Fast semi-device-independent quantum random number generator based on unambiguous state discrimination

Jonatan Bohr Brask,[1] Anthony Martin,[1] William Esposito,[1] Raphael Houlmann,[1] Joseph Bowles,[1, 2] Hugo Zbinden,[1] and Nicolas Brunner[1]

[1] *Group of Applied Physics, Université de Genève, 1211 Genève, Switzerland*
[2] *ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*

The generation of random numbers is of paramount importance in modern science and technology, in particular cryptography. Here, we develop a new approach to quantum random number generation based on unambiguous quantum state discrimination. We consider a prepare-and-measure protocol, where two non-orthogonal quantum states can be prepared, and a measurement device aims at unambiguously discriminating between them. Because the states are non-orthogonal, this necessarily leads to a minimal rate of inconclusive events whose occurrence must be genuinely random and which provide the randomness source that we exploit. Our protocol is semi-device-independent in the sense that the output entropy can be lower bounded based on experimental data and few general assumptions about the setup alone. It is also practically relevant, which we demonstrate by realising a simple optical implementation achieving rates of 16.5 Mbits/s. Combining ease of implementation, high rate, and real-time entropy estimation, our protocol represents a promising approach intermediate between fully device-independent protocols and commercial QRNGs.

Many tasks in modern science and technology make use of random numbers, including Monte Carlo simulation, statistical sampling, cryptography, and gaming applications [1]. In general, a good random number generator is desired to produce output with a high entropy and at a high rate. For applications requiring security, such as cryptography and gambling, the randomness must be certified relative to any untrusted parties. Due to the inherent randomness in quantum physics, in recent years, intense effort has been devoted to extracting randomness from quantum systems, and quantum random number generation (QRNG) is now commercially available [2].

QRNG can be implemented in a simple setup, exploiting the randomness in a quantum measurement. For example, one may send a single photon onto a balanced beam splitter and detect the output path [3–5]. Other variants measure the arrival time of single photons [6–9], the phase noise of a laser [10–12], vacuum fluctuations [13, 14], and shot-noise in mobile phone cameras [15]. However, the principle is essentially the same. The device produces a string of raw bits, which in general contains some amount of randomness but is not perfectly random. In order to extract a final (almost) perfectly random bit string, one uses a randomness extractor. The correct use of such extractors requires a good estimate of the entropy of the raw data. This can be obtained via detailed theoretical modelling of the setup [16, 17], but this is usually cumbersome and challenging. Moreover, any mismatch between the model and the implementation, or the instability of the device may jeopardize the security of the protocol.

It turns out that these problems can be circumvented via the so-called device-independent (DI) approach to randomness certification. In a setup violating a Bell inequality, the entropy of the output data can be certified without any detailed knowledge of the physical implementation [18, 19]; see [20] for a review. This provides a highly reliable and secure form of randomness, as it allows the physical devices to be completely untrusted and is thus robust against imperfection in implementation. However, it is technologically extremely challenging to realise as it requires Bell-inequality violation with no post-selection. So far, only proof-of-principle experiments were reported [19, 21], achieving very low bit rates.

More recently, an intermediate approach termed semi-DI has been discussed, exploring the trade-off between ease of implementation and strong security [22–26]. Usually based on a prepare-and-measure setup (hence avoiding the complication of a Bell test), these schemes gain ease of implementation by introducing some level of trust in the devices used. Still, they require only general assumptions about the physical implementation, such as bounded dimension [27–29], trusted measurement devices [30–33], or a trusted source [34]. While significant progress has been achieved, it is fair to say that the right balance between simplicity, performance, and security has yet to be identified.

Here, we explore a novel approach to quantum random number generation, based on unambiguous quantum state discrimination (USD). Specifically, a quantum system is prepared in one out of two quantum states which are non-orthogonal and hence cannot be distinguished with certainty. However, by performing a USD measurement, the two states can be unambiguously distinguished (i.e. without false positives), at the price of having a certain minimal rate of inconclusive events [35]. The occurrence of these inconclusive events must be genuinely random (if not, the states could be distinguished better), and this is the source of quantum randomness that we use. Our protocol is semi-DI in the sense that the output entropy can be lower bounded based on experimental data and a few general assumptions about the setup. The concept is general, and can thus be implemented in a variety of physical systems. We have implemented the

