Editors' Suggestion   Featured in Physics

Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution

Wen-Zhao Liu,[1,2,3] Yu-Zhe Zhang,[1,2,3] Yi-Zheng Zhen,[1,2,3] Ming-Han Li,[1,2,3] Yang Liu,[4] Jingyun Fan,[5] Feihu Xu,[1,2,3] Qiang Zhang,[1,2,3] and Jian-Wei Pan[1,2,3]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China*
[2]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, People's Republic of China*
[3]*Shanghai Research Center for Quantum Sciences, Shanghai 201315, People's Republic of China*
[4]*Jinan Institute of Quantum Technology, Jinan 250101, People's Republic of China*
[5]*Shenzhen Institute for Quantum Science and Engineering and Department of Physics, Southern University of Science and Technology, Shenzhen 518055, People's Republic of China*

(Received 4 January 2022; accepted 30 June 2022; published 27 July 2022)

The security of quantum key distribution (QKD) usually relies on that the users' devices are well characterized according to the security models made in the security proofs. In contrast, device-independent QKD—an entanglement-based protocol—permits the security even without any knowledge of the underlying quantum devices. Despite its beauty in theory, device-independent QKD is elusive to realize with current technologies. Especially in photonic implementations, the requirements for detection efficiency are far beyond the performance of any reported device-independent experiments. In this Letter, we report a proof-of-principle experiment of device-independent QKD based on a photonic setup in the asymptotic limit. On the theoretical side, we enhance the loss tolerance for real device imperfections by combining different approaches, namely, random postselection, noisy preprocessing, and developed numerical methods to estimate the key rate via the von Neumann entropy. On the experimental side, we develop a high-quality polarization-entangled photon source achieving a state-of-the-art (heralded) detection efficiency about 87.5%. Although our experiment does not include random basis switching, the achieved efficiency outperforms previous photonic experiments involving loophole-free Bell tests. Together, we show that the measured quantum correlations are strong enough to ensure a positive key rate under the fiber length up to 220 m. Our photonic platform can generate entangled photons at a high rate and in the telecom wavelength, which is desirable for high-speed generation over long distances. The results present an important step toward a full demonstration of photonic device-independent QKD.

DOI: 10.1103/PhysRevLett.129.050502

Introduction.—Quantum key distribution (QKD) [1,2] allows two distant users to share secret keys with information-theoretic security [3]. The security of QKD usually relies on the assumptions that the devices are trusted and well characterized [4–6]. However, the imperfections of the practical devices may provide potential back doors or side channels for adversaries [7,8]. Measurement-device-independent QKD [9,10] (with a recent development in [11]) was proposed to prevent the side-channel attacks on detectors, but leaves the state-preparation devices to be precisely calibrated. Device-independent QKD [12–15] further relaxes the security assumptions on the devices. Given the following assumptions [15], i.e., (i) quantum theory is validity, (ii) no unwanted information leakage from communicating parties to adversaries is allowed, (iii) the communicating parties have local trusted randomness to decide inputs of their measurement devices, (iv) the classical postprocessing units are trusted, and (v) an authenticated public classical channel is shared between the communicating parties, its security can be guaranteed solely based on the violation of Bell inequalities.

The realization of device-independent QKD is nontrivial with current technologies, where the loophole-free violations of the Bell inequalities are usually required [16,17]. Especially in the photonic implementations, the efficiency loss of photons due to transmission and detection becomes a key issue. Although distinguished experiments without the detection loophole have been made [18–30], a much higher efficiency (over 90%) is normally required in the realization of device-independent QKD [15,31–34]. Although recent theoretical progress has been made in reducing the required efficiency [35–43], a practical protocol for a real platform remains elusive.

