High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole

Yang Liu,[1,2] Xiao Yuan,[1,2,3] Ming-Han Li,[1,2] Weijun Zhang,[4] Qi Zhao,[3] Jiaqiang Zhong,[5] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Luo-Kan Chen,[1,2] Hao Li,[4] Tianyi Peng,[3] Yu-Ao Chen,[1,2] Cheng-Zhi Peng,[1,2] Sheng-Cai Shi,[5] Zhen Wang,[4] Lixing You,[4,*] Xiongfeng Ma,[3,†] Jingyun Fan,[1,2,‡] Qiang Zhang,[1,2,§] and Jian-Wei Pan[1,2,¶]

[1]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,
University of Science and Technology of China, Shanghai 201315, 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]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology,
Chinese Academy of Sciences, Shanghai 200050, People's Republic of China*

[5]*Purple Mountain Observatory and Key Laboratory of Radio Astronomy, Chinese Academy of Sciences,
2 West Beijing Road, Nanjing, Jiangsu 210008, People's Republic of China*

(Received 16 May 2017; revised manuscript received 30 July 2017; published 3 January 2018)

Quantum mechanics provides the means of generating genuine randomness that is impossible with deterministic classical processes. Remarkably, the unpredictability of randomness can be certified in a manner that is independent of implementation devices. Here, we present an experimental study of device-independent quantum random number generation based on a detection-loophole-free Bell test with entangled photons. In the randomness analysis, without the independent identical distribution assumption, we consider the worst case scenario that the adversary launches the most powerful attacks against the quantum adversary. After considering statistical fluctuations and applying an 80 Gb × 45.6 Mb Toeplitz matrix hashing, we achieve a final random bit rate of 114 bits/s, with a failure probability less than 10^{-5}. This marks a critical step towards realistic applications in cryptography and fundamental physics tests.

DOI: 10.1103/PhysRevLett.120.010503

Introduction.—Random numbers are widely used in applications ranging from numerical simulation and cryptography to a lottery. While the foremost property of random number generators (RNGs) in many applications is the distribution uniformity of its outputs, secure information processing applications such as cryptography demand additionally that the devices to produce randomness must be secure against any adversaries, regardless of classical or quantum mechanics. Classical RNGs have a deterministic nature and hence are not random. Quantum random number generators (QRNGs) rely on the unpredictability in breaking quantum coherence and are theoretically unpredictable. However, the unpredictability may be jeopardized in practice because the adversary may gain information about the devices and even maliciously manipulate the devices of QRNGs, which is often undetected by a finite set of statistical tests. Device-independent QRNGs (DIQRNGs) certify the randomness unconditionally based on the loophole-free violation of Bell's inequality, offering a reliable way of generating genuine randomness and therefore holding great promise for future applications. (See Refs. [1,2] for a review of QRNGs.)

Considering a loophole-free Bell test experiment. Alice and Bob are honest parties at two remote sites, each receives one of a pair of entangled photons and measures its quantum state with a randomly selected measurement setting. Alice and Bob may not trust the devices because the devices may be prepared by the adversary. The experiment observes the no-signaling theorem, i.e., even at the speed of light, no information of measurement setting is conveyed to the source prior to the emission of entangled photon pairs (to close randomness loophole) and no information about Alice's (Bob's) measurement setting and measurement outcomes are conveyed to Bob (Alice) prior to his (her) state measurement (to close locality loophole). The photon-detection efficiency is sufficiently high for the experiment to be free from the detection loophole. Local hidden variable theories (based on classical determinism) set a bound to the correlation measurement between Alice and Bob. Breaking the bound exhibits quantum correlation, which cannot be explained by classical deterministic mechanisms. This nonlocal quantum correlation certifies that Alice and Bob's measurement outcomes possess genuine quantum randomness which is unaccessible to the adversary, irrelevant to the implementation devices [3,4].

As we deepen the understanding of DIQRNGs [5–13], the security analysis becomes more efficient in producing randomness and more robust to noise. In particular, the entropy accumulation theorem formulated by Dupuis, Fawzi, and Renner [12] converts a single-shot result to the multiple-shot case. Exploiting the entropy accumulation theorem, Arnon-Friedman, Renner, and Vidick proposed a DIQRNG analysis method without the assumption of independent identical distribution (i.i.d.), which nevertheless produces randomness with yield approaching the value for the i.i.d. case [13]. The analysis is against the quantum adversary. So far there have been two reported experimental studies on DIQRNGs. One was based on a detection loophole-free Bell test experiment with entangled ions [14], which produced random bits at a rate of 1.5×10^{-5} bit s^{-1} without the assumption of i.i.d. The analysis is against the classical adversary. The other one was based on a detection loophole-free Bell test experiment with entangled photons [15], which produced random bits at a rate of 0.4 bit s^{-1}, albeit with the assumption of i.i.d.

