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*

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 to eliminate the numbers that can be predict due 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 Gbit/s.

In the last few years there has been an increasingly growing interest in randomness. Randomness is indeed an essential ingredient not only in Cryptography but also in experiments of Foundations of Quantum Mechanics. In the first case randomness is necessary to guarantee the security of the protocols, being them classical, quantum or even post-quantum. In the second case, randomness is necessary to rule out pre-determinism in experiments such as for the violation of Bell's inequalities [1] and "Wheeler's delayed choice". In both these applications, it is indispensable that the source of randomness generates a random variable X which identically and independently distributed with respect to any other variable E, outside the future light cone of X.

In this respect, quantum random number generators (QRNGs), i.e. devices which generate a random variable by suitably measuring some observables of a quantum system, have always been regarded as the perfect source of randomness. The typical example is the "which way" (WW) QRNG [2–4] where a photonic qubit is prepared as a polarization eigenstate of the observable σ_Z. The random variable X, associated to the outcome of the measurement of σ_X, is therefore unpredictable because the preparation and measurement are performed on two mutually unbiased bases.

In general for real QRNGs implementations, the unpredictability of X is limited by the non-ideality of the devices. Perfect state purity and perfect projective measurements are indeed hardly achievable. For example, a WW-QRNG with an optical source emitting photons in a completely mixed polarization state, is just the photonic version of a fair coin [5]. In this case, the observed randomness is just apparent, as it can be attributed to the observer ignorance about the source degrees of freedom. However, the outcomes are perfectly predictable to someone who knows the coin's equations of motion.

More formally, mixedness leaves room for quantum side information. An eavesdropper, Eve, holding a quantum system correlated with the QRNG, might be able to retrieve side information E and then become able to guess X by measuring her system.

However, by using randomness extractors, the QRNG user, Alice can still be able to distill unpredictable random numbers from X [6, 7]. For this purpose, it is of fundamental importance that Alice correctly evaluates the *quantum conditional min-entropy* $H_{\min}(X|E)$, i.e. the maximal achievable amounts of bits which are uniform and uncorrelated from any classical or quantum side-information accessible to Eve [8].

In this work we therefore propose and experimentally realize [9] a protocol which enables the user to evaluate a lower bound to the conditional min-entropy for a continuous variable (CV) QRNG [12–14], where the generated random variable, P, is associated to the measurement outcomes of the momentum $\hat{P}$ quadrature observable of the electromagnetic field.

The method assumes a trusted measurement device and a complete untrusted source, i.e. a *source-device-independent* (SDI) scenario where no assumptions are required on the dimension of the Hilbert space of the source (cf. [10]). The rationale behind the SDI approach is its closeness to the experimental reality: as a real quantum system is difficult to prepare and keep in a pure state, as the hardware can be optimized to minimize its impact on the numbers.

In the untrusted source scenario, the state ρ_A of the quantum system 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 $H_{\min}(P|E)$ only by performing a complete quantum state tomography.

However, an alternative and simpler approach consists in estimating a lower bound, $H_{\mathrm{LOW}}(P|E)$. 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 by Furrer *et al.* [**?**].

Our method to estimate the content of true random bits for source-device-independent CV-QRNG is summa-

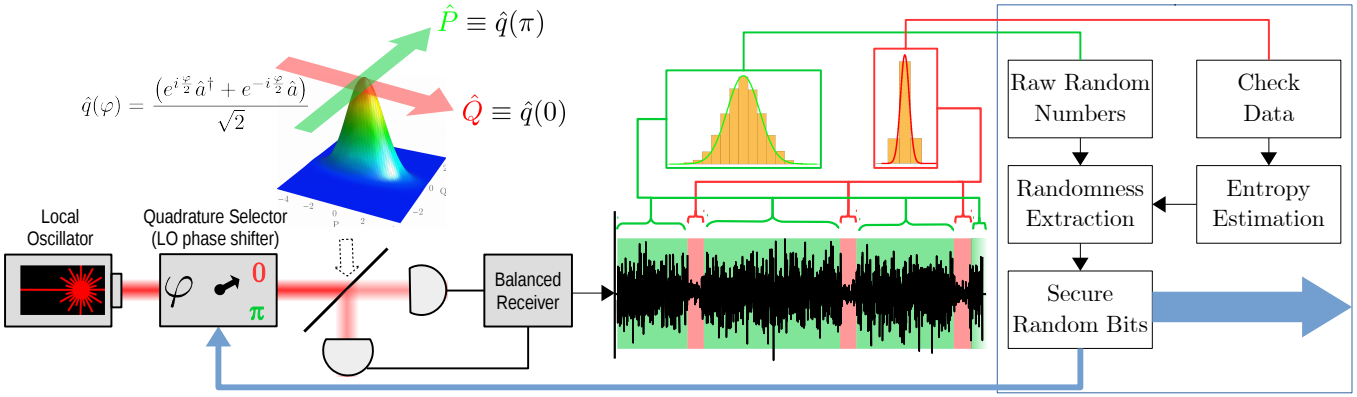

FIG. 1. Random numbers are obtained by measuring the position quadrature of a Gaussian state with optical homodyne. These numbers are "secured" by applying a strong randomness extractor calibrated on a conservative bound of $H_{\min}(P_{\delta p}|E)$. Such bound is obtained by randomly measuring the complementary quadrature, i.e. the momentum one. Part of the secure bits are "re-invested" in the process to sustain the random quadrature switching.

