True random numbers from amplified quantum vacuum

M. Jofre,[1,*] M. Curty,[2] F. Steinlechner,[1] G. Anzolin,[1] J. P. Torres,[1,3] M. W. Mitchell,[1] and V. Pruneri[1,4]

[1]*ICFO-Institut de Ciencies Fotoniques, Castelldefels, E-08860 Barcelona, Spain*
[2]*ETSI Telecomunicación, Dept. Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain*
[3]*Dept. Signal Theory and Communications, Universitat Politècnica de Catalunya, E-08034 Barcelona, Spain*
[4]*ICREA-Institució Catalana de Recerca i Estudis Avançats, E-08010 Barcelona, Spain*
[*]*marc.jofre@icfo.es*

Abstract: Random numbers are essential for applications ranging from secure communications to numerical simulation and quantitative finance. Algorithms can rapidly produce pseudo-random outcomes, series of numbers that mimic most properties of true random numbers while quantum random number generators (QRNGs) exploit intrinsic quantum randomness to produce true random numbers. Single-photon QRNGs are conceptually simple but produce few random bits per detection. In contrast, vacuum fluctuations are a vast resource for QRNGs: they are broad-band and thus can encode many random bits per second. Direct recording of vacuum fluctuations is possible, but requires shot-noise-limited detectors, at the cost of bandwidth. We demonstrate efficient conversion of vacuum fluctuations to true random bits using optical amplification of vacuum and interferometry. Using commercially-available optical components we demonstrate a QRNG at a bit rate of 1.11 Gbps. The proposed scheme has the potential to be extended to 10 Gbps and even up to 100 Gbps by taking advantage of high speed modulation sources and detectors for optical fiber telecommunication devices.

OCIS codes: (030.0030) Coherence and statistical optics; (230.0230) Optical devices; (270.0270) Quantum optics.

References and links

1. F. Galton, "Dice for statistical experiments," Nature **42**, 13–14 (1890).
2. R. Corporation, ed., *A Million Random Digits with 100,000 Normal Deviates* (The Free Press, 1955).
3. T. Kanai, M. Tarui, and Y. Yamada, "Random number generator," International patent WO2010090328 (2009).
4. G. Ribordy and O. Guinnard, "Method and apparatus for generating true random numbers by way of a quantum optics process," US patent 2007127718 (2007).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
6. N. Cerf and L.-P. Lamoureux, "Network distributed quantum random number generation," International patent GB2473078 (2009).
7. N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Wiley Publishing, Inc., 2010).
8. N. Metropolis and S. Ulam, "The Monte Carlo Method," J. Am. Statist. Assoc. **44**, 335–341 (1949).
9. S. Banks, P. Beadling, and A. Ferencz, "FPGA Implementation of Pseudo Random Number Generators for Monte Carlo Methods in Quantitative Finance," in Proceedings of the 2008 International Conference on Reconfigurable, Computing and FPGAs, RECONFIG'08, (IEEE, 2008), pp. 271–276.

