Source-Device-Independent Ultrafast Quantum Random Number Generation

Davide G. Marangon,[1] Giuseppe Vallone,[1,2] and Paolo Villoresi[1,2]
[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova 35131, Italia
[2]Istituto di Fotonica e Nanotecnologie, CNR, Padova 35131, Italia
(Received 11 November 2015; revised manuscript received 4 August 2016; published 8 February 2017)

Secure random numbers are a fundamental element of many applications in science, statistics, cryptography and more in general in security protocols. We present a method that enables the generation of high-speed unpredictable random numbers from the quadratures of an electromagnetic field without any assumption on the input state. The method allows us to eliminate the numbers that can be predicted due to the presence of classical and quantum side information. In particular, we introduce a procedure to estimate a bound on the conditional min-entropy based on the entropic uncertainty principle for position and momentum observables of infinite dimensional quantum systems. By the above method, we experimentally demonstrated the generation of secure true random bits at a rate greater than 1.7 Gbit/s.

DOI: 10.1103/PhysRevLett.118.060503

Introduction.—Quantum random number generators (QRNG) exploit intrinsic probabilistic quantum processes to generate true random numbers. The first QRNG was based on the decay of radioactive nuclei [1], while nowadays the versatility of light is mostly employed: as possible examples, we recall QRNGs based on photon *welcher weg* [2–4], photon time of arrival [5–7], or vacuum quadratures [8–11]. In most of the QRNGs, the assessment of the randomness of the generated numbers is obtained by applying statistical tests on the output bits: passing the tests is the only method used to certify the randomness. In case of failure (attributed to hardware problem), numbers are algorithmically postprocessed until the tests are passed.

However, *a posteriori* statistical tests cannot certify that the numbers are not known to someone possessing side information about the generator. For instance, it is not possible to eliminate hardware noise, which is a source of classical side information for an eavesdropper, Eve, who may be able to control it. Hence, a statistical test *a posteriori* cannot establish whether the numbers are originated by the quantum process or by the noisy hardware. Moreover, even assuming a QRNG with an ideal noiseless hardware, a statistical test cannot reveal whether the output arises from a quantum measurement and then it is intrinsically random. For instance, a polarization welcher weg QRNG with an optical source emitting photons in a completely mixed state can be seen as the photonic version of a fair coin. The random sequence can be predicted by Eve if she knows the coin's equations of motion (i.e., she has classical side information) or if she holds a quantum system correlated with the QRNG (i.e., she has quantum side information).

The quantity that evaluates the amount of side information on a random sequence Z is the so-called conditional quantum min-entropy $H_{\min}(Z|E)$ [12], whose value is generally hard to estimate. For instance, in the device independent (DI) framework, $H_{\min}(Z|E)$ can be related to violation of a Bell's inequality. However, these protocols are very demanding from the experimental point of view since they require loophole-free Bell tests [13–15]. This difficulty can be measured in terms of the secure generation rates: the two seminal proofs of principle of DI random number generation [13] and [16] that closed the detection loophole achieved rates of 1.5×10^{-5} and 0.4 bit/s, respectively. Such rates are very low compared to the rates achievable outside the DI framework. Therefore, although recent experiments of Bell's inequality violation have closed also the no-signaling loophole [17–20], the complexity of the setups make it difficult to hypothesize a practical use of DI certified random numbers in a near future.

On the other hand, assuming the absence of local hidden variable theories, true random numbers can be obtained by *a priori* characterization of the quantum system: by a quantum state tomography [21] or by checking the quantum system dimensions [22].

In this work we propose and experimentally realize an efficient protocol for the secure and ultrafast generation of random numbers exploiting the quadrature measurement of the electromagnetic field in a *source-device-independent* (SDI) scenario i.e., assuming a trusted measurement device and a complete untrusted source.

The method is based on the evaluation of a lower bound for $H_{\min}(Z|E)$. We exploit the *entropic uncertainty principle* for continuous variable (CV), i.e., infinite dimensional quantum systems, following the QRNG certification protocol introduced in Ref. [23] for the finite dimensional case. In that protocol, no assumptions are made on the dimensions of the Hilbert space of the source and the bound to the quantum min-entropy is estimated by switching between two measurement basis. The method was later extended in Ref. [24] for Shannon entropies in a detection "squashing" framework. Similarly to Ref. [23], the present

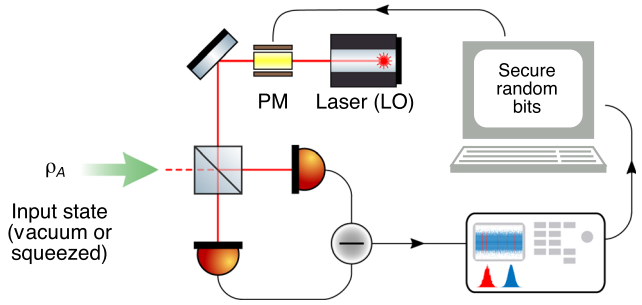

FIG. 1. Scheme of the source-device-independent CV-QRNG [phase modulator (PM), local oscillator (LO)]. The input state is the vacuum (or a squeezed state).

