A self-testing quantum random number generator

Tommaso Lunghi,[1] Jonatan Bohr Brask,[2] Charles Ci Wen Lim,[1] Quentin Lavigne,[1]
Joseph Bowles,[2] Anthony Martin,[1] Hugo Zbinden,[1] and Nicolas Brunner[2]

[1] *Group of Applied Physics, Université de Genève, 1211 Genève, Switzerland*
[2] *Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland*

The generation of random numbers is a task of paramount importance in modern science. A central problem for both classical and quantum randomness generation is to estimate the entropy of the data generated by a given device. Here we present a protocol for self-testing quantum random number generation, in which the user can monitor the entropy in real-time. Based on a few general assumptions, our protocol guarantees continuous generation of high quality randomness, without the need for a detailed characterization of the devices. Using a fully optical setup, we implement our protocol and illustrate its self-testing capacity. Our work thus provides a practical approach to quantum randomness generation in a scenario of trusted but error-prone devices.

Given the importance of randomness in modern science and beyond, e.g. for simulation algorithms and for cryptography, an intense research effort has been devoted to the problem of extracting randomness from quantum systems. Devices for quantum random number generation (QRNG) are now commercially available. All these schemes work essentially according to the same principle, exploiting the randomness of quantum measurements. A simple realization consists in sending a single photon on a 50/50 beam-splitter and detecting the output path [1–3]. Other designs were developed, based on measuring the arrival time of single photons [4, 5], the phase noise of a laser [6, 7], vacuum fluctuations [9, 10].

A central issue in randomness generation is the problem of estimating the entropy of the bits that are generated by a device, i.e. how random is the raw output data. When a good estimate is available, appropriate post-processing can be applied to extract true random bits from the raw data (via a classical procedure termed randomness extractor [11]). However, poor entropy estimation is one of the main weaknesses of classical RNG [12], and can have important consequences. In the context of QRNG, entropy estimates for specific setups were recently provided using sophisticated theoretical models [13, 14]. Nevertheless, this approach has several drawbacks. First, these techniques are relatively cumbersome, requiring estimates for numerous experimental parameters which may be difficult to precisely assess in practice. Second, each study applies to a specific experimental setup, and cannot be used for other implementations. Finally, it offers no real-time monitoring of the quality of the RNG process, hence no protection against unnoticed misalignment (or even failures) of the experimental setup.

It is therefore highly desirable to design QRNG techniques which can provide a real-time estimate of the output entropy. An elegant solution is provided by the concept of device-independent QRNG [15, 16], where randomness can be certified and quantified without relying on a detailed knowledge of the functioning of the devices used in the protocol. Nevertheless, the practical implementation of such protocols is extremely challenging as it requires the genuine violation of Bell's inequality [16, 17]. Alternative approaches were proposed [18] but their experimental implementation suffers from loopholes [19]. More recently, an approach based on the uncertainty principle was proposed but requires a fully characterized measurement device [20].

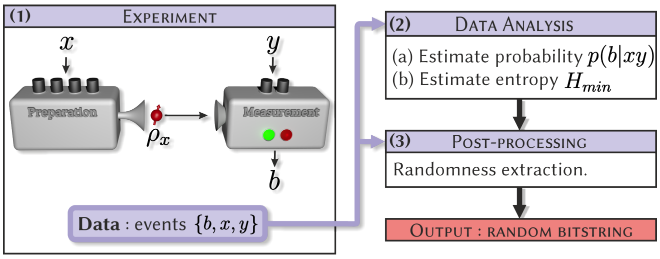
(1) Experiment
x
y
Preparation
Measurement
ρ_x
b
Data : events $\{b,x,y\}$
(2) Data Analysis
(a) Estimate probability $p(b|xy)$
(b) Estimate entropy H_{min}
(3) Post-processing
Randomness extraction.
Output : random bitstring

FIG. 1. **Sketch of the protocol.** The self-testing QRNG protocol consists in 3 distinct steps. **(1)** First, an experiment is performed where, in each round, the user chooses a preparation x and a measurement y, and obtains an outcome b. **(2)** From the raw data, the distribution $p(b|x,y)$ can be estimated leading to an estimate for the value of the witness W, from which the entropy of the raw data can be quantified. **(3)** Based on the entropy bound, appropriate post-processing of the raw data is performed, in order to extract the final random bit string.

Here, we present a simple and practical protocol for self-testing QRNG. Based on a prepare-and-measure setup, our protocol provides a continuous estimate of the output entropy. Our approach requires only a few general assumptions about the devices (such as quantum systems of bounded dimension) without relying on a detailed model of their functioning. This setting is relevant to real-world implementations of randomness generation, and is well-adapted to a scenario of trusted but error-prone providers, i.e. a setting where the devices used in the protocol are not actively designed to fool the user, but where implementation may be imperfect. The key idea behind our protocol is to certify randomness from a pair of incompatible quantum measurements. As the incompatibility of the measurements can be directly quantified from experimental data, our protocol is self-testing.

