Downloaded from orbit.dtu.dk on: Apr 19, 2024

DTU Library

Self-testing quantum random-number generator based on an energy bound

Rusca, Davide; van Himbeeck, Thomas; Martin, Anthony; Brask, Jonatan Bohr; Shi, Weixu; Pironio, Stefano; Brunner, Nicolas; Zbinden, Hugo

Published in:
Physical Review A

Link to article, DOI:
10.1103/physreva.100.062338

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Rusca, D., van Himbeeck, T., Martin, A., Brask, J. B., Shi, W., Pironio, S., Brunner, N., & Zbinden, H. (2019). Self-testing quantum random-number generator based on an energy bound. *Physical Review A*, *100*(6), Article 062338. https://doi.org/10.1103/physreva.100.062338

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Self-testing quantum random-number generator based on an energy bound

Davide Rusca,[1] Thomas van Himbeeck,[2,3] Anthony Martin,[1] Jonatan Bohr Brask,[1,4] Weixu Shi,[5,1] Stefano Pironio,[2,3] Nicolas Brunner,[1] and Hugo Zbinden[1]

[1]*Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland*
[2]*Laboratoire d'Information Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*
[3]*Centre for Quantum Information and Communication, Université Libre de Bruxelles, Belgium*
[4]*Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark*
[5]*College of Electronic Science, National University of Defense Technology, Hunan, Changsha 410073, China*

(Received 3 May 2019; published 30 December 2019)

We introduce a scheme for a self-testing quantum random-number generator and demonstrate it experimentally. Compared to the fully device-independent model, our scheme requires an extra natural assumption, namely, that the mean number of photons of the signal optical modes is bounded. The scheme is self-testing, as it allows the user to verify in real time the correct functioning of the setup, hence guaranteeing the continuous generation of certified random bits. The scheme is based on a prepare-and-measure setup, which we implement in a proof-of-principle experiment using only off-the-shelf optical components. The randomness generation rate is 1.25 Mbits/s, comparable to commercial solutions. Overall, we believe that this scheme achieves a promising trade-off between the required assumptions, ease of implementation and performance.

DOI: 10.1103/PhysRevA.100.062338

I. INTRODUCTION

The device-independent (DI) approach allows for certified quantum random-number generation (QRNG) based on minimal assumptions [1–3]. In particular, no detailed knowledge about the internal working of the quantum devices is needed and the output can be guaranteed to be random from the point of view of a hypothetical adversary, even in the extreme case where the adversary itself prepared the devices. These ideas have generated considerable interest in recent years (see [4] for a recent review) and first proof-of-principle experiments have been reported [2,5–7].

While conceptually fascinating, the fully DI approach is still at the moment far from being practical since it requires loophole-free Bell tests, which not only are extremely challenging to implement but feature rates in state-of-the-art experiments that are orders of magnitude lower than commercially available QRNGs. This has motivated the development of alternative solutions (see, e.g., [8–18]), often referred to as semi-DI (or self-testing), exploring intermediate possibilities between the fully DI setting and the more standard "device-dependent" approaches to QRNG, which require a full characterization of the devices (see, e.g., [19–24]). Such semi-DI solutions are much easier to implement than fully DI protocols, but rely on some extra, even though limited, assumptions on the devices. Though the introduction of these extra assumptions may at first seem a departure from the DI ideal, one should realize that the DI model also requires a certain number of assumptions that are far from being trivially satisfied in practice, such as no information leakage from the devices or that the software used to acquire and process the data functions correctly.

In the present work, we introduce a QRNG protocol, which we believe achieves an excellent trade-off between the required assumptions, performance and ease of implementation. The scheme is based on a prepare-and-measure scenario and thus requires no entanglement or Bell test. In turn, we report a proof-of-principle experiment that features only standard off-the-shelf optical components and achieves randomness generation rates of the order of MHz, hence comparable to commercial QRNGs. Moreover, the output randomness can be certified based on few natural assumptions. Compared to the fully DI model, our scheme requires an additional assumption, namely, that the signal sent by the source is optical modes with an average number of photons that is upper bounded. This assumption is arguably quite natural in an optical setup, where the mean photon number can be directly measured and monitored. Our scheme does not require the assumption of identical and independently distributed runs (i.i.d. hypothesis) and is thus robust to any sort of memory effects and temporal drifts. The scheme is "self-testing," allowing the user to verify in real time the correct functioning of the setup, hence guaranteeing the continuous generation of certified random bits.

