Applied Physics Letters ARTICLE scitation.org/journal/apl

Fast self-testing quantum random number generator based on homodyne detection

Cite as: Appl. Phys. Lett. **116**, 264004 (2020); doi: 10.1063/5.0011479
Submitted: 21 April 2020 · Accepted: 20 June 2020 ·
Published Online: 2 July 2020

Davide Rusca,[1,a)] Hamid Tebyanian,[2] Anthony Martin,[1,b)] and Hugo Zbinden[1]

AFFILIATIONS

[1]Départment de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland
[2]Dipartimento di Ingegneria dell'Informazione, Universita degli Studi di Padova, 35131 Padova, Italy

[a)]**Author to whom correspondence should be addressed:** davide.rusca@unige.ch
[b)]**Present address:** Universite Cote d'Azur, CNRS, Institut de Physique de Nice, Parc Valrose, 06108 Nice Cedex 2, France.

ABSTRACT

Self-testing and semi-device independent protocols are becoming the preferred choice for quantum technologies, being able to certify their quantum nature with few assumptions and simple experimental implementations. In particular, for quantum random number generators, the possibility of monitoring, in real time, the entropy of the source only by measuring the input/output statistics is a characteristic that no other classical system could provide. The cost of this possibility is not necessarily increased complexity and reduced performance. Indeed, here we show that with a simple optical setup consisting of commercially available components, a high bit generation rate can be achieved. We manage to certify 145.5 MHz of quantum random bit generation rate.

Quantum random number generators have been a developing topic in the past two decades. The interest of these devices resides in the fact that the randomness of the output string can be proven thanks to the intrinsic nature of quantum mechanics and does not need a stochastic model in order to evaluate the amount of entropy the experiment can produce.

However, while there exist many examples of quantum random number generators (QRNGs) that exploit many different quantum phenomena,[1–6] the challenge resides into proving that the randomness produced has, actually, a quantum origin. To do so, the device must be completely characterized in order to separate all possible sources of classical noise that could be foreseen by a malicious party. This first class of QRNGs is often referred to as device dependent (DD) QRNGs since their behavior is strongly related to the characterization of the device.

A different approach is instead given by the device independent (DI) approach.[7–9] In this case, it is possible to certify the randomness of the output in the most paranoid scenario in which the device itself is built by an adversary. While this approach is interesting and gives the highest level of security for a QRNG device, it has itself some drawbacks. First of all, the experiment relies still on some assumptions that must be verified, such as the space-like separation of the two measurement sites, but the greatest roadblock toward applications is the complexity of the devices and their low throughput rate, which is orders of magnitude lower than for standard DD-QRNGs.

For this reason, recently another approach has been investigated, the semi-device independent or self-testing QRNG.[10–22] The idea is, with few assumptions on the device, to implement a QRNG as simple as the existing commercial devices with a higher degree of security. Different experiments based on either uncharacterized sources[11,14,15] or uncharacterized measurement[13,16] devices have been presented. Finally, another approach combining a completely uncharacterized measurement with a partially characterized source has been developed. These protocols rely on assumptions on the dimension[10,12] of the produced quantum states, on their overlap,[18] or on their energy.[22]

In this work, we develop a semi-device independent QRNG featuring a simple and practical self-testing implementation with a performance of hundreds of certified Mbits/s. The only simple and easily verifiable assumption on the source is that the emitted states are limited in energy. The measurement device, based on a homodyne measurement, can remain completely uncharacterized. Note that a similar approach based on a heterodyne measurement has been demonstrated independently.[23]

As in a previous experiment,[22] the security framework is based on recent theoretical work.[21,24] The device can be modeled as a prepare and measure scenario. The source prepares one of two quantum states in an optical signal depending on a binary input x and sends them to a measurement device that outputs a binary value b. The prepared state and the measurement may depend on a correlated random

variable λ. The probability of each output conditioned on the input value can be then written as

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

where ρ_x^{λ} is the quantum state prepared by the source and M_b^{λ} is the positive-operator valued measure (POVM) element corresponding to the output b with $x, b \in \{0, 1\}$. In order to certify the quantum randomness in output b and separate it from classical noise represented by the classical variable λ, we make use of the analysis presented in Ref. 24.

Without any constraint on the prepared state and without any additional assumptions, the measured input output probabilities (correlated classically by an unknown classical hidden variable) could be easily described by a deterministic model. In our case, the two states can be arbitrarily chosen, but their energy must be limited. This assumption is referred to as "average energy" assumption since the quantity to be bounded is the following:

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

which represents the upper bound on the average energy (normalized with respect to the lowest photon energy of the optical signal) transmitted between the source and the measurement; in this formula, N represents the photon number operator and ω the bound chosen. The normalized energy is in this way given by the average number of photons transmitted in each signal.

