
- [20] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Nat. Photonics* **4**, 686 (2010).
- [21] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, *New J. Phys.* **13**, 013043 (2011).
- [22] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [23] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [24] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, *Phys. Rev. A* **85**, 042307 (2012).
- [25] X.-B. Wang, *Phys. Rev. A* **87**, 012320 (2013).
- [26] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, *Nat. Commun.* **5**, 3732 (2014).
- [27] F. Xu, H. Xu, and H.-K. Lo, *Phys. Rev. A* **89**, 052333 (2014).
- [28] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, *Phys. Rev. A* **93**, 042324 (2016).
- [29] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X. B. Wang, and J. W. Pan, *Phys. Rev. Lett.* **117**, 190501 (2016).
- [30] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, *Phys. Rev. Applied* **12**, 054034 (2019).
- [31] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, *Nature (London)* **557**, 400 (2018).
- [32] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, *Phys. Rev. A* **98**, 062323 (2018).
- [33] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (IEEE Computer Society, Los Alamitos, CA, 1998), p. 503.
- [34] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).

- [35] V. Scarani and R. Renner, *Phys. Rev. Lett.* **100**, 200501 (2008).
- [36] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.128.190503> for calculations about secure key rates, the state of the twin-field after phase postselection method, detailed experimental results, and calculations about key rates considering nonideal vacuum sources.
- [37] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **123**, 100505 (2019).
- [38] R. Drever, J. L. Hall, F. Kowalski, J. Hough, G. Ford, A. Munley, and H. Ward, *Appl. Phys. B* **31**, 97 (1983).
- [39] R. V. Pound, *Rev. Sci. Instrum.* **17**, 490 (1946).
- [40] 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).
- [41] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, *Appl. Phys. Lett.* **96**, 161102 (2010).
- [42] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen *et al.*, *Nature (London)* **589**, 214 (2021).
- [43] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu *et al.*, *npj Quantum Inf.* **7**, 1 (2021).