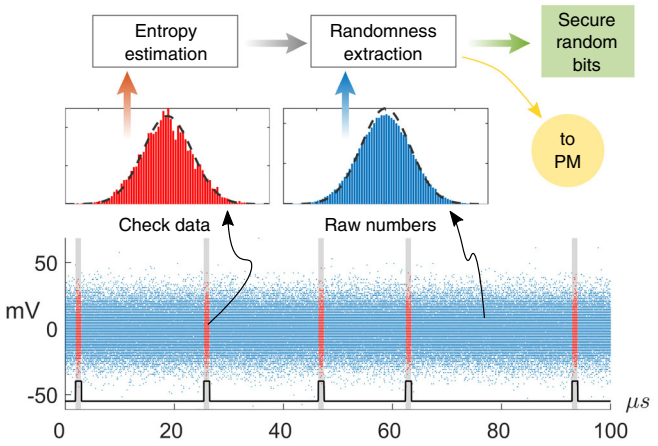

FIG. 2. Experimental homodyne measurement of the vacuum state. Raw random numbers and check data are obtained by measurements in the momentum $\hat{P}$ (blue points) or position $\hat{Q}$ (red points) quadrature, respectively. According to the protocol described in the text, the check data are used to estimate a bound on the quantum entropy $H_{\min}(P_{\delta p}|E)$. Raw numbers are "secured" by applying a strong randomness extractor calibrated $H_{\min}(P_{\delta p}|E)$. Part of the secure bits are "reinvested" in the process to sustain the random quadrature switching. With a solid black line we show the signal sent to the phase modulator (PM, see Fig. 1).

scheme does not require any assumption on the dimension of the Hilbert space of the source.

Review of CV-QRNG.—In a typical scenario, a CV-QRNG user (Alice) generates random numbers by measuring the momentum quadrature $\hat{P}$ of a quantum state ρ_A (typically the vacuum) of an electromagnetic field mode. With CV systems, the finite resolution of the experimental devices leads to a "discretization" of the measurements (see Supplemental Material [25] for more details). More specifically, a coarse grained version $\hat{P}_{\delta p}$ of the quadrature operator, can be obtained by introducing a partition $\{I^k_{\delta p}\}$ of its possible output values $p \in \mathbb{R}$. In the above expression, $I^k_{\delta p}$ are the half-open intervals $I^k_{\delta p} = (k\delta p, (k+1)\delta p]$, with $k \in \mathbb{N}$ and δp the *precision* of the measurement. Alice measures the POVMs $\{\hat{P}^k_{\delta p}\}$ with elements $\hat{P}^k_{\delta p} = \int_{I^k_{\delta p}} dp|p\rangle\langle p|$ and stores the outcomes p_k appearing with probability $\mathfrak{p}(p_k) = \mathrm{Tr}[\rho_A \hat{P}^k_{\delta p}]$ in a classical register $P_{\delta p}$. For cryptographic applications Alice needs to evaluate the probability $\mathfrak{p}_{\mathrm{guess}}(P_{\delta p}|E) = 2^{-H_{\min}(P_{\delta p}|E)}$, that an adversary (Eve) has to guess correctly the outcome of a measurement by adopting an optimal strategy. The guessing probability depends on the quantum conditional min-entropy $H_{\min}(P_{\delta p}|E)$, which represents the maximal content of true random bits achievable for each measurement from the system A, i.e., uniform and uncorrelated from any classical or quantum side information held by an eavesdropper [14,26].

Previous works on CV-QRNGs assumed that the state ρ_A is pure [9]. In this case, the conditional quantum min-entropy reduces to the classical min-entropy $H_\infty(P_{\delta p}) = -\log_2[\max_k \mathfrak{p}(p_k)]$. Eve's best strategy consists in betting on the most probable value, namely, $\mathfrak{p}_{\mathrm{guess}}(P_{\delta p}) = \max_k \mathrm{Tr}[\rho_A \hat{P}^k_{\delta p}]$. Other works assumed the eavesdropper intrusion limited to the classical noise [9,11], which unavoidably affects the experimental apparatus. However, to generate true randomness it is necessary to consider also quantum side information: indeed, the most general scenario includes the possibility of an eavesdropper which has full control of the quantum system E correlated with the system A. It is worthwhile to stress that such a scenario is not "paranoid" but indeed very realistic, since it results from relaxing the *strong* assumption of the system A being in a pure state.

