


Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator

Marco Avesani^{1,*}, Hamid Tebyanian¹, Paolo Villoresi¹, and Giuseppe Vallone^{1,2}

¹*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italia*

²*Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, Padova 35131, Italy*

 (Received 5 May 2020; revised 11 August 2020; accepted 25 January 2021; published 11 March 2021)

Randomness is a fundamental feature of quantum mechanics, which is an invaluable resource for both classical and quantum technologies. Practical quantum random-number generators (QRNGs) usually need to trust their devices, but their security can be jeopardized in the case of imperfections or malicious external actions. In this work, we present a robust implementation of a semi-device-independent QRNG that guarantees both security and fast generation rates. The system works in a prepare-and-measure scenario, where measurement and source are uncharacterized, but a bound on the energy of the prepared states is assumed. Our implementation exploits heterodyne detection, which offers increased generation rate and improved long-term stability compared to alternative measurement strategies. In particular, due to the tomographic properties of heterodyne measurement, we can compensate for fast phase fluctuations via postprocessing, avoiding complex active phase-stabilization systems. As a result, our scheme combines high security and speed with a simple setup featuring only commercial-off-the-shelf components, making it an attractive solution in many practical scenarios.

DOI: [10.1103/PhysRevApplied.15.034034](https://doi.org/10.1103/PhysRevApplied.15.034034)

I. INTRODUCTION

Many quantum random-number generators (QRNGs) trust the performance of their apparatus, modeling their components as perfect devices [1–3]. Although quantum mechanics provides assurance about the random behavior of a quantum process, the practical implementation may be vulnerable to imperfections. Indeed, the trust on the devices may allow information leakage, if the devices are correlated with the environment under the control of an adversary.

Therefore, the security of a practical QRNG is linked to the number of required assumptions, where fewer assumptions imply better security [4]. From this point of view, device-independent (DI) protocols [4,5] offer the highest level of security. In this scenario, the instruments are treated as black boxes, and nothing is assumed about their inner working principles. However, all DI protocols require the loophole-free violation of a Bell inequality, which is extremely demanding from an experimental point of view. Moreover, despite the advancements presented in recent demonstrations [6–11], the generation rate of DI protocols is orders of magnitude lower than what is required by practical applications.

Alternative scenarios are required to meet the needs of speed and security. In order to achieve a better trade-off

between generation rate and security a different approach, called semi-DI, has been recently proposed [12]. The semi-DI approach, by including some assumptions on the working principle of the devices without requiring their full characterization, offers a solution to overcome experimental complexity and low-generation-rate issues of DI protocols. Few different semi-DI protocols have been proposed that require a trusted source [13,14] or measurement [15–18]. Other protocols do not require to trust specific components of the setup but they make assumptions on the overlap [19] or the energy [20–22] of the emitted states [11] or assumptions on the dimension of the Hilbert space [23,24].

However, the performances offered by semi-DI protocols are dramatically higher than the DI ones, matching, and sometimes surpassing, the generation rates of commercial QRNGs [12]. In particular, continuous-variable (CV) implementations are an attractive solution in this context with respect to discrete-variable (DV) ones since they can exploit a larger Hilbert space, fast detectors, and they require only standard commercial-off-the-shelf (COTS) components typical of the telecom market. As a result, they feature higher generation rates with simpler optical setups.

In the present work, we introduce a semi-DI QRNG based on heterodyne detection that assumes an upper bound on the energy of the emitted states. Our implementation ensures an excellent generation rate on a par

*marco.avesani@unipd.it

with commercial solutions and improved security. Additionally, this scheme is realized with an easy-to-implement all-fiber setup. The scheme is based on a prepare-and-measure scenario; therefore, no entanglement is necessary. The assumption required for the execution of the protocol is related to the energy of the states emitted from the source, which is monitored in real-time during the execution of the protocol. We should emphasize that the state’s preparation is independent and identically distributed (IID) in every round. No IID assumptions are required on the measurement station.

The tomographic capabilities of the heterodyne detection allow us to sample the full phase space, enabling us to track and compensate fluctuations and drifts of the signal phase via software in postprocessing, without any active stabilization system. This feature makes our implementation more practical with respect to other alternative measurement strategies, where active real-time phase stabilization is required.

The amount of secure and certified randomness is obtained by numerically bounding the quantum conditional min-entropy via semidefinite programming (SDP), with an approach similar to the one described in Ref. [19]: we note that the energy assumption is required for every round of the protocol. Compared to Ref. [19] our solution is based on a bound on the energy of the prepared states, rather than the overlap, since the first can be easily monitored experimentally. Moreover, it has a substantially higher generation rate, due to the exploitation of high-speed balanced detectors used in CV measurements rather than slow single-photon detectors.

We note that a similar approach, based on a different measurement apparatus, has been proposed independently in Ref. [25].

II. THE PROTOCOL

A. Semi-DI QRNG based on overlap bound

The general scheme of our QRNG is illustrated in Fig. 1. Please check the order and appearance for all parts of all figures. Also note that the figure labels have been adjusted so that the roman and italic characters match the main text. Please check and confirm that no errors have been introduced.

In the first step, the preparation box, after taking a binary input $x \in \{0, 1\}$, emits a quantum state ρ_x , which is sent to the measurement box that performs a measurement with binary outputs $b \in \{0, 1\}$. As in previous semi-DI QRNG [20–22], we assume here that who realized the device has full knowledge of the state preparation and measurement, and the full system has only classical correlations with the environment. We note that this approach is particularly relevant in practical applications. Moreover, the IID hypothesis is considered.

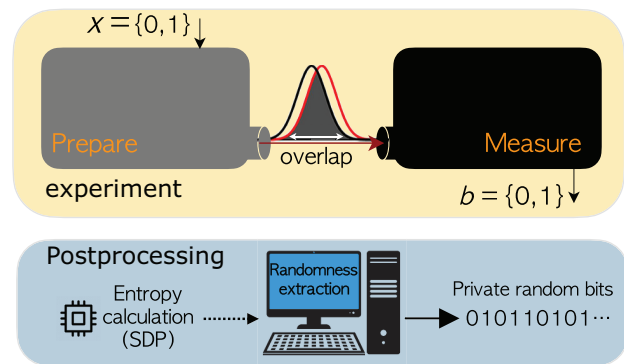


FIG. 1. General idea of the semi-DI QRNG protocol.

It is worth noticing that the preparation and measurement devices are considered as uncharacterized with a single assumption: the energy of the prepared states is upper bounded, as expressed by the following relation:

$$\langle \hat{n} \rangle_{\rho_x} \leq \mu, \quad (1)$$

where \hat{n} is the photon-number operator. As obtained in Ref. [20], when $\mu \leq 0.5$, the upper bound on the energy implies a lower bound on the overlap between the two states. From the bound on the overlap, it is possible to follow the approach of Ref. [19] to obtain the amount of certified private randomness. Indeed, from the obtained conditional probability outcomes $p(b|x)$ it is possible to compute the conditional min-entropy by a SDP, which estimates how much private random bits are available out of generated bit strings. A randomness extractor [26], based on the evaluation on the conditional min-entropy H_{\min} , reduces the string of generated raw bits to a shorter one, which is private and genuinely random.