II. SECURITY FRAMEWORK

We first present our QRNG protocol, which builds upon the general framework for self-testing (or semi-DI) RNG introduced in [25]; note that technical details about the security analysis are deferred to a companion paper [26]. We consider a prepare-and-measure scenario with a binary input x for the preparation device, and a binary output b for the measurement device. For each input, the preparation device sends to the measurement device an optical multimode signal in some quantum state. In addition, there may be internal classical noise affecting both the state preparation and the measurements, possibly in a correlated way. The observed input-output correlations in a single use of the device can then

 ©2019 American Physical Society

be written,

$$p(b|x) = \sum_{\lambda} p(\lambda)\,\mathrm{Tr}\left[\rho_x^{\lambda} M_b^{\lambda}\right], \tag{1}$$

where ρ_x^{λ} are the prepared states, M_b^{λ} are elements of a positive-operator valued measure (POVM) defining the measurement, and $x, b \in \{0, 1\}$, while λ is arbitrary and represents the classical noise.

We aim to certify genuinely quantum randomness in the output b. This means we need to separate any apparent randomness in b due to the classical noise λ from that originating from the inherent randomness in the quantum measurements. Furthermore, we want to do this with only limited characterization of the devices. In particular, neither the states nor the measurements are known to the user. The certification will be based on the input-output correlations $p(b|x)$, together with an assumption about the average mean photon number (throughout the entire experiment) of the emitted quantum states. This assumption is much weaker than the one appearing in the work of [16], where the requirement was to bound the mean energy of each pulse sent by the source. By this assumption instead, the energy of each pulse can freely fluctuate during the experiment without reducing the security provided by our proof. Apart from this assumption, the devices are treated as black boxes [note that writing (1), we also implicitly assume that the devices do not share prior entanglement].

Our central assumption, which we refer to as the "energy" assumption, is formulated as

$$\sum_{\lambda} p(\lambda)\,\mathrm{Tr}\left[\rho_x^{\lambda} N\right] \leqslant \omega_x, \tag{2}$$

where N is the multimode photon number operator and ω_x represents a bound on the average photon number (i.e., the energy) of the quantum light states emitted by the preparation device.

In Ref. [25], it was shown that all correlations which can be obtained by mixing deterministic strategies using classical shared randomness must obey

$$|E_0 - E_1| \leqslant 2(\omega_0 + \omega_1), \tag{3}$$

where we defined $E_x := p(0|x) - p(1|x)$.

We now introduce a physical setup in which this bound can be violated. Such a violation implies that the devices' behavior cannot be explained deterministically and thus that genuine quantum randomness is produced at the output of the measurement device.

The setup is shown in Fig. 1. Depending on the input x, the amplitude of a signal coherent state (produced by a laser) is modulated such that the output amplitude for $x = 0$ is 0, while for $x = 1$ it is α. The transmitted state is then measured by interfering it with a local oscillator with amplitude β on a beam splitter, followed by single-photon threshold detection in one output port. The other output port is simply ignored. The beam splitter has transmittivity t^2 and reflectivity $r^2 = 1 - t^2$. In the event that the detector does not click, we assign the output $b = 0$, while $b = 1$ corresponds to a click. This protocol is a hybrid combination of the two protocols shown in [25], i.e., the on-off keying (OOK) and the binary phase-shift keying (BPSK). Our protocol has the same modulation

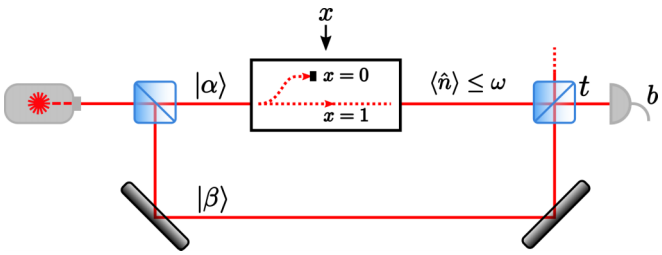

FIG. 1. Self-testing quantum random-number generation based on bounded energy. A signal coherent state is modulated depending on the input x. The signal is blocked for $x = 0$ and transmitted for $x = 1$ and the average energy after the modulation is bounded by ω. The signal is mixed with a local oscillator on a beam splitter with transmittivity t^2 and measured by a single-photon detector.

of the source state as the OOK and the kind of interferometric detection presented in the BPSK; however, the protocol presented here requires, instead of two balanced linear detectors, only a threshold single-photon detector. The probabilities for the detector not to click can be computed explicitly,

$$p(0|0) = e^{-\eta|r\beta|^2}, \tag{4}$$

$$p(0|1) = e^{-\eta|t\alpha + r\beta|^2}, \tag{5}$$

where $\eta \in [0, 1]$ represents a combined transmission and detection efficiency accounting for losses and inefficient detectors [27]. The remaining probabilities are determined by normalization.