Here, we report a proof-of-principle experiment of device-independent QKD based on polarization-entangled photons in the scenario of asymptotic limit. We accomplish this via significant theoretical and experimental efforts. On the theoretical side, we propose a protocol that greatly enhances the loss tolerance of the experiments, thereby reducing the efficiency threshold of our setup to about 86%. The idea of our protocol is to postselect the outcomes of the key generation basis [44,45], and then add noise [37] to the remaining strings. The lower bound of the key rate is computed via the recent achievement in estimating the quantum conditional entropy [43]. On the experimental side, we develop an entangled-photon source with the state-of-the-art efficiency of about 87.5%, which surpasses the values reported in previous full-photonic experiments that perform loophole-free Bell tests [18–30], and makes the device-independent experiments possible. Combining the experimental and theoretical advances, we present an experiment of device-independent QKD under fiber length up to 220 m. To maintain a high efficiency, our experiment does not implement the random basis selection [28–30] and the finite-key effect, which are essential for future research toward the real generation of secret keys. However, our experiment verifies that the measured correlations are strong enough to guarantee a positive secret key rate, thus presenting an important step toward a full photonic demonstration.

Protocol.—Our protocol is a modification of the protocol described in [15]. As shown in Fig. 1, entangled photon pairs are shared between Alice and Bob. Considering each of the N rounds of experiments shown in Fig. 1, Alice randomly chooses binary input $x \in \{1,2\}$ and obtains binary outcome $a \in \{0,1\}$, and Bob randomly chooses triple input $y \in \{1,2,3\}$ and obtains binary outcome $b \in \{0,1\}$, where a, $b = 0$ denotes a "click" event on the respective detector, and a, $b = 1$ denotes a "no-click" event. The total probabilities of joint measurement for outcomes (a,b) and inputs (x,y) are denoted as $P(a,b|x,y)$.

Given the raw outcomes $P(a,b|x,y)$, we further introduce the random postselection and noisy-preprocessing approaches before distilling the final keys (see Sec. I.A of Supplemental Material for details). We randomly set part of the N rounds corresponding to the measurement inputs $(\bar{x},\bar{y}) = (1,3)$ as "key-generation round" and the rest as "test round" to test nonlocal correlations, where $\bar{x}$, $\bar{y}$ represent the input for "key-generation round." First, we conduct the random postselection $\mathcal{V}$ over all the "key-generation round," where Alice and Bob each randomly and independently discard bits "1" with probability $1-p$, and keep all the rest of the bits (containing all bits "0" and p of bits "1"). Then, both Alice and Bob announce the discarded rounds via an authenticated public channel. Those renounced "key-generation rounds" from either Alice or Bob will be simultaneously discarded by both parties, regardless of the outcome of the other side. Next, Alice further locally performs a noisy preprocessing $\mathcal{N}$, to generate the noisy raw keys by flipping each bit of her remaining string with probability p_N. Finally, an error correction step allows Alice to share the raw key with Bob, and secret keys can be distilled after privacy amplification. The full procedure for our protocol is as follows.

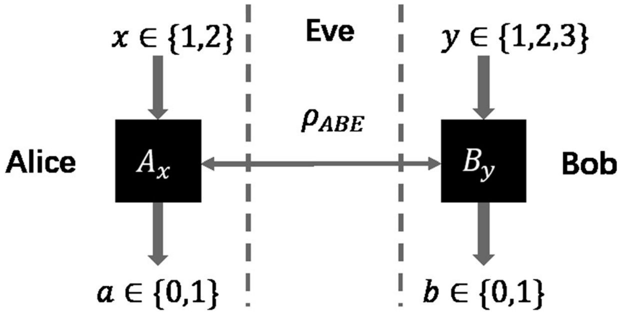

FIG. 1. An illustration of the device-independent QKD protocol. Alice and Bob share a pair of entangled photons potentially controlled by Eve (ρ_{ABE}). Alice performs a measurement to her share with binary input $x \in \{1,2\}$ and binary output $a \in \{0,1\}$. Bob performs a measurement to his share with triple input $y \in \{1,2,3\}$ and binary output $b \in \{0,1\}$.

Assumptions [15]: In addition to the assumptions under the device-independent QKD regime mentioned above, the devices are memoryless and behave identically and independently during the implementation. Correspondingly, the adversary also extracts information in an identically distributed way by performing individual measurements on each round.