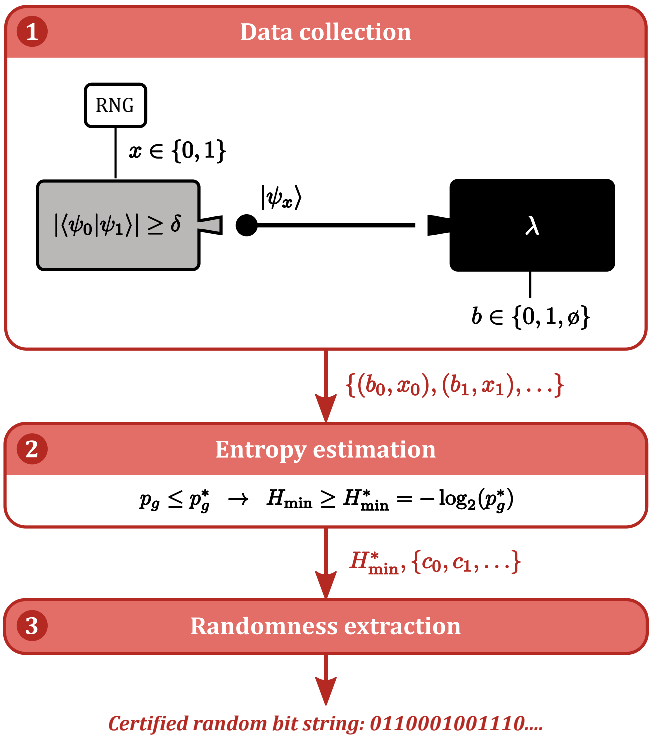
1
Data collection
RNG
$x \in \{0,1\}$
$|\langle\psi_0|\psi_1\rangle| \geq \delta$
$|\psi_x\rangle$
λ
$b \in \{0,1,\emptyset\}$
$\{(b_0,x_0),(b_1,x_1),\ldots\}$
2
Entropy estimation
$p_g \leq p_g^* \rightarrow H_{\min} \geq H_{\min}^* = -\log_2(p_g^*)$
$H_{\min}^*, \{c_0, c_1, \ldots\}$
3
Randomness extraction
Certified random bit string: 0110001001110....

FIG. 1. **Steps of the QRNG protocol.** **(1)** Data is generated in a prepare-and-measure setup. The prepared states are known to have a certain minimal overlap, hence the preparation device is a 'gray box', while nothing is assumed about the measurement device, which is a 'black box'. **(2)** From the collected data, a conditional probability distribution for outputs given inputs is estimated, and from this, a bound on the entropy in the output data is evaluated. **(3)** Based on the entropy bound, a string of certified perfectly random bits are extracted from the output data.

protocol in a simple optical setup featuring only standard components.

The conceptual scheme is illustrated in Fig. 1, and more details can be found in [36]. The central assumption of the protocol is that the overlap of the two possible states output by the preparation device is lower-bounded. In other words, we assume that the states are non-orthogonal and hence not deterministically distinguishable. However, a detailed description of the states is not required. Any measurement which attempts to distinguish the states without errors is the subject to a minimal rate of inconclusive events. This is a fundamental limit of quantum theory; if a better measurement were possible, this would have dramatic consequences, e.g. instantaneous transmission of information. Importantly, it is not possible to predict in advance whether a particular round of the experiment will be conclusive or inconclusive. Clearly, if that were possible, then a better measurement could be implemented. Therefore, the occurrence of inconclusive events is a genuinely random quantum phenomena.

Using the knowledge of the state overlap and the observed measurement data, it is then possible to bound the genuine quantum randomness in the data. Specifically, defining bits c encoding whether each round is conclusive or inconclusive, the min entropy of this string of bits can be bounded. One can understand the protocol as verifying that the measurement device is indeed performing a USD measurement, i.e. self-testing of the device.

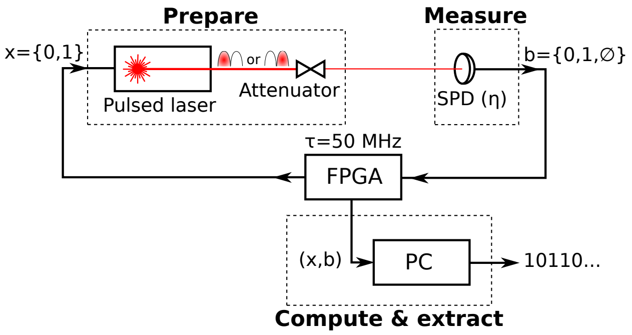

FIG. 2. **Experimental implementation of the QRNG.** Weak coherent states are prepared by a pulsed laser source and measured by a single-photon detector. An FPGA controls the experiment and passes the data to a computer for entropy estimation and randomness extraction.