SDI-CV random number generator.—In the untrusted source scenario, the state ρ_A is, in general, *mixed*: it can be purified by a state ρ_{AE}, namely, $\rho_A = \mathrm{Tr}_E[\rho_{AE}]$, where E can be identified with the already mentioned eavesdropper, or with the system "environment." We note that the mixedness of ρ_A corresponds to common physical situations: any decoherence or imperfection in the state preparation leads to correlations with the environment E. In this general case, Alice can estimate the exact value of $H_{\min}(P_{\delta p}|E)$ only by performing a complete quantum state tomography.

However, a simpler approach consists in estimating a lower bound. This can be obtained by exploiting the *entropic uncertainty principle* (EUP) for conditional min- and max-entropies in the presence of infinite dimensional quantum memories introduced in Ref. [27]. The EUP can be summarized as follows: let us consider a tripartite state ω_{ABE} with Alice, Bob, and Eve holding infinite dimensional quantum systems A, B, and E, respectively. Alice measures quadratures $\hat{P}_{\delta p}$ and $\hat{Q}_{\delta q}$ on $\omega_A = \mathrm{Tr}_{BE}[\omega_{ABE}]$ and she stores the outcomes in two classical systems $P_{\delta p}$ and $Q_{\delta q}$. The EUP is written as

$$H_{\min}(P_{\delta p}|E) + H_{\max}(Q_{\delta q}|B) \geq -\log_2 c(\delta q, \delta p), \qquad (1)$$

where

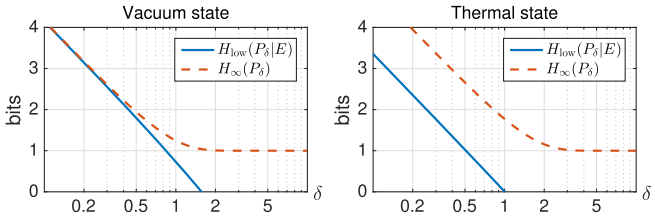

FIG. 3. Comparison between the classical min-entropy $H_\infty(P_\delta)$ and the bound $H_{\rm low}(P_\delta|E)$ on the conditional min-entropy in function of the measurement precision δ. We show the values of $H_\infty(P_\delta)$ and $H_{\rm low}(P_\delta|E)$ for the vacuum state (left) and a thermal state (right) with variance $\sigma^2_{\rm th} = 3/2$. For the vacuum state, both estimators attain the same value when the precision of the measurement increases ($\delta \to 0$). For the thermal state, i.e., a mixed state, the classical min-entropy always overestimates the true content of randomness.

$$c(\delta q, \delta p) = \frac{1}{2\pi}\delta q \delta p S_0^{(1)}\left(1, \frac{\delta q \delta p}{4}\right)^2, \tag{2}$$

and $S_0^{(1)}$ is the 0th radial prolate spheroidal wave function of the first kind [28]. In Eq. (1), the conditional max-entropy $H_{\max}(Q_{\delta q}|B)$ expresses Bob's lack of knowledge about q_k. The term $c(\delta q, \delta p)$ is the "incompatibility" of the measurement operators; i.e., it is maximal if the operators are maximally complementary.

For a QRNG, the system B coincides with A and the max-entropy $H_{\max}(Q_{\delta q}|B)$ reduces to $H_{\max}(Q_{\delta q})$, the Rényi entropy of order 1/2 [12]. Then, it is straightforward to derive the lower bound $H_{\min}(P_{\delta p}|E) \geq H_{\rm low}$ with

$$H_{\rm low}(P_{\delta p}|E) \equiv -\log_2 c(\delta q, \delta p) - H_{\max}(Q_{\delta q}). \tag{3}$$

Our method to estimate the content of true random bits for source-device-independent CV-QRNG is summarized in Figs. 1 and 2 and works as follows: (i) Alice prepares the state ρ_A (the vacuum or a squeezed state), measures it in the $\hat{P}$ quadrature (called *data* quadrature), and generates *raw* random numbers; (ii) the measurement is randomly swapped to the $\hat{Q}$ quadrature (called *check* quadrature): Alice estimates $H_{\max}(Q_{\delta q})$ by using the outcomes of the check quadrature measurements by

$$H_{\max}(Q_{\delta q}) = 2\log_2 \sum_k \sqrt{\mathfrak{p}(q_k)}; \tag{4}$$

(iii) the bound of $H_{\min}(P_{\delta p}|E)$ is evaluated by using Eq. (3); (iv) a quantum randomness extractor calibrated on $H_{\rm low}$ is applied to the raw random numbers. An initial random *seed* for the measurement switching is required, but the protocol is able to expand the initial randomness as in the protocol introduced in Ref. [23].