Very recently, several experiments demonstrated the violation of Bell's inequality with both locality and detection loopholes closed simultaneously [16–19]. It was also shown that the randomness loophole can be progressively addressed with cosmic RNGs [20–22], which take advantage of randomness at a remote celestial object to set the time constraint of local hidden variable mechanisms deep into cosmic history. These works pave the way to construct a practical DIQRNG. Here we report an experimental study of a DIQRNG based on a detection loophole-free Bell test with entangled photon pairs, with randomness extraction of 114 bits s^{-1} and uniformity within 10^{-5}. The randomness generation analysis is against the most powerful quantum adversary attacks and does not rely on the independent identical distribution assumption. Our experiment marks a critical step for generating DIQRNGs for practical applications.

Proposal.—The DIQRNG protocol is based on the Bell test experiment, namely, a Clauser-Horne-Shimony-Holt (CHSH) game [23]. In each experimental trial, Alice and Bob perform state measurements upon receiving random inputs x and y and produce outputs a and b, respectively. According to local hidden variable models, the correlations described by probability distributions $p(ab|xy)$ in the i.i.d. scenario are factorable with $p(ab|xy) = \sum_\lambda p(\lambda)p(a|x,\lambda)p(b|y,\lambda)$. The J value of the CHSH game satisfies an inequality,

$$J = \frac{1}{4}\sum_{abxy}\beta_{abxy}p(ab|xy) - 3/4 \leq 0, \tag{1}$$

where the pay-off coefficient is given by

$$\beta_{abxy} = \begin{cases} 1, & \text{if } a \oplus b = xy \\ 0 & \text{if } a \oplus b \neq xy \end{cases}, \tag{2}$$

with $\oplus$ standing for sum modulo 2. Quantum theory allows $J > 0$ as opposed to local hidden variable models.

In practice, all Bell test experiments have finite statistics. Instead of approximating probability distributions based on the i.i.d. assumption, we introduce the Bell value J_i in experimental trial i,

$$J_i = \begin{cases} 1, & \text{if } a_i \oplus b_i = x_i y_i \\ 0 & \text{otherwise} \end{cases}. \tag{3}$$

The CHSH game value is an average of J_i for all n experimental trials,

$$\bar{J} = \frac{1}{n}\sum_{j=1}^{n} J_i - 3/4. \tag{4}$$

Here, we consider the case that the average probability of measurement setting choice is unbiased, $p(xy) = 1/4$. Violating the inequality in Eq. (1), $\bar{J} > 0$, indicates the presence of genuine quantum randomness in the measurement outcomes. The randomness can be quantified by the smooth min-entropy $H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E)$ based on the CHSH game value $\bar{J}$ and the number of experiment trials [13], which is bounded by

$$H_{\min}^{\varepsilon_s}(\mathbf{A}B|\mathbf{X}YE) \geq nR_{\text{opt}}(\varepsilon_s, \varepsilon_{\text{EA}}, \omega_{\text{exp}}). \tag{5}$$

Here $\mathbf{A}$ ($\mathbf{B}$) and $\mathbf{X}$ ($\mathbf{Y}$) denote the input and output sequences of Alice (Bob), respectively; E denotes side information of a general quantum adversary; ε_s is the smoothing parameter; ω_{exp} is the expected CHSH game value. ε_{EA} is the probability of aborting the protocol; $H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E)$ describes the amount of unpredictable randomness that can be extracted from the outputs $\mathbf{AB}$ against the inputs $\mathbf{XY}$ and any adversary E; as a conservative estimation, we take the lower bound $R_{\text{opt}}(\varepsilon_s, \varepsilon_{\text{EA}}, \omega_{\text{exp}})$ as the theoretical amount of randomness on average for each trial. $\varepsilon_{\text{QRNG}}^c$ is the *completeness* error, i.e., the probability for a protocol to abort for an honest implementation is at most $\varepsilon_{\text{QRNG}}^c$. The lower bound for the smooth min-entropy $H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E)$ is smaller when the average probability of measurement setting choice is biased (see Supplemental Material [24] for detailed protocol description, which includes Refs. [11–13,25,26]).