We now briefly review how the min-entropy can be estimated. With complete generality, any preparation device will generate the pure quantum state $|\psi_x^\lambda\rangle$ with probability $p(\lambda)$ for each input x . We stress that the preparation of mixed states can always be achieved by a convex combination of pure states. As written above, we assume that the full system has no quantum correlation with the environment. The constraint, Eq. (1), implies a lower bound on the state overlap, namely [20]

$$|\langle \psi_0^\lambda | \psi_1^{\lambda'} \rangle| \geq 1 - 2\mu. \quad (2)$$

In the following, we consider only the case $\mu \leq 0.5$, where the above bound is not trivial. On the other hand, the measurement device can be modeled as a binary outcome positive-operator-valued measurement (POVM) $\{\Pi_b^\lambda\}$ with $\Pi_0^\lambda + \Pi_1^\lambda = \mathbb{1}$. The variable λ represents classical shared randomness between preparation and measurement devices, and corresponds to the “strategy” of an adversary that builds the devices is pursuing in order to

guess the output bits b . Each strategy λ is associated with a corresponding probability $p(\lambda)$. Similarly to other semi-DI and DI protocols, we assume that the input x is independent from λ [22]. The states $|\psi_x^\lambda\rangle$ and the POVM Π_b^λ could be arbitrary, but they are constrained by Eq. (2) and by the measured conditional probabilities, namely

$$p(b|x) = \sum_{\lambda} p(\lambda) \langle \psi_x^\lambda | \Pi_b^\lambda | \psi_x^\lambda \rangle. \quad (3)$$

Given the measured probabilities $p(b|x)$ and the assumed bound on the energy μ , the guessing probability of an adversary P_g averaged over the preparation probability p_x is given by the following relation:

$$P_g = \sum_{x,\lambda} p_x p(\lambda) \max \{ \langle \psi_x^\lambda | \Pi_0^\lambda | \psi_x^\lambda \rangle, \langle \psi_x^\lambda | \Pi_1^\lambda | \psi_x^\lambda \rangle \}. \quad (4)$$

From the above equation, P_g is the maximum guessing probability of the outcome averaged over x and λ . The fraction of private random bits that can be extracted by the raw output sequence is given by the min-entropy

$$H_{\min} = -\log_2 \left[\max_{\{|\psi_x^\lambda\rangle, \Pi_b^\lambda, p(\lambda)\}} P_g \right], \quad (5)$$

where the maximization is performed over all possible preparation and measurement strategies that satisfy the constraints given in Eqs. (2) and (3). The upper bound on P_g can be efficiently solved through semidefinite programming, as reported in Ref. [19] and reviewed in Appendix A. In particular, we employ the dual formulation of the SDP, since it provides few advantages with respect to the primal. First, since it involves a maximization problem it always returns a lower bound on the min-entropy, thus never overestimating it. Secondly, it is less computational demanding. Indeed, since the objective function is linear in $p(b|x)$, after an optimal solution has been found, a new (nontight) lower bound with different $p(b|x)$ can be easily evaluated, without running the optimization again. Finally, with the dual formulation finite-size effects due to the limited statistics can be easily taken into account.

We point out that it is also possible to derive a different bound on the min-entropy by constraining the energy of the emitted states, using the framework described in Refs. [20, 22]. This scenario has been experimentally implemented using single-photon detectors in Ref. [21] and homodyne measurement in a recent parallel work.

The number of random bits that can be generated, expressed by Eq. (5), is guaranteed by the laws of quantum mechanics. In order to intuitively explain why randomness can be generated, it is possible to consider the measurement as a device that should discriminate between the two

input states, with $p(1|0)$ and $p(0|1)$ the ‘‘error probabilities.’’ When the energy is upper bounded and thus the overlap of two states is lower bounded, there is no binary outcome measurement able to perfectly distinguish them, making the probabilities $p(1|0)$ and $p(0|1)$ both vanishing. Indeed, the minimal error chance $p(b \neq x)$ is bounded by the state overlap, namely

$$p(b \neq x) = \frac{1}{2} [p(1|0) + p(0|1)] \geq \frac{1}{2} - \sqrt{\mu - \mu^2}. \quad (6)$$

In Appendix C a detailed derivation of Eq. (6) is presented. Thus a nonvanishing overlap, which happens for $\mu \leq 0.5$, implies a nonvanishing error rate that can be employed as a randomness source. We stress here that in this protocol no assumption is made on the performance of the apparatus; therefore, possible noise due to unavoidable technical imperfections are already included in the above analysis.

Notably, neither the selection of the states nor the measurements are known, and randomness certification is only based on the input-output correlations $p(b|x)$, and the upper bound μ on the energy.

B. Implementation with heterodyne

In our experimental implementation, as displayed in Fig. 2(A), the source generates the coherent states $|\psi_0\rangle = |\alpha\rangle$ and $|\psi_1\rangle = |-\alpha\rangle$, with $|\pm\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} [(\pm\sqrt{\mu}e^{i\phi})^n / \sqrt{n!}] |n\rangle$, where $\alpha = \sqrt{\mu}e^{i\phi}$, μ is the mean photon number and ϕ is the relative phase between the signal and LO. Depending on the input x , the phase of a coherent state (produced by a cw laser) is modulated such that the output phase for $x = 0$ is ϕ , while for $x = 1$ it is $\pi + \phi$. We note that μ is precisely the upper bound, Eq. (1), on the state energy.

We underline that the input x must be independent of the devices and in particular, it should be uncorrelated with λ . In our experiment, x will be generated from a classical RNG (e.g., pseudo RNG). The receiver is represented by a heterodyne detector that can be modeled by the POVM $\Pi_\beta = 1/\pi |\beta\rangle\langle\beta|$. The transmitted state is indeed measured by interfering it with a local oscillator on a 90° hybrid, followed by balanced detectors in the output ports.

Considering that the heterodyne detection provides information on both field quadratures X and P , any measurement outcome can be represented by a complex number β and associated to a point in the (X, P) phase space. These points can then be gathered in two sets, corresponding to $x = 0$ and $x = 1$, respectively, as shown in Fig. 2(C). Next, we determine the centroids C_0 and C_1 of each of these two sets. The axis of the segment C_0C_1 divides the phase space into two regions: each heterodyne measurement β is associated to the $b = 0$ or $b = 1$ output if β belongs to the region containing C_0 or C_1 , respectively. From the heterodyne detection POVM Π_β , it is easy to

