Experimental Realization of Device-Independent Quantum Randomness Expansion

Ming-Han Li,[1,2] Xingjian Zhang,[3] Wen-Zhao Liu,[1,2] Si-Ran Zhao,[1,2] Bing Bai,[1,2] Yang Liu,[1,2] Qi Zhao,[1,2] Yuxiang Peng,[3] Jun Zhang,[1,2] Yanbao Zhang,[4] W. J. Munro,[4] Xiongfeng Ma,[3,*] Qiang Zhang,[1,2,†] Jingyun Fan,[1,2,5,6,‡] 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, 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]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, People's Republic of China*

[4]*NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[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*

[6]*Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, People's Republic of China*

(Received 18 October 2020; accepted 4 January 2021; published 4 February 2021)

Randomness expansion where one generates a longer sequence of random numbers from a short one is viable in quantum mechanics but not allowed classically. Device-independent quantum randomness expansion provides a randomness resource of the highest security level. Here, we report the first experimental realization of device-independent quantum randomness expansion secure against quantum side information established through quantum probability estimation. We generate 5.47×10^8 quantum-proof random bits while consuming 4.39×10^8 bits of entropy, expanding our store of randomness by 1.08×10^8 bits at a latency of about 13.1 h, with a total soundness error 4.6×10^{-10}. Device-independent quantum randomness expansion not only enriches our understanding of randomness but also sets a solid base to bring quantum-certifiable random bits into realistic applications.

DOI: 10.1103/PhysRevLett.126.050503

Randomness is a fundamental element of nature and ubiquitous in human activities. Intrinsically, randomness comes from the breaking of quantum coherence [1–3]. The loophole-free violation of a Bell inequality [4–9] certifies entanglement, a special form of coherence, in a device-independent manner. This is the essence of device-independent quantum random number generation (DIQRNG) [10–12], and the rigorous security analysis makes it possible to design experiments secure against general attacks even under the extreme condition that the experimental devices themselves are not trusted [1–3]. The random bits certified in the loophole-free DIQRNG experiments are at the highest level of security among its kind being unpredictable to any strategies based on quantum or classical physics [13–15]. Randomness is required for setting the inputs of a Bell test, however, and in previous experimental realizations, more randomness is consumed than the certified [11,13–15]. As it becomes publicly known after the experiment, the input randomness is consumed and cannot be reused. Otherwise, an adversary can take advantage of the information leakage and compromise the security of DIQRNG [10]. Theoretically, the amount of input randomness can be made arbitrarily small for the certification of the Bell inequality violation and further the randomness generation [16], and it is possible that the amount of generated randomness surpasses the input, which is randomness expansion. Randomness expansion compensates the store of randomness for the consumption and provides more, eliminating the potential risk in security due to the *circular* involvement of randomness.

The realization of device-independent quantum randomness expansion (DIQRE) has remained an outstanding challenge as it poses even stricter requirements than the loophole-free violation of Bell inequalities and DIQRNG. In fact, the latter two tasks are prerequisites for randomness expansion. Besides, DIQRE requires a highly biased input probability distribution [16,17], which causes larger statistical fluctuations and takes more statistics for successful certification. Consequently, it is experimentally more demanding to realise DIQRE in a reasonable time. For instance, higher detection efficiency, higher visibility, and a more robust system behavior are required. While entangled atomic systems [5,8] promise a large violation of Bell inequality, these systems are currently constrained by low event rates, making it hard to obtain decent experimental statistics within a reasonable time frame. Entangled

photonic systems [6,7,9,13–15,18] on the other hand exhibit a relatively small violation of Bell inequality, but can be operated at very high event rates, thus providing an opportunity to achieve randomness expansion. We present here a concrete realization of DIQRE secure against a general quantum adversary taking advantage of two recent advancements [19]. One is the development of cutting-edge single-photon detection with near unity efficiency [21], which makes entangled photon-based loophole-free Bell test experiments viable. The other is the development of theoretical protocols [11,16,17,22–25], which allows for the efficient generation of randomness secure against quantum side information in device-independent experiments, such as the quantum probability estimation (QPE) method [24]. Below, we briefly describe the spot-checking QPE method and our procedure to apply it to realize DIQRE.