The DIQRNG may be implemented with the following procedure in the experiment: (1) Bell test: (i) In experimental trial i, Alice and Bob receive random inputs X_i and Y_i and produce outputs A_i and B_i, respectively. (ii) We assign a CHSH game value J_i according to the pay-off in Eq. (3) and calculate the average pay-off according to Eq. (4). (iii) We abort the protocol if $\bar{J} < \omega_{\text{exp}} - \delta_{\text{est}}$. Here the completeness error is upper bounded by $\varepsilon_{\text{QRNG}}^c \leq \exp(-2n\delta_{\text{est}}^2)$, where $\delta_{\text{est}} \in (0,1)$ is the width of the statistical confidence interval for the Bell violation estimation test. (2) Randomness estimation: Conditioned on the violation of Bell's inequality in the experiment, either the protocol aborts with probability greater than $1 - \varepsilon_{\text{EA}}$ or the experiment produces randomness given by Eq. (5).

(3) Randomness extraction: For a given failure probability of less than 2^{-t_e}, we apply the Toeplitz-matrix hashing extractor with a matrix of size $n \times H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) - t_e$ to extract $H_{\min}^{\varepsilon_s}(\mathbf{AB}|\mathbf{XY}E) - t_e$ random bits that is ε_s close to the uniform distribution. Here, we set $t_e = 100$.

Experiment.—The experimental layout is shown in Fig. 1. We enclose a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop. With the injection of pump pulses at a wavelength of 780 nm and pulse width of 10 ns at a repetition rate of 100 kHz, the loop emits polarization-entangled photon pairs at the degenerate wavelength of 1560 nm via a spontaneous parametric down-conversion process. The two photons of the pair travel in opposite directions. They are subject to polarization state measurements by Alice and Bob and are detected by superconducting nanowire single-photon detectors (SNSPDs). In each experimental trial, the dichotomic photon-detection results of the SNSPDs, 1 for "click" and 0 for "no click," are time tagged for correlation analysis.

In our experiment, the overall single photon detection efficiency is determined to be $78.6\% \pm 1.5\%$ for Alice and $80.2\% \pm 1.5\%$ for Bob [27]. The two-photon interference visibility is measured to be $99.5\% \pm 2\%$ ($97.8\% \pm 1.5\%$) in the horizontal (diagonal) basis. Using Eberhard's method [28], we generate nonmaximally entangled state, $\cos(20.5°)|HV\rangle + \sin(20.5°)|VH\rangle$ and set angles of half-wave plates in polarization state measurements to be $A_1 = -84.0°$ or $A_2 = -118.7°$ for Alice, $B_1 = 6°$ or $B_2 = -28.7°$ for Bob, respectively, to have an optimum violation of Bell's inequality (see Supplemental Material [24] for the detailed experimental setup, which includes Refs. [27–31]).

Previous Bell test experiments assigned measurement settings (xy) randomly with inputs from locally generated QRNGs [16–19]. For the current experiment, which targets to demonstrate the feasibility of random number generation via device-independent means against the quantum adversary, the settings are preset manually with parameters given by the Eberhard's optimization procedure as described above. So we require randomness and locality assumptions. Both loopholes may be closed by employing RNGs [20–22] and Pockels cells to randomly alternate the measurement base settings. The total photon detection efficiencies are high to close the detection loophole. We repeat the experiment by an equal number of trials ($N = 1 \times 10^{10}$) per measurement setting choice xy and record the number of correlated events $N_{ab|xy}$ (see Table I). According to Eq. (4), the J value of the CHSH game is given by

$$J_N = J_{A_1B_1} + J_{A_1B_2} + J_{A_2B_1} + J_{A_2B_2} - 3/4, \qquad (6)$$

with the Bell value J for settings $x = A_i$, $y = B_j$, and outputs ab given by

$$\begin{aligned} J_{A_1B_1} &= (N_{ab=00|A_1B_1} + N_{ab=11|A_1B_1})/N, \\ J_{A_1B_2} &= (N_{ab=00|A_1B_2} + N_{ab=11|A_1B_2})/N, \\ J_{A_2B_1} &= (N_{ab=00|A_2B_1} + N_{ab=11|A_2B_1})/N, \\ J_{A_2B_2} &= (N_{ab=01|A_2B_2} + N_{ab=10|A_2B_2})/N. \end{aligned} \qquad (7)$$