Arguments:
N is the number of rounds
p is the postselection probability to keep a bit "1"
p_N is the noisy preprocessing probability to flip a bit
x_i are the inputs for Alice, randomly selected in $\{1,2\}$
y_i are the inputs for Bob, randomly selected in $\{1,2,3\}$

Protocol:

(1) For every round i, Alice and Bob agree that part of rounds corresponding to $(\bar{x}_i,\bar{y}_i) = (1,3)$ are the "key-generation round" to generate the string of raw keys, and the rest corresponding to $(x_i,y_i) \in \{1,2\} \times \{1,2,3\}$ are the "test round" to test the nonlocal correlations. The rest of the steps are all performed on the rounds corresponding to $(\bar{x}_i,\bar{y}_i)$.

(2) *Random postselection* [45]. Alice and Bob each randomly and independently discard bits "1" with probability $1-p$, and keep all the rest of the bits (containing all bits "0" and p of bits "1").

(3) Alice and Bob announce the discarded rounds via an authenticated public channel, and keep rounds not mentioned by either party.

(4) *Noisy preprocessing* [37]. Alice generates the noisy raw keys $\hat{a}_{\bar{x}}$ by flipping each of her remaining bits with probability p_N, where $\hat{a}$ denotes a bit after noisy preprocessing and subscript $\bar{x}$ represents that it is postselected.

(5) *Error correction and privacy amplification.* After a one-way error correction protocol and a privacy amplification procedure, the secret keys can be distilled.

We remark that the random postselection effectively removes a fraction of "nonclick" events that contain few correlations and lots of errors, and therefore suppress the cost of error correction [45]. The noisy preprocessing decreases the correlations between Alice and Eve by mixing the probability distributions with randomness [37]. These two approaches jointly contribute to the enhancement of experimental loss tolerance (see Sec. I.A of Supplemental Material for details).

Key rate estimation.—We consider the collective attack model where the devices behave in an independent and identically distributed manner and the devices are memoryless [46,47] during the implementation of the protocol. In the process of random postselection, given the outcomes (a, b) and the definition p_α for a certain "key-generation round," where $p_\alpha = 1$ if $\alpha = 0$ and $p_\alpha = p$ otherwise, the probability it can be retained is given by $p_{\mathcal{V}_p} = \sum_{(a,b)\in\mathcal{V}_p} \omega_{ab} P(a, b|\bar{x}, \bar{y})$, where $\mathcal{V}_p$ represents the set of postselected rounds and $\omega_{ab} = p_a p_b$. In the infinite-key scenario, given the set of bipartite correlations $\{P(a, b|x, y)\}$ that character the devices, the secret key rate r with error correction can be lower bounded by the Devetak-Winter rate [48],

$$r \geq p_{\mathcal{V}_p}[H(\hat{A}_{\bar{x}}|E, \mathcal{V}_p \to \mathcal{N}_{p_N}) - f_e H(\hat{A}_{\bar{x}}|B_{\bar{y}}, \mathcal{V}_p \to \mathcal{N}_{p_N})], \tag{1}$$

where $\mathcal{N}_{p_N}$ denotes the set of string after noisy preprocessing given postselected set $\mathcal{V}_p$, $\hat{A}_{\bar{x}}$ denotes the noisy raw key of Alice after random postselection and noisy preprocessing, $H(\hat{A}_{\bar{x}}|E, \mathcal{V}_p \to \mathcal{N}_{p_N})$ represents the single-round conditional von Neumann entropy that quantifies the strength of the correlations between Alice and Eve, $H(\hat{A}_{\bar{x}}|B_{\bar{y}}, \mathcal{V}_p \to \mathcal{N}_{p_N})$ represents the single-round cost of one-way error correction from Alice to Bob, and f_e is the error correction efficiency.

As a proof-of-principle experiment, we consider the perfect error correction with Shannon limit $f_e = 1.0$, which is reachable in the case of infinite data size [49] (see Sec. I.C of Supplemental Material for details). We then adopt the method in Refs. [43,49] to show that the single-round conditional von Neumann entropy $H(\hat{A}_{\bar{x}}|E, \mathcal{V}_p \to \mathcal{N}_{p_N})$ can be bounded by a converging sequence of optimizations that can be subsequently computed using the Navascués-Pironio-Acín hierarchy [65,66] (see Sec. I.B of Supplemental Material for details). Note that for all "test rounds," Alice and Bob save the outcomes without any postselections since the Bell tests are implemented without detection loophole [44]. (For more detailed security proof of protocol, please refer to Sec. I.C of Supplemental Material and Ref. [45]).

