Certified Randomness from Untrusted Sources and Uncharacterized Measurements

Xing Lin,[1,3,4] Rong Wang,[2,1,3,4] Shuang Wang,[1,3,4,*] Zhen-Qiang Yin,[1,3,4,†] Wei Chen,[1,3,4]
Guang-Can Guo,[1,3,4] and Zheng-Fu Han[1,3,4]
[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[2]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong SAR, China*
[3]*CAS Center for Excellence in Quantum Information and Quantum Physics,*
University of Science and Technology of China, Hefei 230026, China
[4]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Received 18 April 2022; accepted 11 July 2022; published 28 July 2022)

Generating random numbers plays an important role in many scientific applications. Compared to pseudorandom number generators, a quantum device is capable of generating true random numbers by the laws of quantum mechanics. However, information-theoretical secure random numbers are regularly based on a perfect device model, which may deviate from a real-world device. To close this gap, we propose a quantum random number generation protocol and experimentally demonstrate it. In our protocol, we make no assumptions about the source. Some reasonable assumptions on the trusted two-dimensional measurement are needed, but we do not require a detailed characterization. Even if considering the most general quantum attack and using the general sources, we achieve a randomness generation rate of over 1 Mbps with a universal composable security parameter of 10^{-10}.

DOI: 10.1103/PhysRevLett.129.050506

Introduction.—Randomness as a valuable resource has been applied in a range of application scenarios from Monte Carlo simulation to cryptography. Because of the predictability and long-range correlation, pseudo- or classical random number generators which rely on the deterministic algorithms or classical physical processes might cause unexpected problems, such as errors of simulation [1] or exposure of secret keys [2]. On the contrary, quantum random number generations (QRNGs), which exploit the intrinsic indeterminacy of quantum mechanics [3], are a suitable alternative and commercially available.

A central issue of QRNGs is quantifying the entropy of the raw randomness. Most existing QRNGs evaluate entropy by building the precise model of the randomness source and well-characterized measurement devices, such as measuring the spatial [4] or time mode of the single-photon [5,6], vacuum fluctuation [7], phase fluctuations of laser [8,9], or Raman scattering noise [10,11]. However, it might not be easy to estimate the parameters of the practical devices precisely, especially for the complicated and even untrusted randomness source. In addition, the parameter estimation of special devices cannot apply to general implementations and not synchronize with the randomness generation. Therefore, it is both theoretically and practically meaningful to design a QRNG that can precisely estimate the entropy without well-characterized or even trusted devices.

A device-independent (DI) QRNG is a reasonable but challenging solution [12–16]. By the violation of Bell inequality, the entropy can be bound without any assumption of the devices. Nevertheless, the high demand for implementations, such as little loss tolerance, and extremely low randomness generation rates, limit its development and urge us to present a more practical protocol at the cost of loosening some paranoid assumptions.

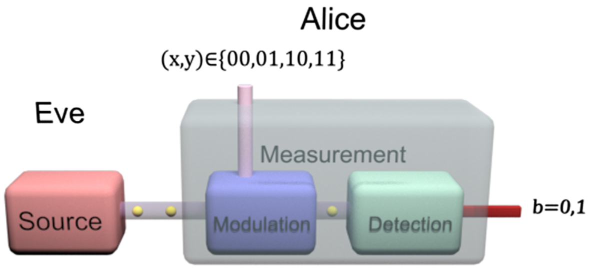
Semi-device-independent QRNGs become an appropriate approach with a faster generation rate and lower difficulty to implement. There are two main orientations widely studied in the field of semi-device-independent-QRNG research. One is abandoning the assumption of a the part of devices, such as the source [17] or the measurement [18], and completely characterizing the other devices. Source-independent (SI) QRNG is one of the areas receiving considerable attention [17,19–25]. However, the measurement devices are usually noisy, and it is too complicated to characterize all of the measurement imperfections, which may lead to some security loopholes [21,25,26]. Another one is the so-called self-testing QRNG [27,28]. This protocol applies a stronger assumption that all the devices are trusted and the dimension of the system is given. Compared with the former one, self-testing QRNG can generate randomness without detailed device characterization of the source and the measurement, which is adapted to arbitrary noise and high loss. Unfortunately, although this protocol delivers extraordinary benefits, the strict assumptions of the device credibility and the source dimension limit the abilities of external quantum eavesdroppers and the selection of the source, which would cause the limitation of its application scenarios. Because of these reasons, we hope there is a