The measurement of the $\hat{Q}$ operator can be regarded as a tool to estimate, with a partial tomography, whether the state ρ_A is pure or not. In order to better illustrate our approach, in Fig. 3 we compare the classical min-entropy $H_\infty(P_{\delta p})$ and the bound in Eq. (3) as a function of the precision $\delta \equiv \delta q = \delta p$. The quantum min-entropy is bounded by these two values, namely, $H_{\rm low}(P_\delta|E) \leq H_{\min}(P_\delta|E) \leq H_\infty(P_\delta)$. Two different input states ρ_A are considered: a thermal state with variance $\sigma^2_{\rm th} = 1/2 + \mu$, where $\mu = 1$ is the mean photon number, and the vacuum state, with variance $\sigma^2_{\rm vac} = 1/2$. For low δ, the classical min-entropy and the bound can be evaluated analytically, giving $H_\infty(P_\delta) \simeq -\log_2[\delta/\sqrt{\pi(1+2\mu)}]$ and $H_{\rm LOW}(P_{\delta p}|E) \simeq H_\infty(P_\delta) - 2\log_2[(\delta/\sqrt{2\pi})\vartheta_3(0, e^{-\delta^2/(2+4\mu)})]$ with $\vartheta_3(z,q) \equiv \sum_n q^{n^2} e^{2niz}$ the Jacobi theta function.

For pure states, equality between $H_{\min}(P_{\delta p})$ and $H_{\min}(P_{\delta p}|E)$ is expected and this is the case for the vacuum. On the other hand, for a thermal state, the classical min-entropy always overestimate the content of true randomness. A thermal state with $\mu > 0$ is indeed mixed and it can be purified by a two mode squeezed vacuum state ρ_{AE}, an optical version of the EPR entangled state [29]. This implies that ρ_A is correlated with the environment system E: if Eve controls the system E, she can gain information on the quadrature outputs measured by Alice.

The gap between $H_{\min}(P_{\delta p})$ and $H_{\min}(P_{\delta p}|E)$ corresponds to the possible leakage of information due to this correlation. We also note that when δ is large, the bound in Eq. (3) underestimates the number of true random bits extractable per measurement because the lower precision implies a looser estimation of the input state.

Classical side information.—In our SDI framework, Alice controls and trusts the measurement device: the local oscillator is monitored, the shot noise and the phase modulator are calibrated [30]. We also assume that Alice optimizes her hardware such that the independence and uniformity of the numbers are not spoiled (e.g., by oversampling or by using unbalanced beam splitters). We now show that our method takes into account effectively also classical side information. Indeed, even if ρ_A were pure and the generator is optimized, the hardware anyway features an intrinsic classical noise which adds in quadrature to the quantum signal. The result is an increase of the quadrature variance with respect to the shot-noise limit 1/2; cf. the data distribution in Fig. 2. For example, for the vacuum input state one observes a variance of $\sigma'^2_{\rm vac} = 1/2 + \langle n_{\rm noise}\rangle$ in all quadratures, as for a thermal state. Because Alice cannot distinguish whether the input state is mixed or pure, the protocol considers the security most conservative option: any observed "mixedness" is treated as if it is caused by some quantum eavesdropping strategy, i.e., the system A entangled with Eve's system E. Hence, any kind of side information will be erased applying quantum randomness extractors [31–33] *properly* calibrated with the conditional min-entropy lower bound. It is clear that the check quadrature has to be measured at random instants. This prevents Eve from carrying out deception strategies

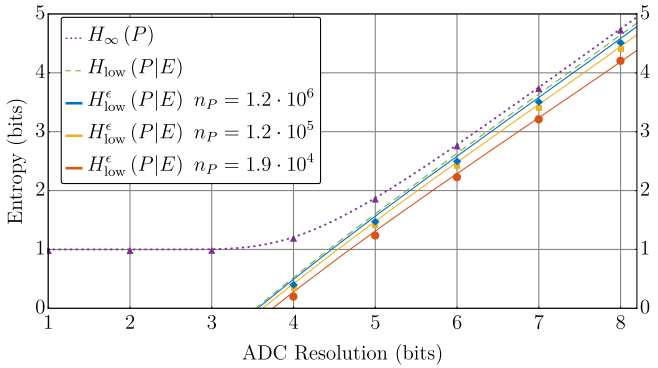

FIG. 4. Entropies as a function of the resolution of the oscilloscope analog to digital converter (ADC). Solid lines are theoretical prediction with the vacuum input state, while dots are the experimental results.

during the check measurements. Therefore, Alice is now able to conservatively bound the amount of true randomness both if an adversary holds a description of the postmeasurement classical-quantum state or may get access to the classical noise. It is worth noting that the real-time estimation of $H_{\min}(P_{\delta p}|E)$ provides a dynamic resiliency against drifts of the classical noise, possibly due to varying experimental conditions (such as temperature or interference with external electromagnetic fields).