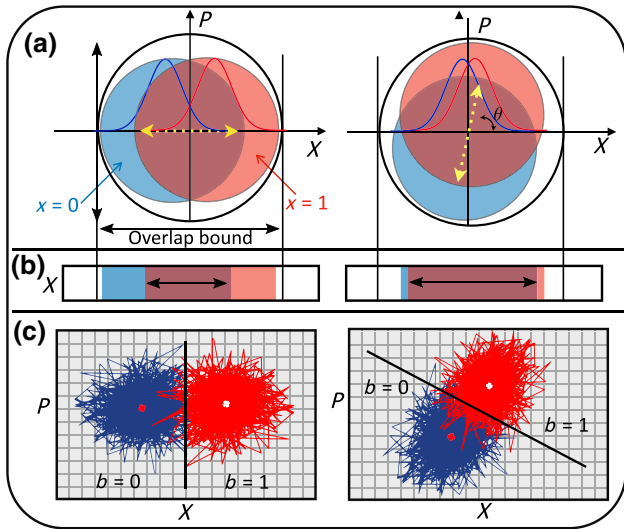


FIG. 2. (a) For $x = 0$ and $x = 1$, the blue and red states are prepared, respectively. In the left panel states with phase $\phi = 0$ are prepared; on the right panel, the prepared states have phase $\phi = \theta$. (b) homodyne detection along X quadrature. When $\theta \neq 0$ the two states become less distinguishable. (c) Heterodyne measurement: for a binary outcome, if the received state is located on the left side with respect to the linear classifier then $b = 0$, otherwise $b = 1$. The state distinguishability does not vary with θ .

compute the theoretical output probabilities as

$$\begin{aligned} p(0|0) = p(1|1) &= \frac{1}{2} [1 + \text{erf}(\sqrt{\eta}|\alpha|)], \\ p(0|1) = p(1|0) &= \frac{1}{2} [1 - \text{erf}(\sqrt{\eta}|\alpha|)], \end{aligned} \quad (7)$$

where η is the overall detection efficiency and $\text{erf}(x) = (2/\sqrt{\pi}) \int_0^x e^{-t^2} dt$ the error function.

Given these probabilities, we can use the SDP to calculate the expected performances of an honest implementation with ideal devices, as a function of α . These expectations are plotted, together with the experimental results, in Fig. 5.

The main advantage of heterodyne detection over alternative measurement strategies is given by its intrinsic robustness to phase drifts. In practical implementations, the relative phase ϕ between the signal and the LO, rapidly drifts over time, due to thermal or mechanical fluctuations. As a result, the measured states rapidly rotate around the center of the phase space [see Fig. 2(A)]. For measurements that are sensitive only to one quadrature, such as homodyne detection, any deviation from the condition $\phi = 0, \pi$ reduces the distinguishability between the two states $|\psi_0\rangle, |\psi_1\rangle$ reducing the extractable randomness [see Fig. 2(B)]. In the extreme case where $\phi = \pi/2, 3\pi/2$, the two states are indistinguishable meaning that no randomness can be certified at all. Thus, for these systems

it is mandatory to implement a fast and active phase-stabilization system, running in real time, that is able to keep the relative phase ϕ fixed at the optimal point. The active stabilization is not trivial to realize and substantially increases the experimental complexity of the system. In contrast, heterodyne detection, being tomographically complete, is able to sample the full phase space and a drift of the relative phase ϕ does not affect the distinguishability of the states $|\psi_0\rangle, |\psi_1\rangle$ and it is equivalent to a rotation of the reference system [see Fig. 2(C)]. So, if the sampling rate of the system is sufficiently fast with respect to the time scale of the fluctuations, the relative phase ϕ can be tracked *a posteriori* via software. With this solution it is possible to overcome much faster drifts with drastically simpler experimental setups. In Appendix B, we describe with more details the differences between heterodyne- and homodyne-detection schemes.

III. EXPERIMENT

A. The optical and electronic part

The experimental setup that implements the scheme represented in Fig. 1 is drawn in Fig. 3. A continuous-mode laser generates a coherent state at 1550 nm. A 99 : 1 beam splitter (BS), is used to split the light into two branches, local oscillator (LO) and signal. The LO is transferred to an automatic variable optical attenuator (VOA) and then is divided again with a 90 : 10 BS. 10% of the light is sent to a power meter (PM) for calibrating the detectors. It should be noted that there is no assumption on the measurement device, and this calibration is done in order to monitor the correct working of the detectors, but is not strictly required and it does not influence the security of the protocol. The remaining 90% of the light is sent to a fiber polarization controller (PC) and then to the LO port of the 90° optical hybrid. The optical signal used to prepare the states $|\psi_x\rangle$, is transmitted to a PC followed by a fiber LiNbO₃ phase modulator (MPZ-LN-20 by iXblue) with a bandwidth of 20 GHz. A pseudo-random binary sequence (PRBS) x is generated in real time by a field-programmable gate array (FPGA) with a rate of 1.25 GHz. The output of the FPGA is amplified with a rf amplifier (iXblue) and then used to drive the phase modulators, adding 0 or π phase shift to the light inside the phase modulator, thus preparing the states $|\psi_0\rangle = |\alpha\rangle$ or $|\psi_1\rangle = |-\alpha\rangle$, respectively.

The modulated light is then conveyed to a mechanical VOA, used to change the magnitude of α before being split by a 90 : 10 BS. 90% of the light is sent to a PM (Thorlabs S154C with a measurement uncertainty of $\pm 5\%$), while 10% is sent to a fixed optical attenuator (OA). With this configuration, after calibrating the attenuation entered by the OA, we can have a one-to-one mapping between the power read on the PM and the optical power sent to the measurement part. For the estimation of the mean photon number μ we consider a time slot of 0.8 ns, determined by

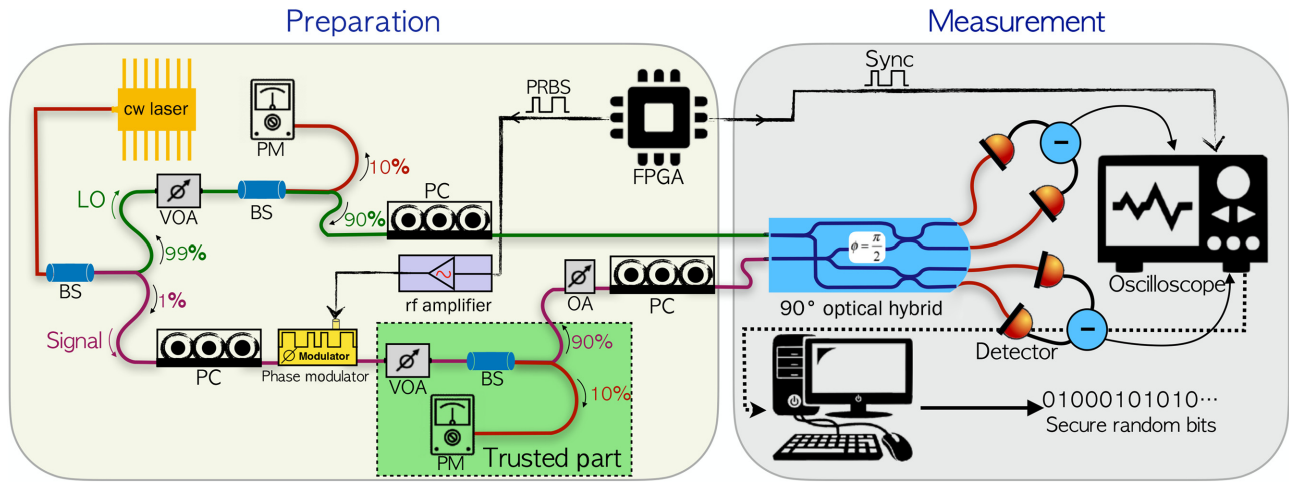


FIG. 3. Experimental setup, which consists of two sections, preparation and measurement. A coherent state is generated by a cw laser and sent to the interferometer. One arm, with 1% of the light (purple path), is employed to prepare the signal, and the other one with 99% of the light (green route), is the local oscillator. In each path, 10% of light is transmitted to PM for monitoring the power. The two paths are combined on the 90° optical hybrid, which is followed by a pair of balanced detectors implementing the heterodyne measurement. An FPGA controls the phase modulator and the synchronization with the oscilloscope.

the system repetition rate. Before entering the signal port of the 90° optical hybrid, the polarization of the optical signal is adjusted with a PC.