The mean photon numbers at the output of the preparation device are

$$\langle N \rangle = \begin{cases} 0 & \text{for } x = 0 \\ |\alpha|^2 & \text{for } x = 1, \end{cases} \tag{6}$$

and we can then take the energy bounds on the transmitted states (2) to be equal to the these mean photon numbers. Note that the local oscillator carries no information about x and is not considered to be part of the prepared state. In particular, no assumption is made on the amount of energy in the local oscillator arm.

In our case, the inequality (3) then becomes

$$\left|e^{-\eta|t\alpha + r\beta|^2} - e^{-\eta|r\beta|^2}\right| \leqslant |\alpha|^2. \tag{7}$$

It is easy to see that for any value of $\eta > 0$, there exist choices of α and β for which (7) is violated. For instance, take $\alpha = \eta t/2$, $\beta = 1/r$. Then one can verify analytically that the inequality is violated for small η by expanding the left-hand side in η, and one can check numerically that it is also the case for all larger η. Thus, for any nonzero efficiency, our scheme admits α and β for which the output b is not deterministic.

Given data that violate (3), we need to quantify the randomness generated by the measurement device. For a device behavior which is independent and identically distributed (i.i.d.) in each experimental round, the optimal asymptotic rate of randomness generation, relative to an observer with knowledge of the input x as well as the internal variable λ, is given by the Shannon entropy $H(B|X, \Lambda) = -\sum_{b,x,\lambda} p(\lambda)p(x)p(b|x)\log_2 p(b|x, \lambda)$ (this follows from the asymptotic equipartition theorem [28]). For any given values of the probabilities $p = \{p(x, b)\}_{b,x}$ and the energy bounds

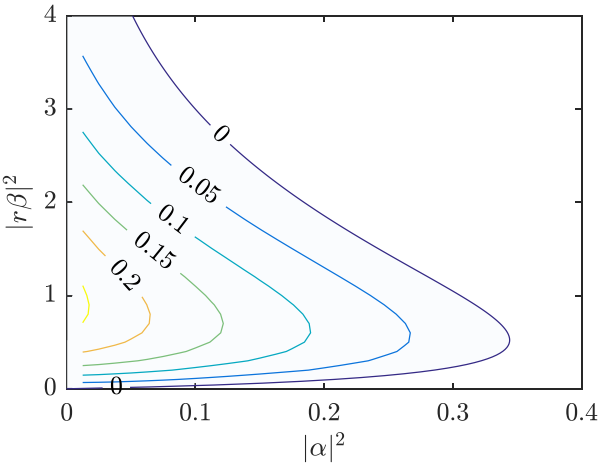

FIG. 2. Asymptotic rate of randomness generation (in bits) as a function of the experimental parameters. The rate is the worst-case entropy $H(B|X\Lambda)$, given the correlations p and the average energy constraint $\bar{\omega}$. These were obtained assuming an identical phase $\arg(\alpha) = \arg(\beta)$, a biased input distribution $p_x(1) = 0.25$, detection efficiency $\eta = 50\%$, and transmission $t^2 = 99\%$. Only the α and β in the shaded region satisfy the inequality (7).

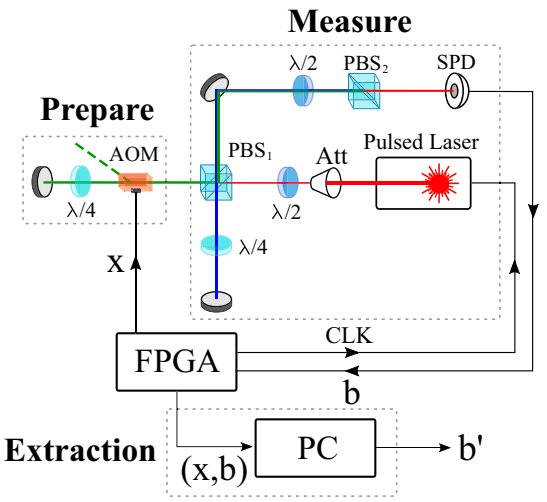

FIG. 3. Experimental setup. A coherent stage is generated by a pulsed diode laser and sent to a Michelson interferometer. One arm (green path) is used to prepare the signal and the other one (blue path) to prepare the local oscillator.