A procedure to realize randomness expansion according to the spot-checking QPE method is given in Table I. The procedure consists of three key steps: parameter assignments, experimental randomness expansion, and randomness extraction. The randomness expansion experiment is based on a sequence of Bell-test trials in the format of Clauser-Horne-Shimony-Holt (CHSH) game [26] (see Fig. 1 for experimental schematics and assumptions). In the ith trial, a source at the central station prepares a pair of entangled photons and sends them to two spatially separated parties, Alice and Bob. A coordinating random number generator independent of the measurement devices and the source generates a bit $T_i = 0$ (or $T_i = 1$) with nonzero probability $1 - q$ (or q), respectively. If $T_i = 0$, the trial is a "spot trial" where Alice and Bob set their input measurement settings to $X_i = 0$, $Y_i = 0$. If $T_i = 1$, the trial is a "checking trial" where Alice and Bob choose their own measurement settings $X_i, Y_i \in \{0, 1\}$ independently and uniformly at random. The value of T_i is kept private from the measurement devices. At the end of the trial Alice and Bob deliver an output $A_i, B_i \in \{0, 1\}$, respectively. For a total number of n experimental trials, we denote the input sequences by $\boldsymbol{X}=(X_1,X_2,\ldots,X_n)$, $\boldsymbol{Y} = (Y_1, Y_2, \ldots, Y_n)$, $\boldsymbol{T} = (T_1, T_2, \ldots, T_n)$, the outcome sequences by $\boldsymbol{A} = (A_1, A_2, \ldots, A_n)$, $\boldsymbol{B} = (B_1, B_2, \ldots, B_n)$, respectively, and further denote $\boldsymbol{Z} = \boldsymbol{XY}$, $\boldsymbol{C} = \boldsymbol{AB}$ and $Z_i = X_i Y_i$, $C_i = A_i B_i$.

In an adversarial picture, the source and measurement devices are prepared by a potentially malicious party, Eve, in advance of the experiment. Generally, the behavior of the quantum devices in each trial can be different and depend on previous events. The final state after the experiment can be described by a classical-quantum state shared by Alice, Bob, and Eve, $\rho_{\boldsymbol{CZE}} = \sum_{\boldsymbol{c},\boldsymbol{z}} |\boldsymbol{cz}\rangle\langle\boldsymbol{cz}| \otimes \rho_E(\boldsymbol{cz})$. We use lowercase letters to denote the values that the variables actually take in an experiment, and $(\boldsymbol{c}, \boldsymbol{z})$ is one specific realization of the experiment's input-output sequence occurring with the probability $\mathrm{Tr}[\rho_E(\boldsymbol{cz})]$. The random variable $\boldsymbol{T}$ can be omitted without loss of generality, as we assume its value to be secret to Eve. The quantum system of Eve, ρ_E, carries the quantum side information of the measurement results. We define the set of all possible joint final states after the experiment to be the model $\mathcal{M}(\boldsymbol{C}, \boldsymbol{Z})$.

For randomness expansion, we determine a quantum estimation factor (QEF) $F(\boldsymbol{CZ})$ with power α for the model $\mathcal{M}(\boldsymbol{C}, \boldsymbol{Z})$. Informally speaking, with a fixed security parameter ε_h, the quantity $\{\log_2[F(\boldsymbol{cz})] + \log_2(\varepsilon_h^2/2)\}/(\alpha - 1)$ witnesses the amount of private randomness extractable from the outputs $\boldsymbol{c}$. To turn it into a rigorous statement, we need to determine a criterion of success before running the protocol. The protocol succeeds if $F(\boldsymbol{cz}) \geq 2^{h_s(\alpha-1)}$, where h_s (bits) is the success threshold.

TABLE I. Procedure for randomness expansion.