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011

10. S. Pironio, A. Acin, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
11. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**, 1675–1680 (2000).
12. O. Kwon, Y.-W. Cho, and Y.-H. Kim, "Quantum random number generator using photon-number path entanglement," Appl. Opt. **48**, 1774–1778 (2009).
13. M. Stipcevic and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," Rev. Sci. Instrum. **78**, 045104 (2007).
14. P. Bronner, A. Strunz, C. Silberhorn, and J. P. Meyn, "Demonstrating quantum random with single photons," Eur. J. Phys. **30**, 1189–1200 (2009).
15. M. Wayne and P. Kwiat, "Low-bias high-speed quantum number generator via shaped optical pulses," Opt. Express **18**, 9351–9357 (2010).
16. M. Fürst, H. Weier, S. Nauerth, D. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**, 13029–13037 (2010).
17. M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," Appl. Phys. Lett. **98**, 171105 (2011).
18. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**, 711–715 (2010).
19. T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett. **98**, 231103 (2011).
20. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**, 728–732 (2008).
21. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**, 312–314 (2010).
22. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," Phys. Rev. E **81**, 051137 (2010).
23. P. R. Tapster and P. M. Gorman, "Apparatus and Method for Generating Random Numbers," US patent 2009013019 (2009).
24. M. J. Collett and C. W. Gardiner, "Squeezing of intracavity and traveling-wave light fields produced in parametric amplification," Phys. Rev. A **30**, 1386-1391 (1984).
25. M. D. Sturge, "Optical absorption of gallium arsenide between 0.6 and 2.75 ev," Phys. Rev. **127**, 768–773 (1962).
26. Y. Suematsu and S. Arai, "Single-mode semiconductor lasers for long-wavelength optical fiber communications and dynamics of semiconductor lasers," IEEE J. Sel. Top. Quantum Electron. **6**, 1436–1449 (2000).
27. P. Barreto and V. Rijmen, "The Whirlpool hashing fFunction," pheattarchive.emporia.edu (2010).
28. Y. Peres, "Iterating Von Neumann's procedure for extracting random bits," Ann. Stat. **20**, 590–597 (1992).
29. N. Nisan and A. Ta-Shma, "Extracting randomness: a survey and new constructions," J. Comput. Syst. Sci. **58**, 148–173 (1999).
30. P. L'Ecuyer and R. Simard, "TestU01: AC library for empirical testing of random number generators," ACM Trans. Math. Softw. **33**, 1–40 (2007).

1. Introduction

The need for random numbers in research and technology was recognized very early [1], and has motivated electronic and photonic advances [2–4]. Random numbers support critical activities in advanced economies, including secure communications [5–7], numerical simulation [8] and quantitative finance [9]. For this reason, there has been intense effort to develop practical true random number generators, to replace existing pseudo-random methods. QRNGs employ a true source of randomness known to science, the randomness embedded into quantum physics. Recently, it has been shown that quantum physics also can be used to verify the randomness of entanglement-based generators [10].

Examples of demonstrated QRNGs include two-path splitting of single photons [11], photon-number path entanglement [12], time of generation or counting of photons [13–17], fluctuations of the vacuum state using homodyne detection techniques [18, 19] as well as interferometric schemes [20–22].

Although any quantum measurement provides some randomness, a practical source must

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011

be simultaneously fast, inexpensive, and robust. For this purpose, fluctuations of the quantum vacuum are very attractive because the electric field amplitude is a continuous quantity, a single measurement can yield many true random bits. True vacuum is also perfectly white, uncorrelated, and broadband; the quantum field renews its random value arbitrarily quickly. Guaranteeing true vacuum is far from trivial, however; any scattered light will contribute a non-random component to the field measurement. Here we demonstrate extraction of random bits from vacuum using optical amplification. In contrast to homodyne detection [18, 19, 23], the method guarantees that the signals originate in vacuum noise, and at the same time achieves high bandwidths, because the requirement for shot-noise-limited detection is removed.

Relative to demonstrated methods for QRNG and achieved speeds, our proposed device is not only highly integrated, using commercially available components, but also has other advantages. In particular, the strong current modulation, well above and below threshold, ensures true randomness from vacuum. This active gain control allows a single device to have both a short coherence time, for rapid extraction of uncorrelated random bits, and a high signal level. In this way, standard photodiodes can be used. Furthermore, due to the high power of the signal pulses, the signal-to-noise ratio (SNR) is high. Hence, several random bits per detection event can be generated, limited by the classical noise of the measurement equipment. To our knowledge, it is the first time that our use of current gain modulation is used in QRNG.