After the optical hybrid, the two pairs of optical signals relative to the two quadratures are sent to two InGaS-balanced photoreceivers (PDB480C-AC) with a bandwidth of 1.6 GHz. At the receiver side, the rf signal generated by the balanced photodetectors and a synchronization signal coming from the FPGA are digitized by a Tektronix DPO70004 Oscilloscope with 4 GHz of analog bandwidth, at a sampling rate of 12.5 Gps and 8 bit of resolution. We average every ten samples in order to obtain signals with the same repetition rate of the source. This oversampling procedure is used to better reconstruct the signal from the balanced detectors, that shows a finite rise time and electronic ringing, due to the high repetition rate of the system. The oscilloscope works in burst mode, saving the acquired data in its internal storage memory. The postprocessing of the data is done offline.

B. Postprocessing and finite-size analysis

Since the signal and LO travel in different fibers, and no active phase stabilization is present, the relative phase between the signal and the LO is subjected to drifts over time. This means the two Gaussian distributions relative to $|\alpha\rangle$ and $|\alpha\rangle$ will start to rotate around the center of the phase space, keeping fixed their overlap and their distance from the center. In order to compensate for these drifts, we perform a software phase tracking and compensation during the postprocessing of the data. This procedure allows for a simpler experimental setup and is able to compensate

fast phase fluctuations. In particular, during the postprocessing we divide the acquired signal into “chunks” of $n = 1000$ samples. For each chunk, we calculate the centroids of the measurement distribution in the phase space for each input state. Choosing $n = 1000$ is a good trade-off between the accuracy of centroid evaluation and phase stability. Indeed, each chunk lasts for less than $1 \mu\text{s}$ while phase fluctuations are at the ms scale.

In this way, it is possible to determine the relative phase ϕ between the signal and the LO. In Fig. 4 the measured phase ϕ is plotted as a function of time. Finally, we use the estimated ϕ to apply a linear classifier and assign an outcome b to each measurement in the considered “chunk.”

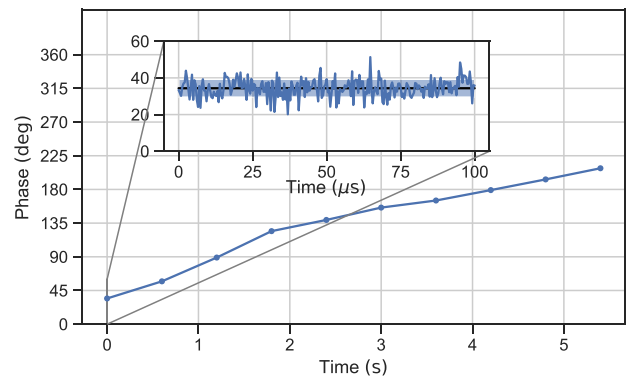


FIG. 4. Relative phase ϕ between signal and LO as a function of time. The system shows a drift of about $32^\circ/\text{s}$, while for time scales comparable with the chunk size no drift is observed (see inset). The shaded area in the inset shows the $\pm 1\sigma$ confidence interval, demonstrating that fast fluctuations are due to statistical noise.

After performing the procedure for all the chunks, then the experimental conditional probabilities $p(b|x)$ are estimated as $\tilde{p}(b|x) = n_{b,x}/n_x$, where $n_{b,x}$ are the number of events for an output b conditioned on an input x and n_x is the total number of transmitted states x . The finite-size effects due to the limited statistics used to estimate the $\tilde{p}(b|x)$ can be included in the min-entropy bounds, as described in Ref. [19]. In particular, we can use the Chernoff-Hoeffding inequality [27] to build a confidence interval for the experimental probabilities $[\tilde{p}(b|x) - \delta(\epsilon, n_x), \tilde{p}(b|x) + \Delta(\epsilon, n_x)]$, where ϵ is the security parameter and

$$\Delta(\epsilon, n_x) = \sqrt{\frac{-\log_2(\epsilon)}{2n_x}}. \quad (8)$$

In order to obtain a reliable lower bound on the min-entropy, we include the correction into the objective function of the dual SDP, such as

$$P_g \geq \min \left\{ - \sum_{b,x} [v_{bx}p(b|x) + |v_{bx}|\Delta(\epsilon, n)] \right\}, \quad (9)$$

where $\Delta(\epsilon, n)$ is the finite-size correction, and v_{bx} is the dual SDP objectives' function's coefficient (more details in Appendix A). Since the bound given by Eq. (9), even if not tight, is estimated over the worst-case single-shot scenario it is also valid for the finite-size regime. Indeed, the smooth conditional min-entropy for n rounds can be bounded in terms of the conditional min-entropy of a single round as shown in Ref. [28] (Lemma 3.2.6): $H_{\min}^\epsilon(\rho_{XE}^{\otimes n}|E^n) \geq nH_{\min}^{\epsilon/n}(\rho_{XE}|E) \geq nH_{\min}(\rho_{XE}|E)$, where we use the IID hypothesis in the first expression. Here $\rho_{XE} = \sum_x P_x |x\rangle\langle x| \otimes \rho_E^x$ represents the classical-quantum state of the classical random variable X and the quantum state ρ_E^x of the adversary, while E represents the (quantum) side information. Since the bound is valid for general quantum-side information it is also valid in our particular case where only classical side information is assumed.

Finally, genuine random bits are extracted from the raw bit string using a strong randomness extractor based on two-universal hashing functions implemented with Toeplitz matrices [26]. The value of the security parameter ϵ_{RE} , associated to the randomness extractor's failure probability, which is given by the leftover hashing lemma, is chosen to be $\epsilon_{RE} \leq 10^{-10}$. Given the composability of the protocol, the final security parameter ϵ_S can be written as $\epsilon_S = \epsilon_{RE} + N_{PE}\epsilon_{PE}$, where N_{PE} is the number of estimated parameters, ϵ_{PE} is the error associated to the finite-key corrections given by $\Delta(\epsilon_{PE}, n)$ to the min-entropy H_{\min} . In our case the final soundness error is set to $\epsilon_S = 5 \times 10^{-10}$, a value compatible with previous proposals.