Experimental realization.—We implemented an all-in-fiber setup with off-the-shelves devices (see Supplemental Material [25] for more details) according to the scheme reported in Fig. 1: the local oscillator was a narrow line 1550 nm laser connected to a phase modulator (PM) driven by a signal generator (SG). The PM output was mixed with the vacuum entering from the unused port of a fiber 50:50 beam splitter and the exiting ports were connected to a balanced receiver with a bandwidth of 1.6 GHz. The output difference current signal was then sampled at an equivalent rate of 1.25 GS/s by a 12 GHz bandwidth fast oscilloscope, which sent multiple acquisitions of m samples each to a PC for offline postprocessing. We identified the momentum and the position observables as the data and the check quadratures, respectively. We set a ratio of $1/20$ between m and the number of check measurements, n_Q. To be compliant with the protocol, a random seed was preinstalled into the SG in order to select the starting instant of five $n_Q = 0.01m$ long check measurement intervals. From these measurements we estimated the variance for the vacuum state to be $\sigma'^2_{\text{vac}} \approx 0.578$, i.e., 15.6% larger than the theoretical value of $1/2$, as a consequence of the electronic noise, which is then treated as an impurity of the input state.

For the practical realization of the protocol, we take into account also the finite-size effects by using the smooth min-entropy, $H^\epsilon_{\min}(Z|E)$. By using Eq. (43) in Ref. [34] and Eq. (2) in Ref. [35] the smooth min-entropy can be bounded as

$$H^\epsilon_{\min}(P_{\delta p}|E) \geq H_{\text{low}}(P_{\delta p}|E) - \frac{1}{\sqrt{n_P}}\Delta \equiv H^\epsilon_{\text{low}}(P_{\delta p}|E), \tag{5}$$

with $\Delta = 4\log_2(2^{1+H_{\max}(Q_{\delta q})/2}+1)\sqrt{\log_2(2/\epsilon^2)}$ and $n_P = m - n_Q$ the number of measurements for the position quadrature and ϵ the security parameter (cf. Ref. [34]). We note that H^ϵ_{low} reduces to H_{low} when $n \to \infty$.

In Fig. 4 we compare the entropies obtained on a typical data set of multiple oscilloscope acquisitions as a function of its internal analog-to-digital converter resolution and for different values of m. A resolution of j bits corresponds to a precision $\delta_j = \Delta V_{\max}/2^j$ with $\Delta V_{\max}$ the oscilloscope full-scale setting. With solid lines we show the theoretical value of H_∞, H_{low}, and H^ϵ_{low} (for different block sizes) in the case of a vacuum input state and a perfect detection device. In particular, for the finite-size case we used a parameter $\epsilon = 10^{-6}$ and three values of n_P (1.2×10^6, 1.2×10^5, and 1.9×10^4). The corresponding experimental values measured in our physical QRNG are represented by dots. The experimental values are very close to the respective theoretical values, and are distributed slightly below them as a consequence of the impurity of the input state. It is evident that H_∞ overestimates the content of true quantum randomness and then the extractor must be calibrated with H^ϵ_{low}. When the resolution is too low (below 4 bits), the conditional min-entropy becomes lower than zero.

As expected for the finite-size corrections, the larger n_P is the higher the value of true random bits achievable, and for $n_P \gtrsim 10^6$ the quantum min-entropy H^ϵ_{low} almost reaches its infinite-size limit H_{low}. In this respect, the highest min-conditional entropy is $H^\epsilon_{\text{low}}(P_{\delta_8}|E) = 4.53 \pm 0.01$ bit per measurement obtained for $n_P \approx 10^6$. Although the ADC nominal resolution is 8 bits, at high sampling rates the effective number of bits (the so-called *enob*) decreases. Hence, we used a conservative bit depth of 5 bits, satisfying the SDI requirement of having a trusted and controlled measurement apparatus. This additional precaution then lowers the entropy to $H^\epsilon_{\text{low}}(P_{\delta_5}|E) = 1.49 \pm 0.01$ bits per sample. To evaluate the secure generation rate, i.e., the net number of true random bits per measurement, r_{sec}, we need to account for the random bits that, in a full implementation of the protocol, would be "recycled" into the SG for the continuous quadrature switching. Here, a given random combination of the instants for five nonoverlapping check intervals can be encoded in a *seed* $t = \lceil \log_2(\binom{100}{5}) \rceil$ bits long. Therefore, r_{sec} is given by $r_{\text{sec}} = (1/m)[n_P H^\epsilon_{\text{low}}(P_{\delta_5}|E) - t]$. By considering the oscilloscope sampling rate, these results imply an equivalent secure bit generation rate of approximately 1.77 Gbit/s.