QRNG that can combine the advantages of the two types of protocols above.

In this Letter, we propose and experimentally demonstrate a semi-device-independent-QRNG protocol with an untrusted source and trusted but error-prone measurement devices. In particular, our protocol removes the key assumptions of the source, including the limited dimensions and lacking security for external eavesdroppers, so it can be grouped into the area of SI-QRNGs but request much lower demand than SI-QRNGs. Some reasonable assumptions on the measurement devices are needed but their imperfections do not need to be characterized. We can quantify the imperfections by entropy estimation and monitor them synchronously with randomness generation. We analyze the randomness based on the universally composable security framework [29,30]. Precisely, by combining the uncertainty relationship for smooth entropies [31,32] and the quantum leftover hashing lemma [33], we extract secure random numbers with a given security level. By applying the two-dimensional measurement, we limit the system dimension to two dimensions, which allows the source to have arbitrary dimensions. Our protocol focuses on common trusted but error-prone two-dimensional coding systems, such as the coding in phase or polarization. The assumption removal of source and the imperfections tolerance of measurement make its security more compatible with its practical devices. We have demonstrated our protocol with a discrete variable experimental system and the general sources, a laser and a halogen bulb. Even if we offer this strong form of security, the randomness generation rate can also be achieved by more than 1 Mbps, which is close to many commercial QRNGs [34].

Protocol description.—The schematic diagram is illustrated in Table. I. Our protocol is formed from three parts: untrusted source, modulation, and detection. In each round, a quantum signal with arbitrary dimensions will be emitted by the untrusted source correlated with the external eavesdropper, Eve. Alice obtains the signal and executes the uncharacterized modulation $\mathcal{F}_y \circ \mathcal{E}_x$ as the settings among four modulations that combined by $x \in \{0,1\}$ and $y \in \{0,1\}$, and then one uncharacterized measurement $\mathbb{M}$. The result should be classified and encoded as a binary outcome $b = \{0,1\}$. In the postprocessing part, Alice computes the probability distributions $p(b|xy)$ to extract the secure random numbers. In the idea condition, the signal states should be the quantum state $|0\rangle\langle 0|$, the modulation is just the encoding approach in the well-known BB84 quantum key distribution (QKD) [35]. Precisely, x represents the bit information corresponding to the operations $\mathcal{E}_0 = I$ and $\mathcal{E}_1 = \sigma_y$, y represents the basis information corresponding to the operations $\mathcal{F}_0 = I$ and $\mathcal{F}_1 = H$, and the measurement $\mathbb{M}$ should be $\mathbb{X}$ with elements $\{\mathbb{M}_m\} = \{|+\rangle\langle +|, |-\rangle\langle -|\}$, where I is the identity matrix, $H = (\sigma_x + \sigma_z)/\sqrt{2}$ is the Hadamard matrix, and σ_x, σ_y, σ_z are the three Pauli matrices, respectively.

TABLE I. Protocol.



Untrusted source:
There are N experimental rounds. An untrusted party correlated with the external eavesdropper, Eve, prepares an N-system quantum state ρ^N with each subsystem labeled by $\{\rho_1, \rho_2, \ldots, \rho_N\}$, respectively, and then sends ρ_i to the trusted but uncharacterized measurement of Alice in each round $i \in N$.