$\omega = \{\omega_x\}_x$ (or linear functions of them), it is shown in [26] how, using semidefinite programming, one can put a lower bound on $H(B|X, \Lambda)$ that is valid for arbitrary decompositions (1) and (2) that use hidden classical noise $p(\lambda)$.

As an illustration, we show in Fig. 2 the entropy for several values of α and β, using $\eta = 50\%$, $t^2 = 99\%$, a biased input distribution $p(1) = 25\%$, and assuming the bound $\sum_x p(x)\omega_x \leqslant \bar{\omega} = p(1)|\alpha|^2$ on the average value of the energies ω_x.

Semidefinite programming

The semidefinite programming (SDP) introduced in [26] not only returns the lower bound on $H(B|X, \Lambda)$, but also provides a self-test or witness certifying this amount of randomness. This self-test consists of a linear function $\gamma[p] - \zeta[\omega]$ in p and ω with the property that $H(B|X, \Lambda) \geqslant \gamma[p] - \zeta[\omega]$. Once such witness is known, it thus suffices to evaluate it on p and ω to obtain a lower bound on $H(B|X, \Lambda)$.

The existence of such a witnesses, which can be computed for any given p and ω, immediately suggests a semi-DI RNG protocol: (1) fix a certain witness (tailored to the expected behavior of the devices); (2) run the devices n times and record the inputs $\boldsymbol{X} = (X_1, X_2, \dots)$ and outputs $\boldsymbol{B} = (B_1, B_2, \dots)$; and (3) compute the value $\gamma[f]$, where $f(x, b)$ are the frequencies of occurrence of $(X_i, B_i) = (x, b)$, and check if $\gamma[f] - \zeta[\omega] \geqslant h$ is above some threshold h. The passing of this test, denoted by "Pass," establishes that the device is working properly.

In the implementation of such a protocol, it is not necessarily the case that the device behaves in a i.i.d. way and its general behavior is now described by an unknown n-round joint distribution $p_{[\boldsymbol{B},\boldsymbol{X},\boldsymbol{\Lambda}]}$. Still the observed value of the linear witness, computed from the observed frequencies, certifies a certain amount of randomness in the output string $\boldsymbol{B}$. Specifically, in [26], it is shown that the distribution $p_{[\boldsymbol{B},\boldsymbol{X},\boldsymbol{\Lambda}|\text{Pass}]}$ conditioned on the passing of the test contains an amount of randomness given by

$$H_{\min}^{\epsilon'}(\boldsymbol{B}|\boldsymbol{X}, \boldsymbol{\Lambda}) \geqslant n\left[h - c\sqrt{\frac{\log_2(\epsilon/2)}{n}} - d\frac{\log_2(\epsilon/2)}{n}\right]. \quad (8)$$

Here, $H_{\min}^{\epsilon'}(\boldsymbol{B}|\boldsymbol{X}, \boldsymbol{\Lambda})$ is the worst-case conditional smooth min-entropy, defined as the largest k such that $\Pr[-\log_2 p(\boldsymbol{B}|\boldsymbol{X}\boldsymbol{\Lambda}\text{Pass}) \geqslant k] \geqslant 1 - \epsilon'$. It roughly corresponds to the largest number of bits that can be extracted from the output string $\boldsymbol{B}$ using a strong extractor, such that the resulting distribution deviates from an ideal distribution (i.e., uniform and independent of $X\Lambda$) at most with probability ϵ'. The security parameter ϵ in the right-hand side of (8), which should be chosen small ($\epsilon = 10^{-10}$ in the following), is related to the smoothing parameter though $\epsilon' = \epsilon/\Pr(\text{Pass})$. This ensures that the protocol is ϵ-sound because the probability of both passing the test and deviating from an ideal distribution $\Pr(\text{Pass}) \times \epsilon' = \epsilon$ is guaranteed to be small. The subleading error terms in (8), given by the constants $c, d > 0$, depend on the choice of witness $\gamma[\cdot]$ and $\zeta[\cdot]$ and are given in [26].