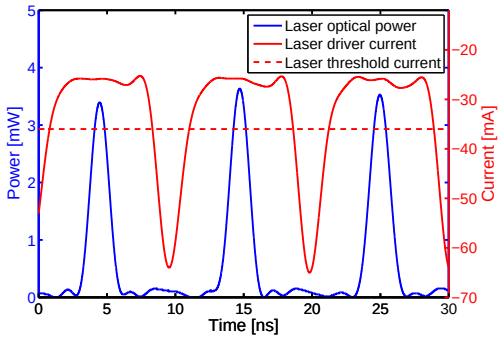
2. Device operation

We use a distributed feedback (DFB) laser diode (LD) as the oscillator, providing single-mode operation and high modulation bandwidth. The DFB LD is directly modulated at around 100 MHz by a train of ~ 1 ns electrical pulses, as shown in Fig. 1(a). A polarization-maintaining, all-fiber unbalanced Mach-Zehnder interferometer (MZI) with a relative delay of $t_{\mathrm{loop}} \approx 10$ ns provides stable single-mode operation of the interferometer, as shown in Fig. 1(b).

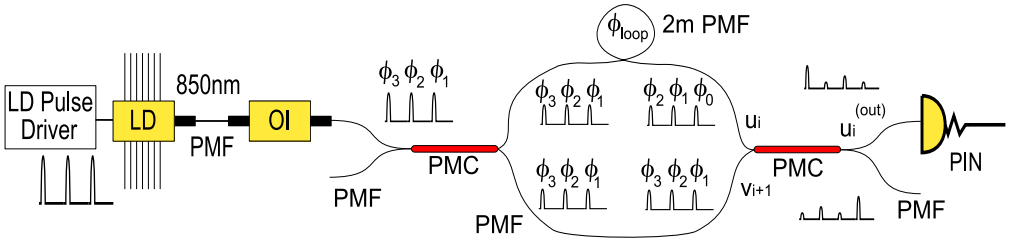
The LD is set with 25 mA DC bias current, far below its threshold value of 36 mA. Phase-randomized coherent optical pulses of 400 ps time width and 3.5 mW peak power are produced. A 30 dB optical isolator (OI) is placed just after the LD to avoid back reflections into the oscillator cavity. Then, the linearly polarized optical pulses are split in power using a polarization maintaining coupler (PMC) with a fixed coupling ratio. In one of the output ports of the PMC, a 2 m polarization maintaining fiber (PMF) patchcord is connected, which corresponds approximately to the equivalent length of the PRF. Both arms of the interferometer are connected to a second PMC where the interference between pulses takes place. The overall interferometer setup, at the output, has power coupling ratios of $T_{12}^2 \approx 49.8\%$ and $R_{12}^2 \approx 40.3\%$, and polarization isolation of 23.98 dB and 25.23 dB for the two arms. At one of the output ports of the interferometer, a 150 MHz photodiode is connected to collect the different interfering optical pulses which are processed by a fast oscilloscope. The oscilloscope is operated with a 200 MHz bandwidth for the input channel, triggered by the system clock reference.

The path delay difference of the interferometer can be adjusted to temporally overlap subsequent pulses. On the one hand, the time delay between interfering pulses can be controlled by fine tunning the propagation properties of the long arm of the interferometer to change the parameter ϕ_{loop}. For instance, by changing the temperature of the optical fiber one can produce a refractive index change and also thermal expansion of a wavelength for a 0.03°C temperature change, corresponding to 4.25 fs. Albeit, the time adjustment range achievable is limited compared to the pulse repetition period ~ 10 ns. On the other hand, the interferometer can be temperature stabilized to 0.01°C to keep the parameter ϕ_{loop} and the PRF changed to increase or decrease the time between successive pulses. The time delay difference between both arms of the MZI is related to the PRF as $\Delta t = 1/\mathrm{PRF}$, which allows an accurate and larger time adjustment range. The path delay difference of the interferometer was adjusted by setting the PRF

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011



(a) Electrical and optical pulse trains generated.



(b) Device optical scheme.