Van Himbeeck *et al.*[21] showed that for a fixed value ω, the set of all possible quantum correlations is larger than the set of deterministic correlations. Furthermore, in the following work,[24] it was proven that if an input/output distribution belongs to the former set but not to the latter, then genuine randomness can be certified. In order to quantify the entropy produced by the input/output statistics of the experiment, the authors developed a semi-definite program (SDP) that returns a lower bound on the conditional Shannon Entropy $H(B|X, \Lambda)$. This bound can be used as witness to certify the amount of genuine quantum randomness. This witness corresponds to a linear function $\gamma[p] - \zeta[\omega]$ that depends only on the input/output probabilities p and the average energy bound ω. The witness defined before can be then used for a semi-device independent protocol where an entropy threshold h is fixed beforehand, and the previously defined witness is tailored over the expected behavior of the device. After running the experiment n times, we check that the linear witness is greater than the threshold h,

$$\gamma[f] - \zeta[\omega] \geq h, \tag{3}$$

where the witness is evaluated with the experimental input/output frequencies f measured from the experiment input/output results.

If the measured data passes the test in Eq. (3), the randomness contained by the output sequence is certified to be[24]

$$H_{min}^{\epsilon'}(\boldsymbol{B}|\boldsymbol{X}, \boldsymbol{\Lambda}) \geq n\left(h - c\sqrt{\frac{\log(\epsilon/2)}{n}} - d\frac{\log(\epsilon/2)}{n}\right), \tag{4}$$

where $H_{min}^{\epsilon'}(\boldsymbol{B}|\boldsymbol{X}, \boldsymbol{\Lambda})$ is the worst-case conditional smooth min-entropy and can be interpreted as the amount of bits that a strong extractor can output from the raw bit sequence generated by the experiment (see Refs. 22 and 24 for more details).

For the implementation, we use the Binary Phase Shift-Keying (BPSK) scheme where the source prepares two coherent states with the same average photon number and a π phase difference, i.e., $|\alpha\rangle$ and $|-\alpha\rangle$. By choosing either state with probability 1/2, the average energy bound ω must be greater than $|\alpha|^2$. This choice is motivated by the fact that implementing such a source is easy and can allow for high repetition rates. Considering all possible measurement strategies, we need to determine the one that can discriminate the two produced state in the best way. Figure 1 shows the comparison of different strategies. The best strategy is given by the min-error discrimination measurement that allows to achieve the Helstrom limit. However, a perfect homodyne measurement, in which the two states are distinguished with respect to the sign of their quadrature, does not fall far behind, not even when noise is taken into consideration. This gives a practical solution even for the measurement itself.

This scheme is implemented as shown in Fig. 2. We generate the two desired states of light by modulating a coherent state with a phase modulator, and we implement a homodyne measurement in order to project the states into the chosen quadrature. The setup is fiber-based and is composed of a continuous-wave (CW) laser at a telecommunication wavelength (1550 nm), which injects light into a balanced Mach–Zehnder interferometer (MZI). The input port of the MZI consists of an optical system of polarization controller (PC) and fiber polarization beam splitter (PBS) to adjust the power going into each arm of the MZI. As it is shown in Fig. 2, the lower arm of the interferometer corresponds to the local oscillator of the homodyne measurement and the upper MZI arm to the preparation stage of the experiment. In this part, the states are modulated by the phase modulator, which is controlled by a binary input sent by a Field Programmable Gate Array (FPGA, Xilinx Virtex 6) at a repetition rate of 1.25 Gbits/s. The input signal is generated by a pseudo-random number generator with periodicity longer than the acquisition block size. (This is to avoid possible correlations with the measurement. True randomness is not needed since it is assumed that this sequence is known by the adversary.[24]) With the laser being continuous, the phase modulation window of 800 ps defines the input states. The states