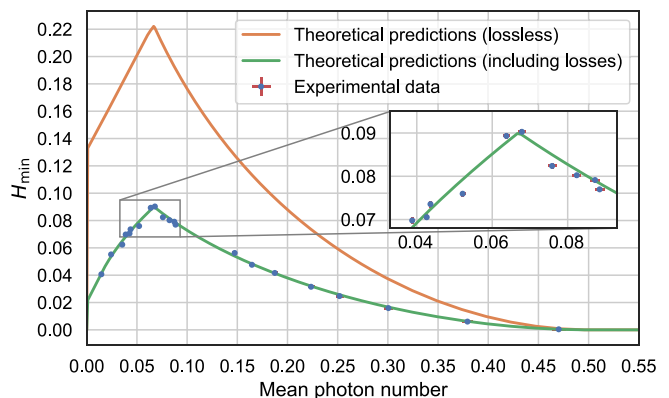


FIG. 5. Conditional min-entropy as a function of the mean photon number. The orange curve is the numerical predictions obtained by SDP. The green curve shows the numerical results of SDP when inefficiencies are considered and shows good agreement with experimental data (blue points).

In this work the postprocessing and the randomness extraction are performed offline on a PC. However, the methods and the implementation described here can be used to generate secure random numbers in real time. In particular, the postprocessing procedure is similar to the phase tracking and carrier recovery of classical coherent communication, which is usually efficiently implemented on FPGA or DSP [29]. Also the randomness extraction can be efficiently implemented on FPGA with high throughput, as shown in Ref. [30].

IV. RESULTS

We perform the experiment for different values of μ . In each run of the protocol the mean photon number is estimated by the optical power captured via the calibrated PM in the signal branch. Given the mean photon number μ together with the measured probabilities $p(b|x)$, the SDP allows evaluation of the conditional min-entropy.

The experimentally estimated min-entropy without finite-size corrections and the corresponding theoretical values are displayed in Fig. 5. For ideal detectors and lossless transmission (blue curve in Fig. 5), the predicted maximum of $H_{\min}(b|x)$ is 0.22 bits per measurement, while experimentally, we achieve 0.09 bits per measurement. This result can be explained by including in the model losses and detector's inefficiency. In any practical implementation all these effects are inevitable and contribute to worse discrimination of the incoming states, decreasing the number of secure random bits with respect to the ideal detector case.

In order to understand what is the significance of these nonidealities, we fit the experimental probabilities to a model where noiseless but inefficient detectors (with efficiency η) are used for the heterodyne detection. A single value of the parameter η is used to obtain the entire

distribution of the min-entropy as a function of α . The maximum-likelihood estimation fit returns a value of $\eta = 0.173 \pm 0.002$. With this value injected in our theoretical model, we rerun the SDP, and we observe that experimental data and theoretical predictions are in perfect agreement.

For the mean photon number corresponding to the maximum generation rate we perform a long run evaluating the finite-size correction. In this run we perform a total number of 6.5×10^9 trials, in order to reduce the impact of finite-size effects. Using the security parameters described in Sec. B and the Chernoff-Hoeffding bounds of Ref. 8 (more details in Appendix D), we obtain a finite-size correction of 0.00057 bits per measurements, achieving an absolute generation rate of about 113 Mbps.

Finally, a statistical randomness test is performed to check for possible problems and patterns in the generated bit string. To do so, we run the NIST and ENT batteries of tests on the extracted numbers. In both cases, all the tests are passed; however, these tests do not certify the randomness but at least reveals possible patterns due to classical noises. In short, it is a way to double check that our system is operating as expected.

V. CONCLUSION

In conclusion, we realize a simple semi-DI QRNG solution, based on heterodyne detection and a single assumption on the maximal energy of the prepared quantum states. With respect to the overlap bound introduced in Ref. [19], this assumption is easier to check experimentally and in this work is carefully monitored in real time. From the experimental point of view, our realization is based on the prepare-and-measure scenario implemented in a simple all-in-fiber optical setup with only COTS components.

Our setup exploits heterodyne detection, as it provides several key advantages with respect to other measurement strategies. First, it allows us to use commercial high-speed balanced detectors instead of slow and expensive single-photon detectors, greatly increasing the performances while reducing the experimental complexity of the system. Secondly, by sampling the entire phase space, it allows us to track the unavoidable phase drift between the signals and the LO. In this way, fast drifts can be compensated via software during the postprocessing, avoiding the need of a complex active phase-stabilization system. As shown in this work, heterodyne detection provides several advantages regarding the experimental implementation with respect to homodyne, which can be directly applied to other semi-DI QRNG protocols [20–22]. With regards to the security analysis, our protocol, similarly to Ref. [19], requires to upper bound the energy of the transmitted states for each round of the protocol, thus requiring an IID assumption. These assumptions can be relaxed employing

the frameworks described in Refs. [20–22], where the IID is not required and a max-average assumption is used.

With this scheme, we are able to generate and certify private random bits at a rate higher than 113 Mbps.

To conclude, we believe that our QRNG represents a great trade-off between the trust on the device, ease of implementation, and performance making it an attractive solution for many practical applications.

APPENDIX A: SEMIDEFINITE PROGRAMMING

In this section we provide additional information regarding the bound on the guessing probability presented in the main text and its formulation via semidefinite programming [31].

If we consider the case of balanced inputs $p(x) = \frac{1}{2}$ and a fixed overlap $\Lambda = 1 - 2\mu$, then for given measured probabilities $p(b|x)$, the guessing probability of an adversary P_g can be upper bounded by

$$P_g \leq \frac{1}{2} \max_{\{p_\lambda, \rho_x^\lambda, \Pi_b^\lambda\}} \sum_{x=0}^1 \sum_{\lambda} p_\lambda \max\{\text{tr}[\rho_x^\lambda \Pi_0^\lambda], \text{tr}[\rho_x^\lambda \Pi_1^\lambda]\}, \quad (\text{A1})$$

where the maximization over $\{p_\lambda, \rho_x^\lambda, \Pi_b^\lambda\}$ is performed subjected to the two constraints given in Eqs. (2) and (3), corresponding to the overlap bound and the compatibility with the experimental probabilities $p(b|x)$. In the previous equation, λ represents classical shared randomness between preparation and measurement device, $p_\lambda = p(\lambda)$ is the associated probability, $\rho_x^\lambda = |\psi_x^\lambda\rangle\langle\psi_x^\lambda|$ are the density matrices of the prepared states and $\{\Pi_b^\lambda\}$ are a binary outcome POVM modeling the measurement device.

Unfortunately in this form there is no efficient way to compute the bound. However, following the same approach described in Ref. [19] and considering that, due to unitary invariance of Eq. (A1), the $|\psi_x^\lambda\rangle$ can be written without loss of generality as $|\psi_0\rangle = |0\rangle$, $|\psi_1\rangle = \Lambda|0\rangle + \sqrt{1 - \Lambda^2}|1\rangle$ with $|0\rangle$ and $|1\rangle$ orthogonal states, it is possible to express the problem as an SDP.