Fig. 1. Unbalanced Mach-Zehnder interferometer. Due to the random phase of the different input pulses, the output signals acquire random amplitudes. (a) Measured drive current (red, upper curve) and detected laser power (blue, lower curve), showing amplitude repeatability and clear pulse separation. (b) (LD Pulse Driver) denotes the electrical pulse generator to directly modulate the laser, (LD) laser diode, (OI) optical isolator, (PMF) polarization maintaining fiber, (ϕ_{0-3}) optical phases of different consecutive pulses, (PMC) polarization maintaining coupler, (ϕ_{loop}) phase introduced by the delay line and (PIN) fast photodiode.

at 97.6 MHz.

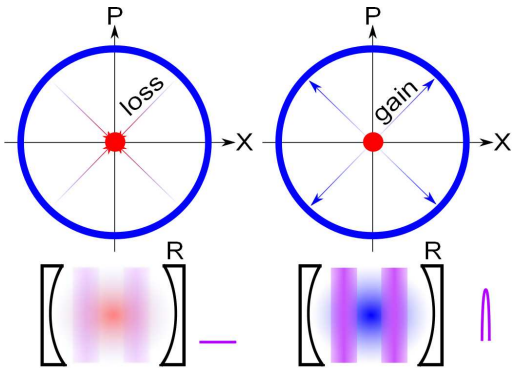
3. Laser physics analysis

The method operates on the field within a single mode of a semiconductor diode laser. As shown in Fig. 2, the laser is first operated far below threshold, producing simultaneously strong attenuation of the cavity field and input of amplified spontaneous emission (ASE). This attenuates to a negligible level any prior coherence, while the ASE, itself a product of vacuum fluctuations, contributes a masking field with a true random phase. The laser is then briefly taken above threshold, to rapidly amplify the cavity field to a macroscopic level. The amplification is electrically-pumped and thus phase-independent. Due to gain saturation, the resulting field has a predictable amplitude but a true random phase. The cycle is repeated, producing a stream of phase-randomized, nearly identical optical pulses. As shown in Fig. 1(b), interference of subsequent pulses converts the phase randomness into a stream of pulses with random energies, which is directly detected and digitized.

During the attenuation phase, the cavity field is described by the Langevin equation:

$$\frac{d}{dt}a = -i\omega a - \frac{1}{2}\gamma a + \Gamma, \tag{1}$$

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011



(a) Loss mechanism scheme. **(b)** Gain mechanism scheme.

Fig. 2. Generation of amplified vacuum within the laser cavity. (a) The LD is first taken below threshold, to attenuate the cavity field to a weak thermal state (in red), independent of its previous value (in blue). (b) The LD is then taken above threshold, so that phase-insensitive amplification brings the field amplitude $|\alpha|$ to a level fixed by saturation, while the phase retains the random thermal-state value.

where a is the field operator for the mode, ω is its angular frequency, γ is the (energy) decay rate and $\Gamma = \gamma^{1/2} a_{\rm res} + \Gamma_{\rm ASE}$ is a noise operator, with $a_{\rm res}$ a reservoir mode. The first term is from attenuation [24], and the second from ASE. We can estimate $\gamma = \gamma_{\rm cav} + \gamma_{\rm mat}$ as follows: The cavity contribution is $\gamma_{\rm cav} = -c\ln(R)/(2nL) = 5\times10^{10}$ s^{-1}, where c is the speed of light in vacuum, $R = 0.3$ is the out-coupler reflectivity, $n = 3.6$ is the refractive index, and $L = 300\mu$m is the cavity length. The material contribution $\gamma_{\rm mat}$ ranges from $c\alpha/n \approx 10^{11}$ s^{-1} at zero current to $\gamma_{\rm mat} = -\gamma_{\rm cav}$ at threshold. Here $\alpha \approx 10^4$cm^{-1} is the intrinsic absorption of GaAs at 852nm [25]. Interpolating, at 70% threshold current, we obtain $\gamma \approx 10^{11}$ s^{-1}, or about 400 dB/ns. This renders completely negligible any prior coherence in the cavity, and the remaining field is an equilibrium between ASE and attenuation. The phase of this field is a true quantum random variable, its value determined by ASE which is driven by vacuum fluctuations. When the laser is taken above threshold, the equilibrated field is amplified, limited by gain depletion [26], to produce observed output powers of $P \approx 3.5$ mW or 1.5×10^7 photons/ns, with about $P/\gamma_{\rm cav} \approx 3\times10^5$ photons in the cavity. The amplification is phase-insensitive, and the phase of the cavity field remains truly random.