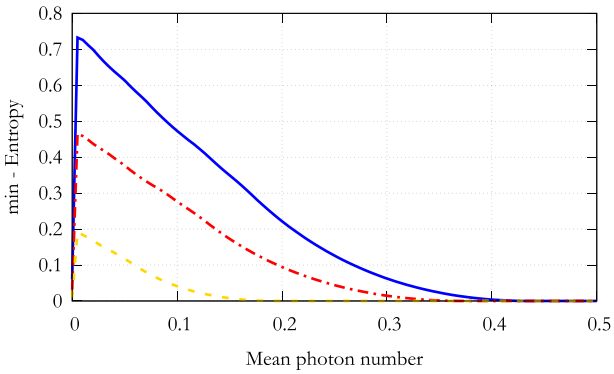

FIG. 1. Extractable randomness per bit with respect to the average photon number of the input state, using the BPSK encoding scheme. The continuous line (blue) corresponds to a measurement strategy that reaches the Helstrom limit, the dashed-dotted line (red) to a perfect homodyne detection scheme, and the dashed line (yellow) to an homodyne detection with added white noise [$p_{noise} = 0.39$ see Eq. (6)].

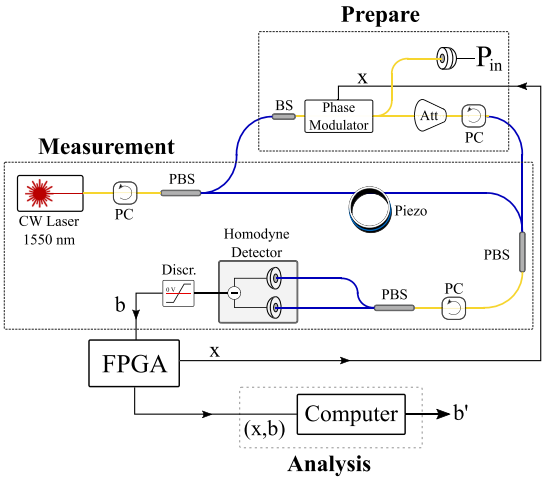

FIG. 2. The experimental setup corresponds to a CW laser at 1550 nm, which injects light into a MZI. The input port is a PBS in order to modulate the amount of energy going into each arm of the interferometer. The top arm, going into the prepare stage, corresponds to the state preparation where the light is modulated by a phase modulator and the average energy is measured by a system of BS, attenuator, and linear detector. The bottom arm corresponds to the local oscillator of the homodyne measurement, and the fiber is wrapped around a piezo in order to stabilize the interferometer phase. The measurement is carried out with two balanced linear detectors.

are then attenuated to the energy value required by the energy assumption taken in the protocol. A set of calibrated 50/50 beam splitter, linear photo-diode, and attenuator allows us to monitor, in real time, the power after the attenuator. In order to find the upper bound on the mean photon number of our signal ($\bar{\mu}$), the following formula is used:

$$\bar{\mu} = \frac{P_{in} \cdot att \cdot \Delta t}{h\nu_{min}}, \tag{5}$$

where P_{in} is the power measured with the photo-diode, att is the calibrated attenuation, Δt is the modulation duration, h is the Planck constant, and ν_{min} is the lower bound on the frequency of the laser. We would like to stress that these three components (beam splitter, attenuator, and linear detector) are the only part of the experiment that must be trusted and characterized. Indeed, the main assumption of the scheme can be defined as the energy of the states (mean photon number) going out of the preparation stage.

The prepared states are then recombined with the LO by a set of two PBSs and PC (that serve the purpose of a variable beam splitter) in order to balance the power transmitted to the balanced photo-diode (Thorlabs PDB480C-AC). The analog signal coming from the homodyne detector is discriminated between positive and negatives values, which corresponds to the discrimination between positive and negative quadrature values. The binary output b, generated in this way, is then collected by the FPGA. Electrical delay lines are used in order to synchronize the input (x) and output (b). Moreover the discrimination is triggered by a clock signal sent by the FPGA and controlled in such a way that the discrimination window is optimized to obtain the best discrimination. To stabilize the phase on the interferometer, a digital optimization is set up over the correlation measured. A feedback signal is sent to a piezo-electric cylinder over which 2 m of fiber is wrapped. The stability of the interferometer is then achieved without the need of an additional source of light. The passive stability of the setup could be achieved by shortening the arms of the interferometer (currently of 6 m each) or by integrating the scheme in a photonic circuit.

Input and output are collected by the FPGA and forwarded to an off-line computer that evaluates the conditional probabilities $p(b|x)$ and that calculates the extraction rate certified by the semi-device independent protocol.

First, we measure the dependence of the maximum extractable randomness with respect to the chosen energy bound (expressed in the mean photon number of the prepared states). As shown in Fig. 3, the amount of extractable randomness has a maximum around 10^{-3} to 10^{-2} photon per states. This value is the result of a trade-off between a small enough energy in order to obtain a uniform probability distribution but high enough energy in order to be able to distinguish between the two input values without being dominated by electrical noise.