Experiment.—A schematic of the experiment is depicted in Fig. 2 which consists of three modules. Pairs of polarization-entangled photons at the wavelength of 1560 nm are generated probabilistically via the

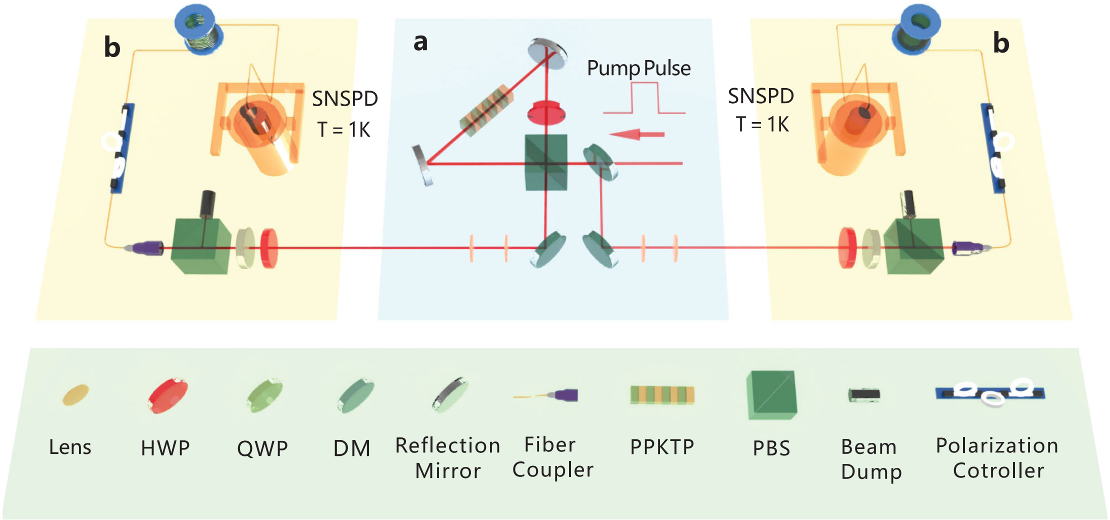

FIG. 2. Schematic of the experiment. a: Entanglement source, creation of pairs of entangled photons: light pulses of 10 ns are injected at a repetition pulse rate of 2 MHz into a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop to generate polarization-entangled photon pairs. The two photons of an entangled pair at 1560 nm travel in opposite directions to two sites Alice and Bob, where they are subject to polarization projection measurements. The PPKTP is placed in the middle of the hypotenuse of the Sagnac loop with a small angle to the light path, which does not significantly affect the upper limit of efficiency that the photonic setup could achieve, but can suppress the reflection of imperfect devices for 1560 nm photons. These enhancements lead to the nonmaximally entangled state generated in our experiment having a better fidelity $99.52 \pm 0.15\%$ as compared to our previous work [26,28,29]. b: Alice and Bob, single-photon polarization measurement: in the measurement sites, Alice (Bob) uses a set of HWP and QWP to project the single photon into predetermined measurement bases. After being collected into the fiber, the single photons transmit through a certain length of fiber and then are detected by a superconducting nanowire single-photon detector (SNSPD) operating at 1 K. HWP, half-wave plate; QWP, quarter-wave plate; DM, dichroic mirror; PBS, polarizing beam splitter.

TABLE I. Efficiencies in existing photonic experiments of *loophole-free* Bell tests and related applications. The efficiencies in the table are averaged over Alice's and Bob's global detection efficiency. (QRNG: quantum random number generation.).