Modulation:
Alice randomly chooses a setting among two values $(x_i, y_i) = 00$, 01, 10, 11 with the probabilities $P_g/2$, $P_t/2$, $P_g/2$, $P_t/2$, respectively, and modulates each state ρ_i by the operator $\mathcal{F}_{y_i} \circ \mathcal{E}_{x_i}$. Ideally, the four states $\mathcal{F}_{y_i} \circ \mathcal{E}_{x_i}(\rho_i)$, respectively, correspond to the four BB84 QKD [35] protocol's states with asymmetric probabilities.

Detection:
Then the modulated state will be measured with the operator $\mathbb{M}$ and the detectors will output a binary outcome $b_i = 0, 1$ in each round.

Randomness generation:
Alice finishes the rounds above and chooses $N(P_g - P_t)$ binary outcome bits from the settings satisfied: $y_i = 0$ as the raw random sequence.

Parameter estimation:
For the remaining $2NP_t$ outcome bits, Alice calculates the frequency distributions $R \coloneqq \sum_i (-1)^{y_i}(b_i \oplus x_i)/2NP_t$ and estimates the randomness generation rate l. If l is negative, these rounds will be aborted.

Randomness extraction:
Alice applies a universal$_2$ hash function to the raw sequence to extract the l bits' final random numbers. With the composable security definition and quantum leftover hashing lemma, the security parameter is ε_{sec}.

Security analysis.—In this section, we first list some assumptions and notions for security analysis, and based on that, we then present our main result and a sketch proof. We assume that (1) the modulators and detectors are trusted but imperfect. Precisely, Eve does not have any prior information about the modulation values (x, y). $\mathcal{F}_y \circ \mathcal{E}_x$ are some uncharacterized complete positive trace-preserving (CPTP) maps. Eve can know the uncharacterized measurement $\mathbb{M}$ but not directly obtain the information of the binary outcome bit b in each round. (2) $\mathcal{E}_x$, $\mathcal{F}_y$, and $\mathbb{M}$ are independent and identically distributed (IID). Precisely, we need the errors to not be dependent on the operator selections. (3) The modulation and measurement are contained in two-dimensional quantum space. Precisely, the incoming states will be modulated within two-dimensional space, such as photon polarization or phase. The detector is restricted to output binary outcomes only. If not, we group all outcomes into a binary one.

Actually, these assumptions are quite natural and not hard to be realized. For the first assumption, since we have trusted the modulator and detector, we have reason to believe that there are no quantum memories embedded in either the modulator or detector. There could be some classical correlations in the devices, for example, Eve can get the imperfect parameters of our devices. But such imperfections would not open any security loophole since our protocol has already allowed uncharacterized modulation and measurement. Moreover, it is also natural that outside cannot access a choice of the setting of x, y and the setting can be decided by a preset random sequence such as some pseudorandom numbers. For the second assumption, for the trusted modulator and detector, we can reasonably assume that they execute the operations in each round. Note that we allow some errors and drifts to exist as long as they are not dependent on the selections of the modulation and measurement, such as afterpulse and dark counts. If these errors are commuted with our operators, we can put the dual of them on the untrusted source and these errors will cause the entropy to decrease [27]. For the third assumption, we do not adopt the fair-sampling assumption to abandon the empty response which is common in the loss-tolerant systems [27]. Instead, we need to use a fixed coding rule to set each outcome, including the no click event, as a binary sequence. This assumption guarantees that our protocol can resist the detection blindness attacks [36] which cannot be tolerated in many present discrete variable semi-device-independent-QRNGs. Further discussions can be found in the Supplemental Material [37].

The dimensions of the source are not limited, and we reduce the dimensions by encoding the outputs. This step is similar to the squashing model which is applied in SI-QRNGs [17,21,25]. The difference is that instead of limiting our detectors to the threshold detectors, we add the assumption that our measurement devices are contained in two-dimensional quantum space and not disturbed by the other degrees of freedom. Our protocol can thus exclude the influence of the dimension.