We have experimentally realized our QRNG based on USD, using weak coherent states, prepared by a laser source, and single-photon detection. The setup is illustrated in Fig. 2. In a first implementation, we used a time-bin encoding. Here the two states are encoded by weak coherent pulses emitted in pairs of time-bins

$$|\psi_0\rangle = |\alpha\rangle|0\rangle \quad , \quad |\psi_1\rangle = |0\rangle|\alpha\rangle. \tag{1}$$

where $|0\rangle$ denotes the vacuum and $|\alpha\rangle$ a coherent state with mean photon number $|\alpha|^2$. The overlap of these states is directly related to $|\alpha|^2$, namely

$$\delta = |\langle\psi_0|\psi_1\rangle| = \exp(-|\alpha|^2). \tag{2}$$

It is then very simple to realise the (optimal) USD measurement, which simply requires a single-photon detector with timing resolution sufficient to distinguish the two time bins. If a click is registered in the early (late) time-bin, the system outputs $b = 0$ ($b = 1$), while if no click is registered, the outcome is inconclusive $b = \emptyset$. In the absence of losses and noise then $p(b = \emptyset) = \exp(-|\alpha|^2) = \delta$, and hence the measurement achieves the minimal possible rate of inconclusive outcomes, while giving no errors. In practice the measurement does not achieve the optimal USD exactly. Typically, detector inefficiency increases the inconclusive rate above that of the perfect USD, while detector dark counts increase the error rate. Nevertheless, randomness can still be extracted.

Using a pulse rate for the laser of 50 MHz, after extraction we were able to generate certified random bits at a rate of 11MHz using this setup. In a second implementation using a variation on the same setup using only single pulses, we achieved 16.5 MHz. This rate is comparable to commercial QRNGs [37]. Thus we have demonstrated that our protocol is practical. At the same time, it offers semi-DI security, in the sense that the amount of trust in the physical implementation is low. Specifically, the main assumption is a bound on the overlap of the prepared states (in our implementation this translates to bounding the coherent state amplitude), but no assumption about the measurement device is needed. Our approach thus combines strong security, allowing the user to monitor the entropy of the output in real time, as well as ease of implementation and high rates.

[1] B. Hayes, Am. Sci. **89**, 300 (2001).

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[3] J. Rarity, P. Owens, and P. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[4] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).

[5] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

[6] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).

[7] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).

[8] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Appl. Phys. Lett. **104**, 051110 (2014).

[9] M. Stipčević and B. M. Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).

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

[11] 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).

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

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

[14] T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).

[15] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Phys. Rev. X **4**, 031056 (2014).

[16] D. Frauchiger, R. Renner, and M. Troyer, arXiv preprint arXiv:1311.4547 (2013).

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

[18] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," Ph.D. Thesis, University of Cambridge (2009), arXiv:0911.3814 [quant-ph].

[19] 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).

[20] A. Acin and L. Masanes, Nature **540**, 213 (2016).

[21] 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).

[22] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).

[23] 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).

[24] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[25] J. Bowles, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 140407 (2014).

[26] E. Woodhead and S. Pironio, Phys. Rev. Lett. **115**, 150501 (2015).

[27] 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).

[28] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, arXiv:1410.3443 (2014).

[29] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski, and M. Bourennane, New J. Phys. **18**, 065004 (2016).

[30] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).

[31] D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).

[32] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).

[33] F. Xu, J. H. Shapiro, and F. N. C. Wong, Optica **3**, 1266 (2016).

[34] Z. Cao, H. Zhou, and X. Ma, New J. Phys. **17**, 125011 (2015).

[35] I. Ivanovic, Phys. Lett. A **123**, 257 (1987); D. Dieks, Phys. Lett. A **126**, 303 (1988); A. Peres, Phys. Lett. A **128**, 19 (1988).

[36] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, arXiv:1612.06566 [quant-ph] (2016), *to appear in Phys. Rev. Applied.*

[37] "http://www.idquantique.com," (); "http://www.picoquant.com," ().