Conclusions.—Ultimate randomness is reachable only by using device independent protocols such as randomness expansion [13] or amplification [14,15]: however, such

protocols are highly demanding from an experimental point of view requiring loophole-free violations of the Bell inequalities. Our SDI protocol enables the ultrafast generation of true random numbers without assumptions on the source of the quantum state, which could be even provided by an eavesdropper. Our method is motivated by experimental requirements: indeed, it is typically difficult to prepare and keep a real quantum system in a pure state. Future steps will consider the possibility of merging our protocol with the metrologic approach introduced in Ref. [36] and with the methods of Refs. [37,38] to take into account imperfections of the measurement device. Besides the security advantage achieved by bounding the smooth min-conditional entropy, we demonstrated the feasibility of the protocol with an ultrafast, cheap, and compact CV-QRNG. It is worthwhile to remark that by using commercial balanced receivers and a fast local oscillator phase shifter, the secure generation rate can be increased to tens of Gbit/s. Further improvements can be envisaged when squeezed states are used as the input state.

The authors wish to thank R. Corvaja, L. Palmieri, and M. Stellini of DEI-University of Padova for the helpful discussions. Our work was supported by the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova, the Strategic-Research-Project QUANTUMFUTURE of the University of Padova.

[1] H. Schmidt, J. Appl. Phys. **41**, 462 (1970).
[2] J. G. Rarity, P. Owens, and P. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[3] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[4] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[5] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Opt. Express **18**, 13029 (2010).
[6] M. Stipcevic and B. M. Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).
[7] M. a. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).
[8] A. Trifonov and H. Vig, US Patent No. 7, **284**, 024 (2007).
[9] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).
[10] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).
[11] T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).
[12] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[13] 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, Nature (London) **464**, 1021 (2010).
[14] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[15] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, Nat. Commun. **4**, 2654 (2013).
[16] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Phys. Rev. Lett. **111**, 130406 (2013).
[17] B. Hensen *et al.*, Nature (London) **526**, 682 (2015).
[18] M. Giustina *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).
[19] L. K. Shalm *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).
[20] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, arXiv:1611.04604 [Phys. Rev. Lett. (to be published)].
[21] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).
[22] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[23] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).
[24] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
[25] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.118.060503 for a review of the formalism of discrete quadrature measurement operators for continuous variables QRNG (Sec. I) and a detailed description of the experimental setup (Sec. II).
[26] D. Frauchiger, R. Renner, and M. Troyer, arXiv:1311.4547.
[27] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, J. Math. Phys. (N.Y.) **55**, 122205 (2014).
[28] H. J. Landau and H. O. Pollak, Bell Syst. Tech. J. **40**, 65 (1961).
[29] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[30] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[31] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).
[32] A. De, C. Portmann, T. Vidick, and R. Renner, SIAM J. Comput. **41**, 915 (2012).
[33] R. Renner, *Information Theoretic Security* (Springer, New York, 2011), p. 52.
[34] F. Furrer, J. Aberg, and R. Renner, Commun. Math. Phys. **306**, 165 (2011).
[35] T. Eberle, V. Händchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel, and W. Reinhard, New J. Phys. **15**, 053049 (2013).
[36] M. W. Mitchell, C. Abellan, and W. Amaya, Phys. Rev. A **91**, 012314 (2015).
[37] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, W. Reinhard, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).
[38] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Phys. Rev. Applied **3**, 054004 (2015).

Supplementary Material of *Source-device-independent Ultra-fast Quantum Random Number Generation*

Davide G. Marangon,[1] Giuseppe Vallone,[1,2] and Paolo Villoresi[1,2]

[1] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italia*
[2] *Istituto di Fotonica e Nanotecnologie, CNR, Padova, Italia*

I. DISCRETIZATION IN CV-QRNG

For a given mode of the electromagnetic field, the generic quadrature operator can be expressed by $\hat{q}(\varphi) = 2^{-\frac{1}{2}}\left(e^{i\frac{\varphi}{2}}\hat{a}^\dagger + e^{-i\frac{\varphi}{2}}\hat{a}\right)$ being $\hat{a}^\dagger$ and $\hat{a}$ the creation and annihilation operators such that $[\hat{a}, \hat{a}^\dagger] = 1$ holds. The canonically conjugated operators usually identified as the *position* $\mathcal{Q}$ and *momentum* $\mathcal{P}$ quadratures observables are given by $\hat{Q} \equiv \hat{q}(0)$ and $\hat{P} \equiv \hat{q}(\pi)$. They satisfy $[\hat{Q}, \hat{P}] = i$. The eigenvalues equations for position and momentum operators are given by $\hat{Q}|q\rangle = q|q\rangle$ with $q \in \mathbb{R}$ and $\hat{P}|p\rangle = p|p\rangle$ with $p \in \mathbb{R}$.