Considering the speed limits of this technique, we note that even at a modulation rate of 20 GHz, i.e., an attenuation time of ~ 0.25 ns, the attenuation is 100 dB. The field contribution remaining from the previous pulse is 3×10^{-5} photons, or ≈ 15 bits below the vacuum fluctuations. The physics of the process can thus support QRNG rates in excess of 100 Gbps.

4. Characterization of the coherence of the laser pulses

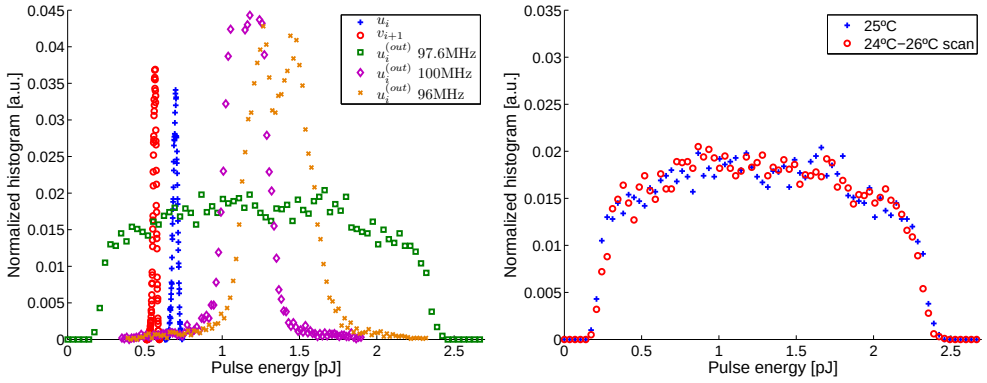
The interferometric setup allows us to determine the first order coherence properties of the laser pulses, described by the correlation functions $G(\tau) \equiv \int dt\ \langle\, \hat{E}^{(-)}(t)\hat{E}^{(+)}(t+\tau)\,\rangle$, or its normalized version $g(\tau) \equiv G(\tau)/G(0)$. Here $\hat{E}^{(\pm)}$ are the positive- and negative-frequency parts of the emitted field $\hat{E}$ and integrals are taken over the duration of the pulse. We expect the pulse energies $G(0)$ to be narrowly distributed, and $g(t_{\rm rep})$ to have near-unit magnitude and random phase, where $t_{\rm rep}$ corresponds to the time between successive pulses given by the pulse repeti-

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011

tion frequency (PRF), as subsequent pulses have very similar envelopes and random phases ϕ. The interferometer output is $\hat{E}_{\text{out}}(t) = T_{12}\hat{E}(t) + R_{12}\hat{E}(t+t_{\text{loop}})$ where T_{12}, R_{12} indicate combined transmission and reflection coefficients through the two beamsplitters. If we define the pulse energy in both arms of the interferometer as $u_i \equiv R_{12}^2 G(0)$ and $v_{i+1} \equiv T_{12}^2 G(0)$, the energy at the output port of the interferometer, $u_i^{(\text{out})} \equiv \int dt \, \langle \, \hat{E}_{\text{out}}^{(-)}(t)\hat{E}_{\text{out}}^{(+)}(t) \, \rangle_i$ is given by