Label	Experiment	Year	Type	Efficiency
(1)	Shalm *et al.* [20]	2015	Bell test	75.15%
(2)	Giustina *et al.* [21]	2015	Bell test	77.40%
(3)	Liu *et al.* [23]	2018	QRNG	79.40%
(4)	Shen *et al.* [24]	2018	QRNG	82.33%
(5)	Bierhorst *et al.* [25]	2018	QRNG	75.50%
(6)	Liu *et al.* [26]	2018	QRNG	78.65%
(7)	Li *et al.* [22]	2018	Bell test	78.75%
(8)	Zhang *et al.* [27]	2020	QRNG	76.00%
(9)	Shalm *et al.* [30]	2021	QRNG	76.30%
(10)	Li *et al.* [29]	2021	QRNG	81.35%
(11)	Liu *et al.* [28]	2021	QRNG	84.10%
(12)	This Letter	2021	QKD	87.49%

TABLE II. The secret key rate as a function of the fiber distance between Alice and Bob. We test the device-independent QKD protocol by adding different lengths of fibers.

Fiber length/m	Key rate/bit · pulse^{-1}	p_N	p
20	2.33×10^{-4}	0.13	0.96
80	5.37×10^{-5}	0.17	0.94
220	1.30×10^{-6}	0.49	0.99

spontaneous parametric down-conversion process in the central module (a). The pairs of photons are sent to two side modules (b), where Alice and Bob perform correlated detections to generate secret keys. The single-photon detection efficiency is, respectively, determined to be $87.16 \pm 0.22\%$ and $87.82 \pm 0.21\%$ for Alice and Bob [49] (see Sec. II.A of Supplemental Material for details), which significantly surpasses the record values in previous loophole-free Bell tests with photons [20–30] (see Table I). Furthermore, the values also surpass the efficiency threshold of 86.2% for device-independent key generation in a realistic scenario [49] (see Sec. I.C of Supplemental Material for details).

According to the numerical studies, we prepare a non-maximally two-photon entangled state $\cos(20.0°)|HV\rangle + \sin(20.0°)|VH\rangle$ and set the measurement settings to $\{-88.22°, 54.29°\}$ and $\{9.75°, 21.45°, -1.07°\}$, respectively, for $x \in \{1, 2\}$ and $y \in \{1, 2, 3\}$ to optimize the probability of key generation, where the values presented in degree are angles of half-wave plates in the polarization measurements by Alice and Bob (see Fig. 2). We experimentally measure a two-photon state fidelity of $99.52 \pm 0.15\%$ with respect to the ideal state and achieve a Clauser-Horne-Shimony-Holt [67] game winning probability of 0.7559 with optimized state and measurement settings (see Sec. III.A of Supplemental Material for details), both substantially improving over previous results [22,23,26,28,29]. We repeat the experiment at a rate of 2×10^6 rounds per second.

Note that as the device-independent QKD itself assumes the validity of quantum theory and that Alice and Bob have trusted random number generators. Nevertheless, the device-independent QKD requires that, in the entire duration of the protocol, the information about the input choices and output results of one party must be unknown at other locations, e.g., Eve's location. Therefore, only closing the locality loophole is not enough to meet the requirement of no unwanted information leakage in the device-independent QKD scenario [15,68]. In our experiment, this is done via the shielding assumption [28,69], which prohibits unnecessary communications between untrusted devices and a potential adversary. For a more definitive experiment to eliminate the shielding assumption, one could use developed electromagnetic shielding techniques, such as materials including sheet metal, metal screen, and metal foam, to avoid possible unwanted information leakage. However, considering the essential photonic channels from entanglement source to both parties, perfect shielding might not be realized experimentally. To reduce experimental complexity, we also alternate the measurement settings instead of randomization to reduce experimental complexity. While these simplifications cannot be adopted in a real-field application of device independent QKD, as we will show, our results demonstrate that the secure key generation is almost achievable using the state-of-the-art technologies.

We conduct 2.4×10^8 rounds of experiment for each of the six combinations of measurement settings (x, y) and perform data analysis following the protocol. With optimized parameters $p_N = 0.13$ and $p = 0.96$, we obtain $H(\hat{A}_{\bar{x}}|E, \mathcal{V}_p \to \mathcal{N}_{p_N}) = 0.560\,206$ with a confidence region $[0.559\,971, 0.560\,442]$ given error probability $\epsilon_t = 10^{-2}$, and $H(\hat{A}_{\bar{x}}|B, \mathcal{V}_p \to \mathcal{N}_{p_N}) = 0.559\,953$ [49]. (see Sec. III.B of Supplemental Material for details). Finally, according to the calculation in Eq. (1), 2.33×10^{-4} bit secret key per pulse is expected to be achieved asymptotically, which corresponds to $[0.17, 4.51] \times 10^{-4}$ key rate after taking into account the confidence region. Furthermore, we show the feasibility to successfully generate secret keys at a fiber length of 220 meters by conducting the same rounds of experiments, for which we reoptimize the experiment over p_N and p. These results are shown in Table II, where the drop of the key rate when increasing the fiber length is mainly due to the decreasing of overall efficiency.