Step 1. Parameter determination.
(1) Assign the least target amount of entropy k_{exp} (bits) to be expanded by;
(2) Assign the soundness error $\varepsilon_S = 2\varepsilon_h + \varepsilon_x \in (0, 1)$ (ε_h for randomness generation, ε_x for randomness extraction);
(3) Assign the probability distribution of T_i, $(1 - q, q)$, with $0 < q < 1$.
Based on these settings,
(1) Determine a valid single trial QEF $F(CZ)$ with power $\alpha > 1$;
(2) Determine the success threshold for randomness expansion h_s (bits);
(3) Determine the largest allowed number of experimental trials N;
(4) Determine the success probability of the protocol $\kappa \in (0, 1)$.
Step 2. Randomness expansion experiment.
(1) Before the experiment, set a classical register $G_0 = 1$.
(2) In the ith trial $(1 \leq i \leq N)$,
(i) *Measurements.*—If $T_i = 0$, set the measurement inputs as $X_i = Y_i = 0$; if $T_i = 1$, randomly set $X_i, Y_i \in \{0, 1\}$. Record the measurement outputs A_i, B_i and the corresponding QEF value $F_i(C_i Z_i)$.
(ii) *Discrimination.*—Update the register with $G_i = G_{i-1} F_i(C_i Z_i)$. If $[1/(\alpha - 1)]\log_2 G_i \geq h_s$, stop the experiment and set $F_j(c_j z_j) = 1$, $j > n$. Goto Step 3.
(iii) If $[1/(\alpha - 1)]\log_2 G_N < h_s$, abort the protocol.
Step 3. Randomness extraction.
Apply a quantum-proof strong extractor to $\boldsymbol{C}$ and obtain near-uniform random bits, with a security parameter no larger than ε_x.

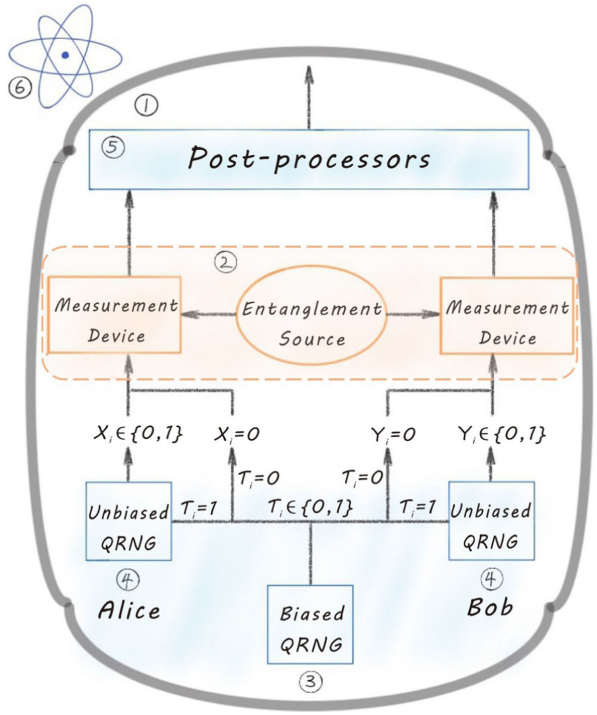

FIG. 1. A schematic demonstration of the experimental setup. The untrusted quantum devices are colored in orange and circled with the dotted line. The trusted parts are colored in blue. Specifically, we make the following assumptions in the protocol: (1) Secure lab: The information exchange with an outside entity is controlled. The devices cannot communicate to the outside to leak the experimental results directly. (2) Nonsignaling condition: In each trial, the measurement process of Alice and Bob is independent of the other party. (3) Trusted coordinator: A well characterized biased random number generator (depicted by "Biased QRNG" in the figure) determines a trial to be "spot" or "checking." The setting is private to the measurement devices and the entanglement source. (4) Trusted inputs: Alice and Bob each have a private random number generator (depicted by "Unbiased QRNG" in the figure) to feed perfect random bits to the measurement device in the "checking trials." (5) Trusted postprocessors: The classical postprocessing procedure is trusted. (6) Quantum mechanism: Quantum mechanics is correct and complete.