We analyze the security under the universal composable security framework. A QRNG protocol is $\varepsilon_{\mathrm{sec}}$ secret if

$$\frac{1}{2}\|\rho_{XE} - U_X \otimes \rho_E\|_1 \leq \varepsilon_{\mathrm{sec}}, \tag{1}$$

where U_X is the fully mixed state of random numbers, ρ_{XE} is the composed state of Alice and Eve, ρ_E is the reduced density operator from ρ_{XE}, and $\|\cdots\|_1$ denotes the trace norm. Based on that, we say our QRNG protocol is $\varepsilon_{\mathrm{sec}}$ secret if

$$l \leq n\left[1 - h\left(\frac{1}{2} - \hat{R}\right)\right] - 2\log\frac{1}{\varepsilon_{\mathrm{sec}}}, \tag{2}$$

where l is the length of secure and final random number, $n = N(P_g - P_t)$ is the length of the raw random number used for extracting the final random number, $h(\cdots)$ denotes the binary entropy function, log denotes the logarithm based on 2, $\hat{R}$ given by

$$\hat{R} \geq R - \sqrt{\frac{N(N-n+1)}{n(N-n)^2}\ln\frac{4}{\varepsilon_{\mathrm{sec}}}} \tag{3}$$

denotes the lower bound of the frequency distributions R when considering statistical fluctuations. Here, similarly to [45], we apply Serfling inequality [46] to estimate it, and in the asymptotic scenario, $l \leq n[1 - h(\frac{1}{2} - R)]$. Here $R = \Pr(b \oplus x = 1|y = 0) - \Pr(b \oplus x = 1|y = 1)$; we emphasize that $\Pr(b \oplus x = 1|y = 0)$ must be no greater than $1/2$, otherwise we take $\Pr(b \oplus x = 0|y = 0) = 1 - \Pr(b \oplus x = 1|y = 0)$ to replace it. Similarly, we assume $\Pr(b \oplus x = 1|y = 1)$ is not greater than $1/2$, otherwise take $\Pr(b \oplus x = 1|y = 1)$ to replace it. The reason R is nonnegative is because it is required by our setting; we abort the protocol once the calculated value of R is negative.

In the following, we present a sketch of the proof, one can go to the Supplemental Material for a detailed proof [37]. First, in each single round, we can view $\mathbb{M}_y \coloneqq \mathbb{M} \circ \mathcal{F}_y$ as two observables with eigenvalues ± 1 on Hilbert space $\mathcal{H}$, and then we prove that $\mathbb{M}_y$ can equivalently be viewed as unknown projective measurement $\mathbb{M}_y^p$ preceded by a quantum operation $\mathcal{G}$, that is $\mathbb{M}_y = \mathbb{M}_y^p \circ \mathcal{G}$. Therefore, we can put the dual of this quantum operation on Eve's attack and consider the projective measurement only. Second, we can suppose that there exists a virtual third party named Fred who holds the classical system of x, and for all randomness generation rounds, Alice, Eve, and Fred share the composed state $|\Psi\rangle_{AEF}^n$ before Alice performs the measurement. Precisely speaking, Fred can record the classical bit x_i in each randomness generation round, so that he holds a bit string denoted by $\boldsymbol{x}$. Similarly to [45], considering a hypothetical experiment in which Alice performs $\mathbb{X}$ measurement for randomness generation and its complementary measurement $\mathbb{Z}$ for testing the information leakage, the intrinsic randomness comes from the following argument: the better Alice is able to guess Fred's classical bits if performing $\mathbb{Z}$, the less information Eve will obtain if performing $\mathbb{X}$. To capture the above logic, we can use the freedom to label $\mathbb{M}_0^p$ as $\mathbb{X}$, as we have not chosen a frame reference for each subsystem yet. Though the unknown measurement $\mathbb{M}_1^p$ may not be the complementary measurement of $\mathbb{M}_0^p$, we can still obtain the upper bound of