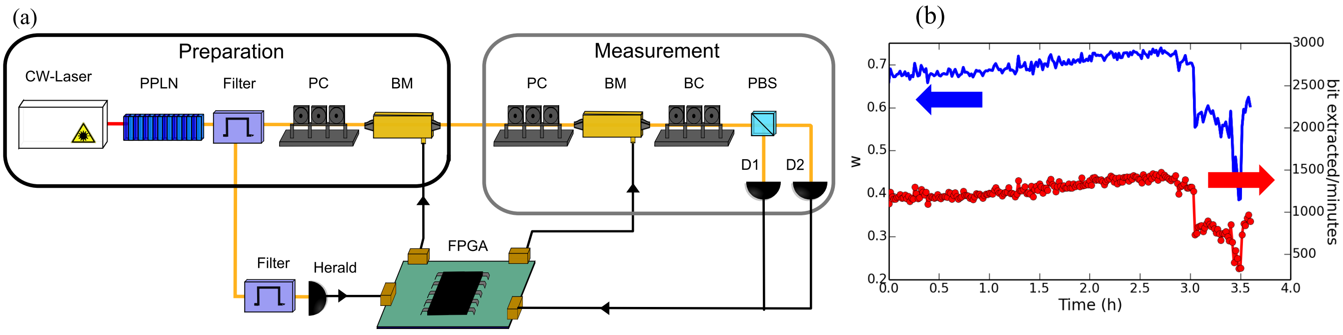

FIG. 2. Implementing the self-testing QRNG. (a) Experimental setup. (b) Real-time evolution of the witness value W (blue) and randomness generation rate (bits extracted per second; red). After 3 hours, the air conditioning in the laboratory is switched off, which leads to misalignment of the optical components. In turn, this leads to a significant drop of the witness value W and corresponding entropy.

That is, the amount genuine quantum randomness can be quantified directly from the data, and can be separated from other sources of randomness such as fluctuations due to technical imperfections. The protocol is sketched in Figure 1. More details can be found in [21]

We implemented the self-testing QRNG with standard technology, using a single photon source and fibered telecommunication components. We implement the complete QRNG protocol, achieving a rate 23 certified random bits per second, with 99% confidence. The experimental setup and results are provided in Figure 2. More details can be found in [21]

Compared to the device-dependent approach, our protocol delivers a stronger form of security requiring less characterization of the physical implementation, at the price of a reduced rate compared to commercial QRNGs such as ID Quantique QUANTIS which reaches 4Mbits/s. A fully device-independent approach [15, 16], on the other hand, offers even stronger security (in particular assumptions (ii)-(iv) can be relaxed, hence offering robustness to side-channels and memory effects), but its practical implementation is extremely challenging. Proof-of-principle experiments require state-of-the-art setups but could achieve only very low rates [16, 17]. Our approach arguably offers a weaker form of security, but can be implemented with standard technology. Our work considers a scenario of trusted but error-prone devices, which we believe to be relevant in practice.

[1] J. Rarity, P. Owens, and P. Tapster, Journal of Modern Optics **41**, 2435 (1994).

[2] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Journal of Modern Optics **47**, 595 (2000).

[3] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Review of Scientific Instruments **71**, 1675 (2000).

[4] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Applied Physics Letters **93**, 031109 (2008).

[5] M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H.-J. Rahn, and O. Benson, Applied Physics Letters **98**, 171105 (2011).

[6] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).

[7] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, OowadaIsao, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nat Photon **2**, 728 (2008).

[8] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express **22**, 1645 (2014).

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

[10] T. Symul, S. M. Assad, and P. K. Lam, Applied Physics Letters **98**, 231103 (2011).

[11] N. Nisan and A. Ta-Shma, Journal of Computer and System Sciences **58**, 148 (1999).

[12] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergniaud, and D. Wichs, Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security CCS '13, 647 (2013).

[13] D. Frauchiger, R. Renner, and M. Troyer, arXiv e-print (2013), arXiv:1311.4547 [quant-ph].

[14] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).

[15] R. Colbeck, "Ph.d. thesis, arxiv:0911.3814," .

[16] 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).

[17] 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).

[18] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011); H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[19] M. Dall'Arno, E. Passaro, R. Gallego, M. Pawlowski, and A. Acin, arXiv e-print (2012), arXiv:1210.1272 [quant-ph].

[20] G. Vallone, D. G. Marangon, M. Tomasin, and PaoloVilloresi, arXiv e-print (2014), arXiv:1401.7917 [quant-ph].

[21] T. Lunghi, J. B. Brask, C. Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).