III. EXPERIMENTAL SETUP AND RESULTS

In order to implement the scheme presented in Fig. 1, we used the experimental setup drawn in Fig. 3. A coherent state is generated by a pulsed diode laser at 655 nm trigged by a field-programmable gate array (FPGA) at 12.5 MHz. A set of half-wave plate (HWP) and polarizing beam splitter (PBS) is used to prepare the local oscillator (β) and the signal (α) and to tune the amplitude ratio between them. To maximize the transmission to the output port of the interferometer, one quarter-wave plate (QWP) is inserted in each arm to rotate the polarization of the incoming light. For each pulse, a pseudorandom binary input x is generate by the FPGA and sent to the acousto-optic modulator (AOM). When $x = 0$, the

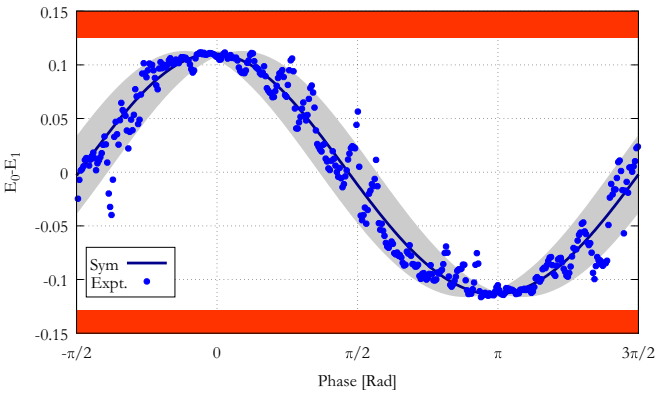

FIG. 4. Correlation function with respect to the phase difference between the two arms of the interferometer. The solid line corresponds to the simulated behavior of the device without phase fluctuation. The gray area corresponds to a relative phase incertitude region of $\pm 10\%$. The red (dark) area corresponds to the region of correlations unachievable once the bound on the energy ω is chosen to be 0.0025.

AOM deflects the light which introduces an additional loss of more than 23 dB.

At the output of PBS_1, the signal and local oscillator are in the same spatial and temporal mode, but have orthogonal polarizations. To make them interfere, they pass through a HWP and PBS_2. The HWP is oriented to achieve a transmission of $t^2 = 99\%$ for the signal. Then, the light is detected by a single-photon detector (SPD) (PerkinElmer SPCM-AQR) with an efficiency of 77% for a dark-count rate around 300 Hz and the digital signal is recorded by the FPGA. Each second, the FPGA sends the data to a personal computer for storage.

In order to bound the average energy on the signal, the power was measured at the output of PBS_1 while obstructing the local oscillator arm. This was done with a linear power meter (Thorlabs PM100D with S122C sensor) with an absolute uncertainty of $\pm 5\%$. The average energy bound was then calculated by considering the attenuation chosen before the interferometer and by dividing the resulting power by the repetition rate. The power on the signal and local oscillator was adjusted in order to maximize the amount of entropy generated based on the results presented in Fig. 2. These measurements were done twice, i.e., before and after the experiment, in order to ensure the stability of the power. Alternatively, the power could be monitored in real time using a beam splitter between the two PBSs, in a similar manner as in Ref. [16].

After the energies of the signal and local oscillator are set, we launch a measurement to estimate the correlation between the modulation of the signal and the detections. The measurement is carried out by changing the relative phase between α and β. This is done by moving the mirror in the local oscillator arm with a piezoelectric translator. The relevant marginals are then estimated as $\overline{p}(b|x) = n_{b,x}/n_x$, where $n_{b,x}$ and n_x correspond to the number of events for an output b given an input x and the total number of state x sent, respectively. Then, we calculated the correlation function $E = p(b = x) - p(b \neq x)$ shown in Fig. 4 as a function of the phase difference between α and β with $\omega_{\text{estimate}} = 0.0022(1)$. The energy of the local oscillator β is set to 99 mean photons per pulse, which corresponds to $(1 - t^2)|\beta|^2 = 0.99$ with $1 - t^2 = 0.01$. The solid line in the figure corresponds to the theoretical prediction for a perfect system (no phase fluctuations) with a signal state with ω_{estimate} mean photon number and global detection efficiency of 55%. We fixed the energy bound $\bar{\omega} = 0.0025 > \omega_{\text{estimate}}$ in order to assure that the general assumption is always verified. The fluctuations in Fig. 4 are due to fluctuations of the relative phase between the signal and local oscillator owing to the instability of the interferometer.