With CV systems, the unavoidable discretization of the measurements due to the finite resolution of the experimental devices has to be considered. More specifically, a coarse grained version of operators can be obtained by introducing a partition $\mathcal{P}_{\delta p} = \{I^k_{\delta p}\}_{k=-\infty}^{+\infty}$ of the measure space $\mathbb{R}$ [**?**]. The elements $I^k_{\delta p}$ are given by half-open intervals such that $I^k_{\delta p} = (k\delta p, (k+1)\delta p]$ where δp is the *precision* of the measurement and $k \in \mathbb{N}$. Alice applies POVMs $\left\{\hat{P}^k_{\delta p}\right\}$ with elements $\hat{P}^k_{\delta p} = \int_{k\delta p}^{(k+1)\delta p} dp|p\rangle\langle p|$ on A and she stores the outcomes p_k in the classical system (register) $P_{\delta p}$. The post-measurement state of $P_{\delta p}$ corresponds to the probability distribution of p_k, and it is given by $\rho_P = \sum_k \mathfrak{p}(p_k)\hat{P}^k_{\delta p}$ where $\mathfrak{p}(p_k) = \mathrm{Tr}\left[\omega_A \hat{P}^k_{\delta p}\right] = \int_k^{(k+1)\delta p} dp\langle p|\rho_A|p\rangle$. Similarly, the discretized $\hat{Q}$ operator is given by the POVMs $\left\{\hat{Q}^k_{\delta q}\right\}$ with elements $\hat{Q}^k_{\delta q} = \int_{k\delta q}^{(k+1)\delta q} dq|q\rangle\langle q|$.

The estimation of max-entropy $H_{\max}(Q_{\delta q})$ is based on the relative frequency of the outcomes of the discretized $\hat{Q}$ operator, as given by eq. (4) of the main text:

$$2^{H_{\max}(Q_{\delta q})} = \Big[\sum_{k=-\infty}^{+\infty} \sqrt{\mathfrak{p}(q_k)}\Big]^2 \tag{1}$$

While the sum in the above equation extends from $-\infty$ to $+\infty$, experimental outcomes range from $-M$ to $+M$ due to experimental finite measurement range. Outcomes which exceed this range are registered as $M+1$ or $-M-1$ outcomes. We estimated the max-entropy by limiting the sum in (1) from $-M$ to M, thus not considering the term $\sum_{k>|M|}\sqrt{\mathfrak{p}(p_k)}$. We can upper bound the latter term, by considering a trial with a total of N measurements: defining $P_M = \sum_{k=-\infty}^{-M}\mathfrak{p}(p_k) + \sum_{k=M}^{\infty}\mathfrak{p}(p_k)$, we expect that $n \sim P_M N$ events result in an outcome out of range. The worst scenario, that maximize the neglected term, is given when each of the n outcomes falls into a different bin. In this situation, we have $\mathfrak{p}(p_k) \approx 1/N$ such that $\sum_{k>|M|}\sqrt{\mathfrak{p}(p_k)} \leq \frac{n}{\sqrt{N}} \approx \sqrt{N}P_M$. Since P_M corresponds to the double sided tail probability of the Gaussian distribution, a narrow distribution (i.e. a small standard deviation σ compared to $M\delta$) corresponds to a low error in the min-entropy estimation. For the experimental data presented in the main text, we have that $M\delta \approx 12\sigma$ which implies a $P_M \approx 10^{-32}$: with the max entropy evaluated on $N \approx 62 \cdot 10^3$ measurements we then estimate that the error introduced by the finite measurement range, is of order of 10^{-30}.

II. EXPERIMENTAL SETUP

A scheme of the experimental setup is reported in Fig. 1 of the Main Text. The local oscillator is provided by a **Thorlabs SFL-1550** fiber coupled laser centered at 1550 nm. The laser is driven by a current and temperature controller which keep the laser operating in a single mode regime. The LO output is therefore sent to a free-space optical polarization control unit realized by means of half and quarter wave-plates. By this device the input polarization can be tuned before entering the phase modulator (PM). The PM is a **Photline MPZ-LN-20** controlled by a signal generator **Agilent 33100** that randomly switch between the two values of φ (0 or π).