Conclusion.—In conclusion, we demonstrate a proof-of-principle experiment of device-independent QKD against collective attacks using a full-photonic setup. The photonic implementation enjoys the advantages of high-rate entangled-photon generations in the telecom wavelength, which is important for the practical applications involving quantum memories or quantum repeaters forming a quantum internet. With a high-quality entangled photon source, we show the measured correlations are strong enough to guarantee a positive secret key rate. However, to actually produce a key, the real-time random basis selection and more information-processing processes, such as error correction, authentication, and privacy amplification in the finite-key case, remains to be done.

For random basis selection, as implemented routinely by us and other groups [28–30], it may normally introduce about 1% additional efficiency loss, which indeed makes the system working at the marginal point of efficiency threshold. However, we remark that the performance of the entangled system could be greatly improved via enhancing the fidelity of the entanglement state with a different type of design of the entanglement source [20]. This is possible to improve the fidelity from 99.5% in our system to about 99.8% (calculated by given visibility). With the improved fidelity, the required efficiency can drop to 84.8%. This would make it possible to introduce random basis switching.

We further remark that it is still tricky to realize a faithful photonic device-independent QKD with finite-key security. Apart from experimental technical difficulties, the protocol remains to be extended to the general-attack scenario [44]. As we adopt three ingredients in the security analysis, i.e., random postselection, noisy preprocessing, and a numerical method to compute the lower bound of von Neumann entropy, the finite-key analysis involving all these ingredients needs to be developed. However, the main problem is that all experimental rounds might be correlated in a general-attack scenario, where Eve would learn more information of the remaining rounds from the discarded ones. This is similar to the problem encountered with the two-way communication protocol [36,70,71], where Alice and Bob have to randomly keep one of the selected two pairs of outcomes. Nonetheless, we noticed that there have been important theory developments in this direction [72]. It is foreseen that the finite-key analysis combining the method to compute von Neumann entropy with the random postselection and noisy preprocessing will be significantly constructive in the future.

We thank Peter Brown, Roger Colbeck, Charles Lim, Nicolas Sangouard, Jean-Daniel Bancal, Yanbao Zhang, Xingjian Zhang for enlightening discussions. This work was supported by the National Key Research and Development (R&D) Plan of China (2018YFB0504300, 2020YFA0309800), the National Natural Science Foundation of China (T2125010, 62031024, 12005091), the Anhui Initiative in Quantum Information Technologies, the Chinese Academy of Sciences, Shanghai Municipal Science and Technology Major Project (2019SHZDZX01) and the Key-Area Research and Development Program of Guangdong Province (2020B0303010001, 2019ZT08X324).

Wen-Zhao Liu and Yu-Zhe Zhang contributed equally to this work.

Note added.—Recently, we noticed two related works were completed based on trapped ions [73] and trapped atoms [74].

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).

[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

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

[6] R. Renner, Int. J. Quantum. Inform. **06**, 1 (2008).

[7] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

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

[10] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[11] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).

[12] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (IEEE, 1998), pp. 503–509.

[13] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[15] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

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

[17] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Phys. Rev. Lett. **119**, 010402 (2017).

[18] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, Nature (London) **497**, 227 (2013).

[19] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Phys. Rev. Lett. **111**, 130406 (2013).

[20] L. K. Shalm *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).

[21] M. Giustina *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).

[22] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang, L. You, W. J. Munro, J. Yin, J. Zhang, C.-Z. Peng, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan, Phys. Rev. Lett. **121**, 080404 (2018).

[23] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **120**, 010503 (2018).