$$u_i^{(\text{out})} \quad = \quad u_i + v_{i+1} + 2|g(t_{\text{loop}})|\sqrt{u_i v_{i+1}}\cos\left(\phi_i - \phi_{i+1} - \phi_{\text{loop}}\right) \tag{2}$$

where $\phi_{\text{loop}} = \omega t_{\text{loop}}$ is the phase introduced by the delay loop. We measure the relevant statistics as follows (data shown in Fig. 3(a)): narrow distributions of u_i and v_{i+1} are directly observed by blocking one or the other path. Interference leads to a broadening of the observed distribution, with the broadest distribution corresponding to $t_{\text{rep}} = t_{\text{loop}}$. From the width of the $u_i^{(\text{out})}$ distribution and the mean values of u_i, v_{i+1}, we can estimate the interference visibility $|g(t_{\text{loop}})| \approx 90.22\%$. To demonstrate that the laser pulses are phase-uncorrelated, we collect statistics both for ϕ_{loop} fixed, and for ϕ_{loop} swept over several π, obtained by heating the fiber loop during acquisition. Results, shown in Fig. 3(b), are statistically identical, indicating the absence of any phase relation between subsequent pulses.



(a) Input and output statistics. **(b)** Statistics for different temperature settings.

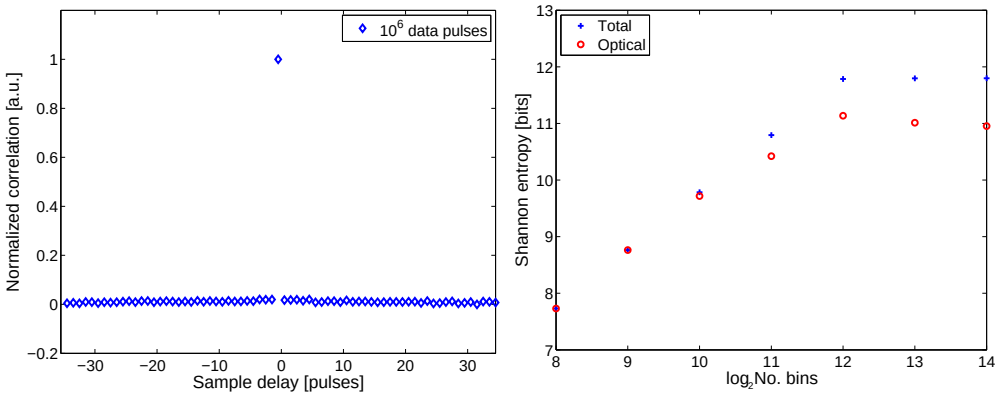
Fig. 3. Inter-pulse coherence measured by output energy distributions. (a) Distributions for: individual pulse energies u_i,v_{i+1}, interfering pulse energies $u_i^{(\text{out})}$ under different PRF and hence different t_{rep}. (b) Output pulse energy histogram for delay-loop temperatures of 25 °C (fixed), and 24 °C to 26 °C (scanned). Loop phase has no observable effect on the distribution, indicating statistical independence of the pulses' phases.

5. Statistical testing

The output of the PIN photodiode was highpass filtered with a cutoff frequency of 40 MHz and digitized using the waveform integration function of an oscilloscope with input bandwidth 200 MHz, sampling speed of 2.5 Gsps and a 12-bit analog-to-digital converter (ADC). The 10 ns time range setting, compliant with the PRF, and sampling speed of the oscilloscope permits to acquire 25 samples over a pulse. The oscilloscope translates the multiple samples per pulse to a single measurement. The nearly uniform distribution of observed energies permits the use of equally-sized encoding bins, and facilitates calibration. Records of 10^6 output pulses were collected in order to characterize the statistical correlations of the acquired raw data and