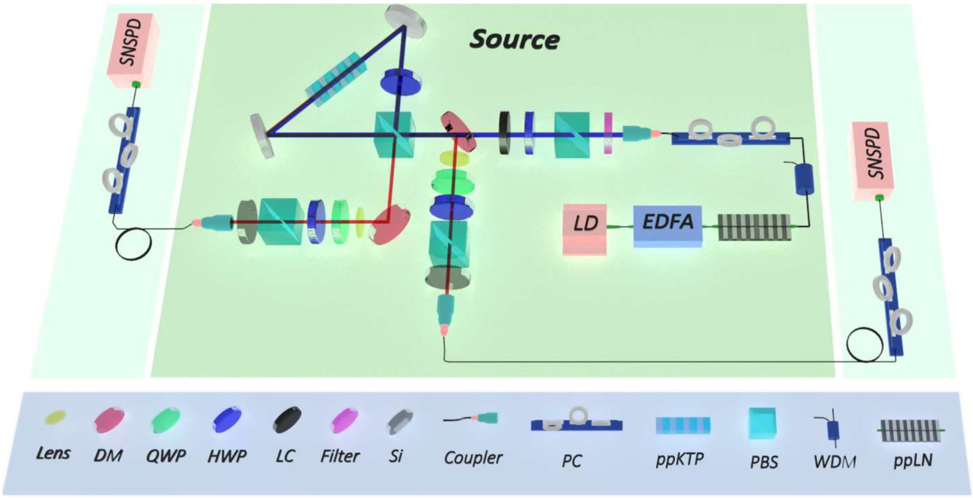

FIG. 1. Schematics of the experiment. Light pulses of 10 ns, 100 kHz from a 1560 nm seed laser (LD) are amplified by an erbium-doped fiber amplifier (EDFA), and up-converted to pulses at 780 nm via second-harmonic generation (SHG) in an in-line periodically poled lithium niobate (PPLN) waveguide. The residual 1560 nm light is removed by a wavelength-division multiplexer (WDM) and spectral filters. A half-wave plate (HWP) and a liquid crystal (LC) is used to adjust the pump polarization. The 780 nm light pulses are focused into a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop to generate polarization entangled photon pairs. After removing the 780 nm pump pulses by dichroic mirrors (DMs) and a 1 mm thick silicon plate, the entangled photons at 1560 nm are subject to polarization state measurements and then sent to superconducting nanowire single-photon detectors (SNSPDs) via a 130 m optical fiber.

TABLE I. Summary of device independent and semi-device-independent QRNG demonstrations (based on the claim and data reported in the references). Highest key rates are selected among the MDI- and SI-QRNG demonstrations. DI: device independent, Semi: semi device independent, MDI: measurement device independent, SI: source independent. In the Analysis column, i.i.d., classical, and general indicate that the theory analysis is considered under the i.i.d. assumption, classical adversary, and general adversary, respectively. In the assumption column, independent+qubit indicates that the experiment considers the independent qubit source and qubit measurement; measure indicates that the measurement is trusted; source indicates that the source is trusted; source fidelity indicates that the fidelity between the prepared states is trusted; and efficiency, locality, and randomness indicate the corresponding loopholes in Bell tests.

QRNG	Type	Analysis	Assumption	Key rate
[32]	Semi	i.i.d.	independent+qubit	23 bps
[33,34]	MDI	i.i.d.	source	5.7 Kbps
[35,36]	SI	general	measure	1.7 Gbps
[37]	Semi	i.i.d.	source fidelity	16.5 Mbps
[14]	DI	classical	efficiency	1.5×10^{-5} bps
[15]	DI	i.i.d.	locality	0.4 bps
This Letter	DI	general	randomness+locality	114 bps

For a total number of experimental trials $n = 4N = 4 \times 10^{10}$, the obtained J value is 3.52×10^{-4}, indicating that our CHSH game rejects local hidden variable models. In our analysis, we set the expected CHSH game value to the one measured in the experiment, $\omega_{\mathrm{exp}} = 3.52 \times 10^{-4}$, $\varepsilon_s = \varepsilon_{\mathrm{EA}} = 1/\sqrt{n} = 5\times10^{-6}$ and $\delta_{\mathrm{est}} = \sqrt{10/n} = 1.58\times10^{-5}$. Correspondingly, after applying an 80 Gb × 45.6 Mb Toeplitz matrix hashing, the experiment produces 4.56×10^7 genuine random bits in total with uniformity within $\varepsilon_s + \varepsilon_{\mathrm{EA}} = 10^{-5}$. The randomness generation speed is 0.00114 bits per trial or 114 bits/s. With such a high yield, the stream of random bits pass the NIST statistic test suite for the first time of its kind (see Supplemental Material [24] for randomness extraction and the result of the NIST statistic test, which includes Refs. [38–40]). A comparison of different experimental studies of DI and semi-DI QRNGs are listed in Table II.