We denote the set of success events as Φ and $\kappa \in (0,1)$ as the predetermined lower bound on the success probability. Then, for an arbitrary state $\rho_{\boldsymbol{CZE}}$ in the model, either the protocol success probability is less than κ, or the smooth min-entropy conditional on the success is lower bounded by [24]

$$H_{\min}^{\varepsilon_h}(\boldsymbol{C}|\boldsymbol{ZE})_{\rho_{\boldsymbol{CZE}|\Phi}} \geq h_s - \frac{1}{\alpha-1}\log_2\left(\frac{2}{\varepsilon_h^2}\right) + \frac{\alpha}{\alpha-1}\log_2\kappa, \tag{1}$$

where ε_h is the smoothing parameter in the smooth min-entropy of $\boldsymbol{C}$ conditioned on $\boldsymbol{ZE}$, and $\rho_{\boldsymbol{CZE}|\Phi}$ represents the normalized state conditional on the success. In particular, this result holds for the general condition. To obtain a lower bound on the ε_h-smooth min-entropy, a lower bound κ on the success probability is required. Literature suggests setting $\kappa = \varepsilon_h$ to obtain a conservative lower bound on the ε_h-smooth min-entropy [23,24]. However, we remark that the lower bound κ is irrelevant for the soundness proof of the randomness generation protocol with QEFs (see Theorem 4 of Ref. [24]). Because at each trial the probability distributions of the input variables T_i, X_i, and Y_i are independent of the previous results and the quantum side information, a valid QEF $F(\boldsymbol{CZ})$ for a sequence of trials can be obtained by chaining the QEFs $F(C_iZ_i)$ for each experimental trial in the sequence [see Sec. I. B in Supplemental Material (SM) [27]].

If the success threshold is met in the experimental randomness expansion procedure, the protocol shall proceed to randomness extraction. We use a quantum-proof strong extractor to extract certified random bits from the output sequence with a security parameter ε_x [49] (see Sec. I. D in SM [27] for details in randomness extraction). Informally speaking, the extractor takes the experimental output sequence $\boldsymbol{C}$ in the Bell test, together with a uniform bit string S, or the seed, as the input, and delivers a string of near-uniform random bits, except for a failure probability no larger than ε_x. We do not consider the seed as entropy consumed in the experiment, since by definition the seed of a strong extractor can be reused albeit at the cost of the security parameter increased by ε_x [49]. Security is not compromised even if the seed is known by Eve after the execution of the protocol, as long as it is independent of the raw data and the classical postprocessing process is authenticated. Guaranteed by the composable security property, the total failure probability of the protocol, or the soundness error, is no larger than $\varepsilon_S = 2\varepsilon_h + \varepsilon_x$ (see Sec. I. D in SM [27]).

In the protocol, technically, an essential step is to find an (almost) optimal QEF for witnessing entropy in the experiment. We begin with taking a sequence of experimental trials as the training set and use it to determine an empirical input-output probability distribution $\nu(CZ)$. With respect to this empirical probability distribution, we perform an optimization program to obtain a single trial QEF $F(CZ)$ and estimate the amount of output randomness per trial by $r_\nu(F,\alpha) = \mathbb{E}_\nu[\log_2 F(CZ)]/(\alpha-1)$, without considering the smoothing parameter and protocol success probability. For a robust experimental system whose behavior is near the empirical knowledge, the average output randomness witnessed by the QEF shall be close to $r_\nu(F,\alpha)$. All three QRNGs for the input settings are accounted for the input randomness, and the average entropy consumption per trial in randomness expansion is given by

$$r_{\text{in}} = h(q) + 2q, \tag{2}$$

where $h(q) = -q\log_2 q - (1-q)\log_2(1-q)$ is the binary entropy, and the coefficient 2 is the amount of

randomness consumed by Alice and Bob in a checking trial. We would expect a successful randomness expansion if $r_\nu(F,\alpha)$ exceeds r_{in}.