By means of 50:50 fiber beamsplitter (BS), the PM output is mixed with the vacuum entering from a closed port of the BS. The superposition of the LO and the vacuum state is detected and converted in current by a pair of InGaAs PINs included in the single self-contained balanced receiver **Thorlabs PDB480C**. This device has a nominal bandwidth of 1.6 GHz and generates an amplified signal of the difference of the PIN currents. Such monolithic configuration helps consistently to reduce the coupling with environmental electromagnetic noise. It is worth to remark that the setup components are "commercial of the shelves" (COTS). The use of COTS devices was motivated by the possibility to demonstrate the feasibility of the method and how security can be provided to CV-QRNG for the common use.

The final stage of the setup consists of an oscilloscope **Tektronix TDS6124C** featuring a bandwidth of 12 GHz that was used as ADC.

In Fig. 1, the typical Power Spectral Density (PSD) of the output signal is reported. In particular the PSD with

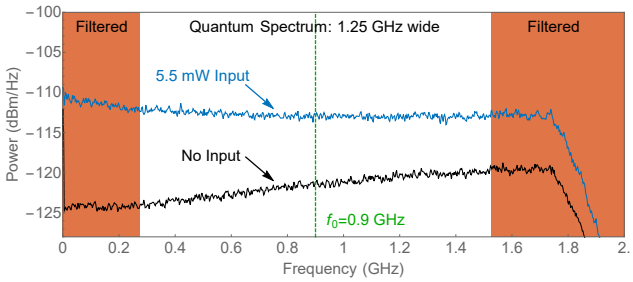

FIG. 1. The power spectral density function of the signals with LO turned off (black line) and with a LO power of 5.5 mW (blue line) is reported. The green shaded region identifies the 1.250 GHz wide region of the spectrum which was considered for the extraction of the raw random numbers. The signal has been downmixed with a sinusoidal carrier at frequency $f_0 = 0.9$ GHz and then filtered with a low-pass filter with 625 MHz cut off frequency.

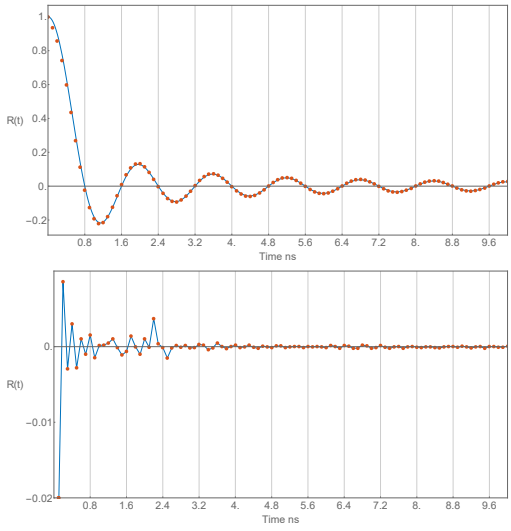

FIG. 2. **Top**: experimental autocorrelation of the filtered data as function of the temporal separation in multiple of the sampling interval T_S. The correlation is modulated according a sinc function. This is indeed the expected behavior once that a signal is filtered by a low pass filter, top inset. By means of the Wiener-Kitchine theorem one can analytically calculate the zeros of the autocorrelation and then the corresponding down sampling frequency in order to achieve a null self-correlation. **Bottom:** by downsampling the original waveforms, the quadrature measurements become uncorrelated.

the LO turned off (black trace) and with a 5.5 mW LO (blue trace) is reported. The study of the spectrum of the signal is of fundamental importance in order to characterize and optimize the measurement device. In order to filter out those regions of the spectrum affected by technical noise and to enhance the signal-to-noise ratio, we digitally downmixed and low-pass filtered the signal. As working region we therefore considered a flat region 1.250 GHz wide, with optimal central frequency at $f_0 = 0.9$ GHz. The *quadrature signal* was obtained by sampling the detector signal at a rate of 10 GSampes/s and then by performing a downsampling to 1.25 GSamples/s, in order to match the Nyquist frequency of the low-pass filter and to eliminate the correlations due to oversampling. On this regard in Fig. 2, we report the correlation before (top) and after (down) the downsampling in function of the temporal separation of the samples. Before downsampling, the correlation shows the sinc modulation imposed by the low-pass filter (the blue curve is the theoretical expected correlation while the orange dots are the average experimental points). After downsampling, the residual correlation is, in average, two orders of magnitude lower. Residual correlations at low separation can be attributed to an artificial component introduced by the oscilloscope at harmonics of 2.5 GHz. Such low correlations is removed by the randomness extractor.