[24] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Phys. Rev. Lett. **121**, 150402 (2018).

[25] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Nature (London) **556**, 223 (2018).

[26] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Nature (London) **562**, 548 (2018).

[27] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, Phys. Rev. Lett. **124**, 010505 (2020).

[28] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Nat. Phys. **17**, 448 (2021).

[29] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang, W. J. Munro, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan, Phys. Rev. Lett. **126**, 050503 (2021).

[30] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, Nat. Phys. **17**, 452 (2021).

[31] L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[32] B. W. Reichardt, F. Unger, and U. Vazirani, Nature (London) **496**, 456 (2013).

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

[34] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).

[35] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 203-214 (2012).

[36] Ernest Y.-Z. Tan, Charles C.-W. Lim, and R. Renner, Phys. Rev. Lett. **124**, 020502 (2020).

[37] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Phys. Rev. Lett. **124**, 230502 (2020).

[38] E. Woodhead, A. Acín, and S. Pironio, Quantum **5**, 443 (2021).

[39] P. Sekatski, J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, and N. Sangouard, Quantum **5**, 444 (2021).

[40] J. R. Gonzales-Ureta, A. Predojević, and A. Cabello, Phys. Rev. A **103**, 052436 (2021).

[41] P. Brown, H. Fawzi, and O. Fawzi, Nat. Commun. **12**, 575 (2021).

[42] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y.-Z. Tan, R. Wolf, V. Scarani, and C. C.-W. Lim, Nat. Commun. **12**, 2880 (2021).

[43] P. Brown, H. Fawzi, and O. Fawzi, arXiv:2106.13692.

[44] L. P. Thinh, G. de la Torre, J.-D. Bancal, S. Pironio, and V. Scarani, New J. Phys. **18**, 035007 (2016).

[45] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **128**, 110506 (2022).

[46] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).

[47] M. Curty and H.-K. Lo, npj Quantum Inf. **5**, 14 (2019).

[48] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[49] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.129.050502 for the current best error correction inefficiency, for the other two methods using complete measurement statistics, for the optimal calculation of the SPDC source, for the numerical simulation, and for the calculation of the key rate and confidence region, which includes Refs. [50–64].

[50] B.-Y. Tang, B. Liu, W.-R. Yu, and C.-Q. Wu, Quantum Inf. Process. **20**, 113 (2021).

[51] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).

[52] T. Cope and R. Colbeck, Phys. Rev. A **100**, 022114 (2019).

[53] K. Garay, J. Palfree, R. Mirin, S. W. Nam, A. U'ren, and L. K. Shalm, Spontaneous parametric down-conversion calculator, http://www.spdcalc.org.

[54] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, Quantum Sci. Technol. **4**, 035011 (2019).

[55] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[56] V. Caprara Vivoli, P. Sekatski, J.-D. Bancal, C. C. W. Lim, B. G. Christensen, A. Martin, R. T. Thew, H. Zbinden, N. Gisin, and N. Sangouard, Phys. Rev. A **91**, 012107 (2015).

[57] T. Kiyohara, R. Okamoto, and S. Takeuchi, Opt. Express **24**, 27288 (2016).

[58] P. J. Davis and P. Rabinowitz, *Methods of Numerical Integration* (Courier Corporation, Chelmsford, Massachusetts, 2007).

[59] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[60] P.-S. Lin, D. Rosset, Y. Zhang, J.-D. Bancal, and Y.-C. Liang, Phys. Rev. A **97**, 032309 (2018).

[61] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[62] E. Y. Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, and C. C. W. Lim, arXiv:2012.08714.

[63] P. J. Brown, S. Ragy, and R. Colbeck, IEEE Trans. Inf. Theory **66**, 2964 (2020).

[64] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio, New J. Phys. **20**, 023049 (2018).

[65] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007).

[66] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).

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

[68] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photonics **12**, 1012 (2020).

[69] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).

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

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

[72] X. Zhang, P. Zeng, T. Ye, H.-K. Lo, and X. Ma, arXiv:2111.13855.

[73] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, arXiv:2109.14600.

[74] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, V. Scarani, C. C. W. Lim, and H. Weinfurter, arXiv:2110.00575.