Before the experiment, we fix the target least amount of near-uniform random bits to be expanded k_{exp}, the smoothing parameter ε_h involved in randomness expansion, the security parameter ε_x in randomness extraction, the success threshold h_s, the largest allowed number of experimental trials N, and a lower bound on the success probability of the protocol κ (see Sec. II in SM [27]). In the subsequent experiment, in each trial the single trial QEF takes a value $F(c_j z_j)$ with a realization $(c_j z_j)$, we keep updating a register G_n by multiplying its value with the latest single-trial QEF value, where n denotes the trial number. Before the experiment, the register G_n is initialized to be $G_0 = 1$. We can stop the experiment in advance if the chained QEF value already exceeds the threshold before reaching the Nth trial.

We realize randomness expansion on our upgraded photonic-entanglement distribution platform [9,13,18]. A sketch of the experimental setup can be found in Sec. III in SM [27]. In the experimental preparation, we enforce the nonsignaling condition by establishing spacelike separation between the measurement events of Alice and Bob, such that the output $A_i(B_i)$ is independent of $Y_i(X_i)$. We achieve a single-photon detection efficiency from creation to detection of 80.50% for Alice and 82.20% for Bob (see Sec. III. B in SM [27]), and measure the average CHSH game value $J = 0.75088$, which surpasses the classical bound of $J \leq 0.75$ substantially over our previous results [9,13,18]. Under this experimental condition, we determine a ratio of $1-q$: $q = 8375$: $1(q = 0.000119)$ for a good randomness expansion result which corresponds to consuming the input entropy at a rate of $r_{\text{in}} = 0.00197$ (see Sec. III. A in SM [27]). We operate our experiment with a 4 MHz repetition rate.

For this experimental demonstration, we set $k_{\text{exp}} = 512$ bits with a total soundness error of $\varepsilon_S = 2\varepsilon_h + \varepsilon_x \approx 2 \times 2^{-32}$ (with $\varepsilon_x = 2^{-100}$). We conservatively set the bound on the protocol success probability $\kappa = \varepsilon_h$ in estimating the output randomness. We take three hours training data (by consuming an amount of randomness $k_0 \approx 8.50 \times 10^7$ bits in 4.32×10^{10} trials), with which we determine a single trial QEF with power $\alpha = 1 + 1.172 \times 10^{-6}$ and an expected output randomness rate $r_\nu(F,\alpha) = 0.00289$ surpassing the input entropy rate by 0.00092. To determine the largest allowable number of trials, we use the protocol success probability with honest devices γ, which relates to the completeness of the protocol (see Sec. I. E in SM [27] for security definition). With $\gamma = 99.3\%$, we determine the largest allowable number of trials to be $N = 2.35 \times 10^{11}$ (open square in Fig. 2), which takes approximately 16 experimental hours, and set the threshold as $h_s = 6.31 \times 10^8$ bits (see Sec. IV. A in SM [27]). If G_n surpasses h_s in no more than N trials, we shall expand our store of randomness by at least 512 near-uniform random bits in the end.

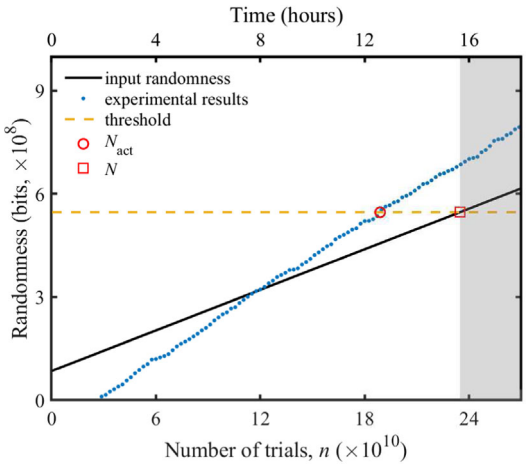

FIG. 2. Randomness expansion of at least $k_{\text{exp}} = 512$ random bits in at most $N = 2.35 \times 10^{11}$ trials with a smoothing parameter $\varepsilon_h = 2^{-32}$ in randomness generation. Blue dotted line: the experimental amount of generated ε_h-smooth min-entropy witnessed by the QEF by the nth trial R_n; black solid line: the amount of entropy consumed by the nth trial $k_0 + nr_{\text{in}}$; yellow dash line: the least amount of ε_h-smooth min-entropy required to be generated for a successful randomness expansion task. Surpassing the threshold before N trials guarantees a successful randomness expansion of at least 512 near-uniform random bits at the end of the protocol, otherwise the protocol fails (represented by the gray area). The open square denotes the largest allowed number of trials and the open circle denotes the actual number of trials to accomplish the task. We note that the experiment can be stopped in advance at the N_{act}th trial. Still, we continue the experiment for a longer period to show the robustness of the experimental setup, as shown in the shaded area (in all, we have accumulated data of approximately 3×10^{12} trials).