In particular, the problem can be rewritten as

$$\begin{aligned} & \underset{M_b^{\lambda_0, \lambda_1}}{\text{maximize}} && \frac{1}{2} \sum_{x=0}^1 \sum_{\lambda_0, \lambda_1=0}^1 \text{tr}[\rho_x M_{\lambda_x}^{\lambda_0, \lambda_1}] \\ & \text{subject to} && M_b^{\lambda_0, \lambda_1} = (M_b^{\lambda_0, \lambda_1})^\dagger, \\ & && M_b^{\lambda_0, \lambda_1} \geq 0, \\ & && \sum_b M_b^{\lambda_0, \lambda_1} = \frac{1}{2} \text{tr} \left[\sum_b M_b^{\lambda_0, \lambda_1} \right] \mathbb{I}, \\ & && \sum_{\lambda_0, \lambda_1=0}^1 \text{tr}[\rho_x M_b^{\lambda_0, \lambda_1}] = p(b|x), \end{aligned} \quad (\text{A2})$$

where $M_b^{\lambda_0, \lambda_1} = p_{\lambda_0, \lambda_1} \Pi_b^{\lambda_0, \lambda_1}$. This optimization problem defines the primal SDP, which can be efficiently solved numerically.

However, since the primal involves a maximization, a solution to the problem provides a lower bound on the guessing probability P_g , not an upper bound. Thus, if the solver does not converge to the exact solution it will overestimate the true amount of private randomness.

This problem can be solved by considering the dual formulation of Ref. A2, which involves a minimization problem and returns an upper bound on P_g . Also in this case it is possible to follow the procedure described in Ref. [19] to derive the dual problem, which can be written as

$$\begin{aligned} & \underset{H^{\lambda_0, \lambda_1}, \nu_{bx}}{\text{minimize}} && - \sum_{b,x} \nu_{bx} p(b|x) \\ & \text{subject to} && H^{\lambda_0, \lambda_1} = (H^{\lambda_0, \lambda_1})^\dagger, \\ & && \sum_x \rho_x \left(\frac{1}{2} \delta_{\lambda_x, 0} \delta_{b, 0} + \frac{1}{2} \delta_{\lambda_x, 1} \delta_{b, 1} + \nu_{bx} \right) \\ & && + H^{\lambda_0, \lambda_1} - \frac{1}{2} \text{tr}[H^{\lambda_0, \lambda_1}] \mathbb{I} \leq 0 \end{aligned} \quad (\text{A3})$$

where $\delta_{i,j}$ is the Kronecker δ .

Interestingly, this dual formulation provides another two advantages when compared to the primal. The first advantage is related to the speed of the computation. With the primal, every time we obtain new data $p(b|x)$, it is necessary to run again the SDP to obtain a bound on the guessing probability P_g . With the dual, since the objective function is a linear function of the $p(b|x)$, after an optimal solution has been found, a new (suboptimal) upper bound can be easily evaluated for different $p(b|x)$, without running the optimization again. This aspect is particularly interesting for real-time applications, where the postprocessing can be done efficiently using a lookup table. Finally, with the dual formulation finite-size effects due to the limited statistics can be easily taken into account.

APPENDIX B: HETERODYNE VERSUS HOMODYNE DETECTION

In this section, we show the differences between heterodyne and homodyne detection.

Homodyne detector measures along only one quadrature, such as X or P , as represented in Fig. 2(a), and the information about the other quadrature is lost, see Fig. 2(b). Distinguishability between the two input states is reduced for values of θ (the phase between the states $|\pm\alpha\rangle$ and the LO) different from 0. Real-time phase stabilization is thus required for homodyne measurement. Indeed, as shown in Fig. 2, when the phase is $\theta = 0$, the possibility of distinguishing the two input states by measuring the X quadrature is maximum. As long as $\theta \neq 0, \pi$, the distinguishability decreases.

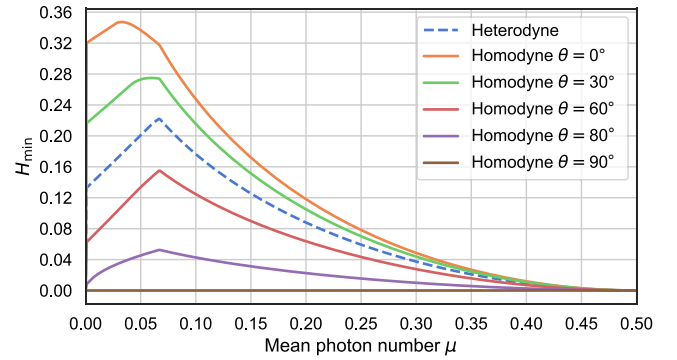


FIG. 6. In this figure, the conditional min-entropy is plotted as a function of the mean photon number for homodyne and heterodyne detection with different phases and no losses ($\eta = 1$). It becomes clear that, when $\theta = 90^\circ$, the min-entropy goes to zero, consequently no random bit can be extracted. This happens due to the fact that when $\theta = 90^\circ$, the two input states show the same distribution in the X quadrature, as if only one state is sent.

Subsequently, the conditional probabilities $p(b|x)$ of obtaining b given x varies as a function of θ and the conditional min-entropy changes accordingly. Indeed, if the input states are the coherent states $|\pm\alpha\rangle$ with $\alpha = |\alpha|e^{i\theta}$, the predicted conditional probabilities with homodyne measurement over the X quadrature are given by

$$\begin{aligned} p(0|0) = p(1|1) &= \frac{1}{2} [1 + \text{erf}(\sqrt{2\eta}|\alpha \cos \theta|)], \\ p(1|0) = p(0|1) &= \frac{1}{2} [1 - \text{erf}(\sqrt{2\eta}|\alpha \cos \theta|)]. \end{aligned} \quad (\text{B1})$$

We note that, differently from Eq. (7), the previous probabilities depend on θ . Moreover, it is worthwhile to note that the above probabilities coincide with Eq. (7) for $\theta = \pi/4$.

On the other hand, information about both quadratures X and P are accessible by performing heterodyne detection, see Fig. 2(c). Thus, the distinguishability is constant as a function of θ and the conditional probabilities $p(b|x)$ will not change.

We show in Fig. 6 the min-entropy in a function of μ for different values of θ for the homodyne and heterodyne measurement. As predicted by conditional probabilities, the min-entropy depends on θ for the heterodyne measurement and for $\pi/4 + n\pi < \theta < \frac{3}{4}\pi + n\pi$ (with integer n) it is always lower than the heterodyne min-entropy. We also show in Fig. 7 the maximum achievable min-entropy for heterodyne measurement in a function of θ (for each θ we choose the μ value that maximizes the min-entropy).

A more detailed comparison between Homodyne and Heterodyne detection, in the case of general d -outcome measurement has been presented in [32].