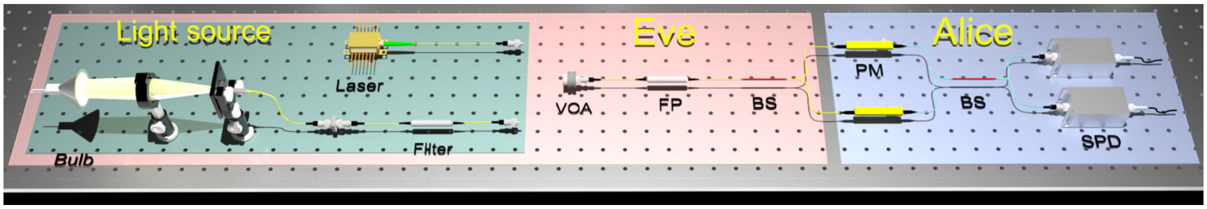


FIG. 1. Schematic representation of the experimental setup. A bulb and a laser are the optional light sources that are controlled by Eve. Alice receives the photons and measures them by two PMs and SPDs. VOA, variable optical attenuator; FP, fiber polarizer; BS, beam splitter; PM, phase modulator; SPD, single photon detector.

uncertainty, Alice guessing Fred's classical bits through the value R. Finally, according to the quantum leftover hashing lemma [29,33], one can extract an $\varepsilon_{\mathrm{sec}}$-secret random string of length l.

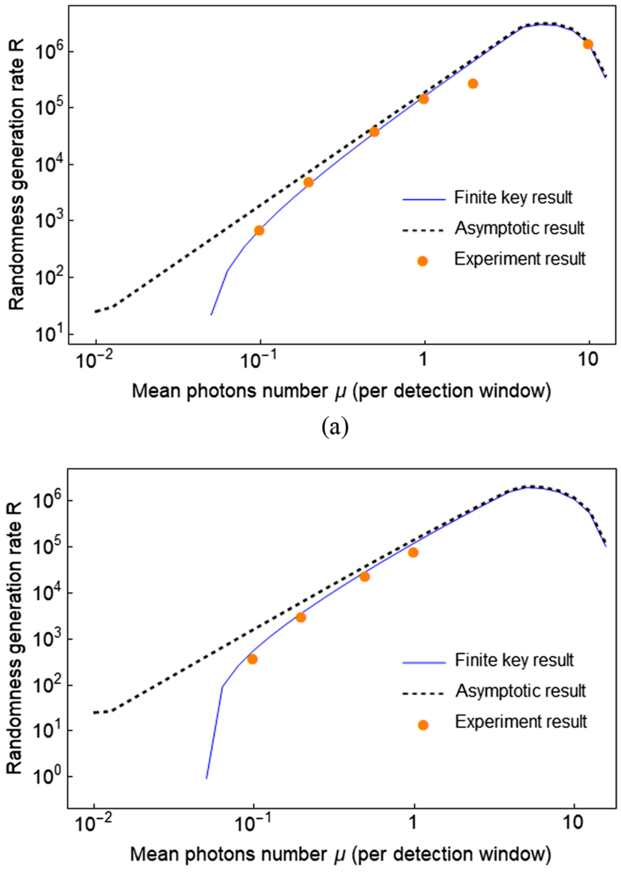
As detailed proof in the following, we can see that the source in our protocol can resist classical and quantum attacks. In particular, we allow that the photons Alice obtained are entangled with the photon clusters controlled by Eve. Note that tolerating the quantum attacks which are not allowed in self-testing QRNGs [27,28,47,48] is one of the key challenges to the analysis for semi-device-independent scenarios.

Experiment.—We demonstrate our protocol by a discrete variable experimental system. Our protocol is unrestricted by the type of the experimental system and with proper coding technology, we can also apply the other systems, such as the continuous variable system. The experiment setup is displayed in Fig. 1, in which the phase coding technology is more suitable for high-speed optical fiber modulation and thus has been applied. The implementation can be divided into two parts: the untrusted source parts controlled by Eve and the all-fiber measurement parts controlled by Alice, which are both formed by commercially available components.