Our result of the randomness expansion experiment (corresponding to Step 2 in Table I) is shown in Fig. 2. We update G_n with the observed QEF values for every latest accumulated 1-min of experimental data. To show the result of quantum expansion more directly, in Fig. 2 we plot the quantity, $R_n = [\log_2 G_n - \log_2(2/\varepsilon_h^2) + \alpha \log_2 \kappa]/(\alpha - 1)$, as shown by the blue dotted line. In view of Eq. (1) and the remark behind it, the quantity R_n can be seen as the amount of ε_h-smooth min-entropy accumulated in the output after n trials (*if* the protocol will succeed). Output randomness emerges after 2.6×10^{10} trials and gradually surpasses the amount of entropy consumed $k_0 + nr_{\text{in}}$ (black solid line). It surpasses the threshold (open circle) after $N_{\text{act}} = 1.89 \times 10^{11}$ trials (about 13.1 h). At this point we can stop the experiment in advance and set the QEF values for the remained trials to be 1. Therefore, we actually generate 5.47×10^8 bits of randomness and consume $k_0 + N_{\text{act}} r_{\text{in}} = 4.39 \times 10^8$ bits of entropy. Afterward, we use the Toeplitz hashing matrix,

a quantum-proof strong extractor [49], to extract near-uniform random bits with security parameter $\varepsilon_x = 2^{-100}$. In the end, we expand our store of randomness by 1.08×10^8 near-uniform random bits, which is far more than the requirement of the expansion task.

Our experimental realization of DIQRE is a substantial progress toward the ultimate understanding of randomness. In particular, this may further inspire the research of other interesting directions of randomness, for example, randomness amplification [50], which, instead of requiring input randomness to be independent of the devices, could amplify the imperfect random bits into perfect ones. Besides, DIQRE might be related with quantum side information proof strong multisource extractors [51]. For these tasks, possible candidates for input randomness source could be cosmic randomness [52] and human randomness [53]. DIQRE, which expands a very small random seed to rather long sequence of random bits without compromising the security, possesses a great potential for realistic applications demanding high level secure randomness.

The authors would like to thank X. Yuan and R. Colbeck for enlightening discussions, and E. Knill for pointing out a mistake in an earlier version. This work has been supported by the National Key R&D Program of China (2017YFA0304000, 2017YFA0303900 and 2017YFA0304004), the National Fundamental Research Program (under Grant No. 2013CB336800), the National Natural Science Foundation of China, Chinese Academy of Science, Guangdong Provincial Key Laboratory Grant No. 2019B121203002, Guangdong Innovative and Entrepreneurial Research Team Program Grant No. 2019ZT08 X324, the Key-Area Research and Development Program of Guangdong Province Grant No. 2020B0303010001, Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), and the Zhongguancun Haihua Institute for Frontier Information Technology.

M.-H. L and X. Z. contributed equally to this work.

Note added.—After finishing this work, we became aware of a similar DIQRE experiment work [54]. This work is based on the probability estimation method [55], which is closely related with the QPE method used in this work, but can only certify randomness in the presence of classical side information. Besides, there is a DIQRE experiment against quantum side information which is based on the entropy accumulation theorem (EAT) [56]. We present a discussion on the comparison of QPE and EAT methods and list the related experimental results in SM [27].