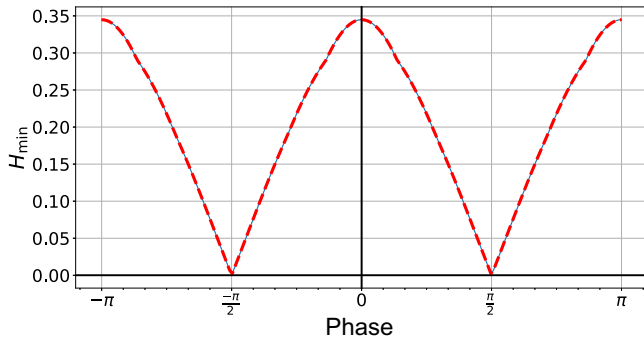


FIG. 7. In this figure, the conditional min-entropy is plotted as a function of the phase θ for homodyne detection in the lossless case ($\eta = 1$). For each value of θ , we choose the μ value that maximizes the min-entropy.

APPENDIX C: THE MEASUREMENT MINIMUM ERROR PROBABILITY

Given two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ that satisfy

$$|\langle\psi_0|\psi_1\rangle| \geq \Lambda \quad (\text{C1})$$

without losing generality, we may write

$$\begin{aligned} |\psi_0\rangle &\equiv |0\rangle, \\ |\psi_1\rangle &\equiv \cos\theta |0\rangle + \sin\theta |1\rangle, \end{aligned} \quad (\text{C2})$$

with $|0\rangle$ and $|1\rangle$ orthogonal states, $0 \leq \theta \leq \pi/2$ and $\cos\theta \geq \Lambda$. The best two-outcome POVM able to discriminate between such two states is projective, namely $\Pi_0 = |\phi_0\rangle\langle\phi_0|$ and $\Pi_1 = |\phi_1\rangle\langle\phi_1|$ with

$$\begin{aligned} |\phi_0\rangle &= \sin\frac{\alpha}{2} |0\rangle + e^{i\phi} \cos\frac{\alpha}{2} |1\rangle, \\ |\phi_1\rangle &= \cos\frac{\alpha}{2} |0\rangle - e^{i\phi} \sin\frac{\alpha}{2} |1\rangle. \end{aligned} \quad (\text{C3})$$

The error probability becomes

$$\begin{aligned} P(b \neq x) &= \frac{1}{2} [p(0|1) + p(1|0)] \\ &= \frac{1}{2} (|\langle\phi_0|\psi_1\rangle\langle\phi_0|\psi_0\rangle|^2 + |\langle\phi_1|\psi_0\rangle\langle\phi_1|\psi_1\rangle|^2) \\ &= \frac{1}{2} [1 - \sin\theta(\sin\theta \sin\alpha - \cos\phi \cos\alpha \cos\theta)]. \end{aligned} \quad (\text{C4})$$

The minimum value of $P(b \neq x)$ is obtained by setting $\phi = \pi$ and $\alpha = \theta$ for which

$$P(b \neq x) = \frac{1}{2} (1 - \sin\theta). \quad (\text{C5})$$

Since $\cos\theta \geq \Lambda$ we have that $\sin\theta \leq \sqrt{1 - \Lambda^2}$ and

$$P(b \neq x) \geq \frac{1}{2} (1 - \sqrt{1 - \Lambda^2}). \quad (\text{C6})$$

For $\Lambda = 1 - 2\mu$ we obtain the result reported in the main text.

APPENDIX D: CHERNOFF-HOEFFDING BOUNDS

In this section we provide additional details about the estimation of the parameters required by the protocol with a finite sample size.

Here we follow the methods described in Ref. [33] where the Chernoff-Hoeffding inequalities are used to bound the required parameters in a quantum key distribution protocol. These results can be directly applied to the scenario considered in this work, providing a composable definition of the parameter estimation.

In Ref. [33] the authors show how the Chernoff bound [34] and the Hoeffding inequality [27] can be employed to derive upper and lower bound on parameters estimated from counting events. In particular, if some tests are passed tighter bounds based on the multiplicative Chernoff bound can be derived. If the tests are not passed, the Hoeffding inequality can be used, which return looser bounds.

Formally, we can express the bounds in the following way.

Lemma 1. *Let X_1, X_2, \dots, X_n , be a set of independent Bernoulli random variables that satisfy $\Pr(X_i = 1) = p_i$, and let $X = \sum_{i=1}^n X_i$ and $\mu = E[X]$, where $E[\cdot]$ is the mean. Let x be the observed outcome of X in a trial and consider the lower bound on μ given by $\mu_L = x - \sqrt{n/2 \ln(1/\varepsilon_1)}$ for certain $\varepsilon_1 > 0$. Then, we can define a confidence interval on x given by*

$$x = \mu + \delta^* \quad (\text{D1})$$

except with error probability γ , where the parameter $\delta^* \in [-\delta, \hat{\delta}]$. Consider also $\varepsilon_2, \varepsilon_3 > 0$ and the following three tests, test_1 , test_2 , and test_3 associated to the following three conditions:

$$\begin{aligned} (2\varepsilon_2^{-1})^{1/\mu_L} &\leq \exp\left\{\left[3/(4\sqrt{2})\right]^2\right\}, & (\varepsilon_3^{-1})^{1/\mu_L} < \\ \exp\{(1/3)\} &\text{ and } (\varepsilon_3^{-1})^{1/\mu_L} < \exp\{[(2e-1)/2]^2\}, & \text{ where } \\ g(x, y) &= \sqrt{2x \ln(y^{-1})}. \end{aligned}$$

Depending on which test is fulfilled, different bounds can be obtained. In particular, as follows.

1. When test_1 and test_2 are fulfilled, we have that $\gamma = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\delta = g(x, \varepsilon_2^4/16)$ and $\hat{\delta} = g(x, \varepsilon_3^{3/2})$.
2. When test_1 and test_3 are fulfilled (and test_2 is not fulfilled), we have that $\gamma = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\delta = g(x, \varepsilon_2^4/16)$ and $\hat{\delta} = g(x, \varepsilon_3^2)$.

3. When $test_1$ is fulfilled and $test_3$ is not fulfilled, we have that $\gamma = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\delta = g(x, \varepsilon_2^4/16)$ and $\hat{\delta} = \sqrt{(n/2) \log(1/\varepsilon_2)}$.

4. When $test_1$ is not fulfilled and $test_2$ is fulfilled, we have that $\gamma = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\delta = \sqrt{(n/2) \log(1/\varepsilon_2)}$ and $\hat{\delta} = g(x, \varepsilon_3^{3/2})$.

5. When $test_1$ and $test_2$ are not fulfilled, and $test_3$ is fulfilled, we have that $\gamma = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\delta = \sqrt{(n/2) \log(1/\varepsilon_2)}$ and $\hat{\delta} = g(x, \varepsilon_3^2)$.

6. When $test_1$, $test_2$, and $test_3$ are not fulfilled, we have that $\gamma = \varepsilon_2 + \varepsilon_3$, $\delta = \hat{\delta} = \sqrt{(n/2) \log(1/\varepsilon_2)}$.

A detailed proof of these relations can be found in the Supplemental Material of Ref. [33].

In this work, we decide to employ conservatives bounds, hence we consider the pessimistic scenario where all three tests fail. In this case, the finite-size corrections are calculated with the Hoeffding inequality, obtaining $\delta = \hat{\delta} = \sqrt{(n/2) \log(1/\varepsilon)}$ and $\gamma = \varepsilon + \hat{\varepsilon}$.