TABLE II. Number of correlated events for equal number of trials (10^{10}) per measurement base settings: A_1B_1, A_1B_2, A_2B_1, and A_2B_2. $a = 0$ or 1 indicates that Alice detects a photon or not, the same for b for Bob. Mean photon number $\mu = 0.15$, violation $J_n = 3.52 \times 10^{-4}$.

Basis settings	$ab = 00$	$ab = 10$	$ab = 01$	$ab = 11$
A_1B_1	9 780 816 728	49 862 593	57 002 217	112 318 462
A_1B_2	9 574 958 251	41 366 122	263 425 568	120 250 059
A_2B_1	9 577 555 854	253 683 380	46 874 032	121 886 734
A_2B_2	9 255 451 323	361 101 111	365 181 363	18 266 203

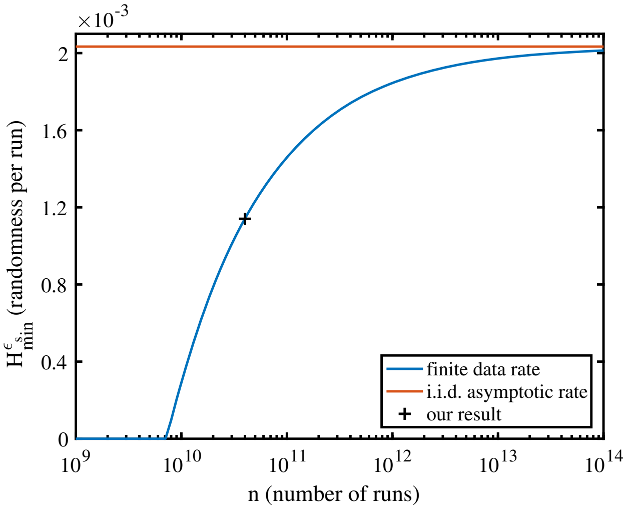

FIG. 2. Randomness generation versus number of experimental trials. We set the expected CHSH game value to be $\omega_{\mathrm{exp}} = 3.52 \times 10^{-4}$, $\varepsilon_s = \varepsilon_{\mathrm{EA}} = 1/\sqrt{n}$ and $\delta_{\mathrm{est}} = \sqrt{10/n}$ for the finite data rate.

With the same parameter setting, we plot the amount of randomness that can be produced by our experiment as a function of the number of experimental trials, which asymptotically approaches the optimal asymptotic value for i.i.d. as shown in Fig. 2. The amount of randomness obtained in the current experiment is about 60% of the optimal asymptotic value.

One may expect to extract more randomness, even by orders of magnitude, for larger violations in the CHSH game with improved experimental parameters such as higher photon-detection efficiency, higher two-photon interference visibility, and optimized mean photon numbers (see Supplemental Material [24]), as shown in Fig. 3.

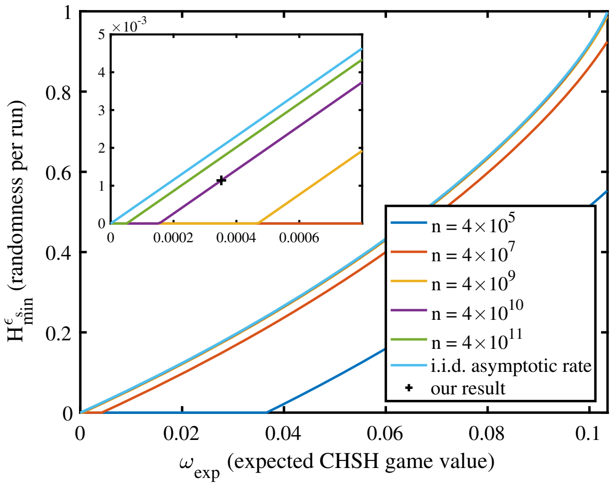

FIG. 3. Randomness generation versus expected CHSH game value. We set $\varepsilon_s = \varepsilon_{\mathrm{EA}} = 1/\sqrt{n}$ and $\delta_{\mathrm{est}} = \sqrt{10/n}$ for finite data rate curves.