rized in Fig. 1 and works as follows: I) Alice prepares the state ρ_A (the vacuum or a squeezed vacuum), measures it in the $\hat{P}$ quadrature (called *data* quadrature) with precision δp and generates *raw* random numbers; II) the measurement is randomly swapped to the $\hat{Q}$ quadrature (called *check* quadrature): Alice estimates the Rényi entropy of order 1/2, $H_{1/2}(Q) = 2\log_2 \sum_k \sqrt{\mathfrak{p}(q_k)}$, by using the measured (with precision δq) outcomes probabilities of the check measurements III); the bound of $H_{\min}(P|E)$ is therefore evaluated by using the EUP which reads

$$H_{\text{LOW}}(P|E) \equiv -\log_2 c(\delta q, \delta p) - H_{1/2}(Q)\,, \qquad (1)$$

where 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; IV) a quantum randomness extractor calibrated on the bound is applied to the raw random numbers. An initial random *seed* for the measurement switching is required, but the protocol is able to quadratically expand the initial randomness as in the protocol introduced in [5].

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. As an example, in Figure 2 we show the Wigner functions of the squeezed and thermal state with the same momentum distribution for the random variable P. The difference between the two position distribution is evident. The impurity of the thermal state may be indeed detected by Alice by observing that that the (check) position quadrature variance is not squeezed. However, it is not necessary to abort the protocol: Alice can still extract random bits by calibrating a quantum randomness extractor with a lower bound conditional of the conditional min-entropy estimated with the protocol presented above.

A proof of principle of the generation protocol was given by realizing a homodyne detection setup for the

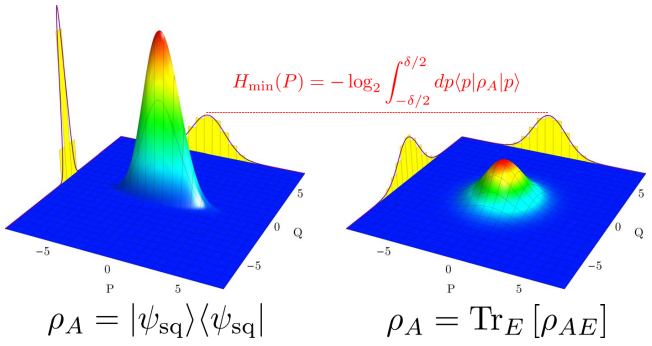

FIG. 2. **left**: Wigner function for a $\mathcal{Q}$-squeezed vacuum state ($\zeta = 2$) and the relative discretized probability distribution (yellow histograms) for the two conjugate quadratures. Since the outcome distribution for $\mathcal{P}$ is wider, the outcomes of momentum measurements (performed with precision δp) are used as random numbers. This is an ideal input state for a CV-QRNG: the state is pure and the randomness extractor can be calibrated by the classical min-entropy $H_{\min}(P_{\delta p})$. **right**: Wigner function of a thermal state, that can be purified by a two-mode squeezed vacuum. The probability distribution for the P outcomes coincides with the distribution obtained with the $\mathcal{Q}$-squeezed vacuum state. In this case, the classical min-entropy over-estimates the true content of randomness, because it does not take into account the quantum side information possessed by Eve.

measurements of the vacuum state quadratures. Commercial large bandwidth detectors and a fast oscilloscope were used to collect the data. In this regard it is worth to stress that, in the estimation of the conditional min-entropy, the protocol takes automatically into account also the classical noise introduced by the hardware. In fact, the classical noise added by the hardware to the quantum noise of the vacuum, makes the check quadrature variance to be larger than the value of 1/2 corresponding to a pure vacuum state. In this way it was pos-

sible to obtain a equivalent rate of secure random bits higher than 1 Gbit/s.

In terms of security and performances, this generation method is halfway between the device independent (DI) and the "full trust" protocols. The DI framework lets the user to achieve the ultimate security, as the conditional min-entropy is related to violation of a Bell's inequality. However, at present time, the typical protocols of randomness expansion and amplification are very demanding from the experimental point of view, since they require loophole-free Bell tests [15, 17, 18].

On the other side, fully trusted generators where the purity of the state is assumed might be faster than our protocol. However, they might also feature lower level of security as they do not provide any means to check whether the state is pure or mixed.

Our protocol therefore results promising for the future applications in Cryptography and for the testing of the foundations of Quantum Mechanics, where both high generation rate and unpredictability are will become indispensable features.

[1] B. Hensen, H. Bernien, AE Dréau, A. Reiserer, N. Kalb,M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán and others, Nature **526.7575**, 682 (2015).

[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] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 52327 (2014).

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

[7] A. De, C. Portmann, T. Vidick, and R. Renner, SIAM Journal on Computing **41**, 915 (2012).

[8] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Th. **55**, 1 (2009).

[9] D.G. Marangon, G. Vallone, and P. Villoresi, arXiv:1509.07390,2015.

[10] 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).

[11] A. Trifonov and H. Vig, US Pat. 7,284,024 (2007).

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

[13] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).

[14] T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. 2–5 (2011).

[15] 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 **464**, 1021 (2010).

[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] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).

[18] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, Nat. Commun. **4**, 2654 (2013).