We apply these upper and lower bounds to the counting events $n_{b,x}$, in order to build an associated confidence interval. Then, we obtain the corresponding bounds to the associated conditional probabilities $p(b|x) = n_{b,x}/n_x$ shown in Eq. (8)

ACKNOWLEDGMENTS

We thank Davide Rusca and Giulio Foletto for useful discussion. This work is supported by ‘‘Fondazione Cassa di Risparmio di Padova e Rovigo’’ with the project QUASAR funded within the call ‘‘Ricerca Scientifica di Eccellenza 2018’’; Italian Space Agency with the project ‘‘Realizzazione integrata di un Generatore Quantistico di Numeri Casuali-QRNG’’; MIUR (Italian Minister for Education) under the initiative ‘‘Departments of Excellence’’ (Law 232/2016); EU-H2020 program under the Marie Skłodowska Curie action, project QCALL (Grant No. GA 675662).

-
- [1] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 15004 (2017).
- [2] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, Optical quantum random number generator, *J. Mod. Opt.* **47**, 595 (2000).
- [3] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger, A fast and compact quantum random number generator, *Rev. Sci. Instrum.* **71**, 1675 (2000).
- [4] Antonio Acín and Lluís Masanes, Certified randomness in quantum physics, *Nature* **540**, 213 (2016).
- [5] Roger Colbeck and Adrian Kent, Private randomness expansion with untrusted devices, *J. Phys. A: Math. Theor.* **44**, 095305 (2011).
- [6] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi Kai Liu, Bradley Christensen, Sae Woo Nam, Martin J. Stevens, and Lynden K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, *Nature* **556**, 223 (2018).
- [7] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, Hao Li, W. J. Munro, Zhen Wang, Lixing You, Jun Zhang, Xiongfeng Ma, Jingyun Fan, Qiang Zhang, and Jian-Wei Pan, Device-independent quantum random-number generation, *Nature* **562**, 548 (2018).
- [8] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, Si-Ran Zhao, Bing Bai, Yang Liu, Peter J. Brown, Jun Zhang, Roger Colbeck, Jingyun Fan, *et al.*, Device-independent randomness expansion against quantum side information, *arXiv:1912.11159* (2019).
- [9] Yanbao Zhang, Lynden K. Shalm, Joshua C. Bienfang, Martin J. Stevens, Michael D. Mazurek, Sae Woo Nam, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Honghao Fu, Carl A. Miller, Alan Mink, and Emanuel Knill, Experimental Low-Latency Device-Independent Quantum Randomness, *Phys. Rev. Lett.* **124**, 010505 (2020).
- [10] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, Collin Schlager, Martin J. Stevens, Michael D. Mazurek, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Mohammad A. Alhejji, *et al.*, Device-independent randomness expansion with entangled photons, *arXiv:1912.11158* (2019).
- [11] Ming-Han Li, Xingjian Zhang, Wen-Zhao Liu, Si-Ran Zhao, Bing Bai, Yang Liu, Qi Zhao, Yuxiang Peng, Jun Zhang, Yanbao Zhang, William J. Munro, Xiongfeng Ma, Qiang Zhang, Jingyun Fan, and Jian-Wei Pan, Experimental realization of device-independent quantum randomness expansion, *arXiv:1902.07529 [quant-ph]* (2019).
- [12] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).
- [13] You-Qi Nie, Jian-Yu Guan, Hongyi Zhou, Qiang Zhang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan, Experimental measurement-device-independent quantum random-number generation, *Phys. Rev. A* **94**, 060301 (2016).
- [14] Zhu Cao, Hongyi Zhou, and Xiongfeng Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New J. Phys.* **17**, 125011 (2015).
- [15] Giuseppe Vallone, Davide G. Marangon, Marco Tomasin, and Paolo Villoresi, Quantum randomness certified by the uncertainty principle, *Phys. Rev. A – At., Mol., Opt. Phys.* **90**, 052327 (2014).
- [16] Marco Avesani, Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 gbps, *Nat. Commun.* **9**, 5365 (2018).
- [17] Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, *Phys. Rev. Lett.* **118**, 060503 (2017).

- [18] Zhu Cao, Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma, Source-Independent Quantum Random Number Generation, *Phys. Rev. X* **6**, 011020 (2016).
- [19] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, *Phys. Rev. Appl.* **7**, 054018 (2017).
- [20] Thomas Van Himbeeck, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio, Semi-device-independent framework based on natural physical assumptions, *Quantum* **1**, 33 (2017).
- [21] Davide Rusca, Thomas van Himbeeck, Anthony Martin, Jonatan Bohr Brask, Weixu Shi, Stefano Pironio, Nicolas Brunner, and Hugo Zbinden, Self-testing quantum random-number generator based on an energy bound, *Phys. Rev. A* **100**, 062338 (2019).
- [22] Thomas Van Himbeeck and Stefano Pironio, Correlations and randomness generation based on energy constraints, [arXiv:1905.09117](https://arxiv.org/abs/1905.09117) (2019).
- [23] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Laviñe, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner, Self-Testing Quantum Random Number Generator, *Phys. Rev. Lett.* **114**, 150501 (2015).
- [24] Gustavo Cañas, Jaime Cariñe, Esteban S Gómez, Johanna F. Barra, Adán Cabello, Guilherme B. Xavier, Gustavo Lima, and Marcin Pawłowski, Experimental quantum randomness generation invulnerable to the detection loophole, [arXiv:1410.3443](https://arxiv.org/abs/1410.3443) (2014).
- [25] Davide Rusca, Hamid Tebyanian, Anthony Martin, and Hugo Zbinden, Fast self-testing quantum random number generator based on homodyne detection, *Appl. Phys. Lett.* **116**, 264004 (2020).
- [26] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner, Leftover hashing against quantum side information, *IEEE Trans. Inf. Theory* **57**, 5524 (2011).
- [27] Wassily Hoeffding, Probability inequalities for sums of bounded random variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [28] Renato Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **6**, 1 (2008).
- [29] Alex Paek and Duncan Mackay, Implementing carrier phase recovery loop using vivado hls (2013), https://www.xilinx.com/support/documentation/application_notes/XAPP1173-carrier-loop.pdf.
- [30] Xiao Guang Zhang, You Qi Nie, Hongyi Zhou, Hao Liang, Xiongfeng Ma, Jun Zhang, and Jian Wei Pan, Review of Scientific Instruments, Tech. Rep. 7, [arXiv:1606.09344v1](https://arxiv.org/abs/1606.09344v1) (2016).
- [31] Stephen Boyd, Stephen P. Boyd, and Lieven Vandenbergh, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).
- [32] Hamid Tebyanian, Marco Avesani, Giuseppe Vallone, and Paolo Villoresi, Semi-device independent randomness from d-outcome continuous-variable detection, [arXiv:2009.08897](https://arxiv.org/abs/2009.08897) (2020).
- [33] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi Kwong Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 1 (2014).
- [34] Herman Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Ann. Math. Stat.* **23**, 493 (1952).