Since the trusted source is not necessary, the choice of the light source is less restrictive, and even daily light, such as the sunlight, can be used [21]. In our setup, for demonstrating the robustness of using coherent and thermal states, we utilize common daily-use light, such as a halogen bulb and a laser, to generate the initial photons. For a high performance of our implementation, we also precisely filter the spectrum and calibrate the polarization of the emitted light. With several filters, the input photons will be filtered to guarantee a bandwidth of no more than 100 GHz and then two synchronously outputting light beams whose phase difference is zero can be separated by the 50/50 beam splitter (BS).

These two light beams as the randomness source are sent into the measurement part and then interfered. Two phase modulators (PMs) are placed on the arms of the interferometer and realize the function of modulation and base selection, respectively, and then the results of interference are detected by two 20 MHz InGaAs gated threshold detectors. Here, we have performed a proof-of-concept implementation for the random modulation and base selection by testing the results of different $\{x, y\}$ in batches. To satisfy the third assumption, we encode the response of no-click and detector D_0 as "0," and the response of double-click and detector D_1 as "1." As our analysis above, the outcomes of no-click and double-click events will be processed with entropy estimation and randomness extraction.

We acquired the total number of effective rounds $N = 10^8$. The final randomness rates under different initial photon numbers are calculated and compared with the simulation model which is demonstrated in Fig. 2. The number of rounds tested in each batch is chosen based on



(a)

(b)

FIG. 2. The simulation and experiment results with different light sources. (a) Results with the laser. (b) Results with the halogen bulb.

the optimal probability distributions of $\{P_g, P_t\}$ in the simulation. The final randomness generation rates achieved the high rate of 1.34 Mbps when using the laser source and 76.4 kbps when using the halogen bulb source. As shown in Fig. 2, with the changes of the photon intensity, the unexpected responses, such as no-click events and double-click events, will lead to different rates. In our protocol, the variations of the parameters will be reflected in the final rates and thus will not lead to overestimation of the entropy.

Finally, the security random numbers are extracted by the Toeplitz-matrix hashing. We performed the standard statistical test, NIST [49], to check the patterns and correlations of a string of final random numbers. The statistical tests cannot offer proof of randomness, while these tests are important to indicate the statistical property of random sequences. Detailed parameters of the devices and results of the statistical test can be found in the Supplemental Material [37].

Conclusion.—In this work, we have proposed a semi-device-independent QRNG with an untrusted source and trusted but uncharacterized measurement devices. By using the uncertainty relationship for smooth entropies, we have achieved secure randomness generation with a given security level. With the commercially available devices, the performance of our implementation can achieve a Mbps randomness generation, which is close to many commercial QRNGs.

Compared with some semi-device-independent QRNGs before, such as SI-QRNG and self-testing QRNG, our QRNG has a more powerful form of security requiring less characterization in measurement and source, respectively. A DI-QRNG can offer even stronger security, however, the state-of-the-art setups and low rates limit its practicality. Our QRNG is an effort to remove the assumptions of the devices as much as possible but guarantee a simple implementation and a high rate. We believe the strong security and the simple but effective scheme will make our QRNG practical in more applications.

We thank Hoi-Kwong Lo for helpful discussions. This work was supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grants No. 61622506, No. 61627820, No. 61822115, No. 61875181 and No. 61675189) and the 111 Project (D20031), and the Anhui Initiative in Quantum Information Technologies. R. W. is financially supported by the University of Hong Kong start-up grant.

X. L. and R. W. contributed equally to this work.

[*] wshuang@ustc.edu.cn

[†] yinzq@ustc.edu.cn

[1] G. Ossola and A. D. Sokal, Phys. Rev. E **70**, 027701 (2004).