In order to estimate the amount of unwanted "classical" or not trusted noise in the experiment, a simple model is used to approximate the experimentally measured data points. The conditional probabilities are modeled as follows:

$$p(b|x) = (1 - p_{noise})p^{id}(b|x) + p_{noise}\frac{1}{2}, \tag{6}$$

where $p^{id}(b|x)$ corresponds to the ideal homodyne measurement with no added noise and perfect state preparation given by the following formulas:

$$\begin{aligned} p^{id}(b|x = b) &= \frac{1}{2}\left(1 + erf\left(\sqrt{2}|\alpha|\right)\right), \\ p^{id}(b|x \neq b) &= \frac{1}{2}\left(1 - erf\left(\sqrt{2}|\alpha|\right)\right). \end{aligned} \tag{7}$$

This model corresponds to a system that works as expected in an ideal way with probability $(1 - p_{noise})$, and with probability p_{noise}, it will

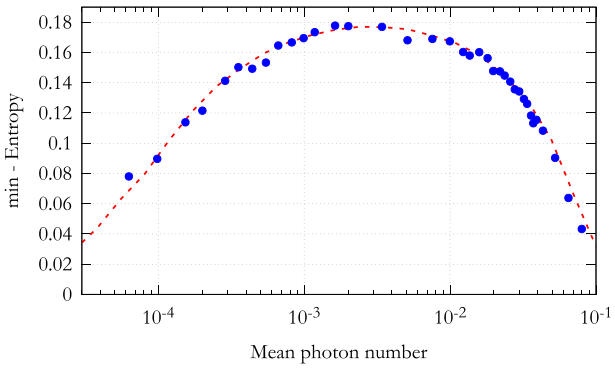

FIG. 3. Amount of entropy per bits per generated state vs the average mean photon number. The average energy bound is chosen equal to the mean photon number to obtain the maximum achievable entropy. The dots correspond to the experimental measured values, and the dashed line corresponds to the theoretical model used to simulate the device behavior.

output a values completely uncorrelated with the input. This probability represents all possible imperfection of the experiment, like state preparation flaws, electrical noise in the detection scheme, etc. The main source of noise is given by the electrical intrinsic Gaussian noise of the homodyne detection scheme, which deteriorates the distinguishability of states with a low mean photon number (this is the main reason why in Fig. 1, the entropy decreases dramatically for mean photon numbers close to zero). All these contributions add up to an estimated value of $p_{noise} = 0.39$. However, the only purpose of this value for our protocol is to be a figure of merit for the experiment since it never appears as a parameter in the security proof. This illustrates the advantage of the self-testing approach that with the sole analysis of the input and output statistics plus few reasonable assumptions, it is possible to certify the amount of entropy generated without the complete characterization of the device. In a completely device dependent scenario, the probability p_{noise} should be perfectly characterized and calculated a priory and then monitored during the experiment in order to certify the genuine randomness of the output.

Once the optimal energy bound has been estimated, we carry out a longer measurement of 1 h in order to test the stability and resilience of the experiment. Following our semi-DI protocol, a threshold h is chosen, which corresponds to the asymptotic, extractable entropy. Each second, the input/output frequencies are estimated, and the assumption is verified. This leads to a post-processing block size of 1.25×10^9 needed to optimize the finite-size effects of Eq. (4). Unfortunately, the large block size and the high repetition rate do not allow for real time extraction with our FPGA. As it can be seen from Fig. 4, the measured power was never higher than the fixed threshold. The operating mean photon number chosen is around 5×10^{-3} by optimizing the entropy per bit and by verifying that the correlation generated was sufficient for the feedback stabilization loop to work. Figure 5 shows the entropy as a function of the time. For each point, it is verified that the entropy generated is higher than the previously fixed threshold. If this condition is fulfilled, the extraction ratio is given by Eq. (4); otherwise, the block is rejected. The choice of the threshold value comes with a trade-off between the amount of extractable bits per state generated and the amount of succeeded rounds in the experiment. In order to maximize the average rate of certified random bits throughout the whole experiment, a threshold value of $h = 0.12$ has been chosen, which has led to a probability of succeeded rounds of 97%. These two values allow the experiment to certify a repetition rate of genuine quantum bits of 145.5 MHz.