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011

to determine the number of extractable random bits per pulse. The normalized correlation of successive samples as a function of sample delay of the raw data is computed as the modulo-N circular auto-correlation for finite length sequences and it is normalized to the maximum, shown in Fig. 4(a). The correlation of data samples follows a delta-function like behavior which indicates a random sequence with low impact of drifts in the system. The quantum random bit content of the recorded signal is determined as follows: The pulse distribution of Fig. 3 is divided into 2^b equally-sized bins and the Shannon entropy is calculated. As shown in Fig. 4(b), the entropy increases linearly with b, up to the value $b = 12$, where it saturates to 11.8 bits of entropy. The same procedure, applied to the detection noise, finds the classical noise entropy. Subtracting the noise entropy, the quantum optical noise contribution reaches a level of 11.1 bits per pulse at $b = 12$. Multiple samples per pulse achieves larger accuracy when used together with higher resolution ADC. This allows to better bound the contribution of the classical noise and thus permits to extract more true random bits per pulse.



(a) Normalized correlation of raw data.

(b) Total entropy of detected pulses and entropy of optical contribution .

Fig. 4. Measured correlation and entropy of acquired pulses. (a) Normalized correlation of successive samples as a function of sample delay of the raw data. The correlation data samples follows a delta-function like behavior indicating a random sequence. (b) Total entropy, calculated from the measured distribution shown in Fig. 3. Distribution is divided into 2^b bins, from which the Shannon entropy is calculated. Optical contribution, up to 11.1 bits per pulse, is found by subtracting entropy of the measured electronic noise.

The observed classical noise, however random it may appear, could in principle be the result of a completely predictable process. Indeed, randomness tests (described below) detect patterns in the recorded classical noise. To completely remove these patterns, we first note that the entropy of the classical noise places an upper bound on the information it can contain. We then remove this quantity of information, using cryptographic hash functions, from the combined quantum and classical noise. We use the Whirlpool hash function [27]; other standard randomness extractors could have also been employed [28, 29]. These cryptographic functions mix the input data bits, increasing the theoretically secure entropy per bit at the cost of losing output bits. The reduction factor of the hash function applied to the collected raw bits is 1.08. As a result, we obtain that the random bit generation rate of the current device accounts to 1.11 Gbps.

We have performed all tests of randomness from TestU01 [30]. Considering the optical pulse

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011

data set, some test fail when applied to the raw data set, while they were successfully passed when applied to the hashed data set. Confirming that the hashing removes any remaining predictable behavior and increases the entropy per bit. Instead, the classical noise data set fails some tests both before and after hashing, using the same hashing factor.

6. Conclusions

In conclusion, we have demonstrated high-bandwidth extraction of random bits from quantum vacuum fluctuations using optical amplification. The use of strong attenuation followed by amplification guarantees that the signal originate from quantum noise, and provides macroscopic signals compatible with the highest bandwidth detection. With commercially-available components, we demonstrate over 1 Gbps true random number generation. The QRNG device is low power consumption, robust, and can be easily automated allowing it to have a long operational lifetime. Consideration of the laser physics indicates that rates above 10 Gbps and even 100 Gbps are possible. The high random numbers generation rate extends the practical applications of our method to erode the dominance of currently used classical RNG choices. The method can be applied to high speed secure communication, to the gambling industry and to cryptography.

Acknowledgments

The authors thank K. Tamaki, B. Qi and X. Ma for stimulating discussions. This work was carried out with the financial support of Xunta de Galicia (Spain) through grant INCITE08PXIB322257PR, and the Ministerio de Educación y Ciencia (Spain) through grants TEC2010-14832, FIS2007-60179, FIS2008-01051, FIS2010-14831 and Consolider Ingenio CSD2006-00019. This work is also supported by FONCICYT-94142.

#150766 - $15.00 USD Received 8 Jul 2011; revised 8 Aug 2011; accepted 1 Sep 2011; published 3 Oct 2011