*xma@tsinghua.edu.cn
†qiangzh@ustc.edu.cn
‡fanjy@sustech.edu.cn
§pan@ustc.edu.cn

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Inf. **2**, 16021 (2016).
[2] A. Acín and L. Masanes, Nature (London) **540**, 213 (2016).
[3] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
[4] J. Bell *et al.*, Physics (Long Island City, NY) **1**, 195 (1964).
[5] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Nature (London) **526**, 682 (2015).
[6] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).
[7] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).
[8] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Phys. Rev. Lett. **119**, 010402 (2017).
[9] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang *et al.*, Phys. Rev. Lett. **121**, 080404 (2018).
[10] R. Colbeck, Ph.D. thesis, Trinity College, and University of Cambridge, arXiv:0911.3814.
[11] 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 *et al.*, Nature (London) **464**, 1021 (2010).
[12] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[13] Y. Liu, Z. Qi, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, Nature (London) **562**, 548 (2018).
[14] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam *et al.*, Nature (London) **556**, 223 (2018).
[15] 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 *et al.*, Phys. Rev. Lett. **124**, 010505 (2020).
[16] C. A. Miller and Y. Shi, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing STOC '14* (ACM, New York, 2014), pp. 417–426.
[17] U. Vazirani and T. Vidick, in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, STOC '12* (ACM, New York, 2012), pp. 61–76.
[18] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li *et al.*, Phys. Rev. Lett. **120**, 010503 (2018).
[19] We do not consider the memory attack in reusing the protocol [20]. For one run of the experiment the memory attacks do not play a role (the randomness remains secure provided the devices used are kept secure after the experiment).
[20] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).
[21] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Rev. Sci. Instrum. **82**, 071101 (2011).
[22] M. Coudron and H. Yuen, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2014) pp. 427–436.

[23] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).
[24] Y. Zhang, H. Fu, and E. Knill, Phys. Rev. Research **2**, 013016 (2020).
[25] P. J. Brown, S. Ragy, and R. Colbeck, IEEE Trans. Inf. Theory **66**, 2964 (2019).
[26] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.126.050503 for properties and optimization of QEF, protocol security definition, details for the experimental realization, randomness extraction, and other discussions of the experimental results and theories, which includes Refs. [28–48].
[28] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A **87**, 012335 (2013).
[29] C. A. Miller and Y. Shi, SIAM J. Comput. **46**, 1304 (2017).
[30] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[31] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[32] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).
[33] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[34] E. Knill, Y. Zhang, and P. Bierhorst, arXiv:1709.06159.
[35] P. Bierhorst, J. Phys. A **49**, 215301 (2016).
[36] M. Jaggi, *International Conference on Machine Learning* (PMLR, 2013), pp. 427–435.
[37] R. Impagliazzo, L. A. Levin, and M. Luby, in *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, STOC '89* (ACM, New York, 1989), pp. 12–24.
[38] D. Frauchiger, R. Renner, and M. Troyer,arXiv:1311.4547.
[39] N. Nisan and D. Zuckerman, J. Comput. Syst. Sci. **52**, 43 (1996).
[40] R. Konig and R. Renner, IEEE Trans. Inf. Theory **57**, 4760 (2011).
[41] A. De, C. Portmann, T. Vidick, and R. Renner, SIAM J. Comput. **41**, 915 (2012).
[42] R. Renner, Int. J. Quantum. Inform. **06**, 1 (2008).
[43] R. Canetti, J. Cryptol. **13**, 143 (2000).
[44] M. Ben-Or and D. Mayers, arXiv:quant-ph/0409062.
[45] C. Portmann and R. Renner, arXiv:1409.3525 (2014).
[46] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[47] NIST statistical test suite, http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html.
[48] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[49] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[50] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[51] R. Kasher and J. Kempe, in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques* (Springer, Berlin, Heidelberg, 2010), pp. 656–669.
[52] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* (Cambridge University Press, Cambridge, England, 2004).
[53] C. Abellán *et al.* (BIG Bell Test Collaboration), Nature (London) **557**, 212 (2018).
[54] 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 *et al.*, arXiv:1912.11158.
[55] Y. Zhang, E. Knill, and P. Bierhorst, Phys. Rev. A **98**, 040304 (2018).
[56] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan *et al.*, arXiv:1912.11159.