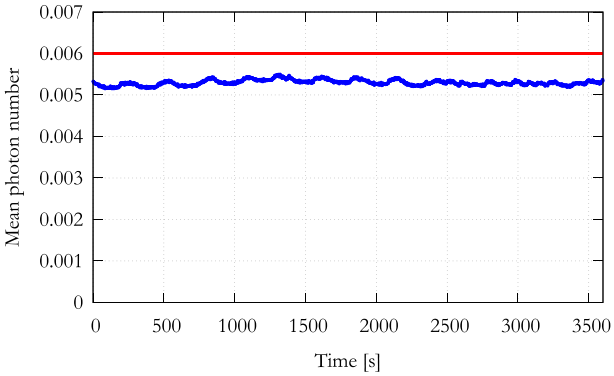

FIG. 4. Measured mean photon number vs time. The blue line (one measured point per second) corresponds to the verified mean photon number measured in the experiment. The red straight line is the energy bound. As it can be seen, the assumption of our experiment is never violated.

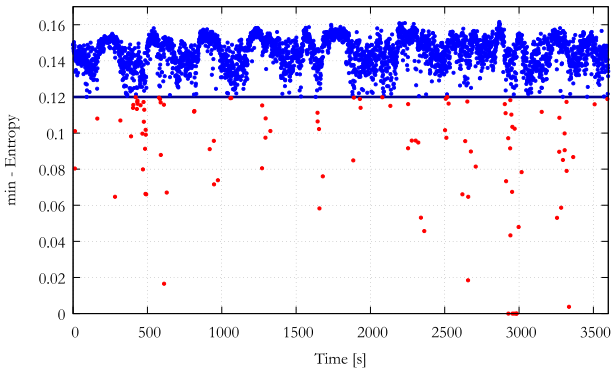

FIG. 5. Amount of entropy per bits per generated state vs time. Each point in the figure corresponds to a 1 s measurement. The solid line corresponds to the threshold h, and each point above (blue) is a succeeded measurement, while each point below this line (red) corresponds to a failure.

The QRNG presented in this work is a simple yet performant implementation of the semi-DI protocol based on energy bounds. We achieved a random bit rate of 145.5 MHz for a measurement during 1 h. The advantage of the system relies not only on its high speed but also on the straightforward implementation, which is highly compatible with a possible integrated optics implementation.

See the supplementary material for the correlations and noise analysis of the system.

We would like to thank Nicolas Brunner, Thomas van Himbeeck, and Stefano Pironio for all the helpful discussions. We acknowledge the support of European Union's Horizon 2020 program under the Marie Skłodowska-Curie project QCALL (No. GA 675662), the Swiss National Science Foundation (Bridge Project No. 40B2-0_176517), and the EU Quantum Flagship project QRANGE.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1]A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Opt. **47**, 595–598 (2000).
[2]T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**, 1675–1680 (2000).
[3]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. Photonics **4**, 711–715 (2010).
[4]B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**, 312–314 (2010).

[5]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**, 1645–1654 (2014).
[6]B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," Phys. Rev. X **4**, 031056 (2014).
[7]R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," Ph.D. thesis (University of Cambridge, 2009).
[8]S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by bell's theorem," Nature **464**, 1021–1024 (2010).
[9]R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," J. Phys. A **44**, 095305 (2011).
[10]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).
[11]G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle," Phys. Rev. A **90**, 052327 (2014).
[12]T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, "Self-testing quantum random number generator," Phys. Rev. Lett. **114**, 150501 (2015).
[13]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 (2014).
[14]Z. Cao, H. Zhou, and X. Ma, "Loss-tolerant measurement-device-independent quantum random number generation," New J. Phys. **17**, 125011 (2015).
[15]D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," Phys. Rev. Lett. **118**, 060503 (2017).
[16]Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," Phys. Rev. X **6**, 011020 (2016).
[17]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**, 1266–1269 (2016).
[18]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).
[19]T. Gehring, C. Lupo, A. Kordts, D. Nikolic, N. Jain, T. Pedersen, S. Pirandola, and U. Andersen, "8 gbit/s real-time quantum random number generator with non-iid samples," arXiv:1812.05377 (2018).
[20]T. Michel, J. Haw, D. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. Lam, and S. Assad, "Real-time source independent quantum random number generator with squeezed states," arXiv:1903.01071 (2019).
[21]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).
[22]D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, "Self-testing quantum random-number generator based on an energy bound," Phys. Rev. A **100**, 062338 (2019).
[23]M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Semi-device-independent heterodyne-based quantum random number generator," arXiv:2004.08344 (2020).
[24]T. Van Himbeeck and S. Pironio, arXiv:1905.09117 (2019).