Conclusion and outlook.—We implement a DIQRNG without the detection loophole, which does not need the assumption of identical and independent distribution and is against the quantum adversary. We report randomness extraction at a rate of 114 bits/s with uniformity within 10^{-5}, marking a critical step in generating DIQRNGs for secure information processing applications and tests of fundamental physics. In the future, actively switching measurement settings, for example, based on cosmic RNGs in a loophole-free CHSH game, can produce genuinely quantum-certified random bits. One can further speedup the randomness production by upgrading the technology such as scaling up the operation repetition rate. One may note that the analysis method in Ref. [13] is efficient in producing quantum-certified randomness based on a CHSH game. However, it remains an open question what the actual maximum extractable randomness is in a CHSH game, furthermore, what is the maximum extractable randomness for a general nonlocal game.

The authors would like to thank Y. Shi for enlightening discussions. This work has been supported by the National Fundamental Research Program (under Grant No. 2013CB336800), the National Natural Science Foundation of China, and the Chinese Academy of Science.

Y. L. and X. Y. contributed equally to this work.

Note added.—Recently, we become aware of a related work [41].

[*] lxyou@mail.sim.ac.cn
[†] xma@tsinghua.edu.cn
[‡] fanjy@ustc.edu.cn
[§] qiangzh@ustc.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] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[3] R. Colbeck, PhD thesis, University of Cambridge, (2009).

[4] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).

[5] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A **87**, 012335 (2013).

[6] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).

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

[8] C. A. Miller and Y. Shi, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM, New York, NY, USA, 2014), pp. 417–426.

[9] K.-M. Chung, Y. Shi, and X. Wu, arXiv:1402.4797.

[10] M. Coudron and H. Yuen, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, USA, 2014), pp. 427–436.

[11] C. A. Miller and Y. Shi, SIAM J. Computing **46**, 1304 (2017).

[12] F. Dupuis, O. Fawzi, and R. Renner, arXiv:1607.01796.

[13] R. Arnon-Friedman, R. Renner, and T. Vidick, arXiv:1607.01797.

[14] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).

[15] 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).

[16] B. Hensen *et al.*, Nature (London) **526**, 682 (2015).

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

[18] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Phys. Rev. Lett. **115**, 250401 (2015).

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

[20] J. Gallicchio, A. S. Friedman, and D. I. Kaiser, Phys. Rev. Lett. **112**, 110405 (2014).

[21] J. Handsteiner, A. S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, A. Mark, H. T. Nguyen, I. Sanders, F. Steinlechner, R. Ursin, S. Wengerowsky, A. H. Guth, D. I. Kaiser, T. Scheidl, and A. Zeilinger, Phys. Rev. Lett. **118**, 060401 (2017).

[22] C. Wu, B. Bai, Y. Liu, X. Zhang, M. Yang, Y. Cao, J. Wang, S. Zhang, H. Zhou, X. Shi, X. Ma, J.-G. Ren, J. Zhang, C.-Z. Peng, J. Fan, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **118**, 140402 (2017).

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

[24] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.120.010503 for detailed theoretical and experimental results.

[25] M. Coudron, T. Vidick, and H. Yuen, in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques: 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, 2013. Proceedings*, edited by P. Raghavendra, S. Raskhodnikova, K. Jansen, and J. D. P. Rolim (Springer Berlin Heidelberg, Berlin, Heidelberg, 2013), pp. 468–483.

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

[27] M. Pereira, F. Becerra, B. Glebov, J. Fan, S. Nam, and A. Migdall, Opt. Lett. **38**, 1609 (2013).

[28] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993).

[29] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010).

[30] P. Dixon, D. Rosenberg, V. Stelmakh, M. Grein, R. Bennink, E. Dauler, A. Kerman, R. Molnar, and F. Wong, Phys. Rev. A **90**, 043804 (2014).

[31] W. Zhang, L. You, H. Li, J. Huang, C. Lv, L. Zhang, X. Liu, J. Wu, Z. Wang, and X. Xie, Sci. China Phys. Mech. Astron. **60**, 120314 (2017).

[32] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).

[33] Z. Cao, H. Zhou, and X. Ma, New J. Phys. **17**, 125011 (2015).

[34] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Phys. Rev. A **94**, 060301 (2016).

[35] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).

[36] D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).

[37] J. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Applied **7**, 054018 (2017).

[38] 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, NY, USA, 1989), pp. 12–24.

[39] D. Frauchiger, R. Renner, and M. Troyer, arXiv:1311.4547.

[40] NIST statistical tests suite, http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html.

[41] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm, arXiv:1702.05178.