To perform a QRNG protocol, we considered 35 blocks of $n = 10^8$ rounds (8 s measurement) in which the interferometer was around a constructive interference. A witness was determined and optimized for this regime by using one trial block and, assuming an average energy assumption $\bar{\omega} = 0.0025$, a threshold was chosen at the value $h = 0.117$, corresponding to a rate (8) of 0.1 bits/round. The test was satisfied in all blocks, giving an average output rate of certified quantum randomness of 1.25 MHz. In order to promote this proof-of-principle experiment to a fully practical device, one would need to actively stabilize the interferometer. This can be done via standard methods; see, e.g., [29]. This procedure would then increase both the extractable entropy and the passing probability.

IV. CONCLUSION

In conclusion, we developed a simple scheme for a self-testing QRNG based on an energy bound. This scheme represents, in our opinion, an excellent compromise between the required assumptions, experimental complexity and performance. From the point of view of security, we believe that weakening the required assumptions without moving to the full DI scenario will be difficult. From the point of view of implementation and performance, progress can still be achieved, for instance, by using integrated optics.

ACKNOWLEDGMENTS

We acknowledge support from the Swiss National Science Foundation (Starting Grant No. DIAQ, Bridge project "Self-testing QRNG" and NCCR-QSIT), the EUs H2020 program under the Marie Sklodowska Curie project QCALL (Grant No. GA 675662), and the EU Quantum Flagship project QRANGE. T.V.H. acknowledges funding from the Fond de la Recherche Scientifique (F.R.S.-FNRS) through a FRIA grant (Belgium). S.P. acknowledges financial support through the Research Associate program of the Fonds de la Recherche Scientifique (F.R.S.-FNRS).

[1] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2009.

[2] 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, Random

numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[3] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, J. Phys. A: Math. Theor. **44**, 095305 (2011).

[4] A. Acin and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[5] 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, Detection-Loophole-Free Test of Quantum Nonlocality, and Applications, Phys. Rev. Lett. **111**, 130406 (2013).

[6] 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, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature (London) **556**, 223 (2018).

[7] 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, Device-independent quantum random-number generation, Nature (London) **562**, 548 (2018).

[8] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).

[9] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, Phys. Rev. A **90**, 052327 (2014).

[10] T. Lunghi, J. B. Brask, Charles Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).

[11] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Experimental quantum randomness generation invulnerable to the detection loophole, arXiv:1410.3443.

[12] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, New J. Phys. **17**, 125011 (2015).

[13] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, Phys. Rev. Lett. **118**, 060503 (2017).

[14] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, Phys. Rev. X **6**, 011020 (2016).

[15] F Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, Optica **3**, 1266 (2016).

[16] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Appl. **7**, 054018 (2017).

[17] T. Gehring, C. Lupo, A. Kordts, D. Nikolic, N. Jain, T. Pedersen, S. Pirandola, and U. L. Andersen, 8 GBit/s real-time quantum random number generator with non-iid samples, arXiv:1812.05377.

[18] T. Michel, J. Haw, D. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Real-Time Source Independent Quantum Random Number Generator with Squeezed States, Phys. Rev. Appl. **12**, 034017 (2019).

[19] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, J. Mod. Opt. **47**, 595 (2000).

[20] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, Rev. Sci. Instrum. **71**, 1675 (2000).

[21] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, A generator for unique quantum random numbers based on vacuum states, Nat. Photon. **4**, 711 (2010).

[22] Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo, and Li Qian, High-speed quantum random number generation by measuring phase noise of a single-mode laser, Opt. Lett. **35**, 312 (2010).

[23] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Opt. Express **22**, 1645 (2014).

[24] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Quantum Random Number Generation on a Mobile Phone, Phys. Rev. X **4**, 031056 (2014).

[25] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).

[26] T. Van Himbeeck and S. Pironio, arXiv:1905.09117.

[27] Since the local oscillator amplitude β is completely free, if the losses are different in each arm, we can just absorb a factor into β to make up for this difference.

[28] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (John Wiley & Sons, 2006).

[29] P. Hariharan, *Optical Interferometry*, 2nd ed. (Elsevier, 2003).