[2] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, in *Proceedings of the 21st USENIX Security Symposium (USENIX Security 12)* (2012), pp. 205–220, https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf.

[3] M. Born, Z. Phys. **38**, 803 (1926).

[4] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

[5] M. Stipčević and B. M. Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).

[6] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).

[7] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).

[8] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).

[9] H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).

[10] P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, Opt. Express **19**, 25173 (2011).

[11] Y.-Y. Hu, X. Lin, S. Wang, J.-Q. Geng, Z.-Q. Yin, W. Chen, D.-Y. He, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Opt. Lett. **45**, 6038 (2020).

[12] S. Pironio, A. Acín, S. Massar, A. Boyer 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).

[13] 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).

[14] P. Bierhorst *et al.*, Nature (London) **556**, 223 (2018).

[15] Y. Liu *et al.*, Nature (London) **562**, 548 (2018).

[16] 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.*, Nat. Phys. **17**, 448 (2021).

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

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

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

[20] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Nat. Commun. **9**, 5365 (2018).

[21] Y.-H. Li, X. Han, Y. Cao, X. Yuan, Z.-P. Li, J.-Y. Guan, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng *et al.*, npj Quantum Inf. **5**, 97 (2019).

[22] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Phys. Rev. X **10**, 041048 (2020).

[23] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Phys. Rev. Applied **12**, 034017 (2019).

[24] Z. Zheng, Y. Zhang, M. Huang, Z. Chen, S. Yu, and H. Guo, Opt. Express **28**, 22388 (2020).

[25] X. Lin, S. Wang, Z.-Q. Yin, G.-J. Fan-Yuan, R. Wang, W. Chen, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, npj Quantum Inf. **6**, 100 (2020).

[26] D. Ma, Y. Wang, and K. Wei, Quantum Inf. Process. **19**, 1 (2020).

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

[28] F. Xu, J. H. Shapiro, and F. N. Wong, Optica **3**, 1266 (2016).

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

[30] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).

[31] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).

[32] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[33] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[34] I. Quantique, Quantis random number generator, http://www.idquantique.com/randomnumbergeneration (Accessed 2014).

[35] 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.

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

[37] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.129.050506 in Section I for details on the security proof, in Section II details on the experiment while Section III shows assumption analysis for our implementation and Section IV gives data analysis, which includes Refs. [38–44].

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

[39] E. L. Wooten, K. M. Kissa, A. Yi-Yan, E. J. Murphy, D. A. Lafaw, P. F. Hallemeier, D. Maack, D. V. Attanasio, D. J. Fritz, G. J. McBrien, and D. E. Bossi, IEEE J. Sel. Top. Quantum Electron. **6**, 69 (2000).

[40] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Phys. Rev. A **84**, 062308 (2011).

[41] W.-B. Liu, Y.-S. Lu, Y. Fu, S.-C. Huang, Z.-J. Yin, K. Jiang, H.-L. Yin, and Z.-B. Chen, arXiv:2204.12156.

[42] W. Zhang, J. Huang, C. Zhang, L. You, C. Lv, L. Zhang, H. Li, Z. Wang, and X. Xie, IEEE Trans. Appl. Supercond. **29**, 1 (2019).

[43] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, Phys. Rev. Applied **2**, 064006 (2014).

[44] J. Argillander, A. Alarcón, and G. B. Xavier, J. Opt. **24**, 064010 (2022).

[45] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).

[46] R. J. Serfling, Ann. Stat. **2**, 39 (1974).

[47] D. Rusca, H. Tebyanian, A. Martin, and H. Zbinden, Appl. Phys. Lett. **116**, 264004 (2020).

[48] H. Tebyanian, M. Zahidy, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, Quantum Sci. Technol. **6**, 045026 (2021).

[49] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Technical Report, Booz-Allen and Hamilton Inc, McLean VA, 2001, https://apps.dtic.mil/